Dual-Level Defense Framework for DDoS Attacked Network

Anjali Sardana
Indian Institute of Technology Roorkee
Roorkee, India

Ramesh C. Joshi
Indian Institute of Technology Roorkee
Roorkee, India

ABSTRACT

DDoS has become one of the thorniest problems in the Internet, and aims to deny legitimate users of the services they should have. In this paper, we introduce novel dual - level framework that consist of attack detection (D-LAD) and characterization scheme for defending against the DDoS attacks. The macroscopic level detectors (MaLAD) attempt to detect voluminous congestion inducing attacks which cause apparent slowdown in network functionality. The macroscopic level characterization process identifies these large volumes attacks that have been detected early in transit domain by MaLAD. The microscopic level detectors (MiLAD) detect sophisticated attacks that cause network performance to degrade gracefully and remain undetected in transit domain. Microscopic level characterization process identifies such attacks that have been detected at border routers in stub domain near the victim by Mi-LAD. We employ the concepts of change point detection on entropy with time to improve the detection rate. Honeypots help achieve high detection and filtering accuracy. Use of honeypots is proposed that help achieve high detection accuracy.

We validate the effectiveness of our framework with simulations on AT&T topology in ns-2 on a Linux platform. Results demonstrate that in addition to being competitive than other techniques, our framework works well in the presence of different DDoS attacks. The compromise of detection and characterization accuracy and time of confirming is a critical aspect and proposed technique provides the demanded solution.

Categories and Subject Descriptors

C.2.3 [COMPUTER-COMMUNICATION NETWORKS]: Network Operations - Network Monitoring; C.2.0 [COMPUTER-COMMUNICATION NETWORKS]: General-Security and protection; C.4 [PERFORMANCE OF SYSTEMS]: Measurement Techniques; K.6.5 [Management of Computing and Information Systems]: Security and Protection – Unauthorized access.

General Terms

Security, Performance, Design, Reliability.

Keywords

DDoS, Framework, Honeypots, Entropy.

1.INTRODUCTION

An ideal DDoS defense system is one that renders any DoS attack impossible. Apart from the fact that no system is perfect, a proactive prevention system requires too many resources to operate and is costly in the absence of attack. Therefore, attack detection and characterization are necessary elements of a complete DDoS defense system. The DDoS attack detection problem consists of designating those points in time at which network is experiencing an attack. Only by timely and accurate detection of DDoS attacks, system can make proper response to escape big loss. The characterization problem consists of selecting the true attacks from a set of possible candidate attacks. The method should be extensible to a wide variety of attacks.

Many techniques have been suggested for DDoS attack detection and characterization. Most of these techniques have one or more limitations. Detecting a DDoS attack is relatively easy at the victim network because it can observe all the attack packets. However, attack packets clog a large part of the network before converging at victim. Early attack detection schemes unfortunately, have to wait for the flooding to become widespread, consequently, they are ineffective to fence off the DDoS timely. Many of the present DDoS attack detection techniques are complex, difficult to deploy or lead to computational and memory overheads.

Our proposed scheme is a hybrid that combines anomaly based approach and honeypots in a way that exploits the best features of these mechanisms while shielding their limitations. It operates on two levels, with macroscopic level detectors (MaLAD) detecting and identifying congestion inducing attacks with high confidence and microscopic level detectors (MiLAD) identifying suspicious flows in presence of honeypots. Unlike earlier proposals for attack detection and characterization that are either based on unreliable assumptions or too complicated to implement, our scheme is simple to understand and implement. It is capable of handling infiltrating, sophisticated as well as highly distributed attacks. Besides being computationally fast and accurate, it adapts to varying network conditions with minimum collateral damage.

The rest of the paper is organized as follows. Section 2 gives the related work. Section 3 describes the overall scheme. Section 4 gives design of dual-level attack detection (D-LAD) scheme. Design of dual-level attack characterization is explained in section 5. Performance of our proposed scheme is evaluated in section 6. Finally section 7 concludes the paper.

2.RELATED WORK

For detection and characterization, one can choose between signature based techniques and anomaly based . Signature based techniques can detect and identify only known attacks whereas in anomaly based techniques , it is difficult to build accurate profile of legitimate traffic and hence they generate high rate of false alarms. Moreover, the Internet traffic is noisy, which makes it difficult to extract meaningful information about attacks from any kind of traffic characteristics. Reason for limited success of attempts at characterization is that they rely on volume based metrics like , which do not provide sufficient information to distinguish attacks and are inaccurate. Some of the solutions have achieved impressive levels of accuracy , but all suffer from common weakness of themselves being exploited to give rise to DoS attacks.

DDoS attacks are launched from distributed sources. Hence the attack traffic is spread across multiple links. As the distance from the victim increases, attack traffic is more diffused and harder to detect because the volume of attack flows are indistinguishable from legitimate flows. Current schemes for early attack detection and characterization are based on identifying aggregates causing sustained congestion on communication links, imbalance between incoming or outgoing traffic volume on routers and probabilistic packet marking techniques . These methods, unfortunately, have to wait for the flooding to become widespread, consequently, they are ineffective to fence off the DDoS timely. Moreover, techniques like lead to severe collateral damage as legitimate traffic in the aggregates is also dropped as a result of misclassified attacks. Volume based techniques can identify attack accurately but only when they have reached the victim as maximum attack traffic is available near victim point for analysis. This poses a major challenge for timely and accurate DDoS attack defense.

3.OVERALL SCHEME

3.1System Model

We use transit stub network model of the Internet as shown in figure 1. Every domain can be classified as either a stub or a transit network. A stub network connects end hosts to the Internet. A transit network interconnects stub networks. As for the scenario of a DDoS attack, each of the attackers, legitimate users and the victim server are connected to a stub network. The traffic usually passes through two stub networks, one on the sender side and the other on the victim side, and one or more transit networks. Our aim is to protect the victim server and its corresponding network from DDoS attacks.

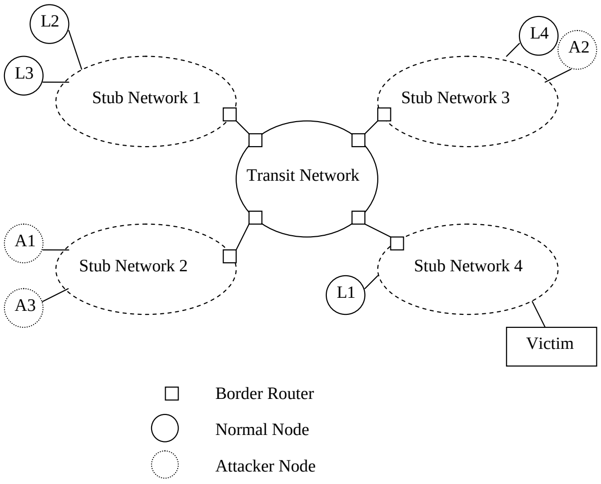

Figure 1. Transit-Stub Network for proposed scheme

3.2Dual-Level Defense Framework

In the proposed framework, detection algorithms are running on the edge routers of transit and stub network. Macroscopic or largest volume of attacks is detected early before they enter the victim network. Macroscopic detectors on edge routers of transit network consistently detect these attacks and do so with a very low false alarm rate. As soon as the attacks are detected at macroscopic level, the macroscopic characterization is triggered. Microscopic attacks may not necessarily impact the network, but they can have dramatic impact on the victim or server. Microscopic detectors located on edge routers of stub domain are used for such attacks and trigger microscopic characterization as soon as attacks are detected. They enable highly sensitive detection. Figure 2 shows the dual level defense scheme.

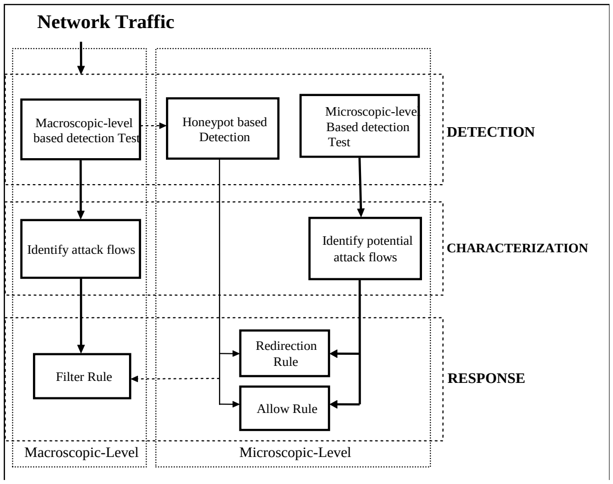

Figure 2. Dual-Level Defense Framework

Lakhina et al [9] observed that most of traffic anomalies despite their diversity share a common characteristic: they induce a change in distributional aspects of packet header fields. Our techniques use traffic feature distribution to detect DDoS attack. We use entropy as a metric for measuring the distribution of traffic features as it exploits inherent feature of DDoS attacks, which makes it hard for attacker to counter this detection by changing their attack signature.

We model the Internet to measure the entropy in transit – stub network. During an attack, the Internet or IP domain is divided into the two networks; one for inside to be protected and the other is for outside where attackers may reside. The entropy is measured by recording the dynamics of packets on the border of the two networks. Packets flowing between these two networks may incur to sustain the current value of the entropy if those packets are in harmony with the system or change abruptly if those agitate the system. In the proposed system we keep track of the value of entropy in time to pinpoint the sudden changes in the value. Those changes are regarded as the installation of attacks in the network.

Since macroscopic attack flows create congestion in the network and stress resource utilization in a router and network, they are dropped using “filter” rule before they enter the network from an operational standpoint. At microscopic level, characterization process is triggered and suspicious flows are redirected to honeypots using “redirect” rule, while legitimate flows are handled normally using “allow” rule.

3.3Traffic Feature Selection

Let an information source have n independent symbols each with probability of choice p_i. Then the entropy H is defined as:

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i \qquad (1)$$

Entropy can be computed on a sample of consecutive packets. The entropy is used to calculate the distribution of randomness of some attributes which are fields in the network packets’ headers. In the proposed dual level detection algorithms, macroscopic detectors are based on entropy calculated over source IP and microscopic detectors are based on entropy calculated over destination IP. We assume that any link or network has a characteristic distribution of IP addresses for initiators of IP traffic and another probability distribution for IP addresses that are the recipients of network traffic. An important network event, such as a DDoS attack, should modify these distributions of source and destination IP addresses in terms of new IP addresses entering the system or certain IP addresses becoming more dominant. The Source IP address based entropy fluctuates to some extent under normal network conditions. But when the entropy values have perceptible changes, attacks are detected. An increase in source IP based entropy indicates distributed attacks (according to equation (1), entropy becomes maximum when distribution is maximally dispersed) whereas a decrease in source IP based entropy indicates a concentrated attack launched from single or a few sources (according to equation (1), entropy becomes zero when distribution is maximally concentrated). A single destination IP address (or alternatively, a very, very few number of unique destination IP addresses) receives many more flows during DDoS. Consequently, a decrease in destination IP based entropy detects the presence of DDoS attacks. During characterization, both macroscopic and microscopic levels make use of source IP address based entropy values to identify the attack flows.

4.DUAL-LEVEL ATTACK DETECTION SCHEME

In this section, the first motivation is to identify DDoS attack packets at early stage and eliminate attack packets before they reach the target. The second motivation is to counter the attacks which resemble normal network accessing patterns and lastly to discriminate DDoS attacks from surge of legitimate traffic or flooding. We also aim to keep the false positives and false negatives minimum during the process.

4.1Macroscopic Level Attack Detector (MaLAD)

MaLAD make use of computing entropies based on source IP addresses and detect an attack if system entropy crosses threshold limits. If the flows are destined to honeypots, attack is confirmed and corresponding attack flows are dropped. Thresholds are optimized according to client requirements and network conditions.

4.1.1Sampling and Detection

Consider a random process $\{X(t), t = j\Delta, j \in N\}$, where Δ , a constant time interval is called time window, N is the set of positive integers, and for each $t, X(t)$ is a random variable. Here $X(t)$ represents the number of packet arrivals for a flow in $\{t-\Delta, t\}$. $X(t)$ As a whole represent our empirical histogram for computing entropy. It is found in our simulation without attack that Entropy $H(X)$ value varies within very narrow limits after slow start phase is over. This variation becomes narrower if we increase Δ i.e. monitoring period. We take average of *H(X)* and designate that as normal Entropy $H_n(X)$. To detect the attack, the entropy $H_c(X)$ is calculated in shorter time window Δ continuously, whenever there is appreciable deviation from $H_n(X)$, attack is said to be detected.

We assume that the system is under attack at time t_a, which means that all attacking sources start emitting packets from this time: the network is in normal state for time $t<t_a$ and turns into attacked state in time t_a. Let t_d denote our estimate on t_a. At time t_d following event triggers

$$(H_c(X) > (H_n(X) + a \times d)) \cup (H_c(X) < (H_n(X) - a \times d))$$

$$attack \Leftarrow true; \qquad (2)$$

Here $a \in I$ where I is set of integers and d is deviation threshold. Tolerance factor or threshold *a* is a design parameter and *d* is absolute maximum deviation in Entropy *H(X)* from average value $H_n(X)$ while profiling for network without attack.

We propose an adaptive approach that continually updates the tolerance factor *a*, to reflect changes in background traffic. By adjusting a baseline, estimates can adjust more or less quickly to changes in the background. Threshold is decided depending on the network conditions.

4.1.2Decision of threshold and defense modes

The proposed detection technique operates in one of the following modes as shown in fig 3:

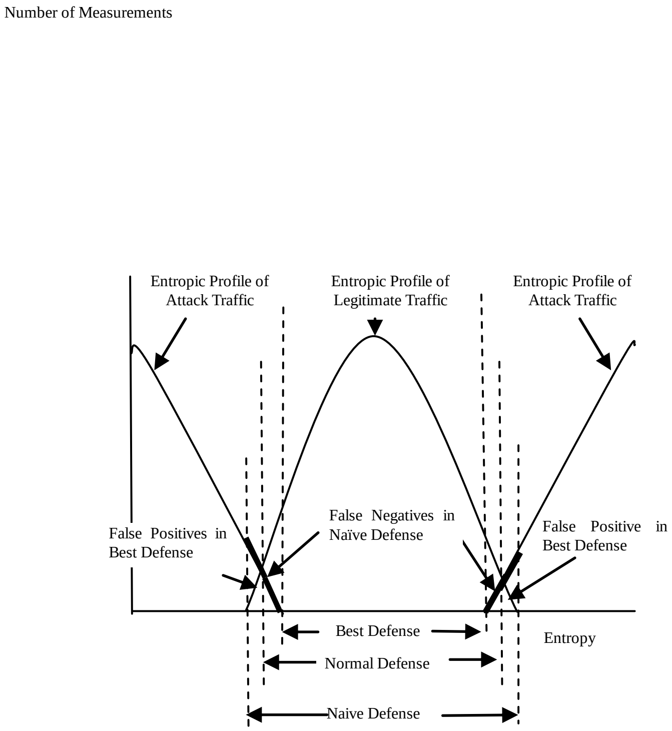
Number of Measurements
Entropic Profile of Attack Traffic
Entropic Profile of Legitimate Traffic
Entropic Profile of Attack Traffic
False Positives in Best Defense
False Negatives in Naïve Defense
False Positive in Best Defense
Best Defense
Entropy
Normal Defense
Naive Defense

Figure 3. Naïve, Normal and Best Defense

Best Defense: The threshold or tolerance factor a is set to low value and hence the normal entropy bandwidth during attack detection is very small. The choice is made to reduce the false negatives to minimum, and is zero in ideal case.

Normal Defense: The threshold or tolerance factor a is set neither too high nor too low. Hence the entropic range that classifies traffic as legitimate is moderate, and the false positives and false negatives are balanced.

Naïve Defense: The threshold or tolerance factor a is set the highest. Hence the entropic range that classifies traffic as legitimate is broad, and the false alarm rate is low, but detection rate is low, too. Naïve defense has the lowest detection sensitivity level and hence it has lowest false positive rate.

The mode of operation is chosen according to attack strength by varying ‘a’ so as to minimize false positives and false negatives.

4.2Microscopic Level Attack Detector (MiLAD)

Distributional changes captured by entropy observed on source IP alone cannot detect stealthy and sophisticated attacks that are crafted to match statistics of normal traffic. For example, the attackers may simulate the normal network behaviors, e.g. pumping the attack packages as Poisson distribution, to disable macroscopic detectors. Also, how to discriminate DDoS attacks from surge legitimate accessing is a major challenge.

In order to detect a DDoS attack, we need to test for changes in our detection feature over time. However, our detection feature is a random variable due to the stochastic nature of Internet traffic. Consequently, we require a mechanism that can accurately discriminate between the onset of a DDoS attack and a temporary random fluctuation in traffic. We therefore apply cumulative sum (CUSUM) to solve this problem. CUSUM is calculated over destination IP address based entropy to detect the attacks. It makes use of the concept of time along with threshold to judge the network condition. If the abnormal condition persists for a certain period or crosses threshold, attack is detected. Destination under attack is identified in case attack is present.

In our destination IP address entropy based DDoS attack detection method, suppose Y_n is the destination IP address based system entropy value calculated on edge router of stub at each sampling interval of $\Delta_{n,}$ and the random sequence is extracted as network service random model. In the normal occasion this sequence is independent and distributed. Assume the variation parameter is the average value of sequence. Before change, this value $E(Y_n) = \alpha$. Before attack, when the network is normal, the distribution of destination IP addresses is stable, and has certain randomness. But when DDoS attack happens on one of the destinations, $E(Y_n)$ will become far smaller than α. Without losing any statistics properties, we transfer the sequence to another random sequence $\{Z_n\}$ with negative average value.

Let $Z_n = -(Y_n - \beta)$, (3)

where α = β. In a given network environment, parameter β is a constant used for producing a negative random sequence $\{Z_n\}$, and thus the entire value of Z_n will not be cumulated along the time. In our detection algorithm, we define that β = α. When the attack happens, Z_n will suddenly become very large and positive. The detection threshold is the limit for the positive, which is the cumulative value of $Z_{n.}$

We use this recursive formula for cumulative sum:

$$S_0 = 0 \qquad (4)$$

where S_n represents the cumulative positive value of Z_n. The bigger the S_n, the stronger the attack is.

We calculate the rate of increase of CUSUM value using the following formula:

$$C_0 = 0$$

$C_n = (C_{n-1} + 1), (S_n > S_{n-1})$

= 0,otherwise (5) where C_n represents a counter and signifies the duration of increase in S_n. It uses the concept of time to judge the network condition. The bigger the C_n, higher the probability that there is an attack.

The judgment function is:

$d_n(S_n, C_n) = 1$, $S_n > T$ OR $C_n > T'$

= 0, otherwise (6)

where dn (S_n, C_n) is the judgement function at time n, the value 1 shows that attack happens, while 0 shows the normal case. T and T' are the detection thresholds. We can control the total attack detection time by setting the value of parameter T'.

The advantage of this improved algorithm is that it comprises implicitly a concept of process cumulating. The function of cumulating process is to avoid false alarm when the network has something abnormal just at a time point like a surge of legitimate access. Thus the threshold based approach leads to a more real time and timely attack detection. Time based approach emphasizes on time tolerance and ignores network anomalies in some allowable range. Network is regarded abnormal if threshold is reached or tolerable limit defined by time period increases.

5.DUAL-LEVEL ATTACK CHARACTERIZATION SCHEME

Our algorithm for dual-level characterization and response are based on the idea to allow as much traffic as possible into the network that network can tolerate, and identify and drop the congestion inducing attack traffic.

5.1Macroscopic Level Attack Characterization

In detection phase if $H_c(X)$ is more than normal $H_n(X)$, then suspected malicious flows tend to have lower frequency values of packet arrivals and the attack is termed as low rate degradation attack. While if $H_c(X)$ is less than $H_n(X)$, normal then suspected malicious flows have high values of number of packet arrivals and the attack is high rate.

At the edge router of transit network, we have aggregate of attack flows and normal flows. Let *F* represent set of active flows. Then,

$$F = F_n \cup F_a \quad (F_n \cap F_a = \phi) \qquad (7)$$

In the above Equation, F_n represent actual normal flows and F_a is set of actual attack flows. Our main task in this module is to find $F_a^* = \{f_1, f_2, \cdot\cdot f_m\} \subset F$ the set of *m* malicious flows. Ideally,

$$(F_a^* \cap F_a = F_a) \quad AND \quad (F_a^* \cap F_n = \phi) \qquad (8)$$

In the above Equation, F_a^* is the set of flows identified as attacks. Now the main problem is to find *m*:-

- For distributed low rate attacks, *m* numbers of least measured packet arrival flows constitute F_a^* (*m* number of flows that contribute least to system entropy).
- For concentrated high rate attacks, *m* number of highest measured packet arrival flows form F_a^* (*m* number of flows that contribute least to system entropy).

An estimate of total attack traffic ϕ_a is used to compute *m* and F_a^*. The expected value of attack traffic ϕ_a can be determined as follows:

$$\phi_a = \phi_{td} - \phi_n \qquad (9)$$

In the above Equation, ϕ_{td} is the total attack traffic received in $\{t_d - \Delta, t_d\}$ and ϕ_n is averaged total traffic. The values of ϕ_n is calculated by averaging total traffic observed from the time bottleneck link utilization is 1 up to time $t_d - \Delta$ .The number of attack flows *m*.can be derived from the following Equation:

$$\sum_{j=1}^{m} X_i^j (t_d + \Delta) \le \phi_a$$

(10)

In the above Equation, *i* is designated flow, *j* varying from 1 to *m* for least or highest measured packet arrivals, and $X(t_d + \Delta)$ represent packet arrivals for flow *i* in next time window after attack is detected.

The condition given in Equation 10 helps macroscopic-level characterization module to segregate *m* flows, which have either least or highest packet arrivals.

5.2Microscopic Level Attack Characterization

Though a system may detect the entire set of attack flow i.e. $F_a^* \cap F_a = F_a$ holds true, but in an attempt to do so, some normal flows will be misclassified as attacks and $F_a^* \cap F_n = \phi$ will no longer be valid.

Hence, at macroscopic-level, set of flows identified as attacks F_a^* are limited to a subset of F_a i.e. set of actual attack flows. They are essentially congestion inducing part of the entire traffic which must be responded to and filtered early in the network. A set of flows

$$F_r = F_a - F_a^* \quad (F_a = F_r \cup F_a^* \quad AND \quad F_r \cap F_a^* = \phi)$$

(11)

remain unidentified at macroscopic-level and is identified at microscopic-level as soon as alarm is generated by Mi-LAD.

As discussed earlier, if there is a decline in system entropy for the destination IP based entropy time series on edge router of stub network, attack is detected. Victim is identified and the characterization is triggered.

5.2.1Identification of Victim

Let $S = \{S_1, S_2, ... S_k\}$ represent a set of servers to be protected with $D = \{D_1, D_2, ... D_k\}$ representing destination IP based flow id for each server in *S*. Let *X(t)* represents the number of packet arrivals for a flow in $\{t - \Delta, t\}$ where Δ is a constant time interval called time window. When there is an attack, the destination IP based system entropy Y_n decreases dramatically, because there is one flow dominating the router. The edge router treats dominant flow as victim of DDoS attack. For the flow id having highest frequency of packet arrivals and least contribution to the destination IP based system entropy, the corresponding server is identified as victim of the attack.

$$Victim = \min(Y_n^1, Y_n^2, ..., Y_n^k) \quad and \quad \max(X^1(t), X^2(t), ..., X^k(t))$$

(12)

In the above Equation, *k* is the number of unique destination IP based flows or the number of servers.

5.2.2Identification of attack flows

Our proposed microscopic-level characterization technique is based on following notion. The attackers or attack tools use same mathematical functions to control the speed of attack packets sent to the victim. In an attack scenario, an attacker uses a random variable *X* to control the generation speed of attack packets. For example, using a constant speed to generate the packets, namely, *P{X=C} =1*, and *C* is a constant; increasing the number of attack packets according to attack time *t*, *X=a.t+b*, *a* and *b* are constants; simulating the network accessing as Poisson process, $P\{X = k\} = \lambda e^{-\lambda} / k!$, *k*=0,1… and λ is a constant; and so on. Based on this observation, the different attack flows of a DDoS attack share the same regularities, which are different from normal traffic in a short time period.

Following theorem is used to prove there is a regularity during the launch of attack provided mathematical functions to control speed of attack is same and network is linear and stable during a short time period.

Theorem: For random variable *X* , and $Y = f(X),$ if $f(.)$ is a linear function, then the entropy $H(X) = H(Y)$

Proof:

Suppose X is a discrete variable, and $X \in \{x_1, x_2, ... x_n\}$, then $Y \in \{f(x_1), f(x_2), ... f(x_n)\}$. Because of the mapping is a one-to-one mapping, therefore, the possibilities of each pair in the two domains are the same, respectively.

$$p(x_1) = p(f(x_1)), p(x_2) = p(f(x_2)), ..., p(x_n) = p(f(x_n))$$

Therefore,

$$H(Y) = -\sum_{i=1}^{n} p(y_i) \log p(y_i) = -\sum_{i=1}^{n} p(f(x_i)) \log p(f(x_i)) = -\sum_{i=1}^{n} p(x_i) \log p(x_i) = H(X)$$

The above theorem shows clearly that the entropy of attack packet generation speed of each zombie is the same, and it exhibits regularity, if mathematical function is the same, although the CPU and the network delay may differ among zombies.

From Equation 7

$$F = F_n \cup F_a \qquad (F_n \cap F_a = \phi)$$

From Equation 12

$$F_s = F_a - F_a^* \quad (F_a = F_s \cup F_a^* \quad AND \quad F_s \cap F_a^* = \phi)$$

Substituting Equation 12 in Equation 7

$$F = F_n \cup F_s \cup F_a^* \, (F_s \cap F_a^* = \phi \, AND \, F_n \cap F_s = \phi \, AND \, F_n \cap F_a^* = \phi)$$

(13)

where, F_a^* is the set of flows identified as attack and filtered at macroscopic-level; F_s is a set of flows identified as suspicious attack flows at microscopic-level. Specifically, source IP based flows destined on victim that share same or very similar entropy and have minimal variations in their source entropy i.e. entropy rate is zero or less than a threshold value, are tagged as suspicious attacks and are included in set F_s . Any flow in set F_n destined to honeypots is tagged as suspicious attack, removed from set F_n and included in set F_s .

We maintain a flow list (*FL*) at the edge router of stub network which is a subset of flows from set *F*. In a time window

$$F(t) = F_n \cup F_s \quad (F_n \cap F_s = \phi)$$

(14)

where $t = j\Delta; \; j \in N; \; \Delta$ is a constant time interval called time window.

Hence the result of the microscopic-level characterization process is recorded in *FL* which contains source IP based flows, with each flow tagged as either normal or suspicious attack.

Ideally, all the flows in set F_s should be identified during the process of microscopic-level characterization. However in practical implementation, we assume that no system is perfect and only a subset F_s^* of set F_s is identified as suspicious and tagged. A set $F_s - F_s^*$ remains unidentified and results in FN. Similarly subset F_n^* of set F_n may be identified as normal, with $F_n - F_n^*$ resulting in FP.

6.PERFORMANCE EVALUATION

This section details out exhaustive experimentation carried out to evaluate the performance of the detection and characterization scheme.

6.1Experiment Design and Procedure

We simulate a network representative of the structure of the Internet. For the study in this paper, we model the Internet as transit stub network. We choose AT&T networking environment and generate its transit-stub model . The 156 node AT&T topology in figure 4 is quite famous and often used for simulations.

It is composed of interconnected transit and stub domains. The transit domain comprises a set of highly connected backbone nodes. Backbone node is either connected to several stub domains or other transit domains. Stub domain usually has one or more router nodes, which have links to transit domains. NS2 topology for AT&T transit stub model has been generated using Georgia Tech Internet Topology Generator (GT-ITM) and extended nam

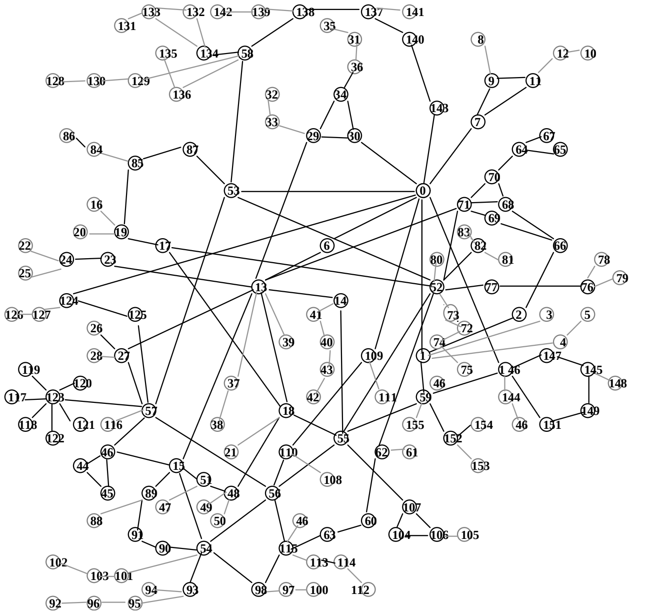

Figure 4. Simulation topology of AT&T transit stub network used in our experiments

Our specific model has 3 core routers, 4 transit nodes with 3 stubs per transit and 4 stub nodes, 5 servers and 137 clients (legitimate clients and attackers). The topology considered is similar to the one used traditionally to depict a typical client-server scenario in the Internet. Transit domain edge routers are point of presence (POPs) of the ISP and stub domains are customer domains attached to POPs.

Table 1. provides the basic parameter set for simulation. The links are assigned as recommended in with the following bandwidths and delays: 10 Mbps bandwidth and 1 ms delay for all inter-stub links (1st level links) and 1 Mbps bandwidth and 10 ms delay for intra-stub links (2nd level links). For the sake of fast simulations, we do not use realistic link capacities (although relative values correspond to realistic cases).

Table 1. Basic Parameters for Simulation

S.N.	Parameter	Value
1.	Number of legal sources	15-48
2.	Number of attackers	1-89
3.	Backbone link bandwidth	100 Mbps
4.	Backbone link delay	0 sec
5.	Bottleneck link BW	10 Mbps
6.	Bottleneck link delay	1 msec
7.	BW for legitimate clients	1 Mbps
8.	Delay for legitimate clients	10 msec
9.	Server link bandwidth	3 Mbps
10.	Server link delay	1 ms
11.	Mean attacker rate	0.1-3.0 Mbps (low rate) 3.0 – 6.5 Mbps (moderate rate) > 6.5 Mbps (high rate)
12.	Mean client load	0.1-7.0 Mbps (low rate) 7.0-9.0 Mbps (moderate rate) >9.0 Mbps (high rate)

Previous studies have shown that request inter-arrival times follow an exponential distribution. Thus, the request arrival process corresponds to a Poisson process, where users arrive independently of one another. Number of attackers and attack rate are varied to impose different attack load. Each simulation experiment has 10 runs (averaged in the graphs). Legitimate clients send requests from time 0 to time 30 seconds and attack duration is from 8-20 seconds.

6.2Results and Discussion

6.2.1Detection of Attack by Ma-LAD

Figure 5(a) shows entropy profile when network is put under attack. This represents DoS and attack is launched with 1 attacker with mean rate varying from 3 Mbps to 50 Mbps. In the first time window after the attack is launched at 8 seconds, there is a dip in entropy value. The persistent low value of entropy reflects that it is a concentrated attack. Similarly, figure 5(b) shows entropy profile when our network is put under distributed attack. In this case attack is launched with 80 attackers with mean rate varying from .05 to 4 Mbps. Positive jump and persistent high value of entropy reflects that it is a distributed attack.

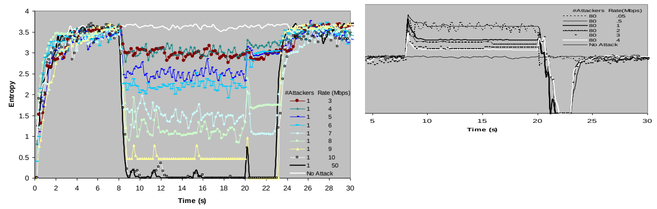

Figure 5. (a) Entropy distribution for DoS (b) DDoS

6.2.2Sensitivity – Specificity Curve

At low attack load of .5 Mbps, optimum value of tolerance factor ‘a’ varies from 6 to 9 (figure 7). At a higher attack load of 5 Mbps, ‘a’ varies from 4 to 6 as shown in figure 8. However, at a very high attack load with 80 attackers (figure 9), optimum value varies from 2-4. Hence it is observed value of ‘a’ decreases with increase in the attack load.

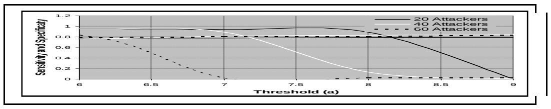

Figure 7. Sensitivity - Specificity Curve: Attack load .5 Mbps

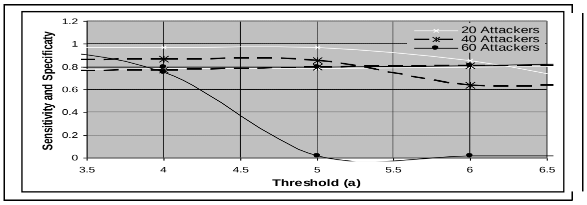

Figure 8. Sensitivity - Specificity Curve: Attack load 5 Mbps

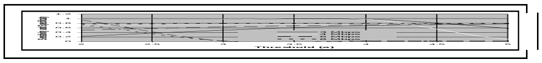

Figure 9. Sensitivity - Specificity Curve: 80 attackers

On the basis of the above observation, we calibrate our macroscopic level detector to work in one of the three modes of defense, namely naïve, normal and best defense The following table lists the values of tolerance factor ‘a’ for different modes of operation.

Table 2 Mapping a to mode of operation

Mode of Operation	Tolerance factor ‘a’
Naïve Defense	6 - 9
Normal Defense	4 - 6
Best Defense	2 - 4

6.2.3Detection of Attack by Mi-LAD

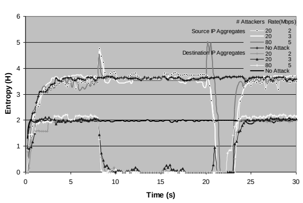

Figure 10. Time series entropy

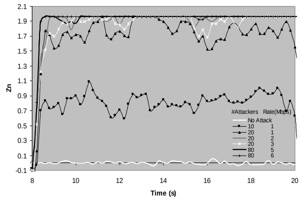

Figure 11. Time series Z_n

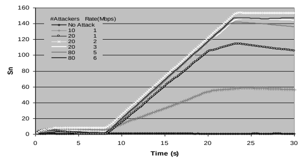

Figure 12. Time series S_n

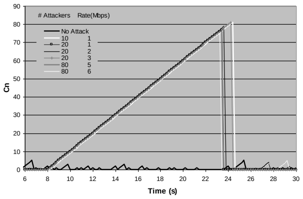

Figure 13. Time series C_n

Figure 10 shows the time series of source IP address based system entropy under normal conditions in the absence of attack as well as in the presence of sophisticated DDoS attacks. There is a significant overlap between the time series of source IP address based system entropy for normal and attack conditions which shows that detection of such attacks is not possible based on source IP address based entropy alone. In such cases, a significant drop in destination domain entropy clearly detects the presence of the attacks as shown in the figure.

Figure 11 shows that in normal condition the sequence of Z_n is negative. As shown in figure 12, when the attack happens, this cumulative value S_n increases rapidly. By setting a threshold T equal to 10 for our network environment, when S_n >T, the system detects the attack. Figure 13 shows the time series value of counter C_n which judges the persistence of abnormal condition in the network over a time period. By setting the threshold T' = 5 for our network environment, when C_n >T', we believe that something abnormal persisted over network tolerance limit and network is attacked. The flash crowds persist for a very small duration and are represented by small positive fluctuations that lie below threshold T' as shown in the figure. Hence, results in figure 13 justify our claim that the approach is able to differentiate between DDoS attacks and flash crowds.

6.2.4Sensitivity of detector to attack detection

We simulate 10 Mbps legitimate traffic originating from 15 clients picked randomly with inter-arrival time of .1 seconds. Attack load is varied from 100 to .0001 Mbps representing thinning factor from 0 to 1000000 respectively. DoS attack is launched with single attacker whereas DDoS attack is launched with 80 attackers sending attack traffic towards victim. Table 3 shows the attack rate in mbps corresponding to various thinning factors.

Our detectors provide a very high detection rate at high rates of attack traffic which almost equals to 1. Even at lower rates of attack traffic our detectors are very effective for attack detection. Figure 14 shows that high detection rates are possible for much lower intensities of attack. For example, a detection rate of nearly 98% is possible for DoS and DDoS events comprising only 0.90% of the total traffic. When attack traffic comprises .09 % of total traffic on average, the detection is still effective but to a lesser degree.

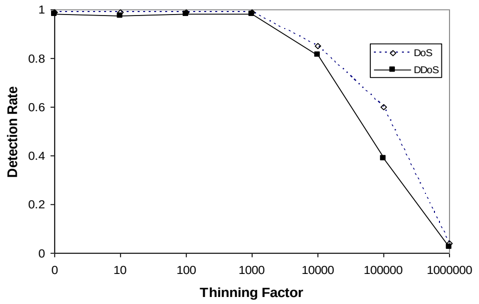

Figure 14. Sensitivity of detector to attack detection

Table 3 Intensity of DoS and DDoS attacks

Thinning Factor	Attack Rate (Mbps)
0	100
10	10
100	1
1000	.1
10000	.01
100000	.001
1000000	.0001

6.2.5Macroscopic Level Characterization

Two kinds of attacks are simulated. The first attack is simulated with a single attacker attacking at a rate of 1 Mbps. Second attack is simulated with 80 attackers with a mean attack rate of .5 Mbps. Figure 15 shows time series entropy of each distinct source IP based flow monitored on edge router of transit network. The

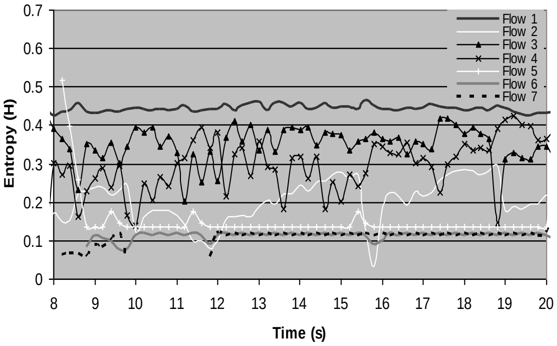

Figure 15. Time series entropy variation of each distinct source IP based flow

Figure shows that flow 5, 6 and 7 are easily distinguishable from other flows. These flows correspond to attack signals. Flows 1 to 4 are noise and correspond to legitimate flows.

In the first case, flow 5 with the least contribution to source IP based system entropy and most frequent packet arrivals was identified as attack flows, with value of *m* corresponding to 1.In the second case, the characterization process triggered as a result of detection, on simulating 80 attackers with 0.5 Mbps attack rate after 8 seconds, alarmed distributed low rate attack and identified flow 6 and 7 (up to flow 85 not shown in the Figure) as the attack flows. These attack flows are signals with less frequent packet arrivals and hence contribute least to the source IP based total system entropy as shown in Figure 5.4. However, such flows being large in number increase the total system entropy at edge router of transit network.

6.2.6Microscopic Level Characterization

We simulated the attack with 10 attackers at rate of 1 Mbps and monitored time series entropy of each distinct Source IP based flow destined to server 118. Figure 16 gives the results of simulation. The set of source IP based flows from 1 to 10 share same entropy space and there are minimal variations in their entropy rate. These dominant signals are effortlessly identified tagged as suspicious attacks.

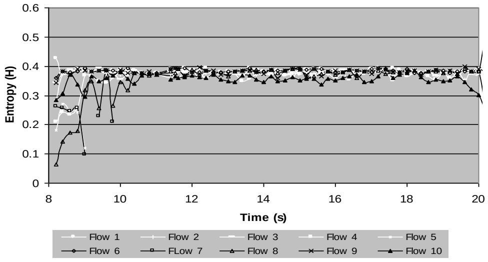

Figure 16. Time series entropy variations of each distinct source IP based flow destined to the victim (server 118) monitored on edge router of stub network ; 10 attackers ;1 Mbps

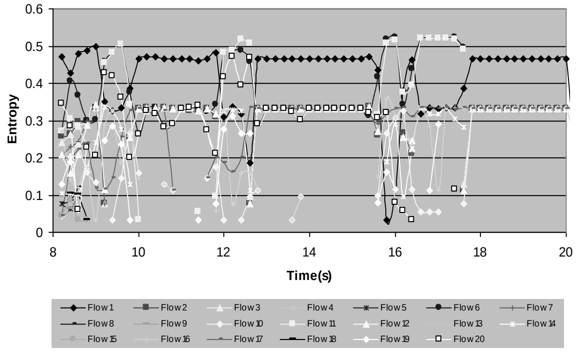

Figure 17 Time series entropy variations of each distinct source IP based flow destined to the victim (server 118) monitored on edge router of stub network; 20 attackers; 2 Mbps

Figure 17 shows the results when previous simulation was repeated with 20 attackers attacking at rate of 2 Mbps. The Figure shows two distinct sets of signals for the 20 flows with no variations in the entropy for each set of flows. The entropy rate for each flow in both sets becomes zero soon after the attack is launched at 8 seconds. This justifies the fact that attacks generated by sophisticated attackers using different attack functions can be easily identified.

6.2.7Performance of the overall scheme

Figure 18 shows the ratio of legitimate and attack packets accepted under different strengths of attack. The strength of attack was increased by increasing the number of attackers from 1 to 80. The Figure shows that more than 90% of the good packets were identified and accepted irrespective of the mode of defense. This clearly justifies our claim that collateral damage caused in the presence of the proposed responsive measure is much less than the damage suffered by legitimate clients in the absence of response, which reduced the throughput to zero as soon as attack was launched. There is no perceivable decrease in the acceptance rate of legitimate packets even if the magnitude of attack increases. Legitimate packets remain unaffected and are not dropped because, before congestion inducing attack packets flood the network resources and cause legitimate packets to drop, they are filtered at macroscopic-level i.e. much early before reaching the victim.

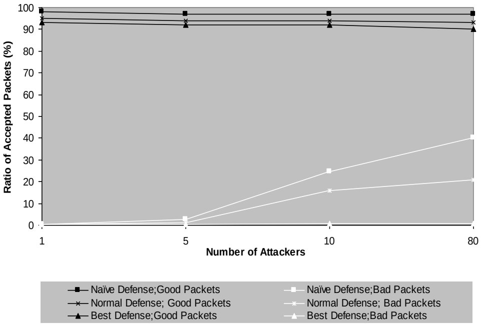

Figure 18. Ratio of accepted packets vs. different number of attackers for three modes of defense

Though, the packet acceptance ratio for good packets remains same with increasing number of attackers, the bad packet acceptance ratio increases with increase in number of attackers and attack strength. The increase is highest for naïve defense, because the system is calibrated to reduce false alarms and hence reduces the detection rate. Hence some attack flows remain undetected and go uncharacterized at macroscopic-level. In case of best defense, the system is calibrated for high detection rate and minimum FN. Therefore bad packet acceptance ratio decreases almost to zero in case of best defense.

Hence, the simulation results indicate that response prototype blocks substantial congestion inducing attack traffic, allowing some of the suspicious traffic into the network, that can be further analyzed before taking any decision, and hence reduces collateral damage.

7.CONCLUSIONS

With the proposed two-fold protection framework, packets with higher probability of being valid are offered preferential service, while packets which have been marginally classified as invalid or suspicious attack at microscopic-level are allowed and directed to honeypots. It drills down to investigate suspicious DDoS flows more closely at honeypots at microscopic-level.

The results in are encouraging for the use of the framework. We find that dual level exposes a lot of anomalies that cannot be detected using volume based methods. Many of these DoS and DDoS events are of fundamentally different type from those exposed by volume – based methods. Finally, the scheme generates relatively few false alarms, as can be tuned to different network environments by optimizing the threshold and calibrating the detector, and has a high detection rate even when it comprises a small fraction of total traffic.

Future investigations are directed to real time implementation of the scheme and extending the scheme to heterogeneous networks.

8.REFERENCES