Vol. (1) No. (1) March 2018

JK Research Journal in Mathematics and Computer Sciences

Investigating the denial of service attack: A major threat to internet and the security of information

Suhail Qadir Mir[1] *Dr. Irshad Ahmad Mir[2] Dr. Bilal Maqbool Beiigh[3]

[1]*Department of Computer Science, University of Kashmir, Srinagar, J&K-India*
[2]*Govt. College for Women, M.A Road Srinagar, J&K- India*

Abstract: The security of Information systems is becoming a pressing need for the organizations & research community in the recent years. Information Security must ensure the confidentiality, integrity and the availability of the information and the information processing & transmission resources. With the advent of the Internet out of these three attributes the statistics shows that the information availability has been compromised extensively in the recent years. This is due to the evolving techniques of DoS (Denial of service) and DDoS (Distributed Denial of Service) attacks. This paper addresses evolving mechanisms of DoS and DDoS attacks and investigates the compromises made on information availability by these DoS Attacks over the last decade and a half. Further this paper presents the development on preventive measures to be applied as a countermeasure. The Section 1 presents the introduction with the growing number of security incidents in a graphical for followed by the DoS and DDoS Attack mechanism in section 2. Section 3 investigates the recent Attack Size in the past decade and the reasoning behind. Section 4 presents an abstract preventive profile for DoS attacks and section 5 concludes the study with future enhancements to be made.

Keywords: *Information Security; Availability; Denial of Service; Information Systems; Security Threat*.

Introduction

With the rapid growth and success of Internet in the last two decades, the Internet has become a game changer in almost every field and has significantly changed its traditional role. With the changing times it has no longer remained just a tool for the researchers or the communicators. Governments are using Internet in *e-Governance* and in number of ways to provide information to the citizens of a nation or to the World at large and this trend is a successful one **[1]** and as expected Governments in future will continue the use of Internet to provide better and transparent governance. Enterprises use Internet for *e-Commerce,* information exchange with business units, partners, suppliers and customers in a very efficient and smooth manner. Research and Educational Institutions use Internet as a tool for assisting in problem solving,

as a platform for collaboration and spreading their Discoveries and Inventions all over the world. Now with such use it is evident that organizations are becoming more and more dependent upon Internet and network based Information Systems.

iamir@uok.edu.in
*Irshad Ahmad Mir

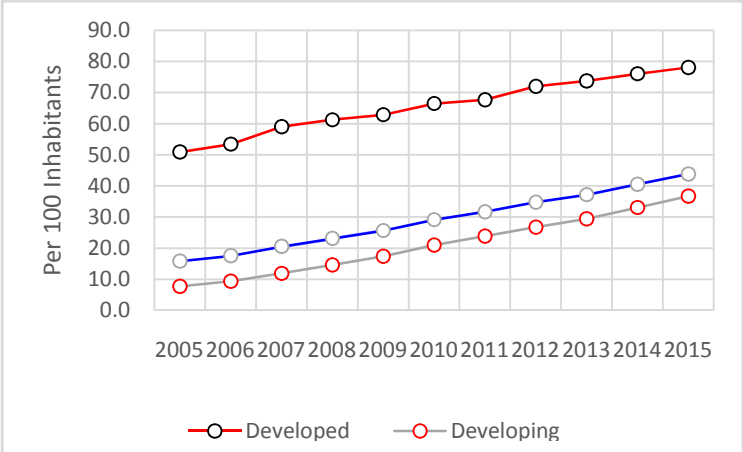

Figure 1: Internet users per 100 inhabitants, world-wide 2005-2015.

Because of its wider reach and its ease it has given them the possibility of growing at a rapid **pace [1, 2, 3, and 4]**. Now with such ease of access and dependence upon Information and Information Resources, the Organizations are exposed to great risk **[5]**, if the access to an Information System is disrupted, manipulated or destructed. The risks are that the valuable Information will be lost, stolen, changed or misused. Unfortunately with the good i.e. Growth of the Internet, came the bad i.e. The Attacks, they have also progressed and increased at a parallel rate.

Figure 1shows the use of internet in the last ten years **[6]**. As expected the graph complements the fact that Internet has grown consistently every year. Now in comparison to this graph, Figure 2,astudy carried out by United States Government **[31]** shows that the growth in cyber security incidents from 2005-2015 in United States, country with maximum number of Internet users . Both the figures and some data from **[12]** prove the fact, that with the growth of the Internet, the attacks have also increased significantly.

An important situation here is, nation's essential services such as, banking system, transportation, power, healthcare, and defense, their conventional way of operations are being replaced on a step-by-step basis by cheaper, more efficient Internet and Network based applications. Historically speaking whenever a nation has attacked any other nation, it is always seen as an attack on a nation's critical services and for that matter the attacking nation has to cross into the physical boundaries of the victim nation. An action of this sort can be blocked and averted by a nation's

security services. However the connectivity of nation's globally through Internet makes the physical boundaries look meaningless to a large extent, as Internet based attacks can be launched from anywhere in the world to disrupt these critical resources

. Some attacks can also bring huge physical destruction to a nation in today's world, because some critical energy resources and nuclear resources are also network controlled in today's world of Science and Information Technology. Although the nuclear arsenal of a nation is under heavy security cover, usually the most secure location in the nation or *Security by Obscurity* **[21]**, but still there have been attacks on such facilities, like recently in 2010 the attack on IRAN's Nuclear facility by a virus named as *STUXNET* **[28],**more of a cyber-weapon with serious physical consequences than just a virus. Unfortunately no Internet based service or any computer or a network is immune from Cyber-attacks, because most of these attacks are based on using ordinary protocols and

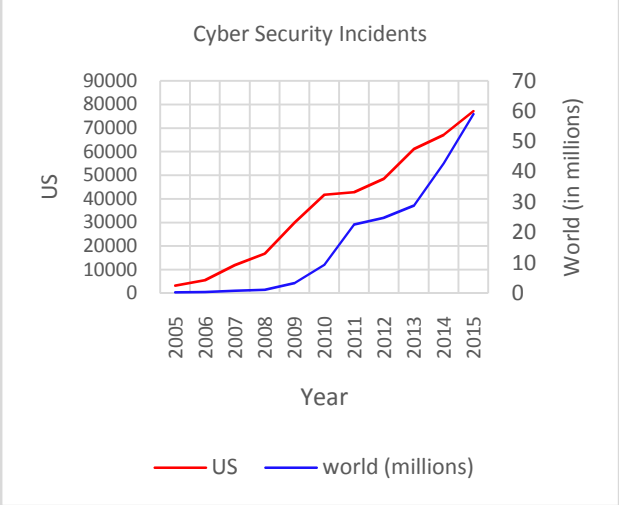

Figure 2:Growing number of Cyber Security incidents reported in US and Worldwide.

attacks, but no remedy for removing them completely. Therefore, the *Security* of the Internet is not confined to information sharing and online businesses only, but it is a serious issue of national security and should be dealt with importance. Since Internet is actually the main information resource and everything revolves around the *Information* i.e. Information creation, processing, access, transmission, reception etc. No matter which application or service we are using on Internet we are always doing one of the above things with the *Information.* Given the risks and attacks to Internet,

Information Systems or any other information resource a user always expects certain assurances before indulging into serious use of the same. The User expects the following things:

1. The Information used is reliable and coming from a trusted and known source. If the source is unknown, there should be enough mechanisms in place to prove that the source is not a malicious one.

2. The Information and related resources are available and accessible, whenever they are needed.

3. Information processing and sharing will be dealt only in the manner which they know and which they expect. Any unexpected situation may be a threat.

The information processing systems in use will process Information in a timely and reliable manner.

Denial of Service Attack Mechanism

Denial of Serviceattack is the major threat to the networks, computers and communications systems today .They have negatively affected services to organizations, individual users, critical Internet infrastructures etc., over the past decade or so **[8]**.*DoS Attack* (including DDoS)is a malicious attempt to disrupt, degrade or prevent the availability **[25]**of an Information resource to the legitimate users. The resources here are disk space, CPU time, the network b9andwidth, memory and other structures like static memory or memory buffers **[13].** DoS attacks are intentional almost all of the times but sometimes unintentional human errors during the designing process or programming, can lead to DoS attacks **[16].** The DoS attack that completely prevents the availability of a resource is called as the *Destructive DoS attack*. While as if the attack is only successful in bringing down the performance of the resource, it's called as a *Degrading (non-destructive) DoS attack*. A DoS attack can be executed from single sour9ce or from multiple sources either as a *logic attack* or as a *flooding attack***[23].** A Logic DoS attack is based on exploiting vulnerability or a security hole in the target system. For example in the Internet Protocol (IP) packet, the Pay Load data size can be modified which may crash an operating system, due to a fault in the OS software. Figure 3 illustrates a common DoS attack scenario in which an *Attacker* (attack machine) sends large number of malicious packets to the *Victim* computer. Because of this attack the legitimate clients

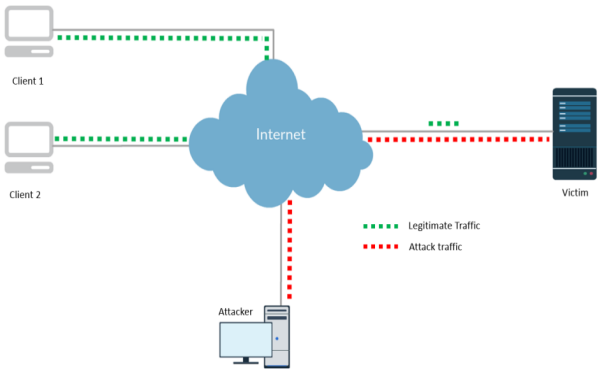

Figure 3: Denial-of-service attack plot.

Client 1 and *Client 2* are denied service from the Victim machine. An attacker always keeps itself anonymous and controls some other machine for their work or uses a forged identity, so most likely the attacker machine here is not the real attacker machine but is an *agent machine* recruited by the Attacker.

A flooding DoS attack on the other hand employs brute force. Legitimate looking but unwanted traffic is sent in huge volumes towards the victim. This results in resources being wasted on illegitimate and false requests. Network bandwidth, data structures like memory allocations are filled with fake data, processing power is wasted on handling of fake requests. These kinds of attacks can be amplified and attacks can be executed and run in a coordinated fashion from multiple sources all over the globe. An attack of this nature from multiples sources is called as *Distributed denial of service attack(DDoS). A DDoS* attack traffic usually comes from a large number of compromised hosts.

These attack packets arrive at the victim in such huge numbers that some critical resources like CPU time, network bandwidth, memory buffers etc. are exhausted is a rapid manner. The huge number of packet arrival either crashes the victim or keeps the victim busy handling the traffic so that the legitimate users are deprived of the service provided by the victim machine. The legitimate clients are deprived as long as the attack lasts. Figure 4 illustrates a common DDoS attack scenario in which the attacker machines *Attacker 1, Attacker 2* and *Attacker 3* send large number of malicious packets to the

Victim computer. Because of this attack the legitimate clients *Client 1* and *Client 2* are denied service from the Victim machine.

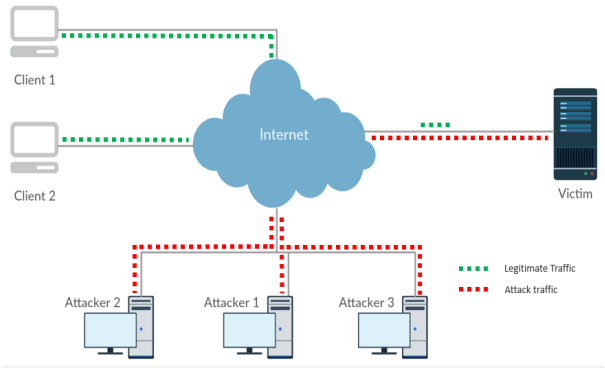

Figure 4: Distributed denial-of-service attack plot.

These compromised hosts have a hierarchy, the bad guy better known as the Attacker controls the *Masters* (also known as handlers), which in turn control a much bigger in number, an army of *Agents*(also known as zombies or daemons). The Agents are handled by masters and masters are handled by the attacker himself to carry out an attack of distributed nature against the victim. *Master (or handler)* is *a* compromised host whose job is to handle and control the working of a large set of agents. *Agent (or zombies or daemons)* is a compromised host whose job is to send attack traffic towards the victim during the DoS attack. A network of this sophistication which contains a main controller (the attacker), masters and agents organized in a structured way i.e. hierarchically is referred to as the *Botnet***[11].** The Botnet is controlled by the owner using software called as Command and Control (C&C) **[14].** Figure 5 gives us the large scale DDoS attacks (above 300 GBps) by 5 lethal botnets recorded since 2014**[7]**.

The main reason that makes DoS attacks attractive and easy to carry out for the attackers is that there are enough automatic tools available to carry out these attacks **[15]**. Without any expert knowledge one can easily carry out these attacks using these tools.

DoS Attacks in Real World

During the last decade and a half, since the occurrence of the first DoS attack **[7],** they have grown in stature significantly.

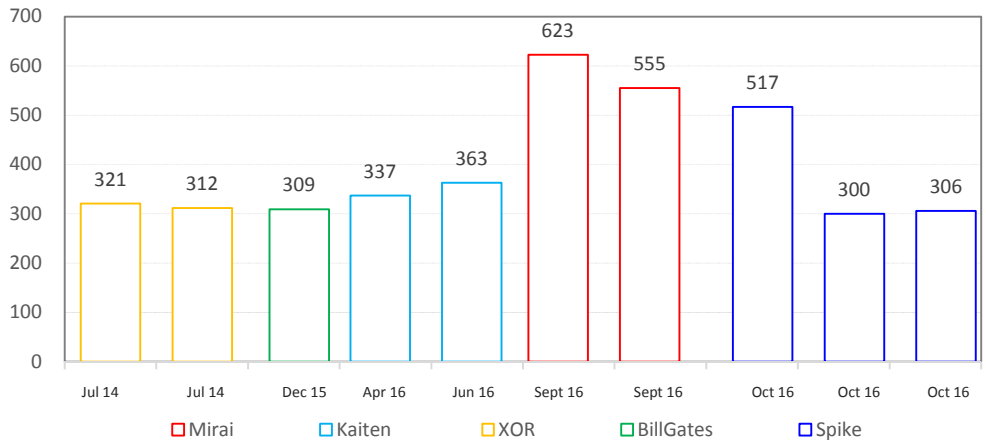

Figure 5: 5 lethal botnets in action in recent years(Data rate Gbps).

A DDoS attack under 10Gbps is too mainstream these days. DDoS attack reported a decade ago attacked at the rate of 8Gbps-this year the attack rate has increased exceptionally. The largest attack reported last in 2016, 2015 and 2014 was 600, 500 and 400 Gbps respectively as reported by ARBOR Networks**[8]**. An analysis of the peak DDoS attacks in the period 2004-2016 is shown in the figure 6. Some other attacks that were reported in the same report were of the rates of 300 Gbps, 200 Gbps and 170 Gbps and there are six more that crossed the 100 Gbps threshold. The reasons for the attacks lately have been nihilism, vandalism, online gaming and ideological hacktivism **[8]**. Some of the high profile Denial of Service attacks that made news during 2010-2015 are discussed in this section.

The year 2015 started with an attack in France on satirical newspaper Charlie Hebdo, who had published and shown disrespect to the Prophet Muhammad (PBUH). In wake of this attack 19,000 French websites were hit by DDoS **[24].** The year 2014 ended with a DDoS attack of huge rate at around 25 Gbps on a Domain Name Service provider DNSimple and about 50 million packets were being sent per second **[17].** Telia the Sweden's Broadband giant was again attacked courtesy of the fact that Telia was closely linked to a police raid on the Pirate Bay **[29]** and experts say this provoked feelings in the hacker community and they believe the group behind this attack was the Lizard Group. In the month of November Supreme Court of Canada and Ottawa Police Services went down due to DDoS attack **[10].**

The month of December in 2013, witnessed lots of DDoS attacks on various gaming sites and servers **[19].** In the month of November the Battlefield 4-PC servers were DDoS attacked thus leaving an army of virtual soldiers unable to compete **[20].** In October of 2012 GitHub was again at centre stage of DDoS attacks, was attacked twice in October and the attacks on banks continued this month also and certain Government websites were also taken down **[24].**

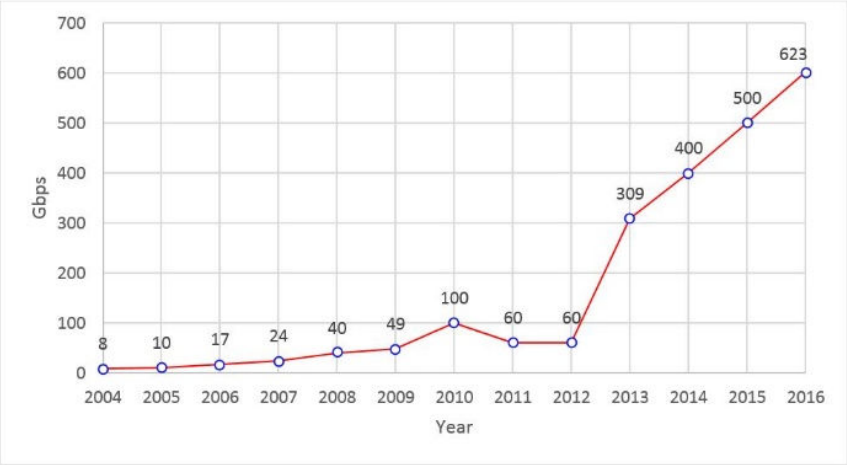

Figure **6:** Peak Attack Size in the past decade **[8]**.

In November of 2011 Internet services in Gaza and West Bank were attacked after Palestine won a Symbolically Significant victory at UNESCO **[27]**. December of 2010 saw an attack on MasterCard, PayPal, Visa and PostFinance. Attack was launched in support of WikiLeaks and lasted more than16 hours. In November an attack of the magnitude 10 Gbps was launched on WikiLeaks to prevent the release of secret cables **[9].** This study on the DoS attacks in the recent years tells us that these attacks are growing at par with the changing technology, the sophistication levels and the new tactics used to attack. If the problem is not taken care of very quickly, the loss it can incur will be huge which can often result in serious consequences. Therefore the solution should be the other way round i.e. the technology used and the mitigation techniques used to curb such attacks should be way ahead in every aspect, to that of the hackers

Counter measures of DoS Attacks.

The Counter measures can be classified into three main categories a) Basic Defense, b) Attack Detection, c) Attack Prevention, as shown in figure 7. The basic defense mechanism is present in

almost every end user system or information system. The second is concerned with detecting any malicious activity inside the system. Intrusion detection is the system which observes and analyses the events generated in a computer or network system to identify maximum security problems. The Intrusion Detection system (IDS) **[22]**is used to monitor the network assets to detect any thing un-usual **[30]**. The goal of an IDS is always to minimize the false positives and avoid false negative. The third one is concerned with mitigating the effects of DoS/DDoS attacks during the attack phase. Various techniques are mentioned in figure 7 and the standout technique today is the *filtering mechanism*, which is concerned

with an open connection to accept any in flow of packets and to setting up a mechanism to detect the load and the malicious packets in the system later on and the latter is concerned with concept of packet filtering and discard the packets with malicious intent at first place. With the new emerging techniques to carry out the DoS and DDoS attacks it

has been evident mechanisms are complex and the level of achieved that thepreventive measure are easy and cost-effective to implement whereas detection mechanisms are complex and the level of achieved security remains unclear. Some of the very well-known defense mechanisms that prevent DoS attack from happening are shown in figure 7**[28]**.

Conclusion & Future Scope

The information security is becoming a long standing challenge for the research community due to its multifaceted nature and the insecure operational environment. Each of the security attribute (confidentiality, integrity and availability) need to be addressed rigorously. Keeping in view the current networked environment this paper presented the most prominent aspect (the availability) of the security and presented an extensive investigation of the last decade and a half of the compromises made. The paper also report some of the best existing preventive countermeasure to ensure the availability of an information system. Having the base set, the future efforts will be to empirically evaluate these preventive measure and their effectiveness in the real working environment.

References

[1] Fang, Z. (2002). E-government in digital era: concept, practice, and development. International journal of the Computer, the Internet and management, 10(2), 1-22.
[2] UNCTAD (2011). Measuring the Impacts of Information and Communication Technology for Development. Current Studies on Science, Technology and Innovation. No 3. Geneva: UNCTAD. Retrieved May 03, 2011 URL http://www.unctad.org/en/docs/dtlstict2011d1_en.pdf.

[3] Melville, N., Kraemer, K., & Gurbaxani, V. (2004). Review: Information technology and organizational performance: An integrative model of IT business value. MIS quarterly, 28(2), 283-322.
[4] Brynjolfsson, E., & Hitt, L. M. (2000). Beyond computation: Information technology, organizational transformation and business performance. The Journal of Economic Perspectives, 23-48.
[5]Alshboul, A. (2010). Information Systems Security Measures and Countermeasures: Protecting Organizational Assets from Malicious Attacks. Communications of the IBIMA.
[6] Sanou, B. (2016). The World in 2016: ICT Facts and Figures. International Telecommunications Union.
[7] Akamai (2017). "Internet of Things and the Rise of 300 Gbps DDoS Attacks", Threat Advisory, Akamai FASTER FORDWARD (2017).
[8] Anstee, D., Escobar, J., Chui, C.F., Sockrider, G. (2015, January 27). 10th Annual Worldwide Infrastructure Security Report. Arbor Networks Inc.
[9] Arora, K., Kumar, K., & Sachdeva, M. (2011). Impact analysis of recent DDoS attacks. International Journal on Computer Science and Engineering, 3(2), 877-883.
[10] Bogart, N. (2014, November 25). Hacker claiming ties to Anonymous targets Toronto, Ottawa Police with DDoS attack. Retrieved from http://globalnews.ca/news/1689115/hacker-claiming-ties-to-anonymous-targets-toronto-ottawa-police-with-ddos-attack/
[11] Botnet. (2017, February 23). In Wikipedia, the Free Encyclopedia. Retrieved 18:07, February 27, 2017, from https://en.wikipedia.org/w/index.php?title=Botnet&oldid=766992978
[12] Centre, C. C. (2003). CERT/CC Statistics 1988-2003. Retrieved 10:03, December 28, 2014, URL http://www.cert.org/stats.
[13] CERT Coordination Center. (Oct. 1997). Denial of service attacks, [Online]. Available: http://www.cert.org/tech tips/denial of service.html, [accessed Jan. 20, 2012].
[14] Command and control (malware). (2017, January 14). In Wikipedia, the Free Encyclopedia. Retrieved 18:08, February 27, 2017, from https://en.wikipedia.org/w/index.php?title=Command_and_control_(malware)&oldid=759947676
[15] Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and Defense mechanisms: classification and state-of-the-art. Computer Networks, 44(5), 643-666.
[16] Plonka. D., (Aug. 2003). Flawed routers flood University of Wisconsin Internet time server, University of Wisconsin, Tech. Rep. [Online]. Available: http://www.cs.wisc.edu/˜plonka/netgear-sntp/, [accessed Jun. 19, 2012].
[17] Eden, A. (2014, December 2). Incident Report DDoS Attack. Retrieved from http://blog.dnsimple.com/2014/12/incident-report-ddos/
[18] Eddy, W. M. (2007). TCP SYN flooding attacks and common mitigations.
[19] Gaming sites and servers. (2013, Dec 30). Retrieved from http://in.ign.com/news/56090/hacker-group-derp-takes-down-multiple-online-gamin
[20] Greenberg, A. (2013, Nov 18). Battlefield 4 PC servers experience DDoS attack. Retrieved from http://www.scmagazine.com/battlefield-4-pc-servers-experience-ddos-attack/article/321506/
[21] Kern, C., Kesavan, A., & Daswani, N. (2007). Foundations of security: what every programmer needs to know. Apress.
[22] Mölsä, J. (2006). Mitigating denial of service attacks in computer networks. Helsinki University of Technology.
[23] Moore, D., Shannon, C., Brown, D. J., Voelker, G. M., & Savage, S. (2006). Inferring internet denial-of-service activity. ACM Transactions on Computer Systems (TOCS), 24(2), 115-139.'
[24] Passeri, P. (2012, Nov 2). October 2012 Cyber Attacks Timeline. Retrieved from http://hackmageddon.com/2012/11/02/october-2012-cyber-attacks-timeline/
[25] Qadir, S., & Quadri, S. M. K. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. Journal of Information Security, 7(03), 185.
[26] Qadir, S., & Quadri, S. M. K. (2017). Victim Based Statistical Filtering: A New Deterrent Against Spoofed Dos Traffic. International Journal of Computer Networks & Communications (IJCNC) Vol.9, No.4, July 2017.
[27]Sherwood, H. (2011, November 1). Palestinians hit by cyber-attack following success at Unesco. Retrieved from http://www.guardian.co.uk/world/2011/nov/01/palestinians-hit-cyber-attack-unesco
[28]Stuxnet. (2016). In Wikipedia, the Free Encyclopaedia. Retrieved 14:56, August 18, 2013, URL http://en.wikipedia.org/wiki/Stuxnet.
[29] Sweden's Telia attack linked to Pirate Bay. (2014, December 12). Retrieved from http://www.thelocal.se/20141212/telia-hit-again-in-new-hacking-attack

[30] Wang, D., Yeung, D. S., & Tsang, E. C. (2007). Weighted mahalanobis distance kernels for support vector machines. Neural Networks, IEEE Transactions on, 18(5), 1453-1462.
[31]GAO. (2013). CYBERSECURITY: National Strategy, Roles, and Responsibilities need to be Better Defined and More Effectively Implemented. United States Government Accountability Office.

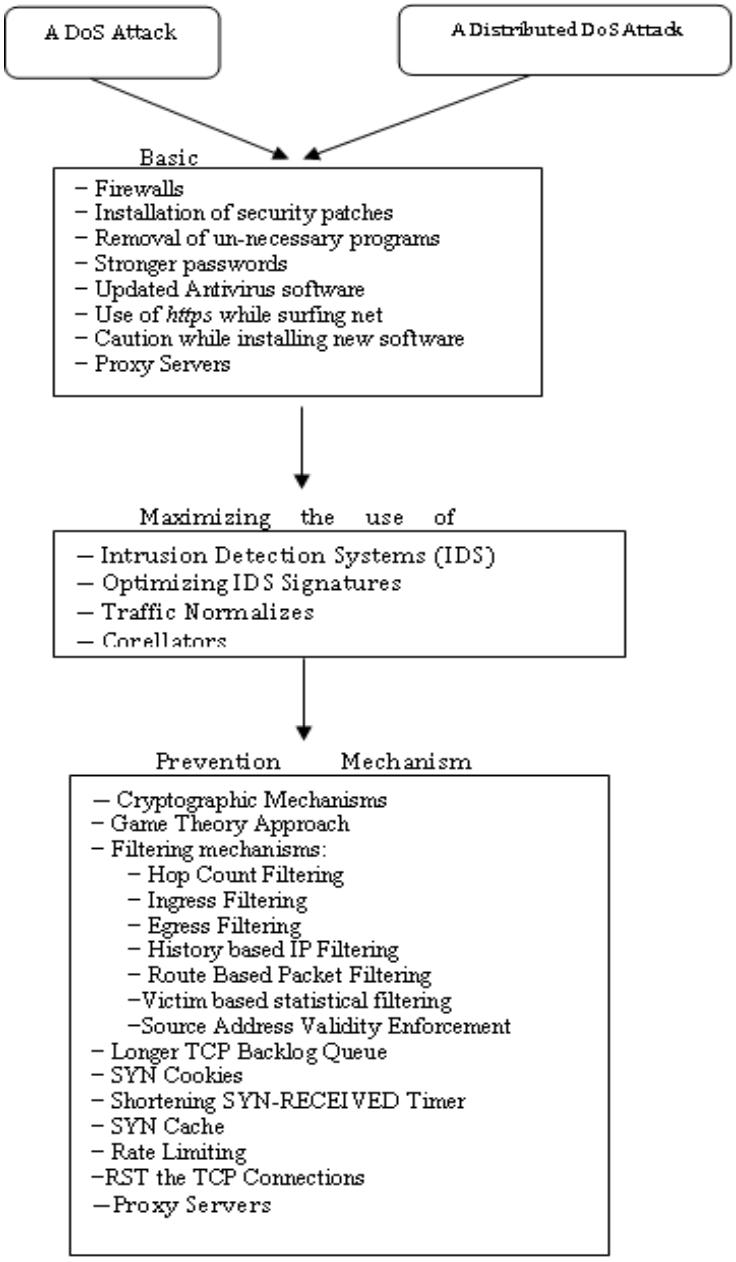

Figure 7:Most common Mechanisms for DoS and DDoS