I.J. Information Technology and Computer Science, **2013, 08, 54-65**
Published Online July 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2013.08.06

Study and Performance Evaluation on Recent DDoS Trends of Attack & Defense

Muhammad Aamir
SZABIST, Karachi, Pakistan
E-mail: aamir.nbpit@yahoo.com

Muhammad Arif
SSUET, Karachi, Pakistan
E-mail: arif.md@hotmail.com

***Abstract*—** Different types and techniques of DDoS attacks & defense are studied in this paper with some recent information on attacks dominated in year 2012 (1st Quarter). We further provide simulation based analysis of an FTP server's performance in a typical enterprise network under distributed denial of service attack. Simulations in OPNET show noticeable variations in connection capacity, task processing and delay parameters of the attacked server as compared to the performance without attack. DDoS detection and mitigation mechanisms discussed in this paper mainly focus on some recently investigated techniques. Finally, conclusions are drawn on the basis of survey based study as well as simulation results.

***Index Terms*—** DDoS, Attack, Defense, Network

I. Introduction

Distributed Denial of Service attacks [1] are exercised by attackers in various forms. These attacks vary from single attacking source to a networked attacking infrastructure. They also vary in degree of automation, from manual efforts to fully automated attacks.

In networked form, a botnet of attacking sources is created. These machines are vulnerable on internet and attackers exploit their vulnerabilities to control them for generating attacks against a victim. These compromised machines are called 'zombies'. Moreover, there are many automated tools available to generate DDoS attacks. These software tools perform almost everything for attacker; such as port scanning, identifying victim's vulnerabilities and protocol loopholes etc. An attacker just configures parameters of attack and the rest is done by automated tools [1-2].

DDoS attack is a common extension of DoS attacks in which the attacking power is increased with numerous attacking sources which are under attacker's control (it refers to 'zombies' in a 'botnet'). A broader classification of DoS attacks is provided in Fig. 1.

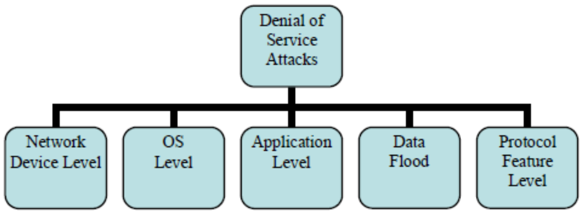


Fig. 1: DDoS attack types in a broader classification

In above classification [1], Network Device Level attack exploits a router's weak point. OS Level attack exploit's OS vulnerability. Application Level attack determines application's vulnerability through port scanning. Data Flood refers to flooding a network or server's connection points to deny services for legitimate clients. This is achieved by sending huge traffic (data packets) towards victim. The protocol feature attack exploits some protocol's weak point such as the requirement of final acknowledgement from client by the server in TCP's three-way handshake.

The remainder of this paper is organized as follows: Section 2 discusses some common DDoS attacks. Section 3 identifies some recent trends of DDoS attacks. Section 4 presents techniques of DDoS attack detection & mitigation. Section 5 presents the simulation analysis. Conclusion is made in the final section.

II. Some Common DDoS Attacks

2.1 Direct and Reflector Attacks

In direct DDoS attacks, zombies directly attack the victim as shown in Fig. 2. On the other hand, in reflector attacks, zombies send request packets with spoofed IP (IP of victim) in source address field of IP packets to a number of other vulnerable computer devices (PCs, routers etc.) and replies generated from such devices are routed towards the victim for an impact desired by attacker. In such a way, reflection of the traffic is seen in these attacks [3]. A classic example is sending ‘ping’ requests with spoofed source IP. In such a case, ‘ping’ replies are sent towards victim. In this way, the attacker is successful in saturating victim’s bandwidth. Architecture of reflector attack is shown in Fig. 3.

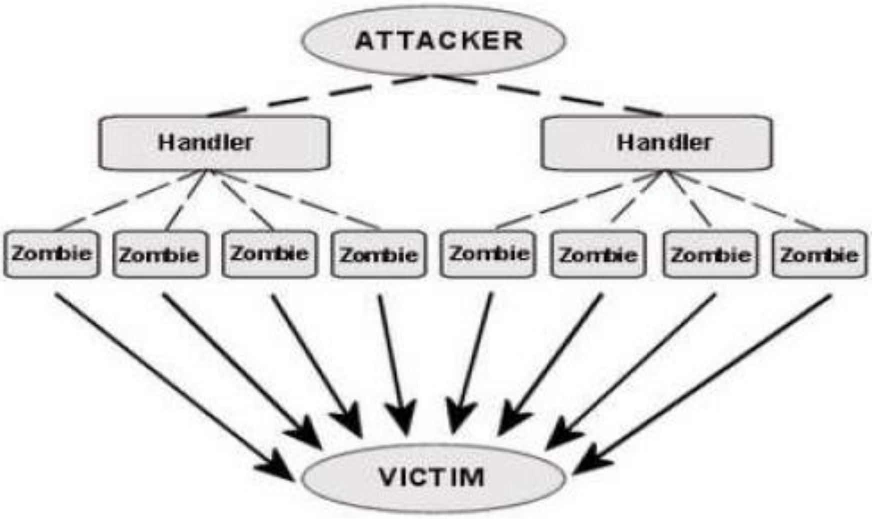


Fig. 2: Architecture of direct DDoS attack

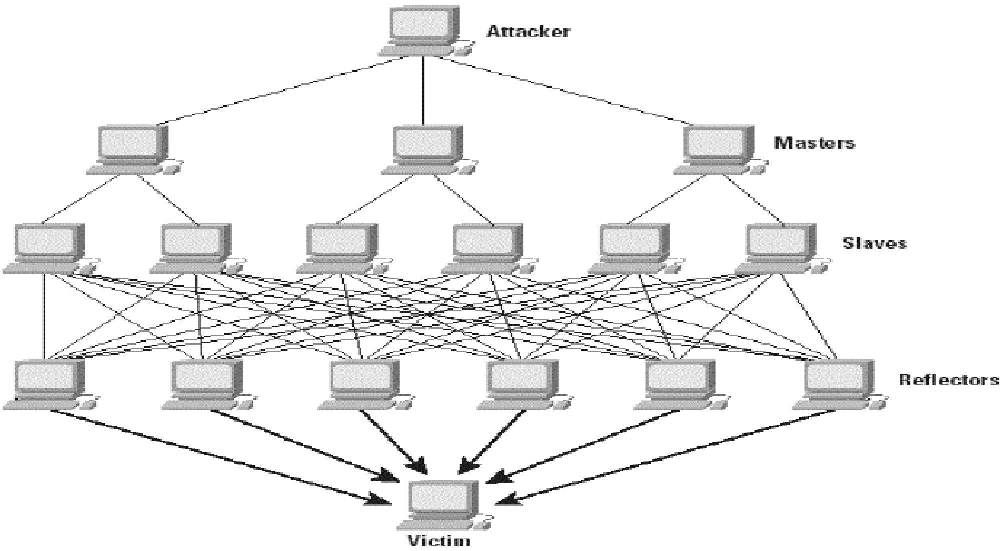


Fig. 3: Architecture of Reflector DDoS Attack (‘Masters’ are Handlers and ‘Slaves’ are Zombies)

In direct DDoS attacks, attacker proceeds with instructions to ‘Handlers’ which perform Command & Control operations to control zombies. Moreover, zombies directly attack victims and also pass the information to handlers [2]. In reflector attacks, modus operandi is almost the same but zombies further exploit reflectors (machines on targeted victim’s network) to flood victim with huge amount of traffic (IP packets).

2.2 Application Layer DDoS Attacks

Since DDoS attacks are very old technique, there have been many researches and implementations to counter such attacks. Many forms of DDoS attack detection and mitigation are now available. However, the major focus of attackers in earlier times has been towards exhausting victim’s services for legitimate users through network layer (layer 3) attacks i.e. modifying IP packet fields or flooding victim’s network with data packets. However, as many defenses are now available against such attacks, attackers have also changed their strategies and started focusing on attacks of application layer (layer 7) [3]. In such attacks, no manipulation is done in IP packets on network layer level; instead, complete TCP connections are made with victim just like legitimate clients. After establishment of successful connections, attackers exhaust server (the victim) with requests of heavy processing for longer times (for instance, heavy image downloading is requested). In this way, server remains busy to process attackers' requests due to which legitimate clients often find their requests unanswered.

Since complete TCP connections are made with servers in case of application layer attacks, such attacks are very difficult to identify and mitigate as normal traffic and attacking traffic are the same at network layer. Therefore, many traditional DDoS detection schemes fail in case of application layer DDoS attacks. Due to the same reason, researchers have also made several attempts in last few years to detect & mitigate application layer DDoS attacks.

In table 1, different forms of common DDoS attacks in network and application layers are mentioned. Fig. 4 and Fig. 5 depict normal TCP three-way handshake operation and TCP ACK attack formation respectively.

Table 1: Common DDoS Attacks in Network & Application Layers

Layer	Attack	Method	Impact
Network	UDP Flood	Sending huge amount of UDP packets towards victim's bandwidth.	Network Congestion due to unavailability of bandwidth to legitimate clients.
	ICMP Flood	Sending huge amount of ICMP packets towards victim's bandwidth.	Network Congestion due to unavailability of bandwidth to legitimate clients.
	TCP Flood	Initiating large number of TCP connections (of spoofed packets) with victim and not acknowledging the same (known as TCP ACK attack)	Unanswered Requests due to unavailability of connections for legitimate clients (Connection buffer i.e. capacity is limited on a given server).
Application	HTTP Flood	Establishing large number of TCP connections with victim and sending requests for heavy processing through HTTP communication.	Unanswered Requests due to unavailability of server's processing cycles for legitimate clients (All processing remains busy for answering attacker's requests of heavy processing).
	HTTPS Flood	Establishing large number of TCP connections with victim and sending requests for heavy processing through HTTPS communication.	Unanswered Requests due to unavailability of server's processing cycles for legitimate clients (All processing remains busy for answering attacker's requests of heavy processing).
	FTP Flood	Establishing large number of TCP connections with victim and sending requests for heavy processing through FTP communication.	Unanswered Requests due to unavailability of server's processing cycles for legitimate clients (All processing remains busy for answering attacker's requests of heavy processing).

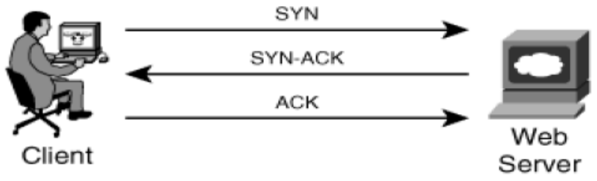


Fig. 4: Three-way handshake in TCP

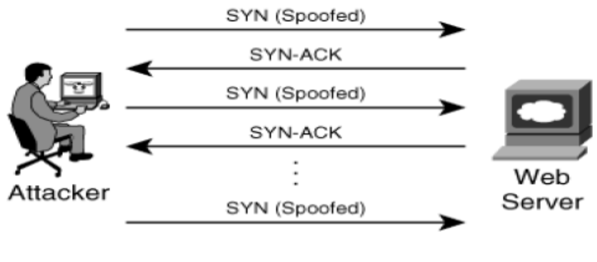


Fig. 5: SYN ACK attack in TCP

2.3 DDoS Attacks in Wireless Networks

Wireless networks are vulnerable to many kinds of attacks including distributed denial of service attacks. Their main vulnerability is shared wireless medium due to which many attacks are possible to exploit and compromise wireless stations. It is possible in almost all variations of wireless networks such as Wireless sensor networks (WSN), Mobile ad hoc networks (MANET) and Wireless local area networks (WLAN) [4-7]. Like traditional wired networks, DDoS attacks on wireless networks are also possible in different layers of communication. Some common forms of DDoS attacks in different layers of wireless networks are indicated in table 2.

Table 2: Some common DDoS attacks in wireless networks

Layer	Attack
Physical Layer	Jamming Attack
	Node Tampering Attack
Link / MAC Layer	Interrogation Attack
	Collision Attack
Network Layer	Black Hole Attack
	HELLO Flood Attack
Transport Layer	SYN Flooding Attack
Application Layer	Overwhelming Attack
	DoS Attack (Path-based)

Jamming attacks in physical layer are one of the most dominating attacks in wireless networks in which signal interference is generated through attacking sources to choke the communication medium. In this way, a denial of service effect is observed for legitimate clients on the network [5].

III. Some Recent DDoS Attack Trends

In this section, we survey a few recent DDoS attack trends on various networks connected to the Internet. We select 'Prolexic Attack Report Q1 2012' of Prolexic Technologies [8] for this analysis. Prolexic Technologies is a trusted DDoS attack mitigation provider in world. The data provided in this analysis covers all attacks dealt by Prolexic throughout the world during first quarter of year 2012.

3.1 DDoS Attacks on Financial Sector Networks

In Fig. 6, huge upward shift of DDoS attack mitigation can be observed in statistics of 'Total bits mitigated' and 'Total packets mitigated' in first quarter of 2012 (compared with last quarter of 2011) in world's financial sector networks. The data shows that DDoS attacks have been increased manifold as well as the need of stronger defense against such attacks in financial sector networks. It is explicitly mentioned on the cover page of attack report of Prolexic Technologies that "Financial services firms get hit by DDoS attacks as malicious packet volume increases 3,000% quarter over quarter". In quarter 4 of 2011, 19.1 TB (Terabytes) of data and 14 billion packets of malicious traffic were mitigated by Prolexic. In first quarter of 2012, a significant increase was observed in malicious traffic with 65 TB of data and 1.1 trillion packets being identified and mitigated. It is further observed that aggregate attack mitigation time in seconds has also been increased more than twice. It shows that attackers are using more sophisticated and automated tools to launch larger magnitudes of attacks at rapid speed for which the defense has to be fast as well. The attackers now seem to be more focused towards financial sectors with evolving strategies. Moreover, the average attack length in seconds has been decreased indicating that the attack tools are now quicker to generate a deeper impact in lesser time.

3.2 DDoS Attacks on All Networks

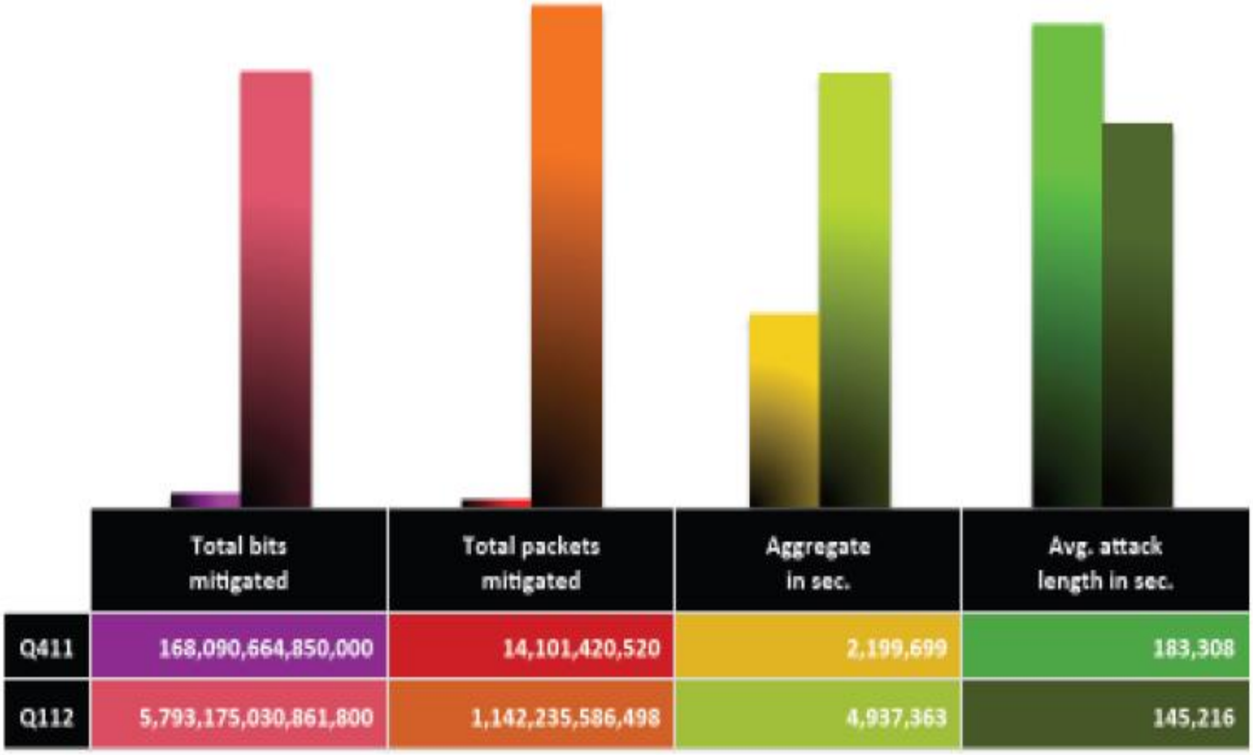
We further provide some information regarding DDoS attack statistics of first quarter of 2012 in all sectors throughout the world including financial sector networks. Some key information extracted from the attack report of Prolexic Technologies regarding first quarter of 2012 is:

1. 25% increase in DDoS attacks*.

2. 25% increase in application layer DDoS attacks*.

3. 28.5 hours of attack duration (previous is 65 hours)*.

* Compared with last quarter of previous year (2011).



	Total bits mitigated	Total packets mitigated	Aggregate in sec.	Avg. attack length in sec.
Q411	168,090,664,850,000	14,101,420,520	2,199,699	183,308
Q112	5,793,175,030,861,800	1,142,235,586,498	4,937,363	145,216

Fig. 6: DDoS attack mitigation statistics in world's financial sector networks provided by Prolexic (Q4-2011 vs. Q1-2012)

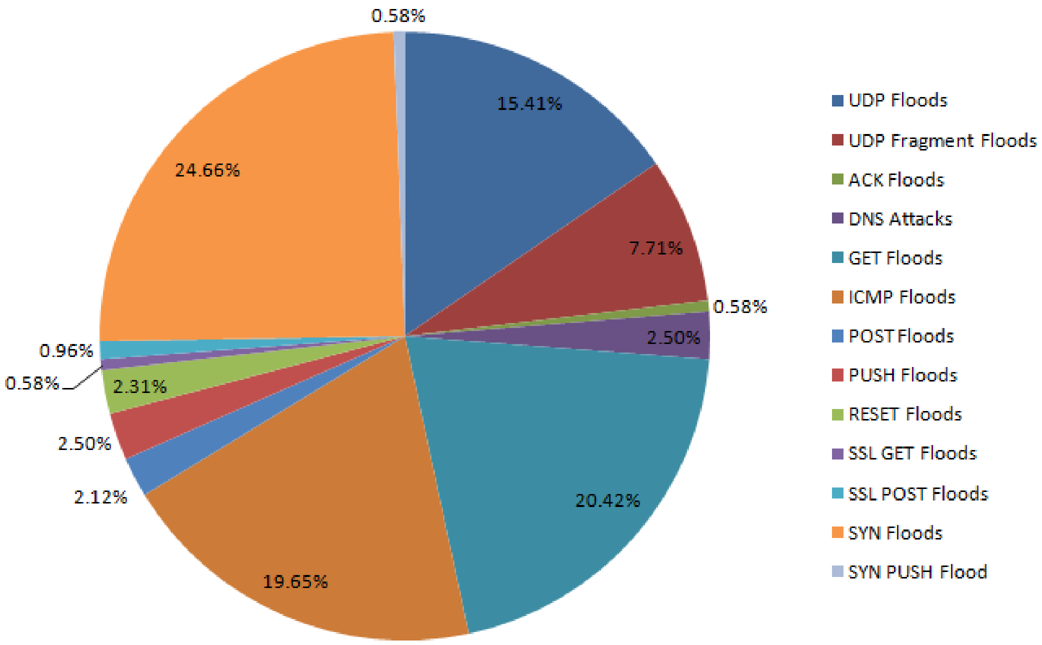


Fig. 7: DDoS attack types (2012 Q1)

In Fig. 7, total DDoS attack types observed in first quarter of 2012 are presented. It can be seen that attackers had more focus towards infrastructure layer (Layer 3) attacks than application layer (Layer 7) attacks in overall scenario. Major attacks found in statistics are SYN flood attacks (Layer 3), ICMP/UDP flood attacks (Layer 3) and GET floods (Layer 7).

In Fig. 8, DDoS attacks per week are presented for the first quarter of 2012 over last quarter of 2011. A noticeable increase in DDoS attacks is shown from mid January to mid March. Moreover, it is observed that January was the busiest month whereas the period of February 12-19 was the most active week for DDoS attacks. In Fig. 9, top ten source countries of DDoS attacks in first quarter of 2012 are mentioned. China is found on top with 30.59% of DDoS attacks.

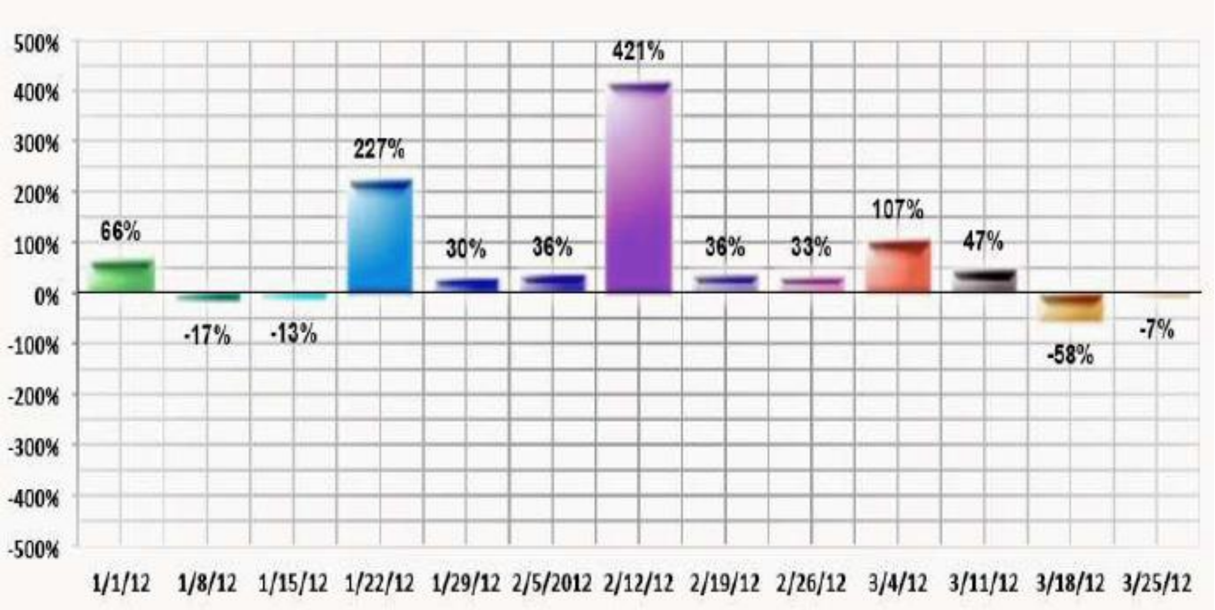


Fig. 8: DDoS attacks per week (2012 Q1 over 2011 Q4)

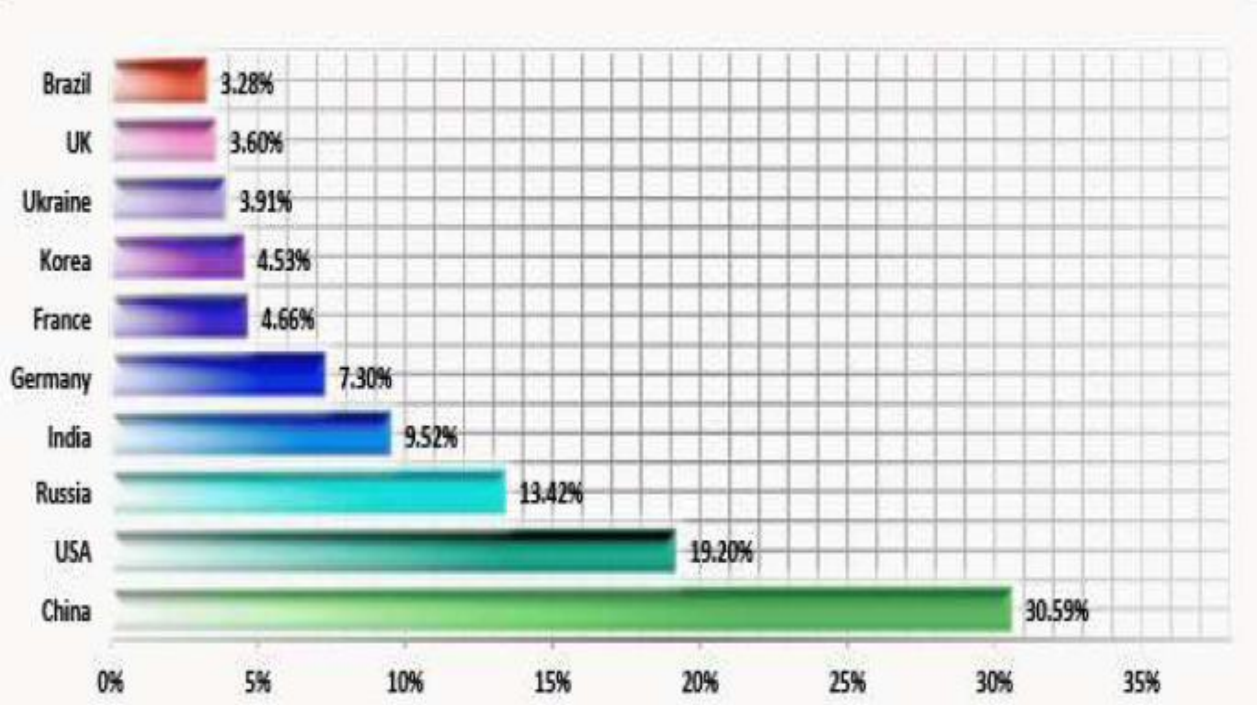


Fig. 9: Top ten source countries of DDoS attacks (2012 Q1)

IV. DDoS Attack Detection & Mitigation

Accurate detection and mitigation of DDoS attacks is a difficult task even today, when we have large number of detection & mitigation tools available. Application layer DDoS attacks are even harder to mitigate due to their legitimate-like traffic features. However, some recent research efforts indicate that researchers are now focused to devise methods of detecting and mitigating application layer DDoS attacks. Moreover, some evolutionary methods of defense against DDoS attacks have been tested in research for some years.

In table 3, some common methods of DDoS detection and mitigation are mentioned which correspond to new dimensions of defense against DDoS attacks as compared to traditional & older methods which have been used for many years e.g. traceback, entropy variations, common traffic anomalies & packet filtering techniques.

Table 3: Some common DDoS mitigation techniques (Evolutionary methods)

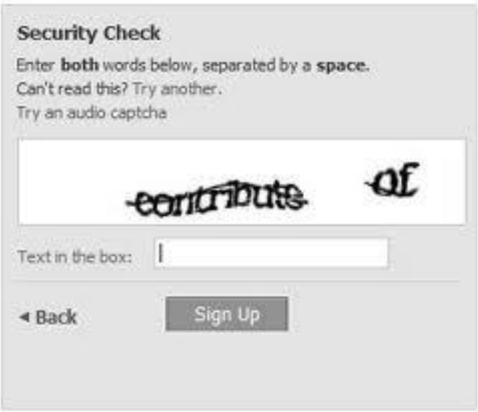
Basis of Defense	Method
Neural Networks [9-11]	Magnitude of attack (number of zombies and attack rate) identification through back propagation neural network.
	Magnitude of attack (number of zombies and attack rate) identification through LVQ model of neural network.
Botnet Fluxing [2]	Fast Flux (IP addresses of same domain are frequently changed).
	Domain Flux (Domain names of same IP address are frequently changed).
Defense Mechanism in Switching / Routing Devices [12]	Packet Forwarding / TCP Blocking in routers.
	TPM hardware chip in switches.

The schemes mentioned in table 3 are mainly for network layer attacks in which malformed packets are sent towards victim. However, special techniques have also been developed to deal with applications layer attacks. In table 4, some common methods of application layer DDoS detection and mitigation are mentioned which further indicate new dimensions of defense against application layer DDoS attacks.

Table 4: Some evolutionary DDoS mitigation techniques against application layer attacks

Basis of Defense	**Method**
Network-wide monitoring [13]	Observing shift in spatial-temporal patterns of network traffic on occurrence of DDoS attack.
Changes in network's aggregate traffic anomalies [14]	Observing packet size and traffic rate parameters through proposed bPDM mechanism to calculate probability ratio test.
Observing changes in network's traffic anomalies through proposed metric [15]	Observing traffic rate, access changes and IP address distribution parameters through proposed hybrid probability metric to analyze proposed grouping thresholds i.e. 'similarity index' and 'variation'.
Observing document popularity in real time web traffic [16]	Observing spatial-temporal patterns of real time web traffic in flash crowd events and analyzing changes on occurrence of DDoS attack through document popularity.
Automated client puzzle [17]	Presenting CAPTHA puzzle images to clients to avoid machine based automated DDoS attacks.

A real challenge in designing defense against application layer DDoS attacks is distinguishing attacking patterns from sudden increase in legitimate requests (referred as 'flash crowd'). As same type of traffic behavior is observed in both forms of connections / requests, an effective mechanism of discriminating them from each other is harder to achieve and implement. Research against application layer DDoS attacks also mainly focus on discriminating application layer DDoS attacks from flash crowd events. CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) puzzle is a promising technique to mitigate application layer DDoS attacks. The client has to pass a challenge-response test to establish connection with a server.


Security Check

Enter **both** words below, separated by a **space**.

Can't read this? Try another.

Try an audio captcha

Text in the box:

Fig. 10: View of CAPTCHA test

In table 5, some latest research efforts against DDoS attacks are highlighted to provide more insight of related information to readers. All research efforts cited in table 5 have been published not before year 2012.

Table 5: Some latest research efforts on DDoS mitigation

Scheme	**Method**
Adaptive Probabilistic Marking (APM) [18]	Observing TTL fields of packets to initiate proposed traceback scheme and reconstruction of attacking path on occurrence of DDoS attack.
Adaptive Selective Verification (ASV) [19]	Increasing legitimate request rate (in adaptive manner upto a threshold level) in consecutive time windows by legitimate clients on occurrence of DDoS attack.
Traffic Pattern Analysis [20]	Observing changes in traffic flow and analyzing patterns using Pearson's correlation coefficient to calculate standard deviations of observed parameters. The analysis to distinguish DDoS attacks from legitimate activities is made through proposed algorithms.
LOT Defense [21]	Establishing tunnel between two communicating gateways through proposed lightweight protocol to prevent traffic against IP spoofing and flooding attacks.

V. Performance Evaluation

In this section, we simulate a hypothetically considered enterprise network under DDoS attack (network's FTP server is under application layer DDoS attack). The simulations are performed in OPNET, an industry accepted simulation tool for its realistic analysis of networking performance measurements [22].

5.1 Baseline Scenario

A baseline scenario is considered as shown in Fig. 11. We have a server setup at one end with FTP, Database and Web servers. On the same side of network, we have a LAN (Local Area Network) of local users. The LAN is configured with 100 Base-T settings and it is terminated at LAN router's ethernet interface. Number of users in this LAN is configured as 10 and they are all active. Effectively, they can also use switch interface as they are local users, the routing is therefore not required to access the servers. LAN router is however utilized to provide ethernet interface to the local users' LAN for connection purpose. In addition to this, we also have a group of remote users; say at some remote site, connected with the network through remote router 'Router-1', the IP cloud (internet) and a firewall. The connectivity of remote users is accomplished with VPN (Virtual Private Network). They are all on the same LAN at remote site which is configured with 100 Base-T settings and connected with the ethernet interface of Router-1. Number of users in this remote LAN is configured as 5 and they are all active as well. Some properties of servers used in the network are mentioned in table 6.

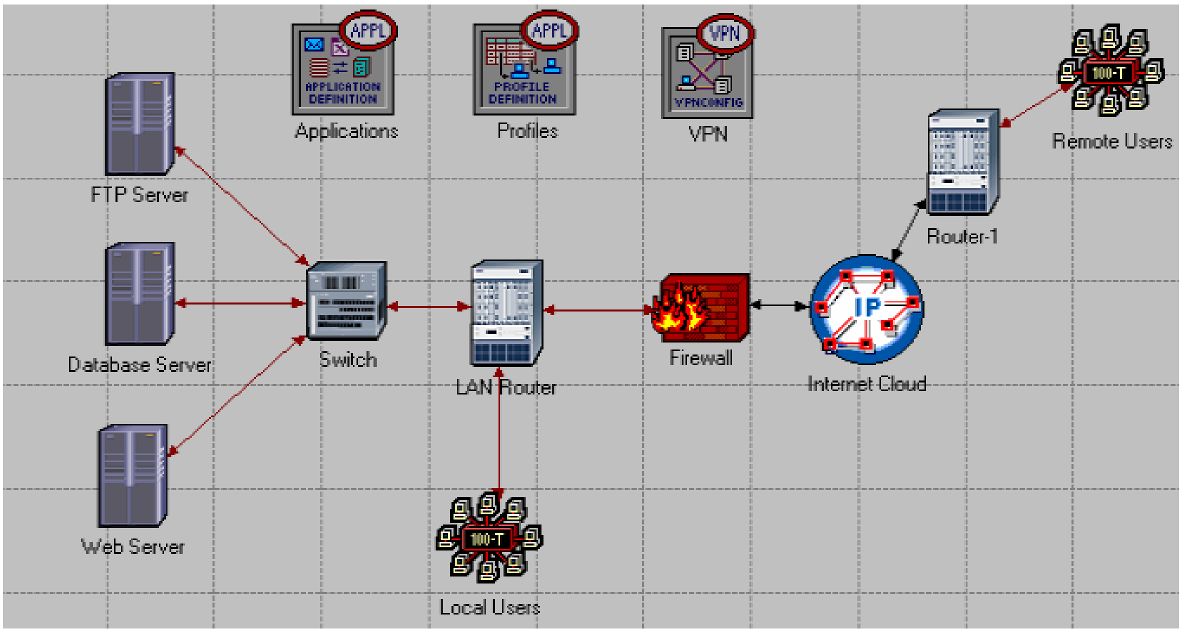


Fig. 11: A hypothetical baseline scenario of an enterprise network created in OPNET

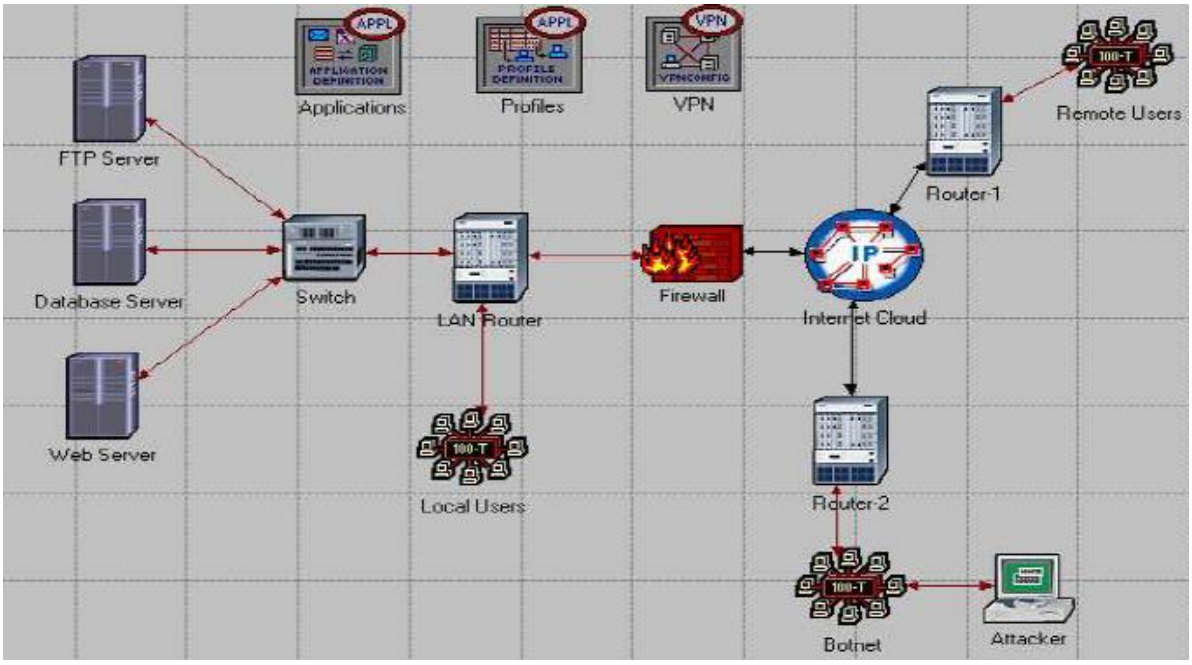


Fig. 12: Attack scenario created in OPNET

Table 6: Properties of servers

Attribute	Value
Operating System (OS)	Sun Solaris
TCP Receive Buffer (bytes)	8760
TCP Delayed ACK Mechanism	Segment / Clock based
TCP Max ACK Delay (sec)	0.200
TCP Fast Retransmit	Enabled
Max Connect Attempts (Retransmission Threshold)	3

5.2 Attack Scenario

In attack scenario, all configurations remain the same as they are in baseline scenario. In addition to this, we assume that an ‘Attacker’ has got control of a botnet (handlers and zombies) and succeeded to pass through the firewall of considered network. It is out of the scope of this analysis how the attacker gets success in controlling the botnet and penetrating the firewall. Ultimately, the attacker launches DDoS attack on network’s FTP server. The attack scenario is shown in Fig. 12.

5.3 Simulation Results & Discussions

In our simulation analysis, we select a few performance metrics which are normally not considered while analyzing network’s behavior under attack scenarios. Usually, the focus remains towards network traffic, its flow and aggregation. However, we obtain some server side parameters to analyze the effect of DDoS attack on server performance along with protocol delay (TCP delay). The following parameters are considered:

(a) CPU utilization and Load (connection requests) on attacked FTP server.

(b) TCP active connection counts of server.

(c) TCP delay in server.

(d) Task processing time of server.

(e) Effect on all above parameters with respect to the change in botnet size.

In order to observe botnet size effect, we consider three botnet sizes with 50, 100 and 200 zombies. It is assumed that handlers are located within botnet and included in the mentioned botnet sizes. We observe the parameters with respect to simulation time of one hour.

5.3.1 CPU Utilization (%)

We observe that CPU utilization in FTP server under baseline scenario is minimal, whereas it increases manifold under attack scenario. Moreover, it is found that increasing botnet size has proportional effect on the CPU utilization i.e. CPU utilization is also increased. This is because as more traffic is sent by the attacker to exhaust the service, more processing is required to process incoming requests by the server. As a result, server is incapable to effectively respond the legitimate requests. In this analysis, CPU utilization of FTP server has increased more than 300 times (percentage utilization) at peak value when the server is under DDoS attack with 200 zombies as compared to the baseline scenario.

5.3.2 Load on FTP Server (requests/sec)

It is observed that load on FTP server is not very high when legitimate users communicate under baseline scenario. On the other hand, when DDoS attack strikes under attack scenario, we observe a shoot in FTP server load with increased connection requests. It is found from the obtained relationship that increased botnet size makes greater impact on server load. The reason behind the fact is that the attacker is sending more traffic to initiate connection requests for which the server responds and hence the load is increased. The ultimate target of attacker in this perspective is to degrade the server’s connection capacity for legitimate requests.

We observe that the average load of 0.8 requests per second is experienced by the server at peak value under attack scenario with 200 zombies as compared to 0.1 requests per second under baseline scenario, hence showing 8 times increase per second.

5.3.3 TCP Active Connection Counts & Delay (sec)

We observe that active connection counts under attack scenario greatly increase as compared to the baseline scenario. It shows how much the server is getting exhausted in connection management processing of attack based traffic so that legitimate users will find a denial in connection establishment with the server. The peak value in our analysis has 225 active connection counts on FTP server under DDoS attack with 200 zombies as compared to average value of only 0.06 counts under baseline scenario. Moreover, increased botnet size exhibits more connection count load on the server.

In Fig. 13, we observe TCP delay and find that the attack scenario induces additional transport layer delay at server’s port which is about 25% more than the delay observed in baseline scenario. It shows that DDoS attack also makes the response of server slow in its connection establishment & maintenance capacity. Moreover, the increased magnitude of attack (increased size of the botnet) has comparatively larger delay effect on the server in the considered network.

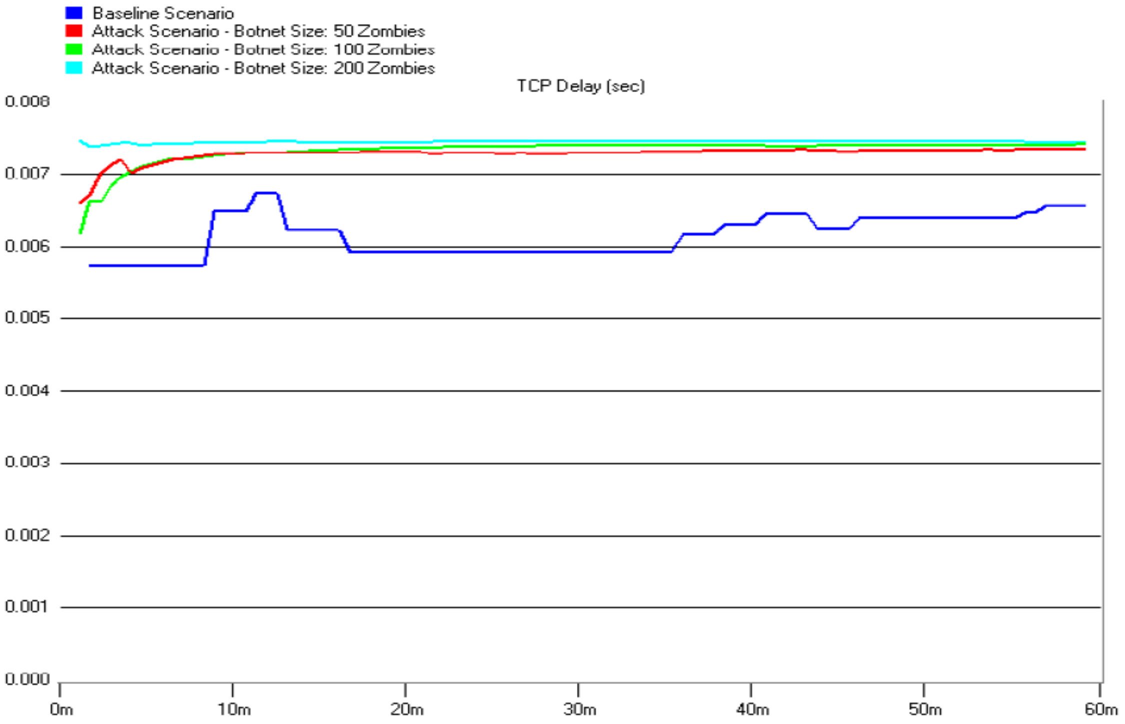


Fig 13: FTP Server – TCP Delay (sec)

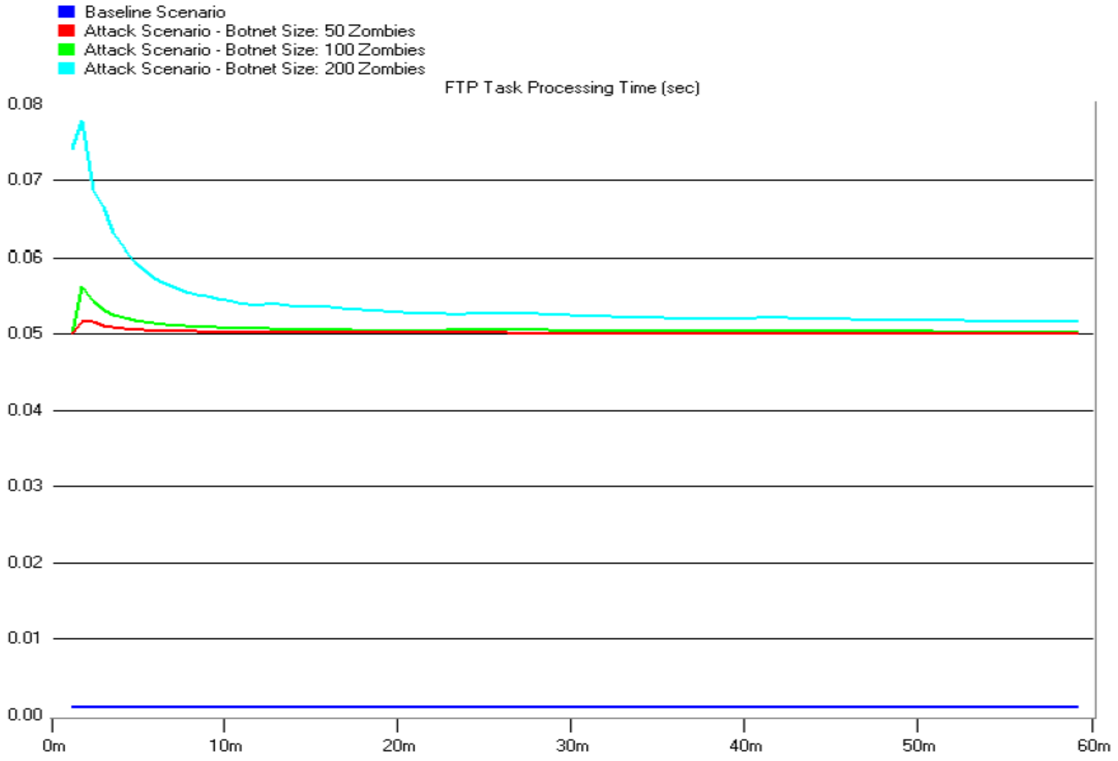


Fig. 14: FTP Server – Task Processing Time (sec)

5.3.4 Task Processing Time (sec)

In Fig. 14, task processing time of FTP server is observed. We find that task processing time greatly increases under attack scenario as compared to baseline scenario. It depicts that the server is made exhausted by sending huge amount of attack traffic for which it has to perform requested tasks. As a result, average processing time (in seconds) per task is increased, degrading services for legitimate requests.

A 50 fold increase is observed in average task processing time of the server when it becomes under DDoS attack. Moreover, the increased magnitude of attack (increased size of the botnet) induces more delay factor in average processing time per task of the server.

VI. Conclusion

In this paper, we provided a review on some common techniques of Distributed Denial of Service attacks and defenses with an emphasis on recently researched and proposed schemes of defense. We also discussed some statistics on DDoS attacks recorded in year 2012 Quarter-1 and presented simulation based performance analysis of an FTP server in scenario of an enterprise network under distributed denial of service attack. Simulations in OPNET showed noticeable variations in connection capacity, task processing and delay parameters of the attacked server as compared to the performance without attack. Botnet size effect on the obtained parameters was observed by considering three botnet sizes i.e. 50, 100 and 200 zombies. We get an idea that application layer DDoS attacks are increasing and their accurate detection is a difficult task and major challenge of future research.

References

[1] Mitrokotsa A, Douligeris C. Denial-of-Service Attacks. Network Security: Current Status and Future Directions (Chapter 8), Wiley Online Library, 2006:117-134.

[2] Zhang L, Yu S, Wu D, Watters P. A Survey on Latest Botnet Attack and Defense [C]. In: Proceedings of 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE, November 2011, 53-60.

[3] Beitollahi H, Deconinck G. Denial of Service Attacks: A Tutorial [R]. Electrical Engineering Department (ESAT), University of Leuven, Technical Report: 08-2011-0115, 2011.

[4] Raymond DR, Midkiff SF. Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses [M]. IEEE Pervasive Computing, 2008, 7(1):74-81.

[5] Pelechrinis K, Iliofotou M, Krishnamurthy SV. Denial of Service Attacks in Wireless Networks: The Case of Jammers [J]. IEEE Communications Surveys & Tutorials, 2011, 13(2):245-257.

[6] Kaur G, Chaba Y, Jain VK. Distributed Denial of Service Attacks in Mobile Adhoc Networks [J]. World Academy of Science, Engineering and Technology, 2011, 73:725-727.

[7] Tupakula U, Varadharajan V, Vuppala SK. Countering DDoS Attacks in WLAN [C]. In: Proceedings of 4th International Conference on Security of Information and Networks (SIN '11), ACM, November 2011, 119-126.

[8] Prolexic Technologies. Prolexic Attack Report Q1 2012. <http://www.prolexic.com>, April 2012.

[9] Agarwal PK, Gupta BB, Jain S, Pattanshetti MK. Estimating Strength of a DDoS Attack in Real Time Using ANN Based Scheme. Communications in Computer and Information Science, Springer, 2011, 157(part 6):301-310.

[10] Gupta BB, Joshi RC, Misra M, Jain A, Juyal S, Prabhakar R, Singh AK. Predicting Number of Zombies in a DDoS Attack Using ANN Based Scheme. Communications in Computer and Information Science, Springer, 2011, 147(part 1): 117-122.

[11] Li J, Liu Y, Gu L. DDoS Attack Detection Based On Neural Network [C]. In: Proceedings of 2nd International Symposium on Aware Computing (ISAC), IEEE, November 2010, 196-199.

[12] Chao-yang Z. DoS Attack Analysis and Study of New Measures to Prevent [C]. In: Proceedings of International Conference on Intelligence Science and Information Engineering (ISIE), IEEE, August 2011, 426-429.

[13] Yuan J, Mills K. Monitoring the Macroscopic Effect of DDoS Flooding Attacks [J]. IEEE Transactions on Dependable and Secure Computing, 2005, 2(4):324-335.

[14] Thatte G, Mitra U, Heidemann J. Parametric Methods for Anomaly Detection in Aggregate Traffic [J]. IEEE/ACM Transactions on Networking, 2011, 19(2):512-525.

[15] Li K, Zhou W, Li P, Hai J, Liu J. Distinguishing DDoS Attacks from Flash Crowds Using Probability Metrics [C]. In: Proceedings of 3rd Intl' Conference on Network and System Security (NSS '09), IEEE, October 2009, 9-17.

[16] Xie Y, Yu SZ. Monitoring the Application-Layer DDoS Attacks for Popular Websites [J]. IEEE/ACM Transactions on Networking, 2009, 17(1):15-25.

[17] Ahn LV, Blum M, Langford J. Telling humans and computers apart automatically [J]. Communications of the ACM, 2004, 47(2):56-60.

[18] Tian H, Bi J, Jiang X. An adaptive probabilistic marking scheme for fast and secure traceback [J]. Networking Science, Springer (Online First), 2012, DOI: 10.1007/s13119-012-0007-x.

[19] Khanna S, Venkatesh SS, Fatemieh O, Khan F, Gunter CA. Adaptive Selective Verification: An Efficient Adaptive Countermeasure to Thwart DoS Attacks [J]. IEEE/ACM Transactions on Networking, 2012, 20(3):715-728.

[20] Thapngam T, Yu S, Zhou W, Makki SK. Distributed Denial of Service (DDoS) detection by traffic pattern analysis [J]. Peer-to-Peer Networking and Applications, Springer (Online First), 2012, DOI: 10.1007/s12083-012-0173-3.

[21] Gilad Y, Herzberg A. LOT: A Defense Against IP Spoofing and Flooding Attacks [J]. ACM Transactions on Information and System Security, 2012, 15(2) (article 6).

[22] Aamir M, Zaidi M, Mansoor H. Performance Analysis of DiffServ based Quality of Service in a Multimedia Wired Network and VPN effect using OPNET [J]. International Journal of Computer Science Issues, 2012, 9(3):368-376.

Authors' Profiles

Muhammad Aamir is M.S. in Information Technology from SZABIST, Karachi, Pakistan. His research interests include Computer Networks, IP based Communication Systems and Network Security. He holds the student membership of IEEE.

Muhammad Arif is pursuing B.S. degree in Telecommunication from SSUET, Karachi, Pakistan. His research interests are Data Communication, RF Technology and Image Processing.

How to cite this paper: Muhammad Aamir, Muhammad Arif,"Study and Performance Evaluation on Recent DDoS Trends of Attack & Defense", International Journal of Information Technology and Computer Science(IJITCS), vol.5, no.8, pp.54-65, 2013. DOI: 10.5815/ijitcs.2013.08.06