International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October2016

Study And Performance Evaluation On Recent Ddos Trends Of Defense On Web Servers

[1]Amadi E.C, [2]Igwe Chinedu, [3]Uduma Kalu

[1-3]Department of information management technology, Federal University of TechnologyOwerri (FUTO), Nigeria.

Abstract

The traditional architecture of World Wide Web is vulnerable to serious kinds of threats including distributed denial of service (DDoS) attacks. Denial of service (DoS) attacks are very common in the world of internet today. The attack aims to deny or degrade normal services for legitimate users by sending huge traffic to the victim (machines or networks) to exhaust services, connection capacity or the bandwidth. The attackers are now quicker in launching such attacks because they have sophisticated and automated DDoS attack tools available which require minimal human effort, as such, there is now an increasing pace of DDoS attacks; This has made servers and network devices on the internet at greater risk than ever before. Due to the same reason, "organizations and people carrying large servers and data on the internet are now making greater plans and investigation to be secure and defend themselves against a number of cyber-attacks including Distributed Denial of Service."(A. Mitrokotsa, and C. Douligeris [2006]).
This paper is a study and performance evaluation on recent DDoS trends of defense on web servers. The paper presents a survey of distributed denial of service attacks and the methods that have been proposed for defense against these attacks. We discussed the introduction of DDoS attacks, DDoS attack history and incidents, DDoS attack tools, and classification of various attack and defense mechanisms. We conclude by highlighting opportunities for an integrated solution to solve the problem of distributed denial of service attacks

Keywords: Distributed Denial of Service (DDOS), DDOS Attacks, DDOS incidents, Defense on web servers.

1.0 Introduction.

The World is highly dependent on the Internet today, and so the availability and security of the Internet is very critical for the socio-economic growth of the society. In our world today, Internet has changed the way of traditional essential services such as banking, transportation, power, health, etc. are being operated. These operations are being replaced by cheaper, more efficient Internet-based applications. It is all because of rapid growth and success of Internet in every sector.

Unfortunately with the growth of Internet, attacks on Internet has also increased incredibly fast. The rapid development of the Internet over the past decade appeared to have facilitated an increase in the incidents of online attacks [B. B. Gupta, R. C. Joshi, Manoj Misra, 2012]. One such powerful and harmful attack is the denial of service (DoS) attack. Distributed Denial-of-service attack is one of them, which poses immense threat on the availability of services from the webserver.

A Distributed Denial of Service (DDoS) attack is a large-scale, coordinated attack on the availability of services of a victim system or network resource, launched indirectly through many compromised computers on the Internet. The DDoS attack is launched by sending an extremely large volume of packets to a target machine through the simultaneous cooperation of a large number of hosts that are distributed throughout the Internet. The attack traffic consumes the bandwidth resources of the network or the computing resource at the target host, so that legitimate

requests will be discarded. The impact of these attacks can vary from minor inconvenience to the users of a web site, to serious financial losses to companies that rely on their on-line availability to do business (Mirkovic, Prier and Reiher, 2002; Papadopoulos, Lindell, Mehringer, Hussain and Govindan, 2003). DDoS is a type of attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack. DDoS flooding attacks are typically explicit attempts to disrupt legitimate users' access to services. Attackers usually gain access to a large number of computers by exploiting their vulnerabilities to set up attack armies (i.e., Botnets). Once an attack army has been set up, an attacker can invoke a coordinated, large-scale attack against one or more targets. A software program controls the computers and for specific purposes, known as ―bots. Bots are small scripts that have been designed to perform specific, automated functions. Bots are utilized by agents for Web indexing or spidering, as well as to collect online product prices or to performing such duties as chatting. However, bots are negatively associated with remote access Trojan Horses (e.g., Zeus bot) and zombie computers that are created for less favorable purposes [H. R. Zeidanloo, A. A. Manaf, 2009]. Bots in large quantities provide the power of a computer to create prime tools for such activities as the widespread delivery of SPAM email, click-fraud, spyware installation, virus and worm dissemination, and DDoS attacks (e.g., black energy bot) [C. Douligeris and D. N. Serpanos, 2007]. DDoS attacks usually take advantage of the weaknesses of a network layer, particularly, SYN, UDP, and Internet control message protocol (ICMP) flooding. Such attacks encroach the network bandwidth and resources of the victim, thus facilitating the denial of legitimate access.

Distributed Denial-of-service attacks occur almost every day, and the frequency and the volume of these attacks are increasing day by day. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack. Distributed Denial of Service (DDoS) attacks are one of the biggest concerns for security professionals. DDoS attacks are among the most difficult problems to resolve online, especially, when the target is the Web server.

1.1 DDoS Attack Background History and Incidents

Distributed denial of service attacks (DDoS) pose a great threat to the Internet. A recent DDoS attack occurred on 20 October, 2002 against the 13 root servers that provide the Domain Name System (DNS) service to Internet users around the world. Although the attack only lasted for an hour and the effects were hardly noticeable to the average Internet user, it caused seven of the 13 root servers to shut down, demonstrating the vulnerability of the Internet to DDoS attacks (Peng, Leckie and Kotagiri, 2003). Distributed denial of service attacks occur when numerous subverted machines (zombies) generate a large volume of coordinated traffic toward a target, overwhelming its resources. DDoS attacks are advanced methods of attacking a network system to make it unavailable to legitimate network users. These attacks are likely to become an increasing threat to the Internet due to the convenience offered by many freely available user-friendly attack tools. Furthermore, attackers need not fear punishment, as it is extremely difficult to trace back the attack and locate even the agent machines, let alone the culprits who infected them.

DDoS attacks continue to be one of the major cyber threats. Security professionals estimate that DDoS attacks are one of the biggest threats and they continue to increase in popularity for hackers. New World Hackers are among the group using DDoS attacks. The popular Anonymous hacking group often uses DDoS attacks to bring down large websites. The group has attacked Google, PayPal, Amazon, and several government entities. Some were successful while others failed. The ones who failed had some of the best security on the market. For instance, attacks against Google failed due to their innovative security that detects attempted DDoS attacks.

What makes these threats effective is that most companies don't have the security defenses to detect and protect against these attacks. Without the right defenses, company resources and data are wide open to DDoS as well as other cyber threats.

1.2 Overview of How DDoS Attacks Work

As defined by the World Wide Web Security FAQ: A Distributed Denial of Service (DDoS) attack uses many computers to launch a coordinated Denial of Service (DoS) attack against one or more targets. The operating systems and network protocols are developed without applying security engineering which results is providing hackers a lot of insecure machines on Internet. These insecure and unpatched machines are used by DDoS attackers as their army to launch attack. These compromised machines are called Masters/Handlers or Zombies and are collectively called bots and the attack network is called botnet in hacker's community. An attacker or hacker gradually implants attack programs on these insecure machines. Hackers send control instructions (from a menu of different varieties of flooding attacks) to masters, allowing them to control all these burgled zombies to launch coordinated attacks on victim sites. These attacks typically exhaust bandwidth, router processing capacity, or network stack resources, breaking network connectivity to the victims. Figure 1.1 below illustrates how DDoS Attacks Work.

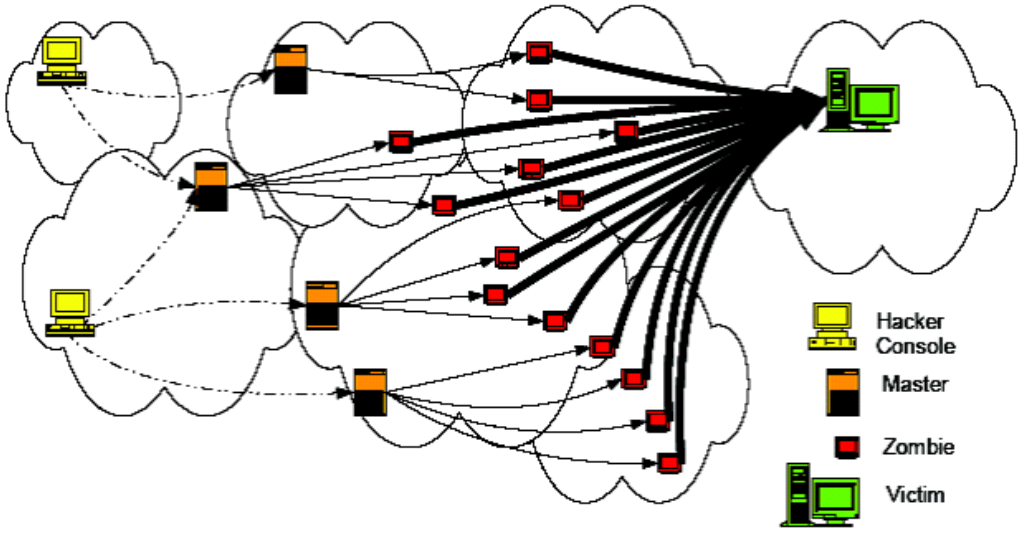

Fig 1.1: How DDoS Attacks Work; Attack Modus Operandi (Daljeet and Monika 2014).

1.3 Reasons for DDoS Attacks

The main aim of a DDOS attack include the following;

- To harm on victim, either for personal reasons like against home computer or for revenge purpose, for secret information theft by damaging victim's resources.
- Attack to gain popularity by making successful attack on popular web servers which give the attack fame in the hacker community.
- Political motive; some attackers usually belongs to the military or terrorist organizations of a country and they are politically motivated to attack a wide range of critical sections of another country (Dhruv & Petal 2014). So, we can categorize DDOS attack based on motivation of the attackers into following categories which includes.

1.4 Characteristics of DDoS attacks

The following are several features of DDoS attacks that hinder their successful detection and defenses:

- DDoS attacks generate a large volume flow to overwhelm the target host. The victim cannot protect itself even if it detects this event. So the detection and defence of DDoS should ideally be near the source of the attack or somewhere in the network.
- It is difficult to distinguish attack packets from legitimate packets. Attack packets can be identical to legitimate packets, since the attacker only needs volume, not content, to inflict damage. Furthermore, the volume of packets from individual sources can be low enough to escape notice by local administrators. Thus, a detection system based on a single site will have either high positive or high negative rates.
- DDoS traffic generated by available tools often has identifying characteristics, making the detection based on statistics analysis possible. However, given the inherently busty nature of Internet, detecting DDoS attacks is error prone.

1.5 Types of DDoS Attacks on Web Servers

In this section, we will discuss most of the DDoS attacks on web servers according to Raghav et al, (2015).

UDP Floods Attack: Transport layer-UDP is a transport layer protocol that is used for DDoS attack. UDP packets flood the random or specified ports of the victim system for unknown applications and if the application is not found then the victim replies with the ICMP Destination Unreachable Packet resulting in system slowdown.

HTTP Flood Attack: This attack uses HTTP GET or POST requests to block the resources of the web server or application. For instance, a request to download a large file from bot to server can significantly consume victim's resources. Application layer-Overloads the specific services of Application level infrastructure.

NTP Amplification: Attackers attack the victim servers with UDP traffic with the help of Network Time Protocol (NTP) servers.

ICMP Flood Attack: Network layer- uses ICMP which is a network layer protocol) to block the network bandwidth and firewall with extra load. ICMP ECHO REQUEST packets flood the victim's system i.e. sending m /packets as fast as possible without waiting for the reply. Hence, it saturates the bandwidth of victim's network connection.

Ping of Death: In Ping of Death attack victim system ends up with the IP packets which are larger than 65,535 bytes when reassembled from the malicious fragments.

ARP Poisoning: Address Resolution Protocol(ARP) Spoofing Attack is carried when attacker sends false ARP packets to gateway informing that its MAC address should be associated with the target's IP address. Hence, allowing attacker to drop or not forwarding the packets to the destination.

SIP Flood Attack: Application layer-Targets login pages with random user Ids and passwords. Attackers flood the Session Initiation Protocol (SIP) proxy servers with SIP INVITE packets with the help of Botnet. It consumes the network bandwidth and server resources of the server making it incapable of providing VOIP service.

Smurf Attack: Attacker sends ICMP ECHO REQUEST packets (with return address spoofed to victim's IP address) to network amplifier and which again sends the packets to the systems within the broadcast address range. These systems send the ICMP ECHO REPLY to the victim which saturates the bandwidth of connection.

PUSH+ACK Attack: In this attack multiple agents send TCP packets to the victim system with PUSH and ACK bits set to zero. Hence, victim unloads all the data in the TCP buffer which leads to system crash.

1.6 Classification of DDoS Attacks

There are two main classes of DDoS attacks: bandwidth depletion and resource depletion attacks.

A bandwidth depletion attack is designed to flood the victim network with unwanted traffic that prevent legitimate traffic from reaching the victim system.

A resource depletion attack is an attack that is designed to tie up the resources of a victim system. This type of attack targets a server or process at the victim making it unable to legitimate requests for service (Huang, Kobayashi and Liu, 2003). Other classes of DDoS attacks include:

Isotropic distribution of attack traffic: In this type of attack, attackers try to distribute attack traffic uniformly throughout all ingress points of attacked autonomous system, in order to defeat aggregate based defense.

Non-isotropic distribution of attack traffic: In this type of attack, attack traffic is aggregated in certain parts of Internet.

Network protocols based classification of DDoS attacks: This basically divide DDoS attacks into TCP, UDP, and ICMP protocols as for semantic and brute force attacks either of these protocol packets are used.

Semantic DDoS attacks: This classification is on the basis of attack packets used. Semantic DDoS attacks are normally launched with control packets like TCP SYN, TCP FIN, ICMP echo packets whereas for launching brute force DDoS attacks control as well as data packets like HTTP, FTP (involving TCP), UDP, and ICMP bogus packets can be used.

2.0 Mitigating DDoS Attacks

This section will discuss some methods that will help prevent the spread of DDoS attacks, by limiting the distribution of the tools and/or limiting the propagation of the offending attack packets. Preventing DDoS attacks is always the first choice of commercial and research organizations as Prevention is a mechanism which stops the attacks before they are actually launched. The Software Engineering Institute recommended the following options in preventing DDoS Attacks:

- Implement router filters. This will lessen your exposure to certain denial-of-service attacks. Additionally, it will aid in preventing users on your network from effectively launching certain denial-of-service attacks.
- If they are available for your system, install patches to guard against TCP SYN flooding. This will substantially reduce your exposure to these attacks but may not eliminate the risk entirely.
- Disable any unused or unneeded network services. This can limit the ability of an intruder to take advantage of those services to execute a denial-of-service attack.
- Enable quota systems on your operating system if they are available. For example, if your operating system supports disk quotas, enable them for all accounts, especially accounts that operate network services. In addition, if your operating system supports partitions or volumes (i.e., separately mounted file systems with independent attributes) consider partitioning your file system so as to separate critical functions from other activity.
- Observe your system performance and establish baselines for ordinary activity. Use the baseline to gauge unusual levels of disk activity, CPU usage, or network traffic.

- Routinely examine your physical security with respect to your current needs. Consider servers, routers, unattended terminals, network access points, wiring closets, environmental systems such as air and power, and other components of your system.
- Use Tripwire or a similar tool to detect changes in configuration information or other files.
- Invest in and maintain "hot spares" - machines that can be placed into service quickly in the event that a similar machine is disabled.
- Invest in redundant and fault-tolerant network configurations.
- Establish and maintain regular backup schedules and policies, particularly for important configuration information.

Krishan Kumar, R.C. Joshi, and Kuldip Singh suggested three precautions against DDoS attacks:

(a) The ISPs are strongly recommended to install ingress filters to stop IP address spoofing.

(b) The end host should repair their security holes as soon as possible, especially for well-known software and protocol bugs.

(c) The end hosts are encouraged to install the Intrusion Detection System (IDS) to prevent from being compromised by the adversary.

2.1 Classification of DDoS Defense Mechanisms

DDoS defense mechanisms can be classified as follows:

i. **DDoS Attack Prevention:** Attack prevention methods try to stop all well-known signature based and broadcast based DDoS attacks from being launched in the first place or edge routers, keeps all the machines over Internet up to date with patches and fix security holes. Signature of the packets is matched with the existing database consisting of known attack patterns at each edge router [Leiner, B.M., Cerf, V.G., 2009].

There are different approaches to prevent DDoS attack against target machine, these include the following:

- Filtering all packets entering and leaving the network protects the network from attacks conducted from neighboring networks, and prevents the network itself from being an unaware attacker. This measure requires installing ingress and egress packet filters on all routers. It is used to filter spoofed IP address but approaches to prevent it needs global implementation that is not practical [Park, K., Lee, H. (2001), Peng, T., Leckie, C., Ramamohanarao, K. (2003)].
- Firewall can allow or deny protocols, ports or IP addresses but some complex attack like on port 80 cannot be handled by it because it is unable to distinguish between legitimate traffic and DDoS attack traffic. Only those attacks can be identified whose signatures are already there in the database. A slight variation from the original attack pattern can leave the attack undetected. Also new attacks cannot be detected [Peng, T., Leckie, C., Ramamohanarao, K. (2003)].

ii. **DDoS Detection:** Attack detection aims to detect an ongoing attack as soon as possible without misclassifying and disrupting legitimate traffic. DDoS detection approaches can be classified as follows:

- **Signature based detection:** Signature based approach employs a priori knowledge of attack signatures. The signatures are manually constructed by security experts analyzing previous attacks and used to match with incoming traffic to detect intrusions. SNORT [Roesch, M. (1999)] and Bro [Paxson, V. (1999)] are the two widely used signature based detection approaches.

- **Anomaly based detection:** Anomaly-based system treats any network connection violating the normal profile as an anomaly. A network anomaly is revealed if the incoming traffic pattern deviates from the normal profiles significantly [Gupta, B.B., Joshi, R.C., Misra, M. (2009)]. Detecting DDoS attacks involves first knowing normal behavior of our system and then to find deviations from that behavior.

iii. **DoS Attack Mitigation and Tolerance:** This aims at reducing the effect of the attack on victim machine during DDoS attack [Gupta, B.B., Joshi, R.C., Misra, M. (2009)].

3.0 RECENT DDOS TRENDS OF DEFENSE

In this section is a critical survey of recent DDoS trends of defense on various networks connected to the Internet.

3.1 Old Dimensions of Defense against DDoS Attacks

Traditional & older DDoS detection and mitigation methods have been used for many years e.g. trace back, entropy variations, common traffic anomalies & packet filtering techniques.

3.2 New Dimensions of Defense against DDoS Attacks

In table 1, some common methods of DDoS detection and mitigation are mentioned which correspond to new dimensions of defense against DDoS attacks.

Table 1: Some common DDoS mitigation techniques

Basis of Defense	**Method**
Neural Networks	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	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	Packet Forwarding / TCP Blocking in routers. TPM hardware chip in switches.

(Source: Muhammad Aamir and Muhammad Arif, 2013)

Table 2: Some evolutionary DDoS mitigation techniques against application layer attacks

Basis of Defense	**Method**
Network-wide monitoring	Observing shift in spatial-temporal patterns of network traffic on occurrence of DDoS attack.
Changes in network's aggregate traffic anomalies	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	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	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	Presenting CAPTHA puzzle images to clients to avoid machine based automated DDoS attacks.

(Source: MECS *I.J. Information Technology and Computer Science,* 2013, 08, 54-65)

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 (Muhammad Aamir and Muhammad Arif, 2013).

Fig. 2: View of CAPTCHA test (Muhammad Aamir and Muhammad Arif, 2013)

Table 3, highlighted some latest research efforts against DDoS attacks to provide more insight of related information to readers. All research efforts cited in table 3 have been published not before year 2012.

Table 3: Some latest research efforts on DDoS mitigation

Scheme	**Method**
Adaptive Probabilistic Marking (APM)	Observing TTL fields of packets to initiate proposed trace back scheme and reconstruction of attacking path on occurrence of DDoS attack.
Adaptive Selective Verification (ASV)	Increasing legitimate request rate (in adaptive manner up to a threshold level) in consecutive time windows by legitimate clients on occurrence of DDoS attack.
Traffic Pattern Analysis	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	Establishing tunnel between two communicating gateways through proposed lightweight protocol to prevent traffic against IP spoofing and flooding attacks.

(Source: MECS *I.J. Information Technology and Computer Science,* 2013, 08, 54-65)

Conclusion

Since the first denial of service (DoS) was launched in 1974, distributed denial of service (DDoS) and other DoS attacks have remained among the most persistent and damaging cyber-attacks. These attacks reflect hackers' frustratingly high levels of tenacity and creativity and create complex and dynamic challenges for anyone responsible for cyber security.

During Internet design, the functionality aspect was of much concern rather than security, due to which this design opens up several security issues that create a room for various attacks on the Internet. Internet security has several aspects such as confidentiality, authentication, message integrity and non-repudiation. Availability is one of the main aspects of Internet security. Denial of service and its variant distributed denial of service attack target the availability of services provided by the webserver.

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. 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

Jose Nazario, , BlackEnergy DDoS Bot Analysis, Arbor Networks, 2007. Available at: http://atlas-public.ec2.arbor.net/docs/BlackEnergy+DDoS+Bot+Analysis.pdf.

B. B. Gupta, R. C. Joshi, Manoj Misra, ANN Based Scheme to Predict Number of Zombies involved in a DDoS Attack, International Journal of Network Security (IJNS), vol. 14, no. 1, pp. 36-45, 2012.

H. R. Zeidanloo, A. A. Manaf, "Botnet command and control mechanisms," in the proc. of Second International Conference on Computer and Electrical Engineering, (ICCEE '09), pp. 564-568, 2009.

HUANG, Q., KOBAYASHI, H. and LIU, B. (2003): Analysis of a new form of distributed denial of service attack, in *Proceedings of CISS03, the 37th Annual Conference on Information Science and Systems*, Johns Hopkins University, Baltimore, Maryland.

C. Douligeris and D. N. Serpanos, "Network security: current status and future directions," Wiley-IEEE Press, 2007.

Arbor Sert, " DDoS and Security Reports: The Arbor Networks Security Blog," 2011.

E. Mills, ―DOJ, FBI, entertainment industry sites attacked after piracy arrests ", 2012.

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

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.

Gupta, B.B., Joshi, R.C., Misra, M.: Defending against Distributed Denial of Service Attacks: Issues and Challenges. Information Security Journal: A Global Perspective 18(5), 224–247 (2009)

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

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

MIRKOVIC, J., PRIER, G. and REIHE, P. (2003): Alliance formation for DDoS defence, in *Proceedings of the New Security Paradigms Workshop, ACM SIGSAC*, Ascona, Switzerland, 11–18.

MIRKOVIC, J., PRIER, G. and REIHER, P. (2002): Attacking DDoS at the source, in *Proceedings of ICNP 2002*, Paris, France, 312–321.

Peng, T., Leckie, C., Ramamohanarao, K.: Protection from distributed denial of service attack using history-based IP filtering. In: Proceedings of IEEE International Conference on Communications (ICC 2003), Anchorage, AL, vol. 1, pp. 482–486 (2003)

Roesch, M.: Snort-Lightweight Intrusion Detection for Networks. In: Proceedings of the USENIX Systems Administration Conference (LISA 1999), pp. 229–238 (November 1999)

Gupta, B.B., Joshi, R.C., Misra, M.: Defending against Distributed Denial of Service Attacks: Issues and Challenges. Information Security Journal: A Global Perspective 18(5), 224–247 (2009)

Muhammad Aamir and Muhammad Arif, 2013: MECS *I.J. Information Technology and Computer Science,* 2013, 08, 54-65