Recent Flash Events: A Study

Avneet Dhingra[1] and Monika Sachdeva[2]
[1]*Department of Computer Science and Engineering,*
Punjab Technical University, Jalandhar, Punjab, India
[2]*Department of Computer Science and Engineering,*
Shaheed Bhagat Singh State Technical Campus, Ferozepur, Punjab, India
E-mail: [1]*manavn@yahoo.com,* [2]*monika.sal@rediffmail.com*

***Abstract*—With the evolving technology, the dependence on Internet, for business, communication and information exchange, has increased manifolds. Disruption of web services, even for small duration, leads to huge losses. The two major reasons for the disruption are DDoS attacks and Flash Events. Both cause the network to be overloaded, thus making the limited resources like-bandwidth, CPU, memory etc., unavailable to genuine users. Thus the need to find strategies to distinguish between the two arises. In this paper, we have explained flash events, their causes, effects, characteristics and also how they differ from DDoS attacks. The paper gives an explanation as to why should the server discriminate between DDoS attack and Flash Event. The Recent flash Events experienced by different websites have been presented so as to get the real world scenario of the same.**

Keywords: Flash Events, DDoS, Characteristics, Comparison of DDoS and Flash Events, Types of Flash Events, Slashdot Effect

I. INTRODUCTION

In the last decade technology has evolved manifolds, thereby changing the way of storing the information and accessing it. All the required communication takes place via Internet. Network links of the Internet act as conduit for transferring information. The society, at large, has started depending on web for business, research and related information flow. Disruption of services of web or malfunctioning of even a small part of network, for a small duration, degrades the performance and leads to huge losses [1].

The performance deterioration can occur due to two main reasons. First, it could be an intentional malicious attempt by attackers to disrupt the victim services. Such an attack is known as Distributed Denial of Service (DDoS) attack. DDoS are conducted using massive botnets which in turn use compromised servers known as Slaves or Zombies. These attacks overwhelm the network resources (CPU, Memory or network bandwidth) with requests, such that their services are rendered unavailable to the legitimate user.

Second, it could be a Flash Crowd which occurs when there is a sudden increase in volume of web traffic such that the response time of a website increases and in some cases also leads to the crash down of the affected website.

Both these situations arise due to variation in volume of the Internet traffic. Both of these lead to inconsistent behavior of the victim to the requests received.

This paper discusses *Flash Events* in detail and compares it with its counterpart-*DDoS attacks*. The major contribution of the paper is to provide an in-depth study of Flash events, its characteristics and its comparison with DDoS attacks.

Section II and III give the definition of flash events and their types. Section IV gives the effects of flash events. Section V describes the features of flash event. The need for discriminating flash events and DDoS attacks is highlighted in Section VI. Comparison of flash events and DDoS are given in section VII. In section VIII, world scenario of flash events is recounted. Section IX concludes the paper.

II. WHAT ARE FLASH EVENTS

The term Flash Event (aka Flash Crowd), for the internet, was inspired by Larry Niven's science fiction short story, "The Flight of the Horse", published in early 1970's. In this story, teleportation machine was invented which could take people back to the time in history when the major event occurred. However, author did not anticipate that huge crowd would teleport themselves to watch a certain event, and that it would lead to confusion and chaos at that particular place of an event.

In today's world of internet, the term is used to describe exponential rise in website traffic, when large number of users send the request for services simultaneously to the website which gives the details of an event. Such a surge leads to performance deterioration [2]. Events causing huge traffic could be some internationally acclaimed sports event like Olympics, Football World cup or release of new product by Apple or Microsoft. It can also occur in case of a natural disaster or a terrorist attack (example: 9/11 attack on America). Sometimes, a low efficiency server is linked to a very popular website like Slashdot or reddit, which may cause huge growth in traffic. Such a flash event is known as Slashdot effect [9].

Sachdeva *et al.* [3], describes flash crowds as "sharp and often overwhelming increase in number of users attempting to access a web site simultaneously in response to some event or announcement". Events which attract flash crowds can be referred as flash events. According to Bhatia *et al.* [1], it is used to describe a situation in which hundreds and thousands of valid users access a computing resource simultaneously. The computing resources could be CPU, network bandwidth or memory. Yu *et al.* [4], describes Flash crowds as "unexpected but legitimate, dramatic surges of access to a server." Wendell and Freedman [5] have explained FC mathematically. For an affected website, it is a time period over which request rate tends to increase exponentially.

If $r_{ti}> 2^{i}.r_{t0}$, ~~V~~i $\in$ [0,k], the website is experiencing a flash crowd, where,

r_i =average per minute request rate over time $t_{i.}$

An event is said to be flash event only if the web server it affects needs to adjust the operation in order to remain available to users.

III. Types of Flash Events

Some flash events can be anticipated well before their occurrence and the sites can prepare themselves accordingly. These are known as *predictable flash events*. The world cup generally experiences a huge surge in the internet traffic. The related websites prepare themselves well in time to take care for such an increase in requests. However, despite number of preparations, Twitter.com faced an outage for 30 minutes during World Cup 2010. Other events like Olympics, online registration of a national level entrance test Gate/JEE etc., declaration of results of similar exam and launch of I-Phone 5 by Apple are a few of the predictable flash events.

The *unpredictable flash events* are the ones where the owners of the affected website are caught unawares. This generally happens in case of some breaking news like terrorist attack, Earthquake, tsunami or an epidemic (like swine flu). Such an event occurred on 11 September, 2001, when CNN experienced a sudden surge in traffic along with other major news websites.

Another type of flash event, known as S*lashdotting or Slashdot effect*, occurs when low performing websites suddenly become popular after being mentioned on a popular website like Slashdot.com. Announcing the publication on Redhat and LNXY caused only a slight increase in the request rate, and the actual flash crowd started when the article was linked by Linux Today and Slashdot. Interestingly, the form of the announcement influenced its resulting traffic surge. Linux Today published a complete article text, whose copy was hosted on the Linux Today server. Slashdot, in turn, published only a hyper link to the original article hosted on the origin server. As a consequence, announcing the article on Slashdot caused a distinctly larger traffic surge compared to publishing the article text on Linux Today. Another important observation is that the traffic surge was sudden, but not instantaneous. The request rate increased from about 30 requests per minute up to over 250 requests per minute within 15 minutes. This observation underlies the assumption that one can predict flash crowds by analysing the trends in request rate [9].

According to Chandra *et al* [15], flash events can also be classified according to load growth rate (time it requires to reach the peak from normal request rate), peak load (what is the maximum traffic it achieves) and duration (for how much time the high load of requests was experienced).

IV. Effects of Flash Events

Flash event generally occurs at an application level. Whenever flash event occurs, HTTP request rate increases suddenly. However, response rate to such requests decreases substantially. In extreme cases the web server may even crash.

Flash events exert heavy load, upto tens or hundred times more than the normal, on target web server, causing the server temporarily unreachable. Due to its overall unpredictability and relatively short duration, the traditional server side provisions lead to under utilization of resources [6].

V. Characteristics of Flash Events

The DDoS attacks and Flash events both lead to the disruption of the services to legitimate users. Thus, it is important to study their features so as to get the in depth knowledge. The overview of characteristics helps to develop a good intuition about what flash events are and how they come into existence [9]. This helps the server owners to proactively prepare themselves for such events.

There is a substantial increase in requests/web traffic up to hundred times more than average request observed daily. This surge in web traffic causes the performance to decline, connections to drop, and sometimes even crash the affected server [3].

This up rise in request rate is, however short lived. When the legitimate clients experience a low performance of website, they stop sending further requests. Gradually, the traffic surge returns to usual levels.

Most of the client requests are generated by the users who belong to same network or who have visited the page before. In other words, the requests are from users known to the server.

Also number of unique traffic clusters is quiet less as compared to source addresses. The requests received by web server follow a zipf-like distribution.

VI. Why Discriminate Flash Events from DDoS Attacks

Flash events and DDoS occur due to sudden and large surge in web traffic. They are quite similar in terms of network traffic phenomenon and both lead to disruption of services. However, the sources of requests received in case of DDoS are not legitimate (from the zombies or slaves), whereas in case of Flash events, they are from genuine users. Thus, it is important to differentiate them, or else, false alarms may be raised. It is a big challenge before the defenders as, if the data interpretation goes wrong, it may cause serious consequences [17]. The detectors may declare legitimate crowd of requests to be DDoS and vice-versa. Also, the techniques to be used for the mitigation of traffic are different for both the cases. In case of flash event, the websites need an internet-wide infrastructure support which is available publicly such as Content Distributed Network (CDN), server proxies and multilevel caches. Some part of the payload is shifted to CDN's or caches so that maximum number of requests can be responded to. In case the spike in traffic is due to DDoS, then different strategies come to play. Main aim in case of DDoS attack is not to respond to illegitimate users. This can be done in number of ways-using graphical puzzles, analysing user browsing dynamics, using honey pots and other methods that help server differentiate between the genuine users and illegitimate user request.

There is a motivation behind every DDoS attack. Motive could be anything from financial gains to political achievements or it could also be just to put forward the views of the attacker group. To obtain the maximum results, attackers use distributed and large number of botnets. They can even mimic flash events or take advantage of the event and send malicious data under the radar. Whenever a spike in internet traffic is detected by server, the first thing to be done is to look at certain parameters to make sure it is flash event. Genuine requests are sieved from the data received and malicious ones are ignored. That raises the need for discriminating flash event from DDoS attack.

As is clear from above discussion, in order to provide continuous service to legitimate users, it is important to study features of both flash events and DDoS and differentiate between the two. The major difference between them lies in their nature and origin such as their access intents and the distributions of their source IP address and the increased and decreased speeds of traffic between them [7, 10].

VII. Comparison of Flash Events and DDoS Attacks

DDoS and Flash Event are voluminous, bursty and unstable. They both cause high rise in network traffic and lead to disruption of services to legitimate users. Studying the differences between the two, help develop effective prediction and defense mechanism.

According to Jung *et al.*, flash events and DDoS have following differences. During Flash events, clients can be effectively aggregated into clusters. In fact, many have been registered in logs. In case of DDoS, the distribution of DoS attackers is geographically distributed in form of Zombies. Very few previously seen clusters are involved [8].

There is a decline in per client request rate during flash event but in case of DDoS there is no change in per client request rate during the surge. In case of flash event, the volume of traffic generated fluctuates and forms random zigzag wave as there is dynamic change in users, whereas the volume of DDoS attack remains stable throughout the attack [10].

Figure 1 and Fig. 2 consist of model graphs of Flash Events and DDOS Attacks showing its various features. Difference in the traffic pattern in case flash event and DDoS attack is clearly visible in the figures, thus, helping to understand their characteristics.

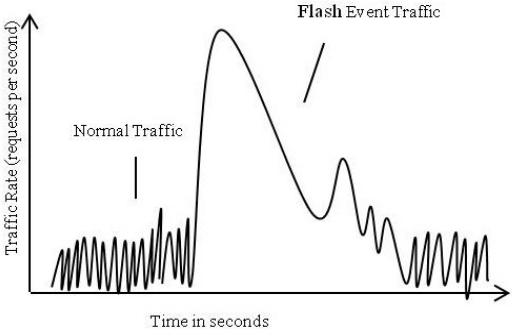

Fig 1 Model Graph for Flash Event

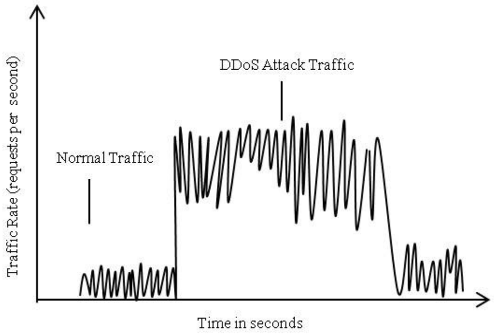

Fig. 2 Model Graph for DDoS Attack

Figure 1 shows that flash events grow rapidly and die out gradually. This is because the Event like any breaking news gets the requests suddenly. As soon as the user realizes the slow response rate, it stops accessing the affected server. After sometime, the Flash crowd declines. Also after certain time, the news has been known and accessed by all interested users. So, the news no longer attracts users, thus, decreasing the traffic.

Figure 2 shows the DDoS model graph depicting sudden rise and sudden fall of requests. It is so because DDoS attacks are conducted using botnets.

In short, the Flash events occur when there is breaking news or a world-wide event. In such a case, large numbers of users throughout the world, send requests to the web server for information. The sudden demand of information leads to outage or crash in the system. DDoS attacks are, however, well planned and programmed using the compromised systems known as zombies/ slaves. Therefore, the starting time and ending time are already defined.

Table I gives the comparison of DDoS attacks and Flash events.

TABLE 1 COMPARISON OF DDOS ATTACK AND FLASH EVENT

DDoS Attack	Flash Events
Network and server get congested and overloaded with the requests	Network and server get congested and overloaded with the requests
The traffic received is malicious and there is no need to respond.	The traffic received is genuine and need to be responded.
DDoS Attacks are always unpredictable. These occur as per the plans of an attacker using network of zombies	Flash Events can be predictable as well as unpredictable. These generally occur in case of a major world event like Olympics, Presidential elections, etc.
Request rate remains the same throughout the attack as the Zombies responsible for it, use automated tool in order to generate traffic.	Request rate per client decreases when compared to general state as the overload at servers result in drops and this forces request rate to drop at client side [3].
The requests received do not follow any particular pattern	The requests follow zipf-like distribution.

VIII. RECENT FLASH EVENTS

The flash events cause the server to get over whelmed with request. This sometimes causes the server's performance to decrease drastically and sometimes leads to crash of server. All this affects the clients using the web services. Frequent outages can lead to decrease in the number of users using the web site. Therefore, server owners use possible new methods to mitigate these events. The main aim of technical engineers, in such a scenario, is to restore the services at the shortest time possible.

The last decade has seen large number of flash events resulting in website outages. In this section, the recent Flash Events have been categorized according to the reason of traffic surge.

A. Flash Events Due to Natural Disasters

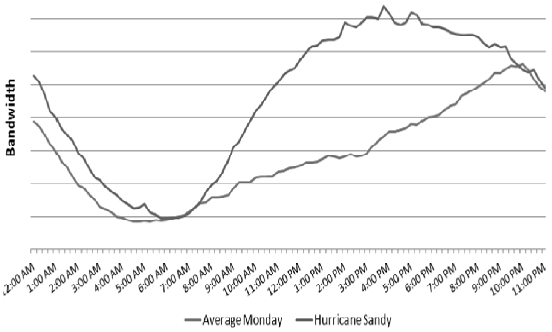

Fig. 3 Internet Traffic During Hurricane 'Sandy'. (*Source*: Sandvine)

In year 2012, super storm *Sandy* hit the eastern coast of The United States. The internet usage on 31 October increase by 114%. Netflix witnessed a traffic volume increase of 150%, while Skype witnessed a service usage increase of 122%, with a notable spike around 5pm. Fig. 3 below shows the East coast (USA) internet traffic for the day.

B. Flash Events Due to Sports

The 2010 World Cup, in South Africa, had the internet traffic exceed all the previous records. The leading social website, twitter, became the major victim. Normally it saw 750 tweets per second on an average day, but the traffic rose to approx. 2,940 tweets per second, whenever a goal occurred. These traffic spikes, overburdened the twitter's internal network capacity. It saw outages and maintenance downtime throughout the world cup [11].

Winter Olympics held in Sochi, Russia, saw a big rise in online traffic. The opening ceremony itself drove more than 1 Tbps of internet traffic.

C. Flash Events Due to Launch of New Software/ Product

According to Techcentral / Ireland's technology news resource, a unique breakdown occurred at Microsoft office, in June 2014 when Exchange Online and Lync Online, part of *Microsoft Office 360*, were unavailable for hours together. The previously unknown flaw had been detected in the directory partition due to which large number of customer could not access the email services. Even though connectivity was resumed, the resulting traffic surge overwhelmed the large number of network elements, thus leading to unavailability of Lync functionality for a little longer time.

On Sept. 18, 2013, Apple launched iOS7. Upon the release, Apple updates became almost 20% of total network traffic. Thousands of students at various universities in US (Ohio University, University of Texas, University of Arkansas), began to download it. This led to the surges as high as 5 times the normal traffic levels. Student newspapers also reported outages or slowdown of campus networks.

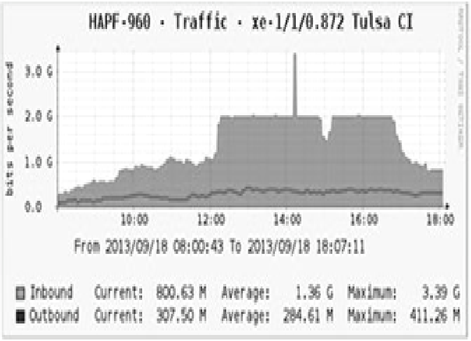

Fig. 4 Graph for Flash Event Occurred on Sept., 18, 2013 Due to Launch of iOS 7 Update on the University of Arkansas' Regional Arkansas Research and Education Optical Network Connection

Figure 4 gives an insight into the internet traffic spike caused by iOS 7's update launch. IOS 7 downloads caused the web traffic on Arkansas' regional Arkansas Research and Education Optical network connection to rise from 1.4 Gb/s to 6 Gb/s.

D. Flash Events Due to Celebrities

The websites of celebrities also sometimes get affected by Flash Events. In August 2013, the unusual trigger led to all the previous records of the Twitter's tweets-per-second to be destroyed. It was the broadcast of anime *master Hayao Miyazaki's* most famous movie "Castle in the Sky". Hundreds and hundreds of Japanese fans of the movie tweeted a magic-word used in the classic anime (short for animation), all at once. The word typed was "balse". It is spoken during movie's climax scene. The flood of tweets peaked at 143,199 tweets-per-second. The other websites like Amazon, Play station, KFC and Nissan, including "balse" button, experienced the failure as soon as the button was pressed [12]. Fig. 5 shows the traffic graph of the day (courtesy: blog.twitter.com). The spike shown is about 25 times the normal traffic.

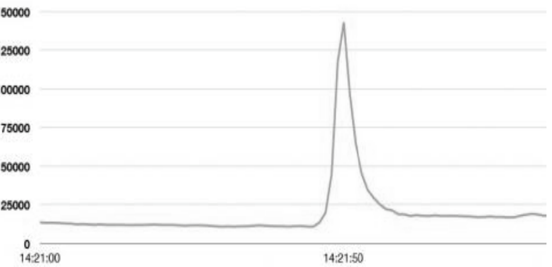

Fig. 5 Spike in Twitter Traffic Due to Sudden Typing of Word 'Balse' by Japanese People. (*Source*: blog.twitter.com)

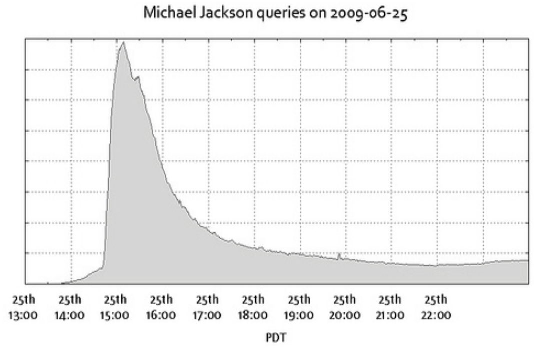

Fig. 6 Internet Spike at Google Search Engine Caused After Michael Jackson's Death. (*Source*: searchengineland.com)

When the *Michael Jackson's* news site TMZ first broke the news of MJ's death in June 2009, people from all over the world accessed the website to confirm it. Due to huge amount of requests at TMZ, it began to experience erratic outages. Other news sites like ABC, CBS, LA Times, AOL, CNN money, also became unavailable (down to nearly 10% availability). Activity at twitter peaked with 25% of all tweets happening at the time the reports confirmed that Jackson had died. In UK, twitter had the busiest day ever. Fig 6 shows the spike in traffic spike at Google when there was an outpour of searches related to Jackson. As we can see the traffic was too much that initially Google thought that it was under an attack.

According to data from Akamai, Internet traffic rose by 24% globally after the breaking news of *Osama Bin Laden's* Death. This high wave of web traffic, crippled CNN's news site. Other major news sites were also slowed down. Some of the requests were rejected also.

Salman Khan, the god-father of Bollywood, sent out a few tweets concerning his unemployed fans. The tweet said that he can talk to his friends to provide employment to his unemployed fans. Within a few minutes of tweeting, the stars Facebook page crashed due to heavy traffic from job-seekers.

E. Flash Events Due to Other Reasons

BestBuy, one of the USA's biggest electronic retailers, left its customers waiting for nearly an hour to complete the checkout process on November, 2012. It was due to huge surge in traffic to its site by the holiday shoppers. Users were greeted with the message: "we were expecting snow but we got a blizzard. Our site is incredibly busy! Please be patient while we shovel you a path" [13].

After the *London attacks* in July 2008, there was an up rise in the internet traffic leading to outages and degrading performances. At peak time, the BBC News website served up to 1.7 gigabits of data every second, with 40,000 page requests per second. The most affected news sites were BBC News, Netcraft, Sky News and MSN which were not available for short time.

IX. CONCLUSIONS

Studying about Flash events, help us get to know the features of flash events and features that differentiate it from DDoS attacks. This study helps to design the defense system which could predict the occurrence of spike in traffic at the web server so that pro-active measures can be taken to mitigate the huge traffic load on the server. The attacker may send malicious data to the server mixing it up with the flash event payload.

Studying the features of flash event helps in having a good insight about what exactly flash events are. Also it helps to know about their existence. Even when the web server owners expect traffic bursts, problems do occur due to non preparedness on the part of the owners or request per second surpassing the extra ordinary numbers. This causes losses due to outages or low performance. Technologies have to be at place in order to avoid outages. If it's a flash event then load balancing is required in order to maintain the response time, else if it is a DDoS attack, then the server need not respond to malicious requests but at the same time needs to take care of genuine users also.

The overall scenario, discussed in this paper, leads to the conclusion that traffic of both DDoS attack and flash event are unstable, voluminous, and occur in short bursts. Even the impact of both is similar. They both lead to complete or partial failure of the services provided by the affected server. Web server is required to identify and serve as many genuine requests as it can respond back to. Thus the need arises to discriminate the genuine users from illegitimate ones. It becomes necessary to see if the request is from some Zombie or slave, or it is the genuine user demanding the information. On the face of it, both requests seem to be coming from the authentic source. To distinguish them we need to learn about their characteristics and features that make them different. Thus, developing the technique to discriminate the data is a challenging job and needs a lot of in-depth study of the related information.

REFERENCES

[1] S.Bhatia, G. Mohay, A.Tickle, E.Ahmed, "Parametric differences between a real-world denial-of-service attack and a flash event," IEEE Computer Society, Sixth International Conference on Availability, Reliability and Security, 2011.

[2] Definition: Flash Crowd, available at, http:// www.catb.org/ jargon/ html/ F/ flash-crowd.html.

[3] M. Sachdeva, Thesis: "A distributed approach for defending the service against DDoS attacks," PhD. Thesis, Sept. 2012.

[4] S. Yu, W. Zhou, W. Jia, S.Guo, Y.Xiang, F.Tang, "Discriminating ddos attacks from flash crowds using flow correlation coefficient," IEEE Transactions on parallel and distributed systems, vol.23, No.6, pp 1073-1080, June 2012.

[5] P. Wendell, M. J. Freedman; "Going Viral" Flash Crowds in an open CDN", IMC'11, Nov.2-4, 2011; Berlin Germany. cs.princeton.edu/~mfreed/docs/flash-imc11.pdf

[6] C.PAN, M. Atajanov, M.B. Hossain, T. Shimokawa, N. Yashida, "FCAN: Flash Crowds alleviation network using adaptive P2P overlay of cache proxies," IEICE Trans. Communication, Vol.E 89-B, No.4, pp-1119, April 2006.

[7] Li. Ke, Z. Wanlei, L. ping; H. Jing, l. Jianwen, " Distinguishing DDoS attacks from Flash Crowds using probability metrics," NSS 2009: Proceedings of 3rd International Conference on Network and System Security, IEEE, pp 9-17

[8] J. Jung, B. Krishnamurthy, M. Rabinovich, "Flash Crowds and Denial of Service attacks: characterization and implications for CDNs and web sites," available at http:// www2. research.att.com/ ~bala/ papers/www02-fc.html.

[9] H.Izycka, "Flash Crowd prediction", Vrije Universiteit Amsterdam, Master's thesis, available at http:// www.globule.org/ publi/ FCP_master2006.pdf.

[10] K.M. Prasad, A.R.M. reddy, K.V. Rao, "Discriminating DDoS attack traffic from Flash Crowds on internet threat monitors (ITM) using entropy variations", AJC & ICT, IEEE, vol.6 6 No.2, June 2013.

[11] R. Miller, "Record world cup traffic slams twitter", available at datacenterknowledge.com, phys.org, June 2010

[12] T. Kontzer, "Twitter spike highlights need to plan for traffic surge", available at network computing.com, Aug., 2013.

[13] G. McQuaid, "How the cloud can help with seasonal traffic spikes", available at nexusbg.com, Dec., 2013.

[14] International Business, P. Goswami, "Salman Khan offers Jobs to Unemployed fans online; Resultant traffic crashes his Facebook Page", available at Ibtimes.co.in, June, 2014.

[15] A.Chandra, P. Shenoy, "Effectiveness of dynamic resource allocation for handling internet flash crowds," available at http://lass.cs.umass.edu/papers/pdf/TR03-37.pdf.

[16] S. Kandula, D.Katabi, M.Jacob, A. Berger, " Botz-4-Sale: surviving organised DDoS attacks that mimic flash crowds," Proceedings Second Symposium Networked Systems Design and Implementation(NSDI '05), 2005.

[17] S. Yu, T. Thapngam, J. Liu, S. Wei, W. Zhou, "Discriminating ddos flows from flash crowds using information distance," Proceedings of the 3rd International Conference on Network and System Security(NSS '09), pp 351-356.

[18] R. Saravanan, S. Shanmuganathan and Y. Palanichamy, "Behavior based detection of application layer distributed denial of service attacks during flash events."

[19] M. Sachdeva, K. Kumar, "A traffic cluster entropy based approach to distinguish DDoS attacks from flash events," Hindawi publishing corporation, ISRN Communication and networking, vol. 2014.