An Entropy Based Approach to Detect and Distinguish DDoS Attacks from Flash Crowds in VoIP Networks

N. Jeyanthi[1] and N. Ch. Sriman Narayana Iyengar[2]

(Corresponding author: N. Jeyanthi)

School of Information Technology and Engineering, VIT University[1]
Vellore,Tamilnadu - 632014, India
School of Computing Science and Engineering, VIT University[2]
(Email: njeyanthi@vit.ac.in)

(Received July 5, 2011; revised and accepted Oct. 5, 2011)

Abstract

Voice over IP (VoIP) is a facility of providing voice services in accordance with IP (Internet Protocol) which provides better QoS (Quality of Service) than Public Switched Telephone Network (PSTN) at comparatively less cost.. Since Internet suffers from various threats, VoIP, which uses IP for servicing the Clients also results in stepping down QoS. One of the major QoS threats is Server Availability. Attackers defeat the server processing capability and gain control over the server by flooding lot of messages or requests and make server resources unavailable to the genuine user, resulting in DDoS (Distributed Denial of Service). But the server must predict the legitimate flood namely Flash crowd and malicious attack flooding usually DDoS. Both DDoS and Flash crowd creates abnormal traffic condition, but in order to improve Goodput, the server must be deployed with the mechanism that should classify legitimate and malicious call requests. This paper observes the traffic condition and the purpose of dealings varies which helps in outwitting the attackers. We also use the entropy packet analysis to minimize the traffic reaching the server. NS2 (Network Simulator 2) with SIP (Session Initiation Protocol) is ued to experiment and analyze the proposed work.

Keywords: DDoS, entropy, flash crowd, IP network, SIP, VoIP

1 Introduction

Internet is vulnerable to a variety of attacks, in which the most prominent attack is Distributed Denial-of-Service (DDoS), a serious threat to availability.. VoIP, which transmits multimedia data via Internet Protocol, suffers from the threats that arefaced by IP. Configuring the server to prevent the overload will degrade performance, because the overload could be caused by flash crowd (legitimate traffic). Hence the server should be implemented with a mechanism to differentiate DDoS attacks from flash crowd so that it can serve legitimate users and can deny attacker request resulting in performance improvement.

DDoS attacks are malicious requests that need not be handled by a server. At the same time, flash crowd consist of legitimate requests, where the server has the responsibility to handle as many requests as possible during a flash event. By doing so, the server can increase its overall performance on the Web resulting in possible additional revenue. If a DDoS attack occurs during a flash event, server should aim to ignore DDoS requests and handle the legitimate requests. This requires the SIP proxy server to be able to distinguish between the two sets of requests.

SIP INVITE, call setup, requests take time to complete its processing. SIP Proxy transaction is maintained by the proxy server during the complete call setup period. The following scenarios may cause abnormal traffic at SIP proxy server:

- A sudden increase in large number of legitimate INVITE requests creating a flash crowd event.
- An attacker populating the SIP Proxy server with malicious request.
- An INVITE request from an attacker who spoofs the legitimate users and trying to access Proxy server.
- Compromising huge number of legitimate hosts by loading the link bandwidth with malicious requests that remain in waiting state and unprocessed state.

Common types of VoIP attacks are described in [16]. DDoS attack is a method used by the attackers who distributed over the network for attacking the target machine by populating the server with malicious requests, whereas

Flashcrowds are legitimate requests that reach the server from large number of legitimate users simultaneously for a small period of time.

The rest of this paper is organized as follows: section 2 reviews the related work of our research, section 3 describes an overview of the proposed approach, section 4 presents the preliminaries of the work, section 5 provides details on experimental simulation setup, section 6 validates proposed approach and section 7 concludes the paper.

2 Related Work

INVITE requests are the requests which acquire certain amount of memory in the server. When these requests are flooded by attackers located in a distributed network, the server's memory resources exhausts quicker and the server becomes unavailable. Table 1 compares the behavior of the network under Flooding Attack and Flash Crowds.

Table 1: Comparison between bandwidth attacks and flash crowds

Influencing Factors	**Flooding Attack**	**Flash Crowd**
Network impact	Congested	Congested
Server impact	Overloaded	Overloaded
Traffic	Malicious	Genuine
Response to traffic control	Unresponsive	Responsive
Traffic type	Any	Mostly web
Number of flows	Any	Large number of flows
Predictability	Unpredictable	Mostly predictable

Fast detection and differentiation between the attackers and legitimate users is necessary to provide better QoS exclusively for time sensitive services such as IP Telephony. Further, the study of web traffic patterns by Jung *et al.* [9], shows that relying on IP addresses is not foolproof because an attacker can launch a DoS attack from a single location using spoofed IP addresses or may also use a network of zombies with real IP addresses.

Methods like Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA), proposed by Kandula *et al.* [10] assumed that human users can identify the distorted images, but the machines can not. Only users who could solve the puzzles get access to the services, will scare away many true users. However, in comparison to web browsers, telephones range from low-end limited functionality IP phones (possibly without any display) to more powerful modern PCs. Therefore, they did not provide effective solutions. Further, in the telephony world, asking for the active involvement of callers to solve audio or image-based puzzles is not an intuitive solution.

The various overloading defense mechanisms or approaches like traceback [11, 20, 25], pushback [6], and Pi [29] etc., require some modifications in the core of the Internet. However, Internet Service Providers (ISPs) are reluctant to install the proposed modifications without some extremely compelling reasons or incentives. Hence, these mechanisms have a limited or very little chance of real-world use.

There are many IETF working drafts [5, 19] proposing overloading indicators to upstream elements by introducing new headers. However, these methods are more suitable among trusted core network elements.

Detection of Hybrid Packet Floods using VoIP Flooding Detection System was proposed by Hemant Sengar *et al.* [22]. It tracks the relationships among VoIP packet streams, and raises an alarm for the observed significant deviations, which alert an onset of a flooding attack. Hellinger Distance (HD) gives an inherent way of estimating the distances between probability measures independent of the parameters. An alarm will be raised if the measured value exceeds a threshold.

Impressing features of HD among other distance measures are,

- Not computationally intensive.
- Has a natural lower and upper bounds of 0 and 1.
- Based on the proportion of the protocol attributes.

They proved by experiment that high detection accuracy with a short detection time, while introducing no perceivable delay, to call setup times utilized by a host of SIP-controlled VoIP protocols. Normal traffic behaviors also change with time. So, dynamic threshold is used to trace the normal traffic behaviors, which will make an attack harder to evade.

Secure transmission can be designed by Marking and Filtering schemes [13]. In marking scheme, each packet which arrives at router will have a genuine marking in it to detect whether the packets arrive from an original source IP address or spoofed IP address. After packet verification, the random key is generated. Then this random key will be encrypted using existing encryption mechanisms like Symmetric Cryptography like DES, AES or Asymmetric Cryptography like RSA, ECC etc. Then server will send the encrypted marking to the client. From now onwards both client and server will communicate with each other using the encrypted marking. In Filtering Scheme: The EMDAF scheme employs a firewall at each of the perimeter routers of the network. This firewall scans the marking field of all incoming packets to selectively filter-out the attack packets. When a packet arrives at its destination, its marking depends only on the path it has traversed. If the source IP address of a packet is spoofed, this packet must have a marking that is different from that of a genuine packet coming from the same address. The spoofed packets can thus be easily identified and dropped by the filter, while the legitimate packets containing the correct markings are accepted and the packet IP address and its encrypted marking is updated in the filter table. Now in the further secure transactions the encrypted marking is verified. If the marking received by server for an existing IP address in the filter table is same then it will be accepted else it will be dropped, which still increases the overhead and packet loss.

An Advanced Entropy-Based DDoS Detection Scheme [28], proposed a DoS attack detection mechanism. This method also distinguishes Flash crowds from legitimate users. But this approach could detect only Low-rate DoS attacks.

In this paper, our main focus is on overloading conditions due to numerous SIP end points distributed over the Internet. In academia there are many efforts [14, 22] to detect and protect VoIP networks from DDoS attacks, while flash crowds still remain overlooked. Further, if we closely look at the IP telephony service, we find that real-time and essential nature of the telephony service makes it different from other regular Internet-based services. Consequently, the most popular and largely deployed overloading protection mechanisms such as request rate throttling, random dropping of requests, and black holing are not appropriate for IP telephony services. Operating under these practical requirements of the IP telephony service and still be able to detect and distinguish all aspects of an INVITE surge that differs in intent only is not a trivial task and obviously sets an ambitious goal.

3 Overview of Approach

Three main phases of our approach are Traffic Analysis, Detection and Classification as in Figure 1, followed by the Pseudo code.

Traffic Analysis:

- Calculate the normal behavior of the network without any attack.
- Continuous monitor for the presence of overload.
- If there exists any deviation in normal behavior, overload must be detected.

Detection:

- Overload detection mechanism used here is Entropy based approach.
- When any overload condition is intimated, Entropy approach calculates the current traffic behavior.
- On comparing the current traffic behavior with normal behavior, we detect the number of attack packets.

Classification:

- We use **Hellinger Distance** to define threshold value, which can be computed by observing normal traffic behavior.
- With an **INVITE surge alert**, **Flash Event** is identified if the protocol behavior distance remains lower than that of the threshold value.
- With an **INVITE surge alarm**, **DDoS attack** is identified if the protocol behavior distance crosses the threshold value.
- We show that DDoS attacks and flash crowds, while similar in the number of INVITEs and message structure, exhibit different traffic patterns.
- The **entropy** measurement of call durations gives an important clue to distinguish between humans and zombies call behavior.

PSEUDOCODE:

```
Continuously sense/monitor the incoming traffic
signal
    Calculate normal behavior with devoid of
    attacks
    Initial traffic is training phase
    Consequent incoming traffic is observing
    phase
Difference between the phases predicts Hellinger
Distance
    Calculate mean and Variance
    Calculate threshold by chebyshev's
    inequality
    IF (packet queuing exists)
    Alarm "Abnormal traffic behavior"
      IF (Abnormal traffic behavior found)
      Calculate Hellinger Distance
        IF (HD¡Threshold)
        Alarm "Flash crowd"
        IF(HD¿Threshold)
        Alarm "DDoS"
ELSE
Alarm "Normal traffic (no overload/packet
queuing)"
```

The initiated traffic is analyzed before being approved by the SIP Proxy Server, Network overload is detected to calculate the traffic value, based on which an alarm is initiated. The detailed designing of our approach is shown in Figure 2.

4 Preliminaries

In the application layer, Session Initiation Protocol (SIP) is the signaling Protocol [18], which enables the communication with the Request methods followed by its Responses as shown in Figure 3.

4.1 SIP Normal Operational Model

SIP is a transactional protocol, in which each transaction consists of a Request. The list of SIP-Request methods

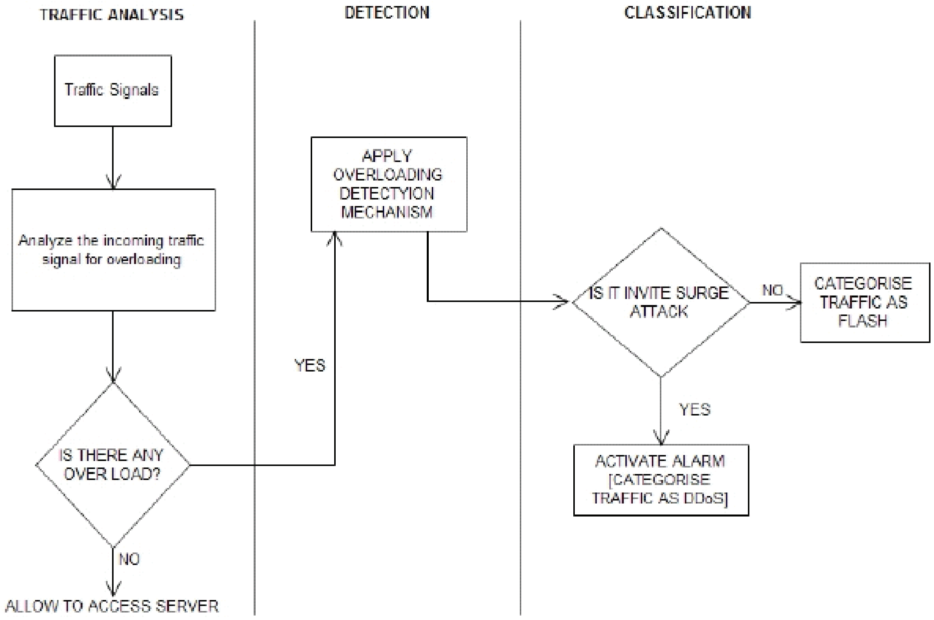

TRAFFIC ANALYSIS
DETECTION
CLASSIFICATION
Traffic Signals
Analyze the incoming traffic signal for overloading
IS THERE ANY OVER LOAD?
NO
ALLOW TO ACCESS SERVER
YES
APPLY OVERLOADING DETECTYION MECHANISM
IS IT INVITE SURGE ATTACK
NO
CATEGORISE TRAFFIC AS FLASH
YES
ACTIVATE ALARM [CATEGORISE TRAFFIC AS DDoS]

Figure 1: Overview of our approach

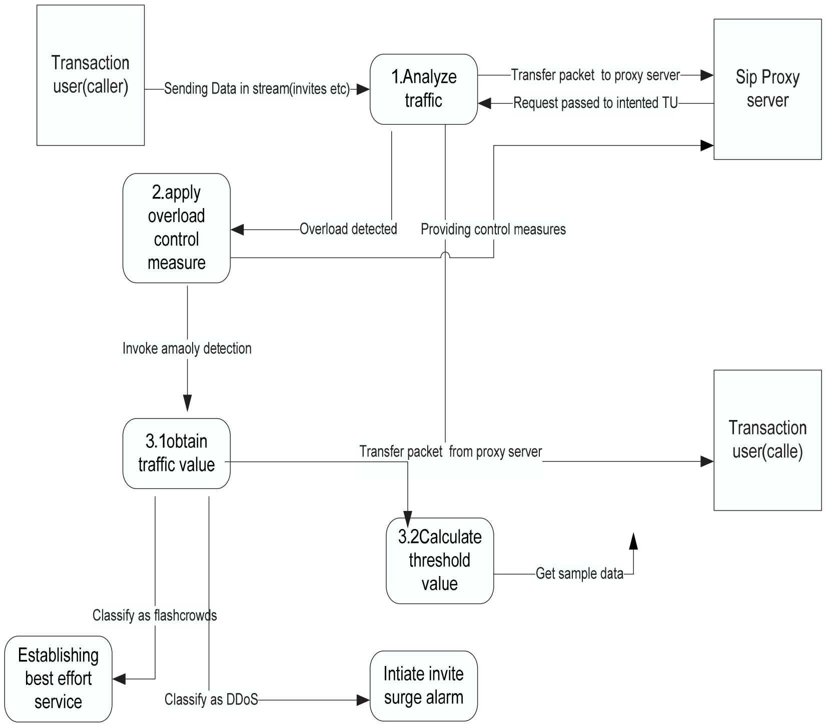

Transaction user(caller)
Sending Data in stream(invites etc)
1.Analyze traffic
Transfer packet to proxy server
Request passed to intented TU
Sip Proxy server
2.apply overload control measure
Overload detected
Providing control measures
Invoke amaoly detection
3.1obtain traffic value
Transfer packet from proxy server
Transaction user(calle)
3.2Calculate threshold value
Get sample data
Classify as flashcrowds
Establishing best effort service
Classify as DDoS
Intiate invite surge alarm

Figure 2: Detailed design of our approach

serve unique purpose as tabulated in Table 2. Its corresponding responses indicate the status of the end nodes shown in Table 3.

Table 2: SIP - Request method

Request Method	Purpose
INVITE	Initiate a Session
ACK	Confirm the final response to an INVITE
BYE	Terminate a session
CANCEL	Cancel searches and "ringing"
OPTIONS	Communicate features supported
REGISTER	Register a client with a location service

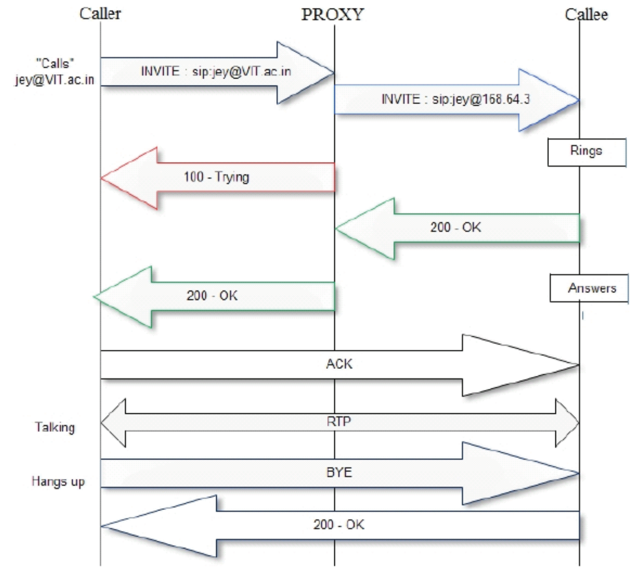


Figure 3: SIP operation

5 VoIP Traffic Behavior under Experiment

Extensive statistical analysis has been conducted to profile the normal behaviors of SIP protocol attributes in VoIP signalling traffic obtained from our realistic VoIP architecture. Here we define protocol attributes as the message types appearing in VoIP signalling traffic. For example, SIP's request and response messages such as INVITE, 200 OK, ACK and BYE etc. are considered as protocol attributes. In this section, we discuss the presence of an intrinsic association among protocol attributes at the application layer.

5.1 Experimental Setup

In order to study VoIP traffic behavior, we build an architecture consisting of a SIP proxy server and subscribers registered to that particular proxy server i.e., legitimate users. The architecture consists of 23 nodes equipped with connection as SIP UAs and SIP proxy server. There is no constraint on the number of nodes chosen. A router with wide area network emulator and an attacker with INVITE flood traffic generator are also part of this construction. Figure 4 shows the layout of the architecture used to spawn VoIP traffic and to assess the performance of proposed detection mechanisms. The talk time (i.e., call duration) between any two subscribers is exponentially distributed in which, packet delay distributions; congestion, loss, bandwidth limitation etc. are configurable. We set the Internet delay to 50 ms and the packet loss rate to 0.42% in our experiments. Our work is simulated in NS2 tool. The SIP proxy server can also built by SER (SIP Express Router [7]). The talk time (i.e., call duration) between any two subscribers is exponentially distributed with mean talk time of 120 seconds. The wide area network emulator ("NISTNet" [1]) connects enterprise networks and SIP server.

Our aim is to prove that our methodology shows higher level of resiliency for a remarkable period of time (before timeout trigger). This has been proved by taking two legitimate users per network for communication and four attackers located at remote site to destruct the server resources. We also tried to show that our method works efficiently and resiliently even if the attackers are equal to the legitimate users of that network.

Normally the number of DDoS attacker in a network may be several hundreds or sometimes thousands who joins to evade server quicker. Even if there exist more number of attackers who populates the packets with huge size can be detected by varying the Hellinger distance at ADS.

This methodology uses the ingrained reliability of SIP and improves stability of server which automatically improves the availability of server, especially the Goodput of server.

Reliability: The continuous transmission of SIP 200 OK responses and end-to-end ACK provides secure and inbuilt reliable communication among users

Stability: More the resiliency of server, more stable the server towards the attacker. This intern also provides more availability to its intended users. The availability of the server can be improved, since we could distinguish the spurious packet before they reach the server at ADS.

Conventions:

Proxy server: Node 5, 6 Victim Server: Node 5;

SIP UA: Node 7, 8, 19, 20 DDoS Attacker: Node 14, 15;

Table 3: SIP - Response method

Status-Code	Category	Example information
1xx	Informational	Trying, ringin g, call is being forwarded, queued
2xx	Success	OK
3xx	Redirection	Moved permanently, moved temporarily, etc
4xx	Client error	Bad request, unauthorized, not found, busy, etc
5xx	Server error	Server error, not implemented, bad gateway, etc
6xx	Global failure	Busy everywhere, does not exist anywhere, etc

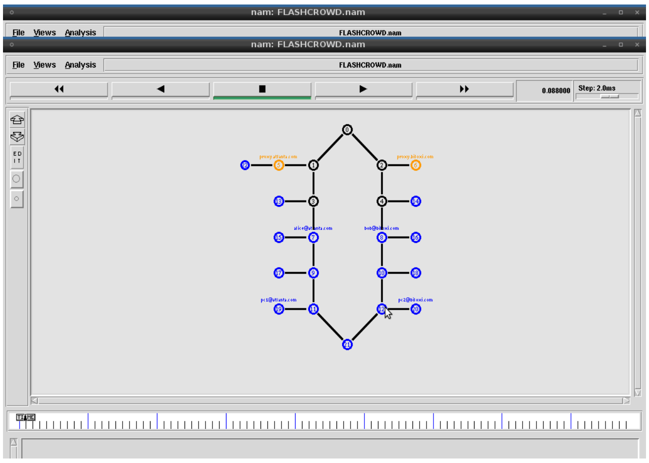
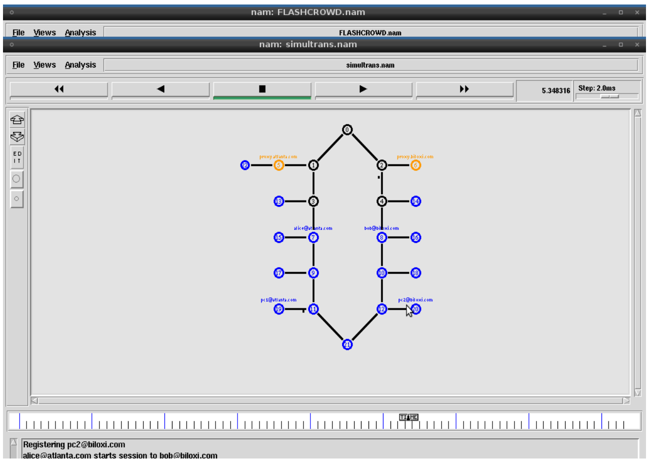


Figure 4: Architecture of VoIP network



Registering pc2@biloxi.com
alice@atlanta.com starts session to bob@biloxi.com

Figure 5: Normal behavior (Ideal traffic with NO overload)

Attack Packets: Red coloured Packets Legitimate Packets: Black coloured Packets;

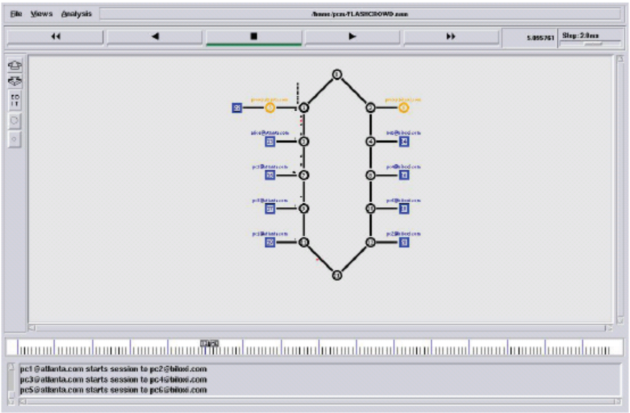
Dummy Destination: Node 22 - This is to redirect the attack packets reaching the server;

Routers: Node 0, 2, 3, 4, 9, 10, 11, 12, 21 ADS: Node 1.

Normal behavior: The normal SIP traffic behavior observed by the ADS near the SIP proxy server. ADS monitor both to-and-fro signaling traffic between subscribers and the SIP proxy server see in Figure 5. Therefore, end-to-end messages are seen twice by the ADS. SIP signalling messages are carried by UDP and UAs use the default T1 timer value of 500 ms. It should be noted that in this paper, the (200 OK) messages correspond to INVITEs only. Because of the Internet network conditions and processing delays at the server, the strict one-to-one relationship between INVITE and other call setup messages, such as (200 OK), ACK etc. are violated. However, under normal conditions these deviations from ideal behavior are small and exhibit strong positive correlations among call setup messages.

Behavior under flash crowd. SIP session establishment behavior under flash crowds is shown in Figure 6. In this period, the call setup messages demonstrate one-to-one relationship with occasional packet drops and retransmissions. In order to simulate a flash crowd event, at the starting of minute, additional INVITEs are introduced, bringing the overall call rate to flood server with legitimate request respectively. The SIP proxy server shows remarkable resiliency and tries to behave normally for the next couple of minutes (depending upon the severity of flash crowd as shown in Figure 6). As we know, a transaction state server keeps a copy of the received request for some time and a transaction context typically consumes 3Kbytes (depending on message type and memory management overhead) [23]. Therefore, after maintaining a certain number of transaction contexts, the SIP proxy server's performance degrades. At this transition point, the call throughput falls quickly and because of the resource exhaustion and processing delays, we observe a sudden jump in INVITE and (200 OK) retransmissions by the SIP UAs. The existing INVITE transactions in the server also start timing out (by sending out [408 Timeout] messages).

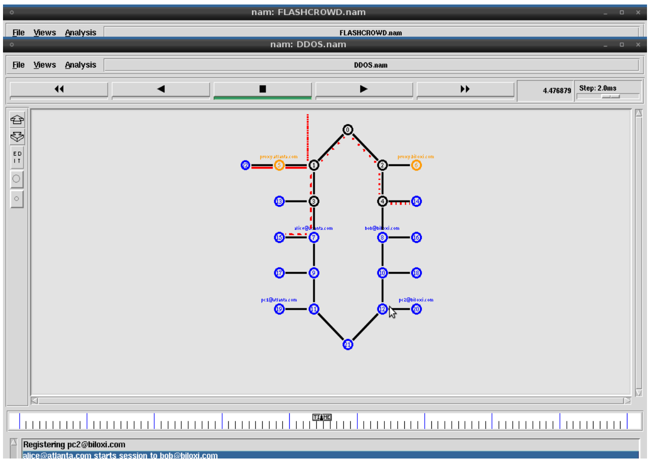
Behavior under INVITE flooding. Figure 10 plots the SIP session establishment behavior under DDoS attack. At the starting of tenth minute, the initial call rate is mixed with additional calls with spoofed source IP addresses. First, the SIP proxy server tries to behave nor-



pc1@atlanta.com starts session to pc2@biloxi.com
pc3@atlanta.com starts session to pc4@biloxi.com
pc5@atlanta.com starts session to pc6@biloxi.com

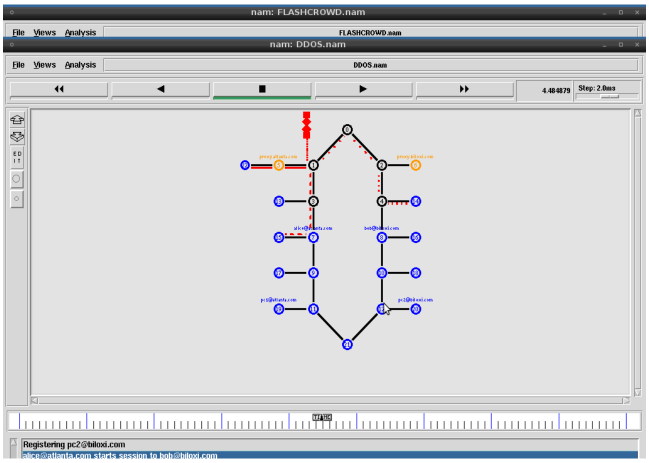
Figure 6: Flash crowd scenario (incoming legitimate traffic request are queued for further request processing)

mally by sending (100 Trying) messages for each of the received INVITE requests and by maintaining their transaction state. For each of the accepted spoofed INVITE requests, the SIP proxy server transmits seven INVITE messages towards the unreachable destination IP address before timing out the transaction state. Secondly, as the flooding rate increases, the major part of server resources are held up by the spoofed requests and these are made available for further reuse only when the transactions time out. At the exhaustion of server resources and due to processing delays, the number of (100 Trying) declines and a fraction of new INVITE requests is refused to be serviced by sending (500 Server Error) messages. Because of the timeouts (i.e., removal of existing transactions) and (500 Server Error) (i.e., refusal of accepting new transactions) messages, the proxy server tries to recover and accepts new requests, but due to unabated DDoS traffic, the server's performance degrades again, showing an oscillatory behavior of recovery and degradation.



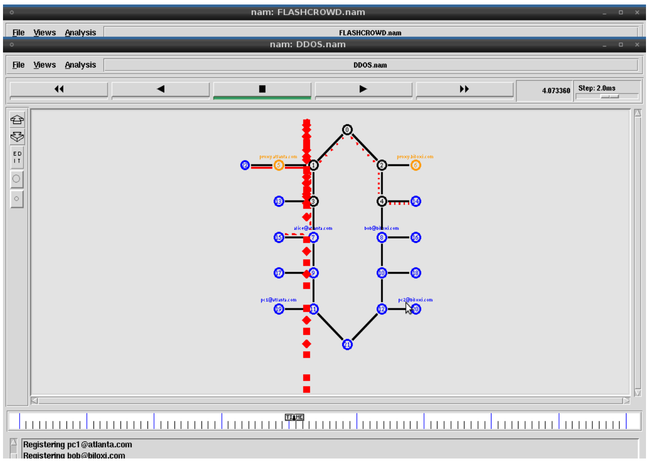
Registering pc2@biloxi.com
alice@atlanta.com starts session to bob@biloxi.com

Figure 7: Packets queued due to uncontrollable incoming attacks packets



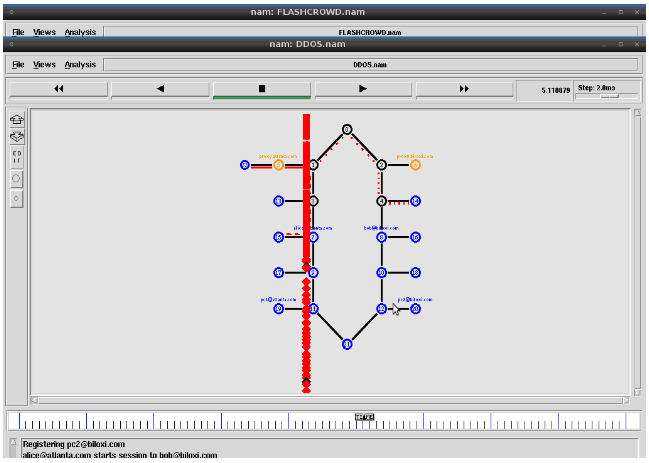
Registering pc2@biloxi.com
alice@atlanta.com starts session to bob@biloxi.com

Figure 8: Packet drop due to continuous overload (i.e,. exceeding the queue limit)



Registering pc1@atlanta.com
Registering bob@biloxi.com

Figure 9: Packet drop increases as the severity of traffic increases



Registering pc2@biloxi.com
alice@atlanta.com starts session to bob@biloxi.com

Figure 10: DDoS causes severe flooding at server (i.e., server resource unavailable even for legitimate users)

Server access is denied to BLACK legitimate packets due to the flooding of RED attack packets. Hence the legitimate packets are dropped because of its inability to access server as shown in the above diagram.

Difference between flash crowd and DDoS attack: The main difference between these two events is in the nature (i.e., intent) of INVITE requests that results in two different observable protocol behavior. Instead of analyzing INVITE requests in isolation, our approach studies call setup transactions (e.g., both INVITE and ACK) revealing many unique characteristics. For example,

1) In flash crowd, the proxy server tries to behave normally if the request arrivals remain unabated. After some time depending upon its severity level server's performance degrades, whereas in flooding attack it happens much quicker. The spoofed INVITE messages do not have corresponding (200 OK) and ACK messages and therefore server resources are exhausted much faster.

2) Because of the lockup of server resources (e.g., transactions are not completed), INVITE flooding attack is more harmful even at smaller rate compared to flash crowd.

3) In INVITE flooding attack, the lockup of server resources and its release (by rejecting new call requests and timing out existing transactions) cause an oscillatory behavior of recovery and degradation. Whereas, in flash crowd the call throughput falls to zero and remains same till the flash crowd subsides.

6 Overloading Detection Mechanism - Validation

Besides the presence of many detection methods, like Path Identification routing scheme and IP traceback, which helps only in detecting the location of attacker and blocking the incoming attack packets. But the location of an attacker changes for every instance of time. In addition to this, these schemes also have a serious disadvantage that these methods of detection uses network resources from server for tracking the attack packets which again creates network overload and overhead. These methods also make the server to spend its time to listen to these attack packets detection.

Instead of doing that, we create a profile for legitimate users in a private network where there exist no attack packets. After the profile creation, HELLINGER DISTANCE is used to compare with the incoming traffic. If there is any deviation from the normal behavior profile, we define the existence of traffic as either Flash Crowds or DDoS. As already mentioned that the locations of VoIP users are dynamic, it is almost wasting the resources in spending time on detecting the location of VoIP attackers.

Anomaly Detection Sensor (ADS) is placed very close to VoIP server. Hence, it's not necessary to worry about the time taken for comparing the incoming and normal traffic profile. The spurious packets could be identified by the ADS and acquire a differential treatment when these packets reaches the server.

ADS identifies anomalies in the stream of packet exhibiting a cyclic behavior in two different phases. In the training phase, the training data set consisting of the attribute set is collected over n sampling periods of duration_t (= 10 sec.) over normal traffic streams. This initial training data set is assumed to be devoid of any attacks and acts as a base for comparison with the next $(n+1)^{th}$ period of the testing data set. Using the Hellinger distance, the distance between these two data sets is measured. If this value exceeds a threshold, an alarm is raised, and if not the testing data set is incorporated in the imminent $(n-1)$ sampled traffic data to obtain a new set of training data. The dynamic nature of the network traffic is supported by the moving window mechanism.

Hellinger Distance:
Hellinger distance is defined by the way of measure theory Let P and Q denote two probability measures that are absolutely continuous with respect to a third probability measure. The square of the Hellinger distance between P and Q is defined as the quantity:

$$d_H^2(P,Q) = \frac{1}{2}(\sqrt{P_\alpha} - \sqrt{Q_\alpha})$$

The Hellinger distance $H(P,Q)$ satisfies the property: $0 \leq H(P,Q) \leq 1$ The maximum distance 1 is achieved when P assigns probability zero to every set to which Q assigns a positive probability, and vice versa. More information about HD is discussed in [3, 17].

Detection threshold and classification. The distribution of measured normal distances is used to calculate the mean μ and variance σ^2. Given these two parameters, we wish to determine the validity of the observed distance d in the testing period. To do so, we assume that the measured distance X is a random variable with mean $E(X) = \mu$ and variance $\sigma^2 = var(X)$. Then, the Chebyshev inequality,

$$\underline{\mathrm{P}}(|X-\mu| \geq t) \leq \frac{\sigma^2}{t^2}\text{for any } t > 0$$

can be used to compute an upper bound on the probability that some random variable X deviates from its mean by more than any positive value t, given only the mean and variance of X. We define a confidence band of $\mu \pm 8\sigma$ as a normal region, in which the proportion of observed distances falling in the region is at least 98.5%. Beyond this normal region, the observed distances are anomalous. Once, an anomalous protocol behavior is detected, the attack classification is done by correlating it with the INVITE surge alarm (discussed later).

Application of detection mechanism. To model security violations, out of all available attributes, we need only a fraction of specific attributes to represent a particular type of attack. To detect INVITE flooding and flash crowd, we choose four SIP protocol attributes of call setup phase, namely INVITE, (100 Trying), (200 OK), and ACK. In the case of authenticated call setup, we can select challenge/response messages as well. Here, the probability measure P is an array of normalized frequencies of pINVITE, p100 Trying, p200 OK, and pACK (i.e., $p\alpha = N\alpha/NTotal$ where α [INVITE, 100 Trying, 200 OK, AC] and NTotal = (NINVITE + N100 Trying + N200 OK + NACK)) over the training data set assuming that we observe NINVITE, N100 Trying, N200 OK and NACK packets in $n \triangle t$ time period. Similarly, during the testing period (i.e., at the $(n+1)^{th}$ sampling duration), Q is an array of normalized frequencies of qINVITE, q100 Trying, q200 OK and qACK. To calculate the HD between P and Q at the end of $(n+1)^{th}$ sampling period, we use $d2H(P,Q)$ formula. Figure 10 shows the HD plot for normal behavior of SIP protocol attribute set. The maximum observed distance is 0 as there is no overload and most of the time the HD shows remarkable closeness between the observed and training data sets. The occasional peaks in the plot overlapped the period where the traffic rate is very low and even a few packet drops and retransmissions result into spikes. At higher rate, the dropping or retransmissions of few packets are masked and do not cause any significant observable deviation. Figure 12 is plotted under flash crowd event. The initial 6 minutes show a normal behavior and at the start of 6th minute, a flash crowd of call requests. We observe that toward the end of 6.33th minute, the distance starts climbing and reaches a maximum of 0.045 at 6.33th minute. In Figure 13, at the start of 3.1th minute spoofed INVITE requests are mixed with the normal requests; consequently, in the very next observation period the distance jumps to 0.128 and then increases to the maximum of 0.135 at the 3.4th minute.

Distinguishing flash crowds from DDoS attacks. By correlating INVITE surge alert (i.e., when the number of calls exceeds the maximum safe limit defined for the server) and anomalous protocol behavior alert, we can distinguish flash crowds from DDoS attacks. As with an INVITE surge alert, if the protocol behavior distance remains lower than the threshold value of $(\mu + 8 \times \sigma = 1.841 \times 10^{-3} + 8 \times (5.40 \times 10^{-3}) \approx 44 \times 10^{-3})$ then it is a flash crowd event. Whereas, in DDoS attack, the protocol behavior distance crosses the threshold value along with an INVITE surge alarm.

The proper setting of threshold value at 10^{-3} achieves three goals: (1) it accommodates both normal peak hour call rate and also night time off-peak hour call rate; (2) it allows the detection of low-rate flooding attacks; and finally, (3) it reduces the possibility of false alarms due to adverse network conditions.

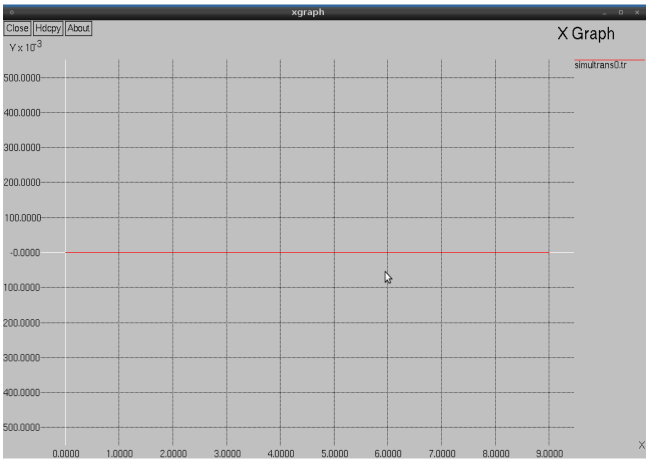


Figure 11: Ideal normal traffic behavior with no overload (i.e., no queuing of packets and no packet drop - initial training phase) x-axis: time y-axis: Hellinger distance

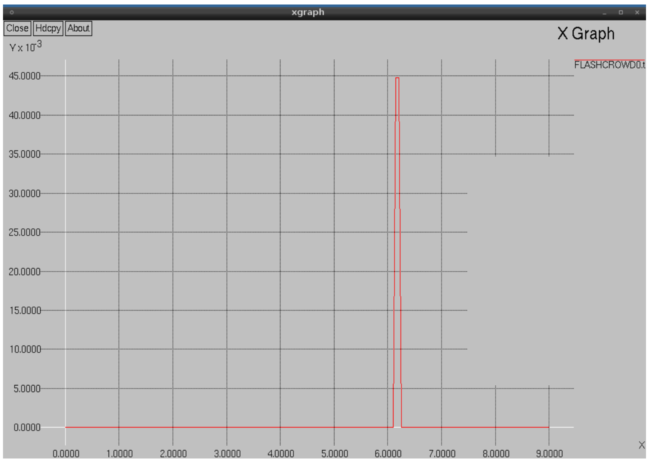


Figure 12: Flash crowd behavior (i.e., HD lies under threshold)

Entropy Classifier. Among the several existing classification methods, entropy classification precisely identifies and records the changes that are deviating from normal behavior. The entropy classifier component makes the attack classification decision based on entropy measurement of call durations, irrespective of whether it is a regular 2-party call or answered by a voice mail system. The call durations are binned into N contiguous bins (of varying lengths). We can interpret the bins as the states xi of discrete random variable X, where $p(X = x_i) = p_i$ [27]. The entropy of the random variable X is then

$$H[P] = -\sum p(x_i) \ln p(X_i).$$

Distributions $p(x_i)$ that are sharply peaked around a

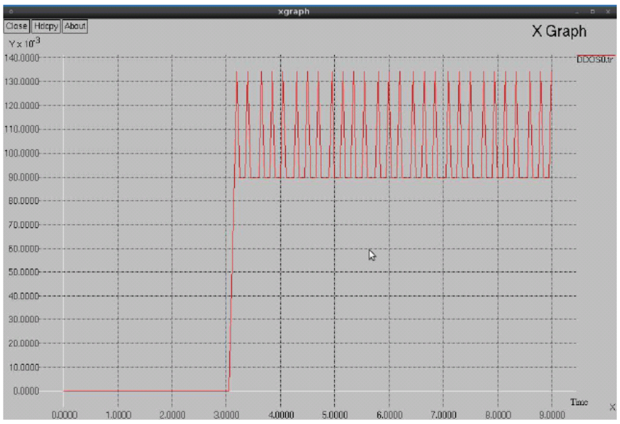


Figure 13: DDoS behavior (i.e., HD exceeds threshold)

few bins will have relatively low entropy, whereas those that are spread more evenly across many bins will have higher entropy. For example, if the entropy is low for our selected attribute of call duration then it indicates predictable patterns of the abnormal call behavior. It could be due to short call durations are skewed toward few selected lower-side bins or may be constant call durations have filled up one particular bin. However, if the measured entropy is high (i.e., call durations are distributed across bins), it indicates the irregular or unpredictable behavior of human conversations. The call logs used in entropy profile creation were collected from VoIP networks. The spoofed attack can be avoided by SIP inbuilt reliability mechanism because the (100 Trying) message in the attribute set is the only per-hop message among other end-to-end messages. It is generated by a stateful proxy server that we want to protect. It leaves an attacker to play with ACK messages only. However, an ACK without valid To tag (sent within 200 OK response) results in (481 Transaction Does Not Exist) error message making such an attack easier to detect.

The covariance analysis model detects the attack on a statistics-based method [2], but the attacker will not be static and will not use the same IP address always. Different detection mechanisms were discussed by several authors [2, 12, 30].

7 Conclusion

This paper analyzes the DDoS and Flash crowds characteristics and proposes a new entropy based DDoS and Flash crowds distinguishing method in VoIP network. We validate our method by simulation, and the results suggest that our method can be used to detect Flash crowds and DDoS attacks on VoIP call processing servers.

Figure 14 shows the simulation of flashcrowd and packets queued for requesting service to the server, which appears to be high only for a short period of time whereas Figure 14 shows the simulation of DDoS and packet queued at server which appears to be more all the time as the DDoS attacker aim is to defeat the SIP proxy server.

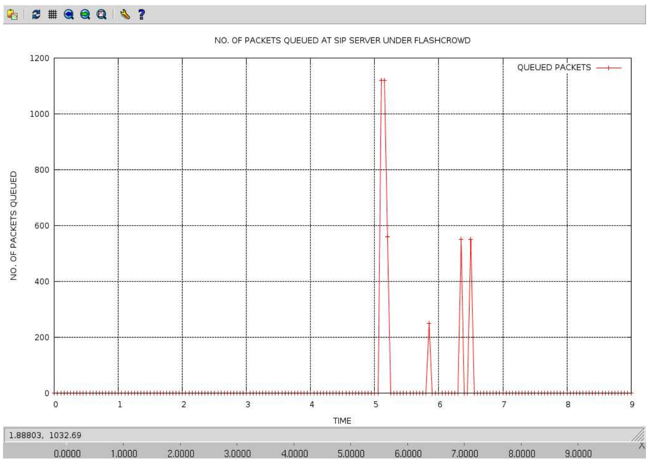


Figure 14: Number of packets queued at SIP server under flashcrowd

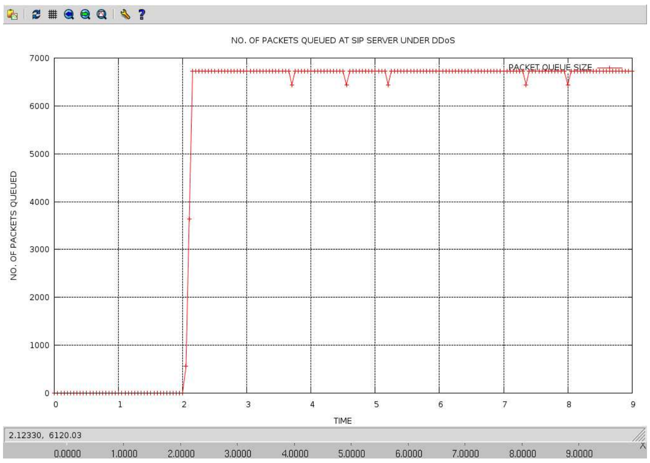


Figure 15: Number of packets queued at SIP server under DDoS

This paper validates the usefulness of the entropy based DDoS and Flash crowds distinguishing method. In this approach we are able to distinguish the normal and abnormal protocol behavior which alarms when server suffers any overload.

Figure 15 shows the simulation of flash crowds and the bandwidth utilised by legitimate users at surge, here the bandwidth affected but periodically comes down to normal when users are not interacting with server. The QoS Parameters of the traffic pattern varies under Normal traffic, during a Flash Event and DDoS attacks as seen in Table 4.

Figure 17 shows the simulation of DDoS and the bandwidth utilised by the attack packets, this keeps oscillating continuously because the resources are accommodated by

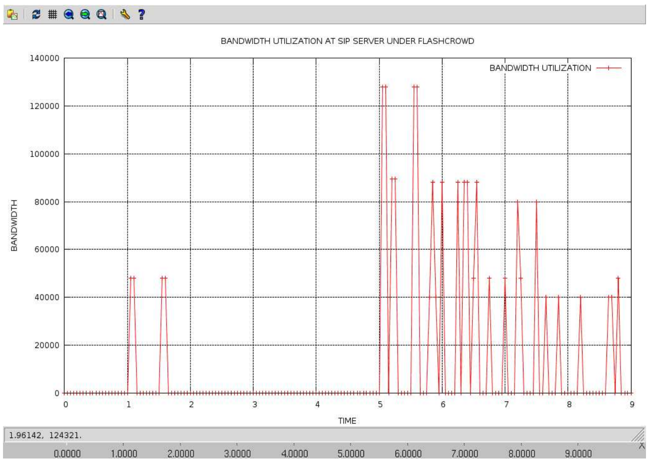


Figure 16: Bandwidth utilization at SIP server under flashcrowd

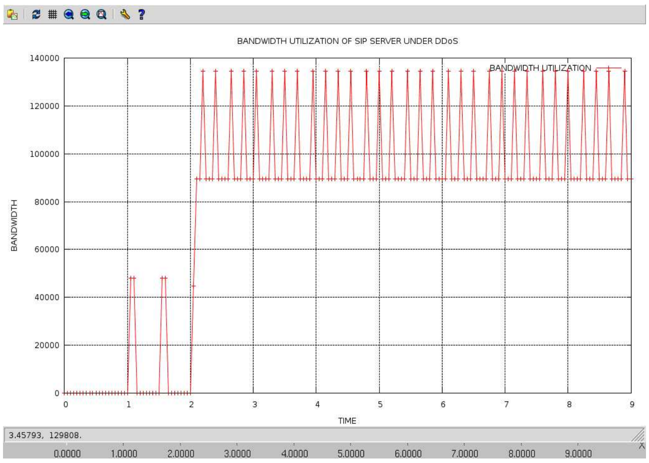


Figure 17: Bandwidth utilization at SIP server under DDoS

attack packets and then flushed because of time out condition.

So our future work is to give differential treatment (i.e.,) to serve legal users and prevent DDoS attacker's intrusion into the VoIP network which improves Goodput and availability of a SIP proxy server.

References

[1] M. Carson and D. Santay, *NIST Net Network Emulation Package*, June 1998. (http://snad.ncsl.nist.gov/itg/nistnet/)

[2] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai,"Denial-of-Service Attack-Detection Techniques," *IEEE Internet Computing*, pp. 82-89, 2006.

[3] M. Fannes and P. Spincemaille, "The mutual affinity of random measures," *eprint arXiv:math-ph/0112034*, Dec. 2001.

[4] B. B. Gupta1, R. C. Joshi, and M. Misra, "ANN Based Scheme to Predict Number of Zombies in a DDoS Attack," *International Journal of Network Security*, vol.13, no.3, pp. 216-225, Nov. 2011.

[5] V. Hilt, I. Widjaja, D. Malas, and H. Schulzrinne, *Session Initiation Protocol (SIP) Overload Control,* Work in Progress, SIPPING Working Group, 2008.

[6] J. Ioannidis, and S. M. Bellovin, *Implementing Pushback: Router-Based Defense Against DDoS Attacks,* NDSS, 2002.

[7] IPTEL. SIP Express Router. SIP Proxy Server. (http://www.iptel.org/ser/)

[8] S. Jin, and D. S. Yeung, "A Covariance Analysis Model for DDoS Attack Detection," *IEEE communications society*, 2004.

[9] J. Jung, B. Krishnamurthy, and M. Rabinovich, "Flash crowds and denial of service attacks: Characterization and implications for CDNs and web sites," *Proceedings of the 11th international conference on World Wide Web New York*, pp. 293-304, NY, USA, 2002.

[10] S. Kandula, D. Katabi, M. Jacob, and A. Berger, "Botz-4-Sale: Surviving organized DDoS attacks that mimic flash crowds," *2nd Symposium on Networked Systems Design & Implementation (NSDI) Boston*, pp. 287-300., MA, 2005.

[11] H. Lee and K. Park, "On the effectiveness of Probabilistic Packet Marking for IP traceback under denial of service attack," *Proceedings of Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 1, pp. 338-347, Anchorage, AK, USA, 2001.

[12] M. Li, Ming Li, and X. Jiang, "DDoS attacks detection model and its applications," *WSEAS Transctions on Computers*, vol. 7, pp. 1159-1168, 2008.

[13] M. Nagaratna, V. Kamakshi Prasad, and S. Tanuz Kumar, "Detecting and preventing IP-spoofed DDoS attacks by encrypted marking based detection and

Table 4: Observed QoS parameters under different traffic behaviors

QoS MEASURES	**BEHAVIOR BEHAVIOR**	**FLASH CROWD**	**DDoS**
THROUGHPUT	834 b/sec	2306 b/sec	64283 b/sec
BANDWIDTH UTILIZATION	120×10^3	190×10^3	760×10^3
SERVER MEMORY ACCOMODATION(Mb)	-	3.4×10^{-3}	25×10^{-3}
JITTER	-	-	Found
PACKET LOSS	0%	0%	50%
PACKET DELIVERY FRACTION	100% with no delay	100% LEGITIMATES WITH ACCEPTABLE DELAY ACCEPTABLE DELAY	84% ATTACKERS ARE CAUSE OF DELAY
HELLINGER DISTANCE	-	< THRESHOLD	> THRESHOLD

filtering (EMDAF)," *Proceedings of 2009 International Conference on Advances in Recent Technologies in Communication and Computing(Artcom)*, pp. 753-755, Oct. 27-28, Kottayam, Kerala, India, 2009.

[14] M. Nassar, R. State, and O. Festor, "Monitoring SIP traffic using support vector machines," *RAID*, LNCS 5230, pp. 311-330, Springer-Verlag, 2008.

[15] NuVox Communications, *Voice and Data Service Provider.* (http: //www.nuvox.com)

[16] T. Peng, C. Lechie, K. Rama, and M. Rao."Survey of network based defense mechanisms countering the DoS and DDoS problems," *ACM Computing Surveys*, vol. 39, no. 1, article 3, Apr. 2007.

[17] D. Pollard, Asymptopia. (http://www.stat.yale.edu/pollard/)

[18] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R.Sparks, M. Handley, and E. Schooler, *SIP: Session Initiation Protocol*, RFC 3261, IETF Network Working Group, 2002.

[19] J. Rosenberg, *Requirements for Management of Overload in the Session Initiation Protocol*, RFC 5390, SIPPING Working Group, 2006.

[20] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP traceback," *IEEE/ACM Transactions on Networking*, vol. 9, no. 3, pp 226-237, June 2001.

[21] H. Sengar, H. Wang, D. Wijesekera, and S. Jajodia, "Fast detection of denial-of-service attacks on IP telephony," *Proceedings of 14th Internal National Work Shop on Quality of Service*, pp. 199-208, New Haven, CT, 19-21 June 2006.

[22] H. Sengar, H. Wang, D. Wijesekera, and S. Jajodia, "Detecting VOIP floods using the hellinger distance," *IEEE Transactions on Parallel and Distributed Systems*, vol. 19, no. 6, pp. 794-805, June 2008.

[23] D. Sisalem and J. Kuthan, *Denial of Service Attacks and SIP Infrastructure,* Technical Report. (http://www.snocer.org/Paper/sisalem dos.pdf)

[24] M. Subramanian and T. Angamuthu, "An Autonomous framework for early detection of spoofed flooding attacks," *International Journal of Network Security*, vol. 10, no. 1, pp. 39-50, Jan. 2010.

[25] A. C. Snoeren, "Hash-based IP traceback," *Proceedings of SIGCOMM' 01*, pp.3-14, San Diego, California, USA, Aug. 27-31, 2001.

[26] J. Udhayan1 and T. Hamsapriya, "Statistical segregation method to minimize the false detections during DDoS attacks," *International Journal of Network Security,* vol. 13, no. 3, pp. 152V160, Nov. 2011.

[27] J. Wang, X. Yang, and K. Long, "A new relative entropy based app-DDoS detection method," *Proceedings of the IEEE symposium on Computers and Communications*, pp. 966- 968, Riccione, Italy 2010.

[28] W. Wang and W. Wu, "Online detection of network traffic anomalies using behavioral distance," *Internation Journal of Communications, Network and System Sciences*, pp. 177-182, 2010.

[29] A. Yaar, A. Perrig, and D. Song, "PI: A path identification mechanism to defend against DDoS attacks," *Proceedings of 2003 IEEE Security and Privacy (SP. 03)*, pp. 93V107, Berkeley, California, USA, May 11-14.

[30] Y. You, Md. Zulkernine, and A. haque, "Detecting flooding-based DDoS attacks," *IEEE Communication Society*, pp. 1229-1234, 2007.

[31] S. Yu, T. Thapngam, J. Liu, S. Wei, and W, Zhou, "Discriminating DDos flows from flash crowds using information distance," *3rd International Conference on Network Security & System*, pp. 351-356, 2009.

[32] J. Zhang, Z. Qin, and L. Ou, "An advance entropy-based DDoS Detection Scheme," *International Conference on Information, Networking and Automation*, pp.67-71, 2010.

N Jeyanthi is a Research Scholar in VIT University, Vellore, Tamilnadu, India. She received her M.Tech in Information Technology with Networking as Specialization from VIT University, India in 2006 and B.E.

in Computer Science and Engineering from Madurai Kamaraj University, Madurai, India in 1999. Her current research interest is on Network Security in Real-Time applications. A life member of Indian Society of Technical Education.

N.Ch.S.N. Iyengar (M.Sc, M.E, Ph.D) currently Director for Perivar EVR Central Library and Senior Professor at the School of Computing Science and Engineering at VIT University, Vellore, Tamil Nadu, India. His research interests include Agent based Distributed Computing, Security aspects of All Networks including VoIP, Intelligent Information retrieval, computational methods, Bio informatics and Fluid mechanics. He has authored and co-authored several books and had nearly 120 research publications in reputed peer reviewed International Journals. He Served as PCM/Reviewer for many International and IEEE conferences. He is chief editor for IJSEA of AIRCC, guest editor for Special Issue on "Cloud Computing and Services" of Int J. of Communications, Network and System Sciences. He is also an editorial board member for many reputed international journals like IJCA, IJCTE, IJSE, IJEMTA, JCMS, and many more.