An Enhanced Entropy Approach to Detect and Prevent DDoS in Cloud Environment

N. Jeyanthi[1], N.Ch.S.N. Iyengar[2], P C Mogan Kumar[1], Kannammal A[3]

[1]School of Information Technology and Engineering, VIT University, India,
[2]School of Computing Science and Engineering, VIT University, India,
[3]Dept. of Computer Applications, Coimbatore Institute of Technology, India
njeyanthi@vit.ac.in, nchsniyengar@gmail.com, kannaphd@yahoo.co.in

Abstract: Distributed Denial of Service (DDoS) attack launched in Cloud computing environment resulted in loss of sensitive information, Data corruption and even rarely lead to service shutdown. Entropy based DDoS mitigation approach analyzes the heuristic data and acts dynamically according to the traffic behavior to effectively segregate the characteristics of incoming traffic. Heuristic data helps in detecting the traffic condition to mitigate the flooding attack. Then, the traffic data is analyzed to distinguish legitimate and attack characteristics. An additional Trust mechanism has been deployed to differentiate legitimate and aggressive legitimate users. Hence, Goodput of Datacenter has been improved by detecting and mitigating the incoming traffic threats at each stage. Simulation results proved that the Enhanced Entropy approach behaves better at DDoS attack prone zones. Profit analysis also proved that the proposed mechanism is deployable at Datacenter for attack mitigation and resource protection which eventually results in beneficial service at slenderized revenue.

Keywords: DDoS, Availability, Cloud computing, Datacenter, Entropy, Enhanced Entropy, Goodput.

1. Introduction

Cloud computing supports resource abstraction i.e. the clients do not require any special hardware or software for complex operations. Cloud DataCenters balance the load by supplying the necessary resources on-demand. DDoS is one of the malicious attacks which results in inestimable loss in Internet business [1]. DDoS attacker may target towards the depletion of network or memory resources of DC either by exhausting of victim bandwidth or by stealing the sensitive information from the victim end [2].

Existing DDoS defense mechanisms could not resolve the problem completely due to their own limitations. Signature-based detection mechanism uses huge database for comparing the incoming traffic, and filters only when any attack threat is detected. Frequent updating is required to improve detection accuracy which imposes huge data processing [3] overhead. Behavior-based mechanism requires small heuristic data for detection.

The proposed behavior-based detection mechanism, “Enhanced Entropy” approach, detects and outwits the attackers at an earlier stage. Dynamic resource provisioning nature of Cloud DC allows the attacker to destroy the resources before attack detection. Even an unsuccessful DDoS attack at cloud DC leads to quicker resource depletion which in turn causes expenses to soar [4] and DoS to legitimate users. After Wiki Leaks servers were brought down by DDoS attackers by the end of November 2010, Wiki Leaks migrated to Cloud security [5]. DC maintains emergency backup mirror servers that synchronize data and could achieve fault tolerant. Hence, the probability of DDoS attacks bringing down a cloud DC performance is far less when compared to traditional infrastructures.

Aim of this proposal is to have better response time at DC even at the time of DDoS. To reduce the amount of unnecessary traffic reaching DC, detection and elimination should be carried out periodically. The proposed Enhanced Entropy approach achieves this at fivefold as: (i) Analyze the incoming traffic condition (ii) detect any deviation from normal (obtuse) traffic i.e., abnormal (acute) traffic (iii) classify the traffic as legitimate or attack (iv) Track aggressive and genuine legitimate behaviors’ using the trust credits (v) Eliminate the detected attackers’ groups and prevent further from accessing DC resources. At each stage, some amount of traffic is identified and outwitted which ultimately reduces the traffic that reaches DC.

The rest of this paper is organized as follows: Section 2 presents surviving techniques. Section 3 overviews the proposed approach. Section 4 reveals the working mechanism. Section 5 shows the evaluated performance. Section 6 lists the benefits and section 7 concludes the work.

2. Literature Survey

DDoS is a type of intentional, targeted attack that disrupts the normal functioning of websites. While it is very easy for hackers to target and direct as many DDoS attacks to any service provider using traditional infrastructures, the cloud security measures make it difficult for them to bring down the cloud [5].

Network attack detection method is based on entropy [6] used source IP, destination IP, alert treat and alert datagram length. This methodology is based on the alerts sent and network features and works well only on class C-class networks. DDoS attack is detected based on the relative entropy distance [7] among the suspicious flow to the possible victim on different paths. If the distances are near or equal attack is identified. Distance calculation causes computation overhead, since this detail can be extracted from the TTL field of the IP header.

Two mode detection mechanisms [8] use dynamic threshold values to detect application layer DoS attackers. This had three sequential methods to detect by analyzing the traffic, which would increase traffic as well as computation cost.

Fast entropy [9] claimed to be better than conventional and compression entropy methods. Fast entropy used different symbols rather than employing computations.

DDoS defense mechanism [10] used hop count filter, anomaly detectors, normal profile creation and attacker profile creation and comparing the incoming traffic to reduce false positive and false negative in order to improve the efficiency attacker detection schemes using Kullback-Liebler Divergence. Over Court Gateways [11] is a credit based system where the well behaving users will gain credit points and the ill behaving users will lose their credit points. When the legitimate users exceed the threshold credit points, the users will be protected in a secure channel by path migration. When any users' characteristic leads to credit point's exhaustion, the users will be blocked to access the server. This DDoS defense mechanism consists of one-hop path splicing, signaling mechanism, path migration, credit-counting system, path migration trigger.

Palvinder Singh Mann and Dinesh Kumar [12], [13] proposed distinguishing of attack and legitimate traffic using mathematical methods like Poisson distribution and Binomial theorem. Hoop Count Inspection with Malicious Probability Rate (HCI-MPR) is suggested to mitigate attack traffic. Computational overhead is a drawback in this.

Entropy-based Input-Output Traffic Mode Detection Scheme [14] is able to successfully detect both long term and short-term denial-of-service attacks that might not be able to detect both at the same time with other approaches but if sophisticated attackers completely understand this detection mechanism, they might be able to modify their attacking technique that causes vulnerability to this defending approach. This technique requires high computation on the defending machine.

Besides the presence of many detection methods, like Path Identification routing scheme and IP trace back, which help only in detecting the location of attacker and blocking the incoming attack packets, this method is well suited for DOS attack and not suitable to DDoS because the location of an attacker changes for every instance of time as they are distributed over the network [15].

It has been already proven that using entropy approach to distinguish the characteristics of legitimates and attackers are efficient. There are certain other kind of overload threats that might not create traffic at DC but could create serious disaster to cloud networks as the DC is busy all the time unlike local servers, DDoS at any point of time, could definitely indulge sensitive information residing at DC. It works well on DDoS traffic but lacks at other kinds of overload threats and also performance is not as expected because of other kinds of threats at normal condition. This motivated us to analyze the reason for lesser performance even at normal traffic condition. To outwit other kind of overload threats we developed an Enhanced Entropy Approach which detects almost any kind of overload threats and is well suited to cloud environment.

The performance of an entropy based [15] mechanism to detect and discriminate DDoS from Flash Events approach has motivated us to work further to improve and deploy in the cloud infrastructure. Enhanced Entropy approach follows behavior-based DDoS defense mechanism which is dynamic in predicting the network condition.

3. Overview of Enhanced Entropy Approach

This section presents the working methodology adopted and the rationales used to describe the parameters.

3.1 Methodology

DC requester can be legitimate or an attacker. Incoming traffic is validated before allowed to access DC by analyzing the network behavior. Figure 1 shows the overview of Enhanced Entropy Approach. The legitimacy at packet analyzer results in improved trust on legitimate clients for allowing access to DC resources. Failing at any level of detection outwits the client from cloud network.

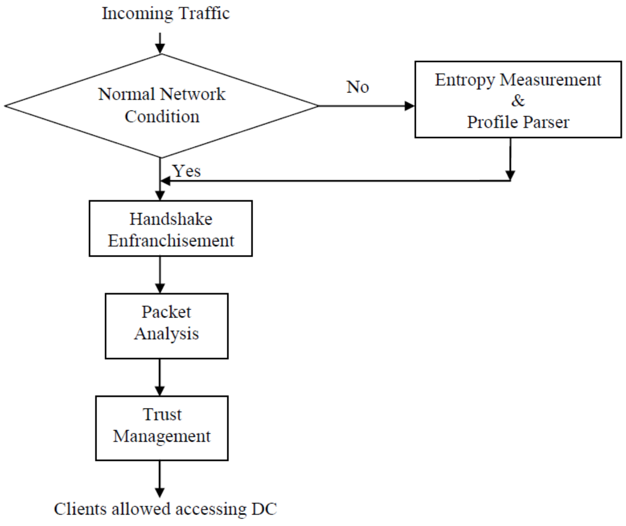
Incoming Traffic
Normal Network Condition
No
Entropy Measurement & Profile Parser
Yes
Handshake Enfranchisement
Packet Analysis
Trust Management
Clients allowed accessing DC

Figure 1. Overview of Enhanced Entropy Approach

3.2 Rationale of Enhanced Entropy Approach

Anti-DDoS hardware has been placed for packet probing. The hardware detection scheme has its own advantage and it detects threats much quicker than Anti-DDoS software Defense mechanism [17]. Google's servers have been laid low for a few hours a couple of times [6] to the DDoS detection mechanism uses simple processors, routers, packet analyzers. This does not impose huge cost.

Legitimate users have to be differentiated from the attackers in order to DC. Both legitimate and attacker have message template that vary in their traffic condition [18]. Figure 2 helps in explaining the characteristics of proposed approach; here the dotted arrows represent the flow at the time of abnormal network condition found at Traffic Analyzer.

3.2.1 Legitimate Characteristics

Legitimate clients are the clients who follow the legitimacy at all stages of our detection. Initially the traffic analyzer predicts the network behavior. Bypassing traffic analyzer, the traffic packets examined at entropy profiler. If the Hellinger Distance lies under threshold, then the incoming traffic will not create harm at DC.

The legitimate must respond to the handshake ping request and their behavior at packet analyzer should also match legitimate to declare as a legitimate client. The legitimacy of the client is rewarded with the credit, called trust credit. Then the client is allowed to access the DC resources.

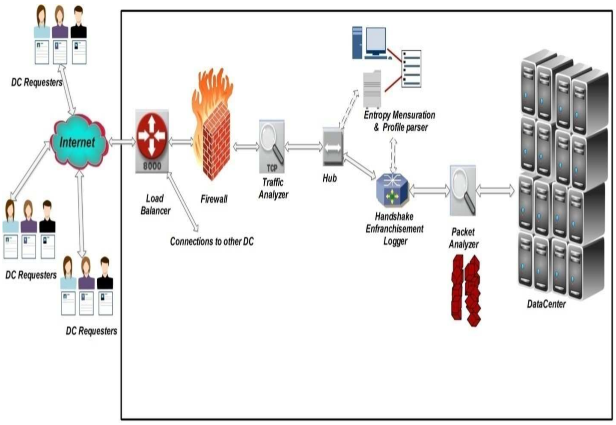

Figure 2. Architecture of Enhanced Entropy Approach

3.2.2 Attacker Characteristics

Distributed attackers traverse the network which leads to abnormality in network behavior. For confirmation, we use entropy profiler which logs the incoming traffic and reports the network traffic divergence using Hellinger Distance. Usually spoof attackers and botnets fail at Handshake Enfranchisement. Here the legitimate and attackers are distinguished. Still the traffic is further reduced at packet analyzer by detecting the aggressive clients based on their heuristic data.

4. Working Mechanism

4.1 Design of the Enhanced Entropy Approach

The flow diagram shown in figure 3 explains the detailed working mechanism of Enhance Entropy approach. Incoming traffic is passed to traffic analyzer (level 1) which preliminarily identifies the network behavior. On bypassing the traffic analyzer, if the abnormal traffic condition is observed, it is then passed for entropy profiling (level 2). Here, the buffered traffic is converted to dataset for determining the Hellinger Distance (HD). Greater HD results in highly acute traffic.

Now, the Incoming traffic is analyzed by entropy profile parser for classifying legitimates and attackers. The handshake requisition (level 3) is generated for each requester. When the requester fails to respond after some trials, the clients are considered as Botnet / spoof attacker (spoofer). The verified packets are again probed at packet analyzer (level 4) based on the heuristic data usually inter-arrival time. This phase allows detecting the difference between legitimate clients and aggressive legitimate clients. Utilizing heuristic data, legitimate clients are awarded with the trust credit (level 5). At each level some amount of traffic has been outwitted to improve the detection efficacy eventually.

The Enhanced Entropy Approach deals with DDoS attack scenarios and to make DC to withstand and serve its intended legitimates even at the time of DDoS attacks. In order to accomplish, the attackers and legitimates characteristics are to be found. A strong detection scheme must be in place which should be dynamic in detecting the attack threats and outwit them earlier, restricting further entry of detected attacker, allowing legitimates requests to process and respond quicker from DC end.

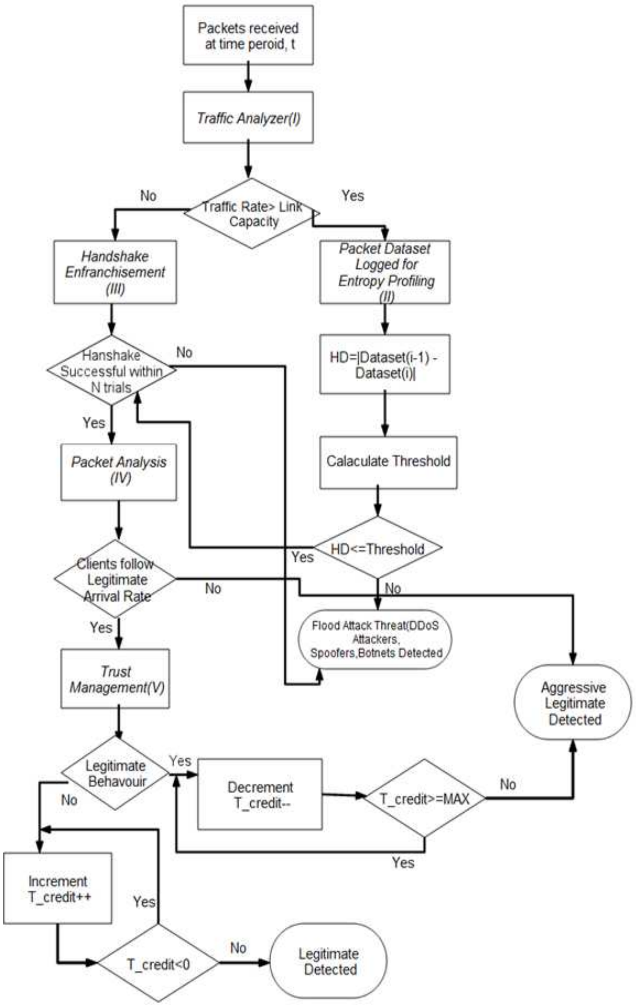
Packets received at time peroid, t
Traffic Analyzer(I)
No
Traffic Rate> Link Capacity
Yes
Handshake Enfranchisement (III)
Packet Dataset Logged for Entropy Profiling (II)
Hanshake Successful within N trials
No
HD=|Dataset(i-1) - Dataset(i)|
Yes
Packet Analysis (IV)
Calaculate Threshold
HD<=Threshold
Yes
Clients follow Legitimate Arrival Rate
No
No
Yes
Flood Attack Threat(DDoS Attackers, Spoofers,Botnets Detected
Trust Management(V)
Aggressive Legitimate Detected
Legitimate Behavour
Yes
No
Decrement T_credit--
T_credit>=MAX
No
Yes
Increment T_credit++
Yes
T_credit<0
No
Legitimate Detected

Figure 3. Flow diagram of Enhanced Entropy Approach

4.2 Traffic Analysis – Level 1: Preliminary Traffic Analysis

Detecting the threats requires continuous monitoring of incoming traffic. Traffic Analyzer is employed to measure the incoming traffic, if any acute traffic is observed, signalled to entropy profiler for further detecting the cause of overload. Buffer capacity is five times the capacity of bandwidth which is presumed to capture packet at traffic rate for further probing. Exceptionally, the traffic exceeding buffer is dropped.

At this stage, only the traffic condition is identified but cause of the traffic overload is precisely detected at other levels.

Algorithm 1: Traffic Analysis

```
Input : Incoming Packets
Output: Network traffic condition
BEGIN
   FOR each time period, t
      Packets are logged at traffic analyzer  for traffic rate computation
       IF (Traffic Rate <= Link capacity)
          Alert "Normal (obtuse) Traffic condition"
          Forward packets to Level 3.
       ELSE
          Alert "Abnormal (Acute) Traffic condition"
          Forward Packets to Level 2.
      END IF
   END FOR
END
```

4.3 Attack Detection - *Level 2: Entropy Profiling*

Entropy is a measure of uncertainty of an outcome. Entropy classification helps in identifying the incoming traffic. This phase is activated only when the network condition is reported as abnormal by Traffic Analyzer. The buffered packet of traffic analyzer can be a random traffic packets at xi (queued at discrete time interval) of random variable X (flooding packets reaches the DC), where $p(X = x_i) = p_i$ [20].

The entropy of the random variable X is then

$$H[p] = -\sum p(x_i)\ln p(x_i) \tag{1}$$

where p (x_i) = probability mass function of a chosen random variable X.

Initially, at the trial phase, the packets are collected and grouped as a dataset by protecting the network without any attacker, this acts as a baseline for future traffic comparison. At monitoring phase, the incoming packets are logged into second buffer as a new dataset; the probabilistic difference reveals the Hellinger distance.

Hellinger Distance is a measure of predicting the variation between two probabilistic distributions. Now let P and Q be the probabilistic distribution with n samples. Here, samples obtained at trial phase represent the P distribution and current traffic samples obtained at monitoring phase represents Q distribution. Now, Pi and Qi are probabilistic samples. Whenever the packets exceed link capacity, the abnormal protocol behavior alert is signalled by Traffic Analyzer. So, the current queued packets are captured by monitoring phase and are compared to trial phase. Now Qi is passed to Pi+1 and Qi+1 calculates the current traffic condition. This scheme continues until Qn. The Hellinger distance H (P, Q) is probabilistic in nature and satisfies the property:

$$0 \le H(P,Q) \le 1 \tag{2}$$

The maximum HD is 1, achieved when P assigns probability zero (ideal traffic condition) to every set of samples of max size queue limit to which Q assigns a positive probability (increase in traffic packet arrival at monitoring phase), and vice versa [16].

Detailed description regarding DDoS defense using Hellinger Distance can be found in [21], [15].

Algorithm 2: Entropy Measurement & Profile Parsing

```
Input : Buffered packets of traffic analyzer, TRIAL phase
Output: Cause of overload
BEGIN
   Buffered packets at traffic analyzer are logged to MONITOR phase
   Difference between the phases yields Hellinger Distance
   Calculate mean and Variance ()
   Calculate Threshold ()
       IF (HD <= Threshold)
          Alert "overload is a cause of legitimate (Flash crowd)"
       ELSE
         Alert "overload is a cause of attack sources (DDoS)"
       END IF
 END
```

Threshold computation and overload classification due to the enormous traffic arrival rate, the threshold in real-time may vary, so the threshold must be made dynamic [22].

4.4 Attack Classification

4.4.1 Level 3: Handshake Enfranchisement

Once the incoming packets pass through the Traffic analyzer and if the network condition is found normal, they are then fed to Handshake enfranchisement module where the client behavior is identified. This phase acts as TCP three-way handshake, in addition the source address validation is performed to authenticate the incoming packets are legitimate, requesters should send request along with the certificate which is induced at the time of user account creation. This certificate acts as write-protected zip code. It is advisable to restrict any new registration or to prioritize them least at the time of DDoS to improve serviceability for the legitimate clients.

For each incoming packet, the packet extraction is exercised to recognize the source address. On recognition handshake enfranchisement activated for the extracted source address.

Figure 4 shows the preliminary transaction of certificate and genuine code exchange which precisely identifies the clients' behaviour. If any one of three transactions fails, it is considered to be an attack attempt, which could be Botnet (if incompatible certification or no certification is received) or spoofer (if no genuine code received until time-out period).

Algorithm 3: Handshake Enfranchisement

```
Input: Buffered packets of traffic analyzer / Packets from Entropy profiler
Output: Botnet, Spoofer threat detected
BEGIN
   Extract packet header for source IP address, $SRC_{addr}$
FOR each $SRC_{addr}$
FOR  i=1 to N
   IF (Certificate validation successful)
      Generate and transmit Genuine code
      IF (Exact combination of certificate + Genuine code matched)
            Alert "Legitimacy approved"
      END IF
   ELSE
  END IF
   i++
END FOR
END FOR
Alert "Spoofer/ Botnet Detected".
END
```

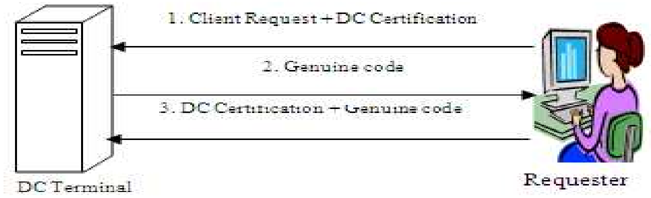
1. Client Request + DC Certification
2. Genuine code
3. DC Certification + Genuine code
DC Terminal
Requester

Figure 4. Handshake Enfranchisement

4.4.2 Level 4: Packet Analysis

The attack threats that could impose abnormal network condition, but still the network is not 100% safe from overload. High-rate DDoS attacks are detected until level 3 but the low-rate DDoS attacks have to be detected. There are some other overload threats that act as legitimate but the intent might be to steal the sensitive information or to corrupt the DC resident data or to create a revenue loss by reserving huge resource at earlier time. They are Low-rate DDoS attack another type of overload threat that is launched by small group of legitimates to degrade the DC performance. This kind of threat is called ***aggressive legitimates attack***. Though these two kinds of attacks are not much considered in any network, it must be considered in cloud networks because the DC holds sensitive information of several work groups; when such DC suffers from aggressive legitimate, it could affect remaining active clients who try to retrieve their sensitive information.

A significant difference between Flash crowd and Aggressive legitimate is that the flash crowd is a cause of large number of simultaneous packets from several legitimates whereas aggressive legitimate is an act of populating more number of packets by single legitimate usually deviates from nominal Inter-arrival rate.

Algorithm 4: Packet Analysis

```
Input: packets validated at Handshake Enfranchisement
Output: Low-rate DDoS, Aggressive legitimates detected
BEGIN
   Extract packet header for source IP address, $SRC_{addr}$
FOR each $SRC_{addr}$
  Predict Inter Arrival Rate, IAR and match with lower bound IAR, $LB_{IAR}$
   FOR i=1 to N
 IF ($IAR < LB_{IAR}$)
     Alert "Low-rate flood detected (Aggressive Legitimate and Low rate-DDoS)"
     Alert "Low rate DDoS attacker outwitted"
  ELSE
     Alert "Legitimate Arrival Rate "
      END IF
   i++
   END FOR
 END FOR
END
```

4.4.3 Level 5: Trust Management

At level 4 all kinds of attack threats are detected irrespective of the attack source. So, the legitimate traffic that passed at all levels of detection are rewarded with the credit points, T_{credit}.

Algorithm 5: Trust Management

```
Input: packets validated at Packet Analyzer
Output: Updated Trust credit points
BEGIN
Extract packet header for source IP address, $SRC_{addr}$
FOR each $SRC_{addr}$
  IF ($SRC_{addr}$ at level 4 detected as (Aggressive legitimate && not DDoS threat))
       IF ($T_{credit\ !=0}$)
          $T_{credit}$ --
        ELSE
          Alert "Outwit Aggressive legitimates"
        END IF
  ELSE
     IF ($T_{credit\ <\ MAX}$)
         $T_{credit}$++
     ELSE
          Alert "Trusted clients will bypass levels of detection for short period of time "
     END IF
  END IF
END FOR
END
```

This credit is increased on successive legitimate behavior and decreased for aggressive behavior of legitimates.

Legitimates are not considered to be aggressive legitimate immediately, they are monitored for some number of trials. When the credit becomes zero, they are considered as aggressive legitimates and outwitted.

On detecting the threats at all prior levels, we employ Trust Credit Points Management is employed to identify the behavior of legitimacy. When the legitimate client reaches maximum T_{credit}, then they are validated periodically at Packet Analyzer to reduce traffic overhead. This scheme also paves way for other legitimates and improves the detection efficacy ultimately.

4.5 Attack Prevention

Traffic Analysis, Detection and Classification precisely categorize the flood threats. So, on detecting these attacks, the attack sources are to be prevented to achieve reduction in traffic arriving at DC. To do so, the attack threats are classified at various levels and are reported to Firewall. That neglects successive transmissions from attack sources.

```
Algorithm 6: Attack Classification
Input: Packet Information
Output: Packets source Restriction
BEGIN
Extract packet header for source IP address, $SRC_{addr}$
FOR each $SRC_{addr}$ packets
  IF ($SRC_{addr}$ found at Restriction list)
    Disallow and drop the packets
  ELSE
    $SRC_{addr}$ is allowed to pass through Traffic Analyzer
  END IF
END FOR
END
```

As time moves on, the Enhanced Entropy detection efficacy can be observed with great efficiency as it outwits attack threats and improves goodput. The Enhanced entropy approach satisfies the above notion and serves the legitimate clients even at the time of DDoS attacks.

5. Experiments and Performance Evaluation

5.1 Experimental Setup

To evaluate performance of proposed approach, a customized world map scenario is created in OPNET simulator. An attack scenario is created that reflects the DDoS attack launched by sophisticated DDoS tools like Low Orbit Ion cannon [23]. [24] [25] explains more about cloud computing support of simulator. The simulator is deployed and assessed for end-to-end response time [25]. Simulator supports DDoS [26] and performance Comparison for QoS (Quality-of-Service) Application in On-Demand Cloud Computing [27] [28]. DC is presumed to be distributed across the globe namely (Vellore, New Delhi, and Moscow, Mexico). The cities are not chosen with any intention. The DCs are created, configured and simulated and there is no physical DC deployed. In order to provide a real-time scenario, each DC is created with 5 physical hosts and 160 VM with TIME_SHARED multi-tasking capability.

Proposed approach is tested with 3 different applications (Email, FTP, DB Query), to check the performance with different sizes of data. There are 1000 legitimate clients and 300 attackers are deployed and distributed around the globe. Vellore DC is assumed as a victim DC to suffer DDoS attack from the distributed attackers.

5.2 Performance Evaluation

5.2.1 Application-specific response time

Response time is the statistic measured as the time elapsed between sending requests and receiving response from server in the network, which includes signaling delay for the connection setup.

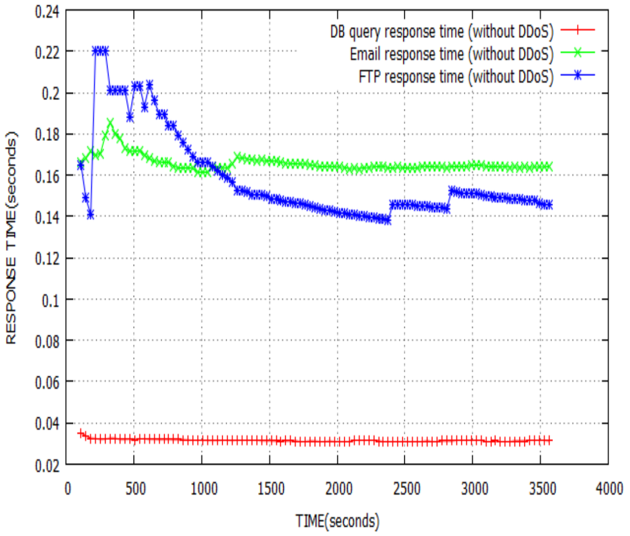

Figure 5a. Response time under no attack

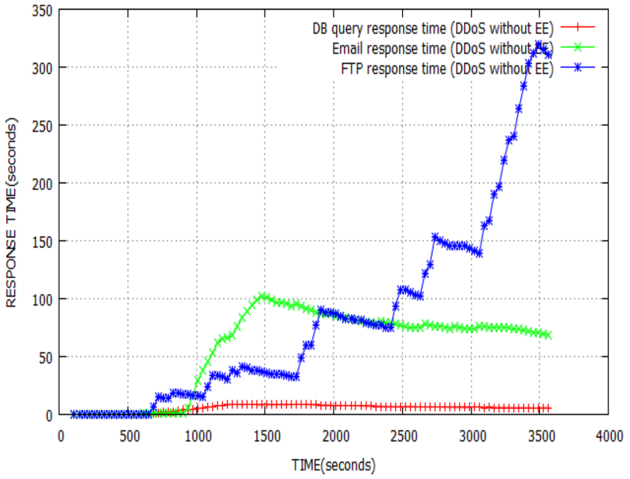

Figure 5b. Response Time under DDoS attack

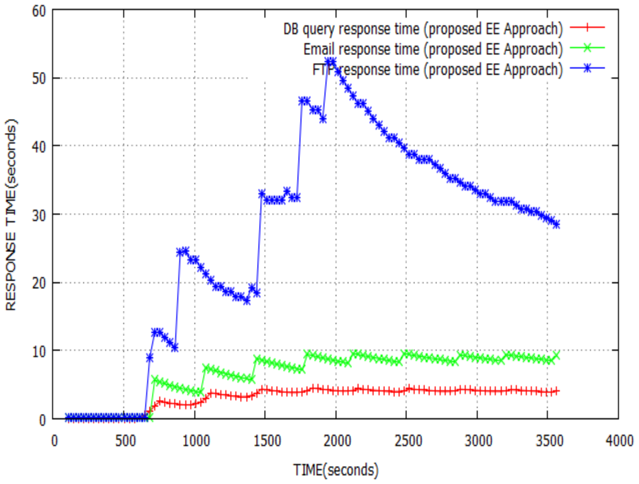

Figure 5c. Response time under EE approach

In figure 5a, it is observable, that the response time is the best which is obtained for calibrating the trail phase of entropy measurement. Figure 5b shows the response time of DC under DDoS attack, where the responses exponentially increase and results poor response due to traffic flood at DC. In figure 5c, the response time rises to certain level which then falls down, and again the traffic is replicated by distributed attackers which still increase the traffic. Once the attacker's detection is successful response time falls down which improve performance of DC. The variation in application specific response time is due to the variability in size of requester's request reaching DC.

5.2.2 Network Traffic Condition

Traffic rate is the statistic that represents the average number of packets received or transmitted by the receiver or transmitter channel per second. The traffic includes both legitimate and attack pattern that attempts to reach DC and recorded at each transaction.

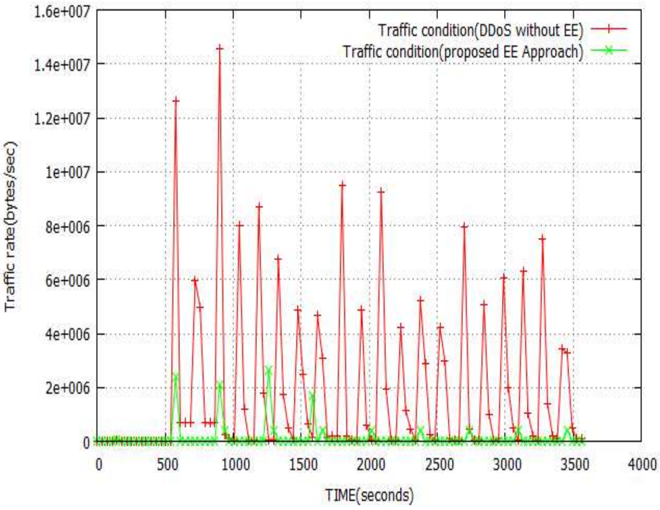

Figure 6. Network traffic condition

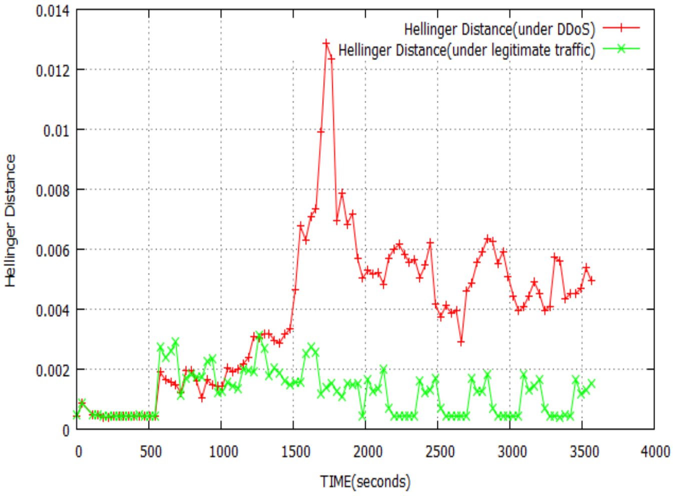

Figure 7. Hellinger Distance measurement of acute

Traffic condition of the network is shown in figure 6, traffic condition under DDoS without Enhanced Entropy (EE) approach, the traffic rate exceeds 14 MBPS which could severely destruct the DC channel and block all the incoming requesters. This huge traffic rate could definitely create disaster to DC by locking up of resources and rarely results in service shutdown. Whereas in the proposed EE approach, once the traffic condition exceeds normal traffic or abnormal traffic is found, they are profiling for entropy measurement. So, as time moves, the attack traffic is considerably reduced as shown in figure 6. Reduction in traffic reduces the DDoS attack threat proportionately.

5.2.3 Hellinger Distance Computation

Hellinger distance is the probabilistic measurement of incoming traffic. The threshold is set to 3.5x10-3 which is not much closer to 1, Hellinger Distance measurement is carried out whenever the abnormal traffic is found at traffic analyzer. When the Hellinger Distance is set close to 0, almost all the incoming traffic overload would be treated as attack threats. When set to optimal, the detection would be quicker. The legitimate traffic in figure 7 has not exceeded threshold as they follow legitimacy of the network. This variation in traffic behavior of legitimates and attackers calculate Hellinger distance and predict the cause of flood is by the legitimate or by attack group.

5.2.4 Detection Accuracy

Figure 8 shows the threats detected at firewall with EE and without EE. DC without EE initially identifies the group of incoming traffic that collides due to the simultaneous activation of requesters, when the DDoS attackers flood at firewall, the firewall could not identify and route the packets to their destination, instead it fails at the time of DDoS due to the increased flood rate.

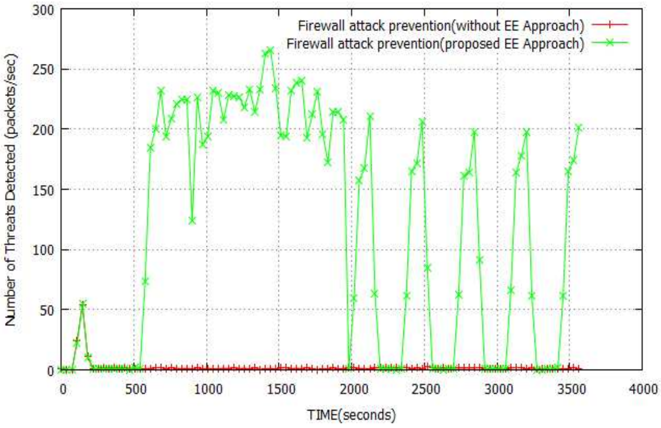

Figure 8. Victim Firewall detection accuracy

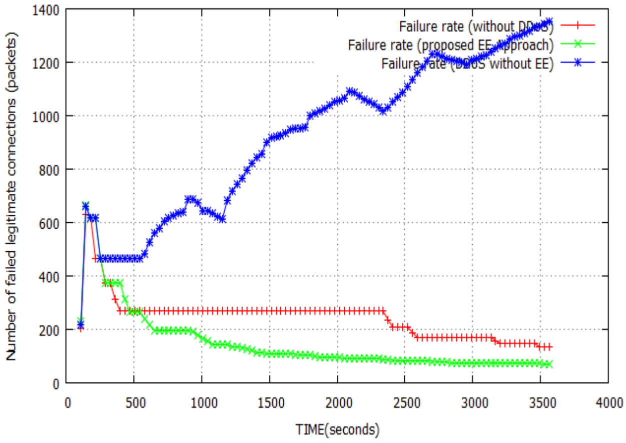

Figure 9. Legitimates Failure rate

Whereas our EE approach detects the initial collision and also at each detection, the attack sources is identified by heuristic dataset and are outwitted at firewall, this ensures increased serviceability of DC to its intended clients. This improvement is obtained due to the enhanced validations made to the entropy profiler.

5.2.5 Failure Rate

Figure 9 shows that legitimates are blocked due to the attackers flood towards DC. And EE approach works well by deleting the aggressive legitimates' connections also. As time moves on, EE approach behaves similar to private network that is of no attack. This advantage is achieved from Packet Analyzer and Trust Credit Points.

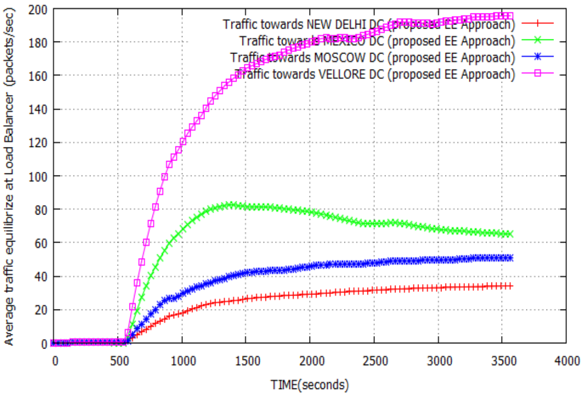

Figure 10. Load balancer efficiency

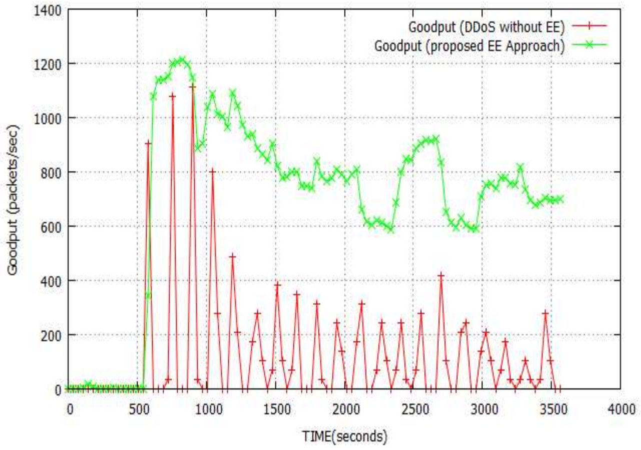

Figure 11. Network Goodput

5.2.6 Load Balancing Policy

Load Balancer acts as a router which analyzes the incoming traffic and forwards the traffic to the appropriate DC. Among the several load balancing policies "Closest DC" policy is chosen. Figure 10 shows the efficiency in load balancing to the DC that is not under attack. The attack prone DC's traffic is diverted towards other DC when the victim DC is unable to process the traffic load. The load diverted towards victim (VELLORE DC) can also be seen in figure 10.

5.2.7 Goodput

Goodput is the rate at which the legitimate packets reach the destined DC. Increase in goodput assures the decrease in legitimates' packet loss and retransmission.

Even though the cloud DC has its own detection schemes to retard DDoS attack, it depends on flood rate. Here, in figure 11, it has been shown that the oscillating behavior towards the legitimate packets proves the DDoS existence, which is far less in EE approach. The little oscillation in EE approach due to the legitimate flood attempt. Dynamic detection can also be found in figure 11. DC without EE is that the DC attempts to service legitimate but because of attack flood rate, it falls down and this behavior is still worse as time moves on. Better Goodput is achieved due to the enhancements made to Entropy Profiler.

6. Benefits of EE Approach

Among many advantages, the most important one of the EE approach is the ability to detect earlier based on the behavior. The response time and other important attributes are efficient than that are listed out in [15]. This approach is experimented with varied number of attackers and found the detection efficacy is suitable for improving the Quality of Service in cloud computing. Detection efficacy is the statistic which measures the number of active attackers at any time.

Detection and prevention at earlier time has an advantage of protecting the resource for other incoming requesters. Detected attackers are prevented at firewall. We tested our experiment with different number of attackers. The experiment is configured to activate the attackers dynamically, so the attackers spoof and enter the DC again to subvert the performance.

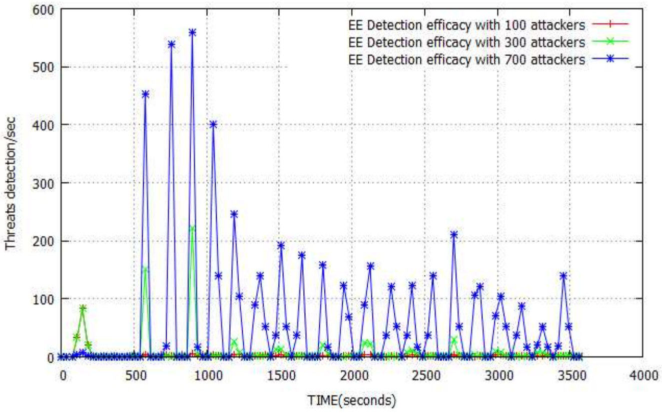

Figure 12. Detection efficacy

The experiment is stress tested with 700 clients to predict the detection efficacy shown in figure 12. This proves that EE mechanism works better even with 700 distributed spoof attackers. End-to-End delay is measured from the time an application data packet is sent from the source TCP layer to the time it is completely received by the TCP layer in the destination node.

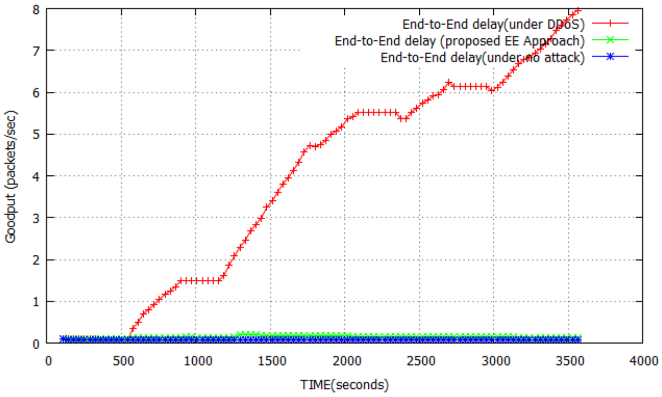

Figure 13. End -to- End delay for legitimate clients

The delay is calculated for the requesters approved as legitimate clients. Figure 13 shows less delay for the legitimate clients who reach the maximum trust credit points and it also resembles the network with no attack. As the number of hops varies on internet, the delay is computed based on the distance from the legitimate source and the target DC. For this reason, we configured DC load balancer to route the requests based on closest DC. Load balancing policy improves performance in terms of delay.

6.1 Profit Analysis

The cost is computed based on the data transmission and memory resident operations at each DC, based on an average sample that is combination of attack traffic and legitimate traffic.

Let N = Time in hours; $Cost_{BW}$ = Bandwidth cost; $Cost_{MEM}$ = RAM cost of each physical equipment; $Cost_{VM}$ = VM cost of each physical equipment, and $Cost_{DS}$ = Data stored within DC. Then the

$$TotalCost\ incurredaDC$$

$$= \sum_{i=1}^{N} \{Cost_{BW} + Cost_{MEM} + Cost_{VM} + Cost_{DS}\} \quad (8)$$

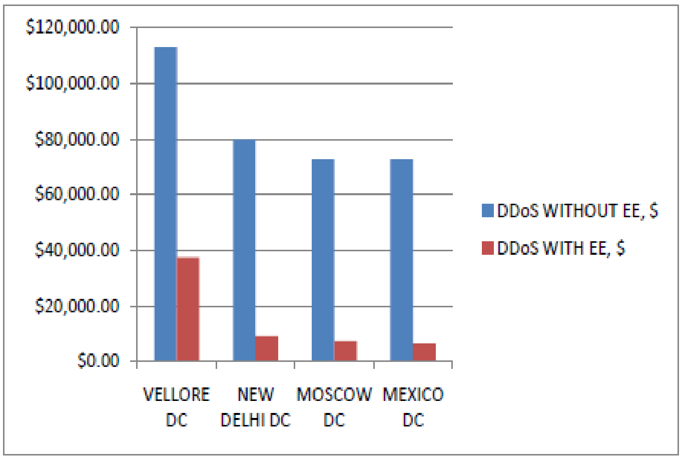

Figure 14. Profit Analysis

Figure 14 that huge cost incurred at Asia DC as it is the victim. This top level result shows that EE approach behaves better in detecting DDoS attacks with efficiently improving revenue. The costs used are 0.1($/Gb) for any data transmission at DC and 0.05($/sec) for any memory resident operations at DC. The extreme difference in profit is due to detection of attacker at their initiation and preventing their subsequent entry towards DC. This paves the way to improve availability with an acceptable response time shown in figure 5 (a), (b) and (c).

In addition to the improved detection efficacy, other benefits have been observed that would improve the choice of deployment.

Enhanced Entropy Strategy – Usually Entropy approaches detects the change in random incoming traffic, but proper enhancements to the entropy approach helps in improving the detection accuracy and to consider other overload condition for detection.

Dynamic traffic prediction – Usage of two buffers (Trial, Monitor) for measuring the Hellinger Distance and threshold helps in logging the recent traffic packets. So, at any point of time, current traffic condition is predicted. This dynamism improves detection accuracy.

Traffic diminution towards DataCenter – Different levels of detection identifies the attack sources and they are outwitted at that particular level of detection. So, only the validated packets are passed onto the next level which eventually reduces the huge traffic reaching DC.

Non-indulgent detection – Probing the packets irrespective of legitimates until they completely bypass all the levels to earn trust credit points. This strict detection highlights the characteristics of aggressive legitimates and outwitted on detection.

Improved Goodput – Measuring the DC's Goodput rather than throughput provides a meaningful result rather measuring throughput. As the attackers are outwitted at each level of detection, number of legitimates reaching DC increases which directly improves Goodput.

7. Conclusion

Proposed Enhanced Entropy approach determines the network condition and precisely detects the cause of overload. The enhancements helps in classifying the attack threats and legitimates and an additional trust mechanism helps us to serve even better for legitimates. Achieving better protection mechanism using Enhance Entropy approach instead of mirror servers saves huge cost (data processing, bandwidth, hardware and software). Simulation results prove the better response time and reduced traffic. Profit analysis shows the efficient resources utilization and allocation for the intended legitimate clients and protects the resources against overload conditions. Since all kinds of overload conditions thoroughly analyze the probability of threat entry is far less which directly reduces bandwidth traffic. Attackers' detection and prevention leads to protection of bandwidth and memory resources which improves profit revenue proportionately.

Future work would be to improve the detection efficacy related to DNS and related spoof threats. Improvement of detection efficacy is in terms of scrutinizing the proposed scheme with several other entropy models. Notion to future work is to strictly restricting the bandwidth attack threats then it is almost impossible to launch memory resource attack towards DCs of cloud computing environment.

References

[1] Zaihong Zhou, Dongqing Xie and Wei Xiong, " A Novel Distributed Detection Scheme against DDoS Attack", Journal of Networks, Vol. 4, No. 9, November 2009, pp. 921-928.

[2] S.Prabha, R. Anitha, "Mitigation of Application Traffic DDoS Attacks with Trust and AM Based HMM Models", International Journal of Computer Applications (0975– 8887), Volume 6, No.9, September 2010, pp.26-34.

[3] Kuochen Wang, Chun-Ying Huang, Shang-Jyh Lin, Ying-Dar Lin, “A fuzzy pattern-based filtering algorithm for botnet detection”, Computer Networks, Volume-55, 2011, pp. 3275–3286.

[4] http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf (accessed on 11 September 2012).

[5] http://www.brighthub.com/environment/green-computing/articles/100322.aspx (accessed on 11 September 2012).

[6] T. Liu, Z. Wang, H. Wang, K. Lu, “An Entropy-based Method for Attack Detection in Large Scale Network”, International Journal of Computer Communication, Vol.7, No. 3,2012, pp. 509-517.

[7] Shui Yu, Member, Wanlei Zhou, Robin Doss, Information Theory Based Detection Against Network Behavior Mimicking DDoS Attacks, IEEE Communications Letters, Vol. 12, No. 4, 2008, pp.319-321

[8] Ying Xuan, Incheol Shin, My T. Thai,Taieb Znati, “Detecting Application Denial-of-Service Attacks: A Group-Testing-Based Approach”, IEEE Transactions On Parallel And Distributed Systems, Vol. 21, No. 8, August 2010, pp.1203 – 1216.

[9] Giseop No, Ilkyeun Ra, “An Efficient and Reliable DDoS Attack Detection Using Fast Entropy Computation Method”, IEEE ISCIT, 2009, pp. 1223-1228.

[10] P. Varalakshmi, S. Thamarai Selvi, “Thwarting DDoS attacks in grid using information divergence”, Future Generation Computer Systems, Available online 18 Nov 2011, ISSN 0167-739X, 10.1016/j.future. 2011.10. 012.

[11] Ping Du, Akihiro Nakao, “OverCourt: DDoS mitigation through credit-based traffic segregation and path migration”, Computer Communications, Volume 33, Issue 18, 15 December 2010, pp. 2164-2175.

[12] Palvinder Singh Mann, Dinesh Kumar, “Improving Network Performance and mitigate DDoS attacks using Analytical Approach under Collaborative Software as a Service (SaaS) Cloud Computing Environment”, IJCST Vol. 2, Issue 1, March 2011, pp.119-122.

[13] Palvinder Singh Mann, Dinesh Kumar, “A Reactive Defense Mechanism based on an Analytical Approach to Mitigate DDoS Attacks and Improve Network Performance”, International Journal of Computer Applications, Volume 12, No.12, January 2011,pp. 975 – 987.

[14] Suratose Tritilanunt, Suphannee Sivakorn, Choochern Juengjincharoen, Ausanee Siripornpisan, “Entropy-based Input-Output Traffic Mode Detection Scheme for DoS/DDoS Attacks”, IEEE ISCIT 2010. pp. 804 – 809.

[15] N. Jeyanthi, N. Ch. Sriman Narayana Iyengar, “An Entropy Based Approach to Detect and Distinguish DDoS Attacks from Flash Crowds in VoIP Networks”, International Journal of Network Security, Vol.14, No.5, 2012, pp.257-269

[16] Sengar, H., "Overloading vulnerability of VoIP networks", IEEE/IFIP International Conference on Dependable Systems & Networks, June 29 2009-July 2 2009, pp.419-428.

[17] http://www.gigenetcloud.com/ddos_software_vs_hardware.html (accessed on 11 September 2012).

[18] J. Jung, B. Krishnamurthy, and M. Rabinovich, “Flash crowds and denial of service attacks: Characterization and implications for CDNs and web sites”, WWW '02 Proceedings of the 11th international conference on World Wide Web, ACM, 2002, pp.293-304.

[19] A. Moses, “The Aussie Who Blitzed Visa,” MasterCard and PayPal with the Low Orbit Ion Cannon, December 9, 2010; http://www.smh.com.au/ technology/ security/the-aussie-who-blitzed-visa-mastercard-and-paypal-with-the-low-orbit-ion-cannon-20101209-18qr1.html (accessed on May 2012).

[20] Jin Wang, Xiaolong Yang, Keping Long, "A new relative entropy based app-DDoS detection method," iscc, In the Proceedings of The IEEE symposium on Computers and Communications, Riccione, Italy 2010, pp.966- 968.

[21] Hemant Sengar, Duminda Wijesekera, Sushil Jajodia, “Detecting VoIP Floods Using the Hellinger Distance”, IEEE Transactions on Parallel and Distributed Systems, vol. 19, No.. 6, JUNE 2008, 794-805.

[22] Jin Tang; Yu Cheng; Chi Zhou, "Sketch-Based SIP Flooding Detection Using Hellinger Distance", IEEE Global Telecommunications Conference, pp.1-6, Nov. 30 2009 - Dec. 4 2009.

[23] http://www.opnet.com/news/press_releases/pr-2010/ OPNET-Introduces-Cloud-Readiness-Service-pr.html (accessed on 17 July 2012).

[24] http://www.opnet.com./services/brochures/OPNET_CloudReadiness.pdf (accessed on 17 July 2012).

[25] Qwasmi, N.; Ahmed, F.; Liscano, R., “Simulation of DDoS Attacks On P2P Networks”, IEEE 13th International Conference on High Performance Computing and Communications (HPCC), 2011, pp. 610-614.

[26] Jha, R.K; Dalal, U.D, “On demand cloud computing performance analysis with low cost for QoS application”, International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT), 2011, pp. 268-271.

[27] Rakesh Kumar Jha, Upena D Dalal, “A performance Comparison with cost for QoS Application in On-Demand Cloud Computing”, IEEE Recent Advances in Intelligent Computational Systems (RAICS), 2011, pp. 11- 18.

[28] N.Jeyanthi, N.Ch.S.N. Iyengar, “MAC Based Routing Table Approach to Detect and Prevent DDoS Attacks and Flash Crowds in VoIP Networks”, Cybernetics and Information Technologies, Vol.11, No.4, 2011, pp.41-52.

[29] N.Jeyanthi, N.Ch.S.N. Iyengar, “Packet Resonance Strategy: A Spoof Attack Detection and Prevention Mechanism in Cloud Computing Environment”, International Journal of Communication Networks and Information Security, Vol.4, No.3,pp.163-173.