A Defense Strategy for DDoS flooding Attacks

Reena[1], Yashpal Singh[2], Sonia Chaudhary[3]
[1,2,3] Department of Computer Science &Engineering,
Ganga Institute of Technology and Management,
Kablana, Jhajjar, Haryana, India

***Abstract*—Distributed Denial of Service (DDoS) is one of the most sophisticated attack technique. Due to its distributed nature, it is not easily to be faced. This paper includes development of a simulation model enabling the study and the analysis of defense techniques against Distributed Denial of Service (DDoS). *StopIt* is a robust, filter-based defense mechanism which is able to deal with various types of massive DDoS flooding attacks but which fails when the DDoS is achieved indirectly, *i.e.* by congestion of a link shared with the victim. Here we will discuss an extension of the StopIt technique for widening its applicability by making it able to cooperate with capability-based mechanisms for defeating indirect attacks. This extended version has been implemented into the ns-3 simulator and its effectiveness has been evaluated under different scenarios.**

Keywords: Distributed Denial of Service (DDoS) flooding attack, StopIt, DiffServ, ns-3 simulator.

I. INTRODUCTION

In computing, a **denial-of-service** (**DoS**) or **distributed denial-of-service**(**DDoS**) **attack** is an attempt to make a machine or network resource unavailable to its intended users. A DoS attack generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. As clarification, distributed denial-of-service attacks are sent by two or more people, or bots, and denial-of-service attacks are sent by one person or system. As of 2014, the frequency of recognized DDoS attacks had reached an average rate of 28 per hour. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. Denial-of-service threats are also common in business,[2] and are sometimes responsible for website attacks. This technique has now seen extensive use in certain games, used by server owners, or disgruntled competitors on games, such as popular Minecraft servers. Increasingly, DoS attacks have also been used as a form of resistance. Richard Stallman has stated that DoS is a form of 'Internet Street Protests'.[4] The term is generally used relating to computer networks, but is not limited to this field; for example, it is also used in reference to CPU resource management. One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately. Denial-of-service attacks are considered violations of the Internet Architecture Board's Internet proper use policy, and also violate the acceptable use policies of virtually all Internet service providers. They also commonly constitute violations of the laws of individual nations.

The first demonstrated DDoS attack was introduced by well known hacker Khan C. Smith during a 1998 illegal Defcon event and later exposed for its use Botnet mechanisms during a lawsuit filed by Earthlink which claims has caused billions in economic damages. Botnet consists of widely scattered and remotely controlled computers called zombies. zombies send a big amount of service requests and data traffic to the target victim in order to exhaust its resources.

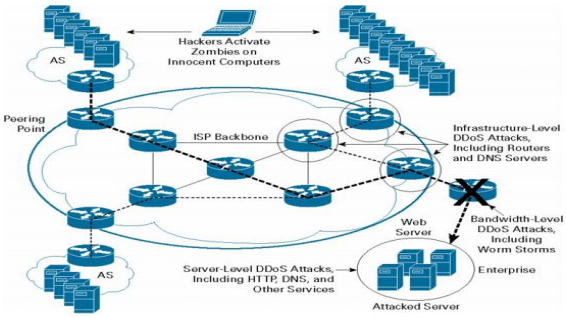

Fig1. Distributed Denial of Service

1.1 METHODS OF ATTACK

A denial-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. There are two general forms of DoS attacks: those that crash services and those that flood services.

A DoS attack can be perpetrated in a number of ways. Attacks can fundamentally be classified into five families:

1. Consumption of computational resources, such as bandwidth, memory, disk space, or processor time.
2. Disruption of configuration information, such as routing information.
3. Disruption of state information, such as unsolicited resetting of TCP sessions.
4. Disruption of physical network components.

5. Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

A DoS attack may include execution of malware intended to:

- Max out the processor's usage, preventing any work from occurring.
- Trigger errors in the microcode of the machine.
- Trigger errors in the sequencing of instructions, so as to force the computer into an unstable state or lock-up.
- Exploit errors in the operating system, causing resource starvation and/or thrashing, i.e. to use up all available facilities so no real work can be accomplished or it can crash the system itself
- Crash the operating system itself.

In most cases DoS attacks involve forging of IP sender addresses (IP address spoofing) so that the location of the attacking machines cannot easily be identified and to prevent filtering of the packets based on the source address.

II. DDoS DEFENSE MECHANISMS

We classify the defense mechanisms against network/transport-level DDoS flooding attacks into four categories: source-based, destination-based, network-based, and hybrid (a.k.a. distributed) and the defense mechanisms against application-level DDoS flooding attacks into two categories: destination-based, and hybrid (a.k.a. distributed) based on their deployment location.

1. *Source-based mechanisms***:** Source-based mechanisms are deployed near the sources of the attack

to prevent network customers from generating DDoS flooding attacks. These mechanisms can take place either at the edge routers of the source's local network or at the access routers of an Autonomous System (AS) that connects to the sources'.

*1.1. Ingress/Egress6 filtering at the sources' edge routers***:** The current IP protocol allows source hosts to alter source addresses in the IP packets. Packets with spoofed source IP addresses cause a huge problem in detecting DDOS flooding attacks. Victims cannot distinguish attack packets from legitimate ones based on source addresses. Although the IPSec protocol can address this problem by authenticating the source addresses of IP packets, this method is not widely deployed among service providers because of its increased overhead. Ingress/Egress filtering mechanisms have been proposed to detect and filter packets with spoofed IP addresses at the source's edge routers based on the valid IP address range internal to the network. However, the spoofed packets will not be detected if their addresses are still in the valid internal IP address range.

1.2. D-WARD: This scheme aims to detect DDOS flooding attack traffic by monitoring both inbound and outbound traffic of a source network and comparing the network traffic information with predefined normal flow models. D-WARD attempts to stop attack traffic originating from a network at the border of the source network. Attack flows are identified and filtered if they mismatch the normal flow models.

1.3. MUlti-Level Tree for Online Packet Statistics (MULTOPS) and Tabulated Online Packet Statistics (TOPS) : MULTOPS is a heuristic and a data-structure that network devices (e.g., routers) at the source subnet can use to detect and filter DDoS flooding attacks. Normally the rate of traffic in one direction is proportional to that in the opposite direction during normal operations on the Internet .Hence, a significant difference between the rates of traffic going to and coming from a host or subnet can indicate that the network prefix is either the source or the destination of an attack. MULTOPS detects and filters DDoS flooding attacks based on this mechanism. One major drawback of MULTOPS is that it uses a dynamic tree structure for monitoring packet rates for each IP address which makes it a vulnerable target of a memory exhaustion attack. An alternative approach called TOPS provides an efficient

method for detecting packet flow imbalances based on a hashing scheme that uses a small set of field length lookup tables. TOPS can improve the accuracy and reduce the false alarm rate of the system by monitoring traffic by protocol, and maintaining a probability distribution of traffic flow rates.

*1.4. MANAnet's Reverse Firewall***:** As opposed to a traditional firewall, which protects a network from incoming packets, the reverse firewall protects the outside from packet flooding attacks that originate from within a network. A reverse firewall limits the rate at which it forwards packets that are not replies to other packets that recently were forwarded in the other direction. Of course, it must be possible to send

Some packets that are not replies, for instance, to start a new conversation. However, such packets must not be transmitted at a high rate. One of the main disadvantages of the reverse firewall is that it is manual and requires the administrators' involvement. Furthermore, the reverse firewall's configuration cannot be dynamically changed at runtime.

*2. Destination-based mechanisms***:** In the destination-based defense mechanisms, detection and response is mostly done at the destination of the attack (i.e., victim). There exist various destination-based mechanisms that can take place either at the edge routers or the access routers of the destinations' AS. These mechanisms can closely observe the victim, model its behavior and detect

any anomalies. Some of the major destination-based DDoS defense mechanisms are as follows:

2.1. IP Traceback mechanisms **:** The process of tracing back the forged IP packets to their true sources rather than the spoofed IP addresses that was used in the attack is

called traceback. There are various IP traceback mechanisms that have been proposed to date. These mechanisms can be classified into two main categories. The first category is packet marking mechanisms. Usually routers in the path to the victim mark packets (i.e., add routers' identification to each packet) so that the victim can identify the path of attack traffic and distinguish it from legitimate The second category is link testing mechanisms in which the traceback process usually starts from the router closest to the victim and iteratively tests its upstream links until it can be determined which link is used to carry the attacker's traffic (i.e., the traceback process is recursively repeated on the upstream router until the source is reached).

2.2. Management Information Base (MIB): MIB data is comprised of parameters that indicate various packet and routing statistics. Continuously analyzing MIB can help victims to identify when a DDoS attack is occurring. During a DDoS attack, it is possible to map ICMP, UDP, and TCP packets' statistical abnormalities to a specific DDoS attack by identifying statistical patterns related to different parameters

*2.3. Packet marking and filtering mechanisms***:** These mechanisms aim to mark legitimate packets at each router along their path to the destination so that victims' edge routers can filter the attack traffic. These mechanisms let the receivers install dynamic network filters to block the undesirable traffic. Packet filtering mechanisms are dependent in part on the strength of the attackers, and when it increases, filters become ineffective and they cannot properly be installed.

*2.4. Packet dropping based on the level of congestion***:** These destination-based DDoS defense mechanisms drop suspicious packets when the network links are congested to a certain level. Packetscore is an example of this type.

*3. Network-based mechanisms***:**

These mechanisms are deployed inside networks and mainly on the routers of the Ass. Detecting attack traffic and creating a proper response to stop it at intermediate networks is an ideal goal of this category of defense mechanisms. Some of the main network-based

DDoS defense mechanisms are as follows:

*3.1. Route-based packet filtering***:** Route-based packet filtering extends ingress filtering to the routers at the core of the Internet. The traffic on each link in the core of the Internet usually originates from a limited set of source addresses. Hence, if an unexpected source address appears in an IP packet on a link, then it is assumed that the source address has been spoofed, and hence the packet can be filtered.

*3.2. Detecting and filtering malicious routers***:** Routers are continuously targeted and compromised. They can be leveraged to empower DDoS attacks. A range of specialized anomaly detection protocols have been proposed to detect malicious routers involved in packet forwarding between routers. For instance, Watchers detects misbehaving routers that launch DDoS attacks by absorbing, discarding or misrouting packets.

*4. Hybrid (Distributed) mechanisms***:** Hybrid defense mechanisms are deployed at (or their components are distributed over) multiple locations such as source, destination or intermediate networks and there is usually cooperation among the deployment points. For instance, detection can be done at the victim side and the response can be initiated and distributed to other nodes by the victim. Some of the hybrid DDoS defense mechanisms are as follows:

*4.1. Hybrid packet marking and throttling/filtering mechanisms***:** Hybrid packet throttling mechanisms usually place the attack detection modules near the victims and execute packet filtering close to the attack sources. In some of these mechanisms, victims under attack install a router throttle at upstream routers several hops away in order to limit the forwarding rate of the packets destined to those victims. Basically these mechanisms are packet filtering infrastructures that are leveraging the routers' support to filter out DDoS flows. It only limits the rate of malicious packets.

*4.2. Capability-based mechanisms***:** These mechanisms let the destination explicitly authorize the traffic it desires to receive (e.g., Portcullis , Traffic Validation Architecture (TVA) and Stateless Internet Flow Filter (SIFF)). In most of these mechanisms, sender obtain the capabilities, which are short-term authorizations, from the receivers and put them as stamps on their packets. Then, the verification points along the path check if the traffic is certified as legitimate or not.

4.3. Active Internet Traffic Filtering (AITF) as a filter-based (datagram) mechanism: Capability-based mechanisms enable a receiver to deny by default all the traffic and explicitly accept only the traffic that belongs to established network-layer connections. The alternative could be the datagram (a.k.a. filtering) mechanism in which a receiver accepts by default all the traffic and explicitly denies the traffic that has been identified as undesirable. The datagram mechanism requires a credible, bounded amount of filtering resources from participating ISPs, which offers incentives to ISPs to deploy it. AITF is a hybrid DDoS defense mechanism which enables a receiver to contact misbehaving sources and ask them to stop sending it traffic. Each of the sources that have been asked to stop is policed by its own ISP, which ensures their compliances. Each ISP that hosts misbehaving sources must either support AITF mechanism (i.e., accept to police its misbehaving clients), or risk losing all of its access to the complaining receiver; this provides a strong incentive for all the ISPs to cooperate; especially when the receiver is a popular point of access. AITF preserves receiver's bandwidth in the face of DDoS flooding attacks at a per-client cost; thus, it is affordable for the ISPs to employ it.

4.4. StopIt is a hybrid filter-based DDoS defense mechanism that enables each receiver to install a network

filter that blocks the undesirable traffic it receives. StopIt uses Passport as its secure source authentication system to prevent source address spoofing. Its design employs a novel closed-control and open-service architecture to battle strategic attacks that aim to prevent filters from being installed and to provide the StopIt service to any host in the Internet.

StopIt operation:

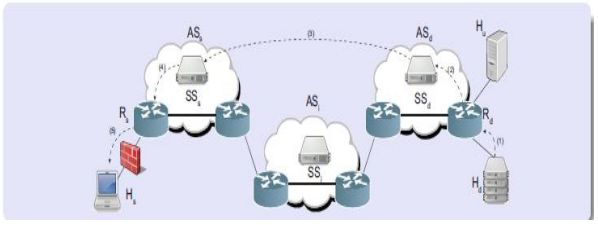

Fig.2 StopIt architecture: How it installs filters on the sources of attack upon detecting the DDoS attack

- The victim Hd detects the attack and send a blocking request to its access router Rd
- Rd verifies that the source Hs is really sending data to the server then, it installs a local filter and it sends a request of flow blocking to the StopIt server SSd
- SSd forwards the request toward the StopIt server belonging to the sourcing AS by using the BGP protocol.
- The StopIt server SSs within the sourcing AS, once received the request, notifies the blocking request to its access router Rs
- Finally, the access router of ASd installs the filter to block the flow for a certain period.

Limitations:

StopIt outperforms filter-based designs such as AITF, and is effective in providing continuous non-interrupted communication under a wide range of DDoS attacks. However, StopIt does not always outperform capability-based mechanisms. For instance, if the attack traffic does not reach a victim, but congests a link shared by the victim, a capability-based mechanism (e.g., TVA) is more effective. Therefore, both filters (a.k.a. datagram) and capabilities are highly effective DDoS defense mechanisms, but neither is more effective than the other against DDoS flooding attacks. StopIt mechanism is vulnerable to the attacks in which attackers flood the routers and StopIt servers with filter requests and packet floods. In order to prevent these attacks, the StopIt framework must ensure that a router or a StopIt server only receives StopIt requests from local nodes in the same AS, or another StopIt server. In doing so, network administrators must manually configure the routers and StopIt requests with the list of hosts, routers, and other StopIt servers. Such manual configuration for an AS with hundreds of thousands of nodes is a burdensome task . Furthermore, StopIt needs complex verification/authentication mechanisms, and misbehaving StopIt server detection mechanisms to be implemented in both hosts and routers which makes it a challenging mechanism to deploy and manage in practice

		Features	Disadvantages	Advantages
Centralized	Source-based	Detection and response are deployed at the source hosts	Sources are distributed among different domains; hence, it is difficult for each of the sources to detect and filter attack flows accurately Difficult to differentiate legitimate and DDoS attack traffic at the sources, since the volume of the traffic is not big enough Low motivation for deployment; since, it is unclear who would pay the expenses associated with these services	Aims to detect and respond (i.e., filter) to the attack traffic at the source and before it wastes lots of resources
	Destination-based	Detection and response are deployed at the destination hosts (i.e., victims)	They cannot accurately detect and respond to the attack before it reaches the victims and wastes resources on the paths to the victim	Easier and cheaper than other mechanisms in detecting DDoS attacks because of their access to the aggregate traffic near the destination hosts
	Network-based	Detection and response are deployed at the intermediate networks (i.e., routers)	High storage and processing overhead at the routers Attack detection is difficult because of the lack of availability of sufficient aggregated traffic destined for the victims	Aims to detect and respond to (i.e., filter) the attack traffic at the intermediate networks and as close to source as possible
Distributed	Hybrid (Distributed)	Detection and response are deployed at various locations: detection usually occurs at destinations & intermediate networks, and response usually occurs at the sources & upstream routers near the sources There is a cooperation among various defense components	Complexity and overhead because of the cooperation and communication among distributed components scattered all over the Internet Lack of incentives for the service providers to cooperate/collaborate Need trusted communication among various distributed components in order to cooperate/collaborate	More robust against DDoS attacks More resources at various levels (e.g., destination, source, and network) are available to tackle DDoS attacks

Table 1 Summary Of Features, Advantages, And Disadvantages Of Defense Mechanisms Against Network/Transport-Level Ddos Flooding Attacks Based On Their Deployment Location

Since attackers cooperate to perform successful attacks, defenders must also form alliances and collaborate with each other to defeat the DDoS attacks. The DDoS defense

community is currently more involved in proposing novel hybrid DDoS defense mechanisms and most of the recently proposed mechanisms belong to the hybrid category. No single deployment point (centralized) can successfully defend against DDoS because of the fundamental challenges we enumerated for each of the deployment points. A hybrid (Distributed) defense mechanism is the best way to combat DDoS Attacks.

III. DIFFSERV

Differentiated services or **DiffServ** is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying and managing network traffic and providing quality of service (QoS) on modern IPnetworks. DiffServ can, for example, be used to provide low-latency to critical network traffic such as voice or streaming media while providing simple best-effort service to non-critical services such as web traffic or file transfers.

DiffServ uses a 6-bit differentiated services code point (DSCP) in the 8-bit **Differentiated services Field** (**DS field**) in the IP header for packet classification purposes. The DS field and ECN field replace the outdated IPv4 TOS fiel most networks use the following commonly defined Per-Hop Behaviors:

- *Default* PHB (Per hop behavior)—which is typically best-effort traffic
- *Expedited Forwarding* (EF) PHB—dedicated to low-loss, low-latency traffic

- *Assured Forwarding* (AF) PHB—gives assurance of delivery under prescribed conditions
- *Class Selector* PHBs—which maintain backward compatibility with the IP Precedence field.

IV. MODELLING WITH NS-3

Here we describe the modeling and simulation of the StopIt mechanism and of the proposed enhancements by using the ns-3 discrete event network simulator specifically designed to test and validates the performance of wireless and wired IP network systems. In particular, ns-3 is one of the fastest and efficient network simulators freely available on the web in which the simulation time discretely moves from one event to another. We developed the proposed strategy by integrating a freely downloadable DiffServ model for ns-3 simulator with the standard operation offered by the StopIt mechanism in order to generate unified simulation framework. In particular the StopIt implementations have been made under the following assumptions:

- IP addresses cannot be spoofed because StopIt deployment in a real network subsumes the use of Passport.
- The only network elements corrupted are the hosts belonging to the botnet.
- Strategic attacks directed to filter exhaustion are not taken into account.
- Only Ipv4 networks are considered
- StopIt servers are already aware of their peers at startup.
- Access routers play also the role of edge routers and are able to install/remove DiffServ SLAs at runtime.

In order to simulate in ns-3 a DDoS attack scenario in presence of the StopIt defense mechanism, we implemented the needed components by introducing suitable classes, that inherit from ns-3 application base class, which respectively reproduce the behavior of a DNS server ,StopIt servers, routers supporting packet filtering and DNS clients. DNS Server models the behavior of a DNS server able to process up to n requests in parallel. In particular, if the DNS server is in the available state, it handles incoming requests as soon as they arrive ;on the contrary, when there are no more available processing resources, the server switch to the busy state and stores the incoming requests into a limited buffer. If the buffer gets filled, incoming requests are dropped. Service time is assumed to follow an exponential distribution with mean 5ms.

A StopItServer reproduces the behavior of a StopIt server. AccessRouter implements the router application which is in charge of packet filtering, dispatching of StopIt requests and DiffServ policy enforcement.

Fig.3. Class hierarchy

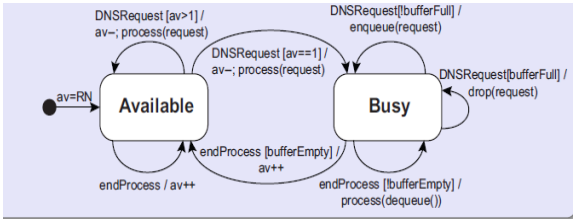

Fig.4. FSA model of the DNS server

V. SIMULATION SCENARIO

The network is split up into three zones:

- The first zone contains ten Ass, each made up of 50hosts, where the traffic sources are located in.
- Second zone: intermediate network
- Third zone: victim's AS.

Simulation Parameters:

Traffic sources:

- 24 VoIP (ilbc mode 30 codec at 13.33kbps) [AF]
- 230 HTTP sources [BE]
- 230 DNS clients (50% malicious) [BE]

Links		DNS Service	
Bandwidth	10 Mbps	Resources	8
Delay	1 ms	Buffer size	200
		Mean service time	5 ms
Legal DNS traffic		**Malicious traffic**	
Packet size	26 bytes	Packet size	78 bytes
Packet rate	1 pkt/s	Packet rate	100 pkt/s

Table2 . Simulation Parameters

VI. DIRECT FLOODING ATTACK

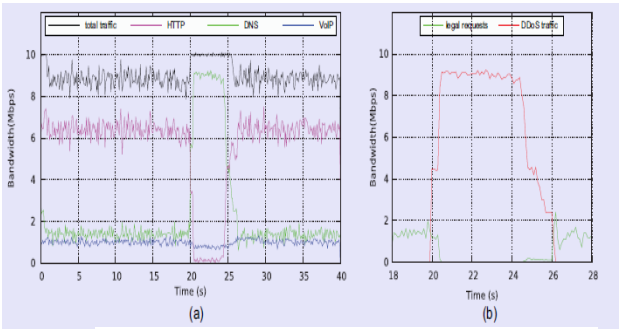

Fig.5.(a) Direct DNS DDoS attack (b) Detail of legal and malicious DNS traffic

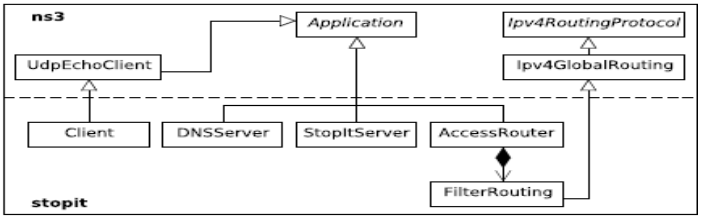

Fig. 6.1.a shows the effectiveness of StopIt in the case of direct attack. The black curve is the total used bandwidth, the purple line represents the HTTP traffic, the blue line is the VoIP traffic and the green one the DNS traffic (both legal and illegal).In simulated scenario, The attack begins at t = 20s and it is detected at t = 23s.In fig6.1.b, during this period the DNS traffic is almost totally made of malicious packets. After the filter is installed the botnet traffic is blocked and VoIP traffic is unaffected due to Diffserv.

VII. CONCLUSION

This paper purposed and validated a novel defense mechanism based on the cooperation of StopIt and DiffServ has been defined and evaluated.The technique overcomes StopIt limitations in that it is able to cope with indirect DDoS flooding attacks. The cooperation between DiffServ and StopIt has the great advantage to be easily implemented in common routers since it is based on widely available technologies. A ns-3 simulation model for the analysis of DDoS attack has been implemented. However, the proposed solution cannot be considered as final because, even if the main services are guaranteed the illegal sources still continue to overload the network. As future work we plan to extend our research by designing suitable detection algorithms that may directly run on edge router devices and exploit StopIt features to block illegal sources also in the case of indirect attacks. Relaxing the constraint of the existence of a StopIt server for each AS. Devise a better technique for exploiting DiffServ capability (e.g by lowering the priority of flooding traffic).

REFRENCES

[1].Modelling and simulation of a defense strategy to face **https://www.distrettocybersecurity.it/keyportal/.../presentazioneddos.pdf**

[2].A Survey of Defense Mechanisms Against Distributed Denial **https://www.d-scholarship.pitt.edu/19225/1/FinalVersion.pdf**

[3].Denial-of-service attack - Wikipedia, the free encyclopedia **https://www.wikipedia.org/wiki/Denial-of-service_attack**

[4].Differentiated services - Wikipedia, the free encyclopedia **https://www.wikipedia.org/wiki/Differentiated_services**

[5].Internet and Distributed Computing Systems: 7th International Conference ... - Google Books