Chapter 1

INTRODUCTION

“There are some things that can’t be controlled.” Leonard Kleinrock

Internet is by far one of the most famous, successful and largest set of communication networks with networks interconnected at planetary scale. Its success is largely attributed to the growth and popularity of communication devices like mobile phones, tablets, iphones, ipads, etc. These devices not only have smaller size which makes them easier to carry and handle, but their storage and computing power has also grown exponentially over the years. This has led to a virtual free space for communication - the internet. The ease with which these gadgets can be used to run wide range of internet-based applications has made the network notoriously famous mean of data transportation. The users can now avail both the conventional as well as present day services of the network. The mushrooming of services fighting for network shared link bandwidths like High Definition Television (HDTv), Internet Protocol Television (IPTv), Peer-to-Peer Television (P2PTv) internet games like Massive Multi-User Online Role Playing Game (MMORPG) , Voice over Internet Protocol (VoIP) communication, web-based multimedia services, etc. has therefore, led to tremendous pressure on the infrastructure. More recently the easy and fast access to internet-based applications has only worsened the situation. To mount to this pressure, the technology that makes it lucrative, is fast becoming the cause of it’s demise. Hackers deliberately make use of infrastructure (software and hardware)
weaknesses to launch attacks and affect the services of the network. Network attacks are popularly known as cyber or denial-of-service (DoS) attacks.

Universally, any individual or an organization that needs to avail network-based services, can do so by getting an Internet Protocol (IP) address and transport layer protocol services to send packets of data to whosoever connected in the IP network. On the other hand though, the receiver has to read address of every incoming packet before finding out the legitimacy of the sender. Even the IP address single handedly is insufficient to establish the authenticity of the sender. *This weakness of the Internet Protocols and openness of the internet enables the malicious users in faking their identities and causing damages to the servers and the services.* The primary intention of an attacker can either be to expose the vulnerabilities of the operating systems, leak private information to damage the goodwill of the concerned party and in doing so build a reputation for oneself or it could only be a harmless act done by a novice for showing ones skill etc. The reason could be anything but the end-user always has to bear the cost of damage.

The heterogeneity of the internet and absence of any centralized control has led to far less predictable powers of the network administrators and service providers. Moreover, there is no means by which the damaging traffic could be stopped from entering the networks. The end result is vulnerability of legitimate users being dangerously exposed to threats and damages. The biggest and yet always unsolvable area in this has been the vulnerabilities of the operating systems, their patches and internet protocols. For example, in the history of cyber attacks, *Morris worm* (1), was the first attack distributed and launched via internet in 1986. It’s huge success forced the organizations like DARPA to take preventive steps so as not to have such types of attacks in the future. As a result in 1988, the Computer Emergency Response Team (CERT) was created to provide internet security. Every year CERT conducts international researches and surveys and publishes reports on cyber threats (2). The organization now has more than 150 cyber security professionals working on major world-wide projects both nationally and internationally. To curb the situation governments world wide have passed numerous laws and punished hackers. In the year
1999 Mitnick (3) was tried in the US court for largest computer-related fraud committed in the U.S. history. At that time the loss of intellectual property was estimated at eighty million. A more recent example of cyber attacks could be - *Avenge Assange Campaign* - launched in 2010 (4), by a group to target the government organizations and corporations that refused donations to *Wikileaks website*. Figure 1-1 shows some of recent news headlines related to distributed DoS attacks.

Analyzing security threats as reported by the United States Computer Emergency Readiness Team (US-CERT) gives an overview on the current state of attacks. There has been paradigm shift in the types of cyber intrusions as well as strength & speed of these attacks. The traditional ones like UDP increased traffic, brute force, Denial of Service (DoS), Distributed Denial of Service (DDoS) are co-existing with the newer breed of Cable break, Census Campaign warning, Clickjacking, DNS as well as cyber

![Recent Headlines](image-url)
intrusions. The presence of organizations like CERT for the past 26 years is proof enough that internet is never going to be free from cyber attacks and will always need better methods to tackle the newer attacks. Researchers are therefore, constantly looking out for better and faster solutions to handle the menace of cyber-attacks.

The openness and heterogeneity of the internet infrastructure and it’s protocols has always been considered it’s strength and has played immense role in it’s success. Presence of varied type of applications and their users has therefore led to diversified traffic. And with no or insufficient visible means to distinguish the regular traffic from the unwanted attack traffic, it is way too difficult for the network administrator to stop the malicious packets from entering the network. Therefore, measuring and monitoring network traffic has become important field of study. Varied techniques & technologies are being used in the successful detection and diagnosis of unwanted malicious traffic in the networks. Detection of abrupt changes in the otherwise regular flow is one such technique being used these days.

The systems specifically designed for measuring network intrusions are known as Network Intrusion Detection Systems-(NIDS) (34), (35). According to their deployed techniques of detection they are categorised as signature-based detection and anomaly-based detection techniques (37). The signature-based detection algorithms require a pre-determined pattern to be matched to, in order to detect an intrusion or an attack (49). But in today’s scenario with fast moving and dynamically changing internet traffic it is a cumbersome and time consuming job unfit for real-time detections. The anomaly detection techniques on the other hand are rather well suited for today’s needs (33). Anomaly detection relies on normal behaviour of the traffic and looks out for an attack or an anomaly as a deviation from the normal behaviour. Over the years several algorithms have been developed to detect anomalies in the network traffic. In the host-based anomaly detection the system is modeled to analyze the host behaviour and any deviation from this behaviour is termed as an anomaly. In the network-based anomaly detection the system is modeled to analyze the behaviour of network traffic and any deviation in the network traffic is characterized as an anomaly (37). In this thesis we have worked on network based anomaly detection for detection of DDoS like
anomalies in the network traffic. This chapter, therefore, helps in understanding the characteristics of regular and malicious network traffic that prompted us to study its behaviour patterns, brief introduction about rate-based network traffic anomalies, their types and classifications and defense mechanisms.

Rest of the chapter includes an overview on internet traffic behaviour in section 1.1, sub-section 1.1.1 with introduction to nature of normal traffic in the network, followed by an overview on the malicious traffic in sub-section 1.1.2. Section 1.2 gives details about the DDoS attacks, which have been studied in this thesis as an anomaly in the network traffic. The section covers types of DDoS attacks in sub-section 1.2.1, DDoS attack targets in 1.2.2 and DDoS attack defense mechanisms in sub-section 1.2.3. Lastly, thesis outline is given in section 1.3.

1.1 INTERNET TRAFFIC BEHAVIOUR

Network traffic variability is an important characteristic of internet traffic (105). It is always present in the network traffic, either due to intrinsic reasons like flow of normal network traffic between two or more communication protocols, or it could be due to extrinsic reasons like anomalous network traffic such as outages, scans, flash-crowds or DoS attacks (2).

Internet QoS is considered to be extremely sensitive to traffic variability. Low QoS by the Internet Service Providers (ISPs) could lead to loss in revenues as well as goodwill. One of the primary sources of extrinsic variability in network traffic are DDoS attacks. Internet services therefore require appropriate handling of DDoS attacks. Current research is therefore, mainly focused on making the network robust to these disruptions.

The biggest difficulty being faced by researchers in handling above said disruptions is that the network traffic is always a moving target. Whether it is normal traffic or anomalous traffic it is always evolving in terms of its bandwidth consumption, its pattern or its variable behaviour. As a consequence, rather than handling of huge data sets of large number of packets of network traffic and modeling them based on
Poisson distributions or Markov modulated point processes, one would prefer to work on aggregated byte or packet count processes. Various models based on aggregated packet analysis have been proposed. The biggest advantage of aggregated processes is that their capturing is fast and adjusts well to the fastly growing internet traffic. Scale-invariance is one such property of aggregated processes that can be explored for measuring variability in network traffic. One of the methods of measuring scale-invariance is self-similarity.

This section presents an overview on the scale-invariant property of network traffic and its impact on the traffic flows. This is important because the aim of this thesis is to use scale-invariant property, self-similarity, for detection of unwanted network disruptions like DDoS attacks. We next discuss self-similarity and its implications on regular and anomalous traffic.

1.1.1 NORMAL TRAFFIC BEHAVIOUR

In the early 90’s, network traffic variability was partially explained with properties of scale-invariance, namely, self-similarity and long range dependence. Self-similarity is a scale invariance property typical of fractals. Mathematically, a self-similar pattern is either an exact or an approximate look-alike to a part of itself. Self similarity of a time-series is its property to preserve similar statistical properties (mean, variance and higher moments) over multiple time scales. Traditional Poisson distribution models, packet train models and fluid flow models on the contrary show noticeable decline in the aforesaid parameters as the time-scales increase, thus, making them unsuitable for the job (5), (6), (8). These models fail to measure the variable traffic behaviour at aggregated levels or require large number of parameters to perform. The differences of aggregated self-similar traffic therefore requires a new look at the modeling and performance measurement of internet like communication networks.

The initial studies of network traffic in Local Area Networks (LAN) exhibited that the LAN traffic possessed the properties of self-similar (SS) (9), (10), (11), (12), (13), (105), (14), (15) or fractal behaviour over time scales that were larger than one second approximately. The presence of this scaling behaviour in packet data
of network traffic was first noticed in the seminal work of Leland et al. for LAN traffic (9), and then for Variable Bit Rate (VBR) video (11), ATM cell traffic (19), and later in the Wide Area Network (WAN) (10) traffic. During the years from 1988 to 2007 the works by P. Abry, D. Veitch, and P. Flandrin (17) and others brought the fractal buzzword to network traffic engineering and led to a renewed interest in network traffic modeling and characterization. They argued against the use of conventional Markov based models for traffic engineering and stressed on the need to introduce traffic models based on fractional behaviour or self-similarity rather than Markovian models. Paxson and Floyd (10) also were able to find self-similar properties in WAN traffic, specifically in Transport Control Protocol (TCP), File Transfer Protocol (FTP) and TELNET connection arrivals. Recently, peer to peer networks have also been found to show self-similar behaviour in their traffic. Crovella and Bestavros (11) were also successful in analyzing the presence of self-similar patterns in web traffic.

From the times when self-similar nature of LAN traffic was explored to the times of self-similarity based applications in internet, the field of heavy-tailed distributions has evolved tremendously. However, the shift from measuring the impact, analyzing the origins, to the applications of self-similarity has been gradual. Different areas ranging from modeling of aggregated network traffic in the internet (9), (11), queuing delays at routers, congestion delays in the links, protocol behaviors like TCP (10), (12), (15) and (22) all look out for self-similar properties. The earlier studies of scale-invariance were focussed on proving the presence of self-similarity in the network traffic. Now-a-days self-similarity is being applied and tested at three different levels in networks; network infrastructure and its protocols being the first level, nature of the data being transferred across intra and inter-continental links as second level and system end-users and end-applications behaviour being the third level. Recently, this property has been used for detection of attacks in network traffic. The focus of this study is the third level analysis of self-similar property. Network intrusions or attacks are launched by attackers as end-users of the applications. The structure of the internet fails to identify the malicious intent of the attackers from the normal
behaviour of its users. Intrusion detection community, therefore, is always looking for techniques to handle these attacks. The possibility of variance in the self-similar behaviour of normal traffic due to attacks has been explored in this work.

1.1.2 ANOMALOUS TRAFFIC BEHAVIOUR

As stated earlier, the variability in network traffic is due to both intrinsic reasons as well as extrinsic reasons. Intrinsic reasons are a resultant of regular network traffic but extrinsic reasons are caused by irregular network traffic like outages, scans, flash-crowds or DDoS attacks. This irregular or unwanted traffic is termed as anomalous traffic. While many studies have been conducted to measure variability and its impact on regular normal traffic, very few have been devoted to study anomalous traffic. The unstable, unpredictable and highly variable behaviour of anomalous traffic makes the task even more difficult. Network users are highly sensitive to low quality of service caused by the DDoS like disruptions. The network administrators and engineers, therefore, have round the clock job to keep looking for policies, techniques, resources etc. to detect and mitigate these anomalies. The administrators need to detect these disruptions in time and then to take appropriate action. A general anomaly detection therefore requires automatic detection and classification of normal and anomalous traffic. But, given the large scale of the internet and varied number of applications with no control or very little control mechanisms this task is not that easy. One of the solutions suggested by the network community takes into account the variation in self-similar nature of network traffic due to anomalous traffic like DDoS attacks.

As is known in the area of network anomaly detection the detection algorithms are applied to aggregated flow-based network traffic. In terms of network engineering, it frees us from time consuming, high cost packet analysis techniques that require reading of individual packet headers of IP protocols for data analysis. The high cost involved in the packet capture and analysis aggregates further in the presence of sudden surge in the network traffic. Because of the flooding nature of DDoS attacks there is always a sudden increase in the number of packets at the time of attack and therefore the cost of per packet data collection becomes very high. Techniques of
self-similarity estimation are of great support here. Because of low recording cost of the traffic intensity at a given frequency, with no need for per packet protocol reading, it is sufficient enough to estimate self-similarity of captured aggregated flow-based traffic. Variance in self-similarity with its low cost in collection of statistics is therefore a good alternative in measuring and locating the attack points.

Studies by (129), (130), (173) have proved the presence of scale-invariance in normal traffic and deviation due to non-bursty behaviours of DDoS flooding attacks. These works are based on the assumption that DDoS attacks completely destroy the scale-invariance property of normal network traffic. We however believe and have tried to prove that presence of DDoS attacks does not cause full loss of scale-invariance. Now-a-days DDoS flooding traffic is generated with the help of automatic programs-bots. It has been shown by Taqqu et. al. in (85) that scale-invariant traffic can be generated by using on-off packet trains of pareto distributions. Attackers can therefore develop tools to generate scale-invariant flooding attacks. On the other hand DDoS attacks like PDoS are already having structure of on-off pulses used to launch attacks.

We therefore have based our work on the view that DDoS traffic does not completely destroy the scale-invariance property of normal traffic. It may however, increase or decrease the variance that can be measured in terms of (H) index.

Hurst exponent or $H$ (23) index is used to determine presence and variability in self-similarity in the network traffic. We know that network traffic exhibits scale-invariance and hurst parameter $H$ is a measure of scale-invariance property, i.e., self-similarity. Under normal circumstances the network traffic follows the self-similar behavior which can be measured with $H$. Whereas in the case of DDoS attacks the self-similar nature of the traffic changes because DDoS attacks and their detection are short-range phenomena. It is because of the fact that the attackers emit packet bursts and attack the target for short periods of time only. This in turn changes the traffic behavior which deviates from the self-similar nature. Various statistical estimators can be used to estimate Hurst parameter (H) and consequently self-similarity. Such estimation is always based on observing mostly the second moment of the processes on various time scales. Wavelets-based estimator is one of the tools used for Hurst
estimation. Wavelets are a mathematical technique that can be used to observe an arbitrary signal on various time scales. The low computational cost and the scale invariance property makes wavelets an excellent tool for analysis of self-similarity in network traffic.

The prima facie objective of our work therefore is to study and apply the scale-invariant property of self-similarity in network traffic, measured through single parameter $H$, for detection of rate based anomalies in the network traffic. The detailed literature survey on various techniques used in anomaly detection based on signal processing techniques is discussed in chapter 2.


1. **Denial-of-Service (DoS) Attacks**: The Internet in its present size (146) is very complex and it is difficult to measure and analyze it. And to add to the challenge of its smooth running it is always under threats. Denial of service (DoS) attacks try to degrade the quality of services available to the legitimate internet users. A DoS attack occurs when the victim server/node receives an unwanted surge of packets due to which the legitimate users fail to receive
required use of services.

Figure 1-2 shows a common denial-of-service attack situation in which an attacker sends a surge of packets to victim server, resulting into denial of services to legitimate clients. DoS attacks are an old form of attacks that involves only one attacking node that is used to launch an attack. These attacks are of two types: *flooding based DoS attacks* and *vulnerability based DoS attacks* (20). The flooding based DoS attacks consume the bandwidth of the affected server by sending very large amounts of packets than the server can handle and as a result server breaks down. Smurf attacks, TCP SYN flooding, etc. are one such type of attacks. Vulnerability based DoS attacks exploit some vulnerability of Internet Protocols that are used for data or message transportation like UDP, TCP, ICMP etc. These attacks are of low volume and thus are difficult to detect. Common examples include Ping-of-Death, Teardrop, Neptune, etc.

2. **Distributed-Denial-of-Service (DDoS) Attacks:** Distributed denial-of-service (DDoS) attacks are denial-of-service attacks that are performed by using more than one attacker node. There are large number of nodes or bots that initiate an attack simultaneously and generate packets that overwhelm the vic-

![Figure 1-3: Distributed Denial of Service attack](image)
tim and as a result the legitimate users are unable to avail the services. These packets have one target i.e. the victim server or victim node. Since the packets are sent from many distributed nodes therefore it is difficult to trace out all the attacking sources. Figure 1-3 depicts a simple distributed denial-of-service attack scenario in which attacking nodes attacker1 and attacker2 send streams of malicious packets to victim server, denying its service to legitimate clients. DDoS attacks are very lethal and hamper the services within seconds of their deployment (155).

![Diagram of distributed denial-of-service attack]

**Figure 1-4:** Pulsating Denial of Service Attack. Source: Kuzmanovic et al. (145)

3. **Pulsating DoS Attacks:** More recently a new breed of DDoS attacks has been discovered by Kuzmanovic and Knightly and are named as Low-rate DDoS attacks or LDoS (145). Pulsating DoS or PDoS are a similar variation of the former attack. In LDoS instead of flooding the communication channels with large number of packets, timed packet pulses of small duration are sent to the target machine. Because there is sudden increase in the number of packets for a short duration of time these pulses help the attacker to disrupt TCP services. When combined with distributed architecture, these pulses of still shorter duration can be so generated such that on reaching their target the impact is very high number of packets for short duration. The attacker in
PDoS attacks periodically sends high-rate traffic over a short period of time.

PDoS attacks were first reported by Asta Networks which did an extensive six-month period analysis of Internet2 Abilene backbone traffic in 2001 and reported the presence of pulsating zombies (21). Instead of sending a surge of attack packets, these zombies sent out small bursts of attack packets to crash the victim server. Figure 1-4 depicts the combined effect of short pulses of length (L), burst rate (R) being sent by sources S1, S2 and S3 in time period (T) at victim server. Although at their respective sources these pulses are small but their aggregated impact is large number of bytes of data at the victim server. As a result the victim fails to provide services to its legitimate users. More on PDoS attacks is covered in chapter 6.

4. **Flash Crowd**: Flash crowd is a large spike or surge in traffic to a particular Web site. Major news websites experience this problem during major world events. Flash events lead to sudden exponential increase in the incoming traffic and as a result the servers cave in (111), (114), (119). Both DDoS attacks and flash events are anomalies in the network traffic yet each one of them differs from the other. DDoS attacks are created by the attackers with an intent to deliberately disrupt the services whereas flash events are an after effect of all of a sudden interest of everyday users in some particular website for small duration of time. A network administrator may never want a DDoS attack whereas a flash event is an increase in revenue and should be handled carefully.

The aim of this thesis, therefore, is the development of algorithms that are worthy of measuring the change in the self-similar characteristics of the computer network traffic in general and internet in particular and signal the changes in order to detect the anomalies like DDoS attacks, pulsating DDoS attacks and flash events in the network traffic. We next give a brief overview of DDoS attacks\(^1\) and their classification based on their types, targets and defense mechanisms.

\(^1\)In this thesis DoS, DDoS, flash-crowds and PDoS attacks have been considered as network anomalies
1.2 CLASSIFICATION OF DDoS ATTACKS

Research in the field of DDoS attack detection has been largely divided into two areas depending upon how the problem is viewed. Based on types of various DDoS attacks the classification is done as ‘DDoS attack types’ and based on attack targets it has been classified as ‘DDoS attack targets’. Ever since DoS attacks and DDoS attacks were discovered in the 80’s, there have been humongous increase in the types and targets of these attacks. There exist various parameters for classification, but most elaborate work on this has been done by Mirkovic et al. in their famous paper (152). In their pioneer work they have created taxonomy of DDoS attacks based on: level of automation, exploitation of the various vulnerabilities, validation based on source-host addresses, impacts on victim, types of the victim server, various possibilities of characterization and attack rate dynamics. \(^2\) We have considered detection of rate-based attacks in this thesis. Rate-based attacks can occur both at the application and network layers of the TCP/IP protocol stack. The attacks have been classified based on constant rate and variable rate as well as slow rate PDoS attacks and high rate flooding attacks.

1.2.1 DDoS ATTACK TYPES

The primary function of the internet was to provide a basic infrastructure so as to enable a common man to be able to send and receive information through IP networks. Therefore while designing the internet no one was held responsible for providing security in the end to end systems and the core network. DDoS attackers exploit this vulnerability of the internet design. With the help of rate-based flooding DDoS attacks or protocol-vulnerability based DDoS attacks the attackers try to inundate the victim servers with large number of unwanted requests and stop the services being provided by the servers. In the following sections we discuss important sub-types of these attacks.

\(^2\)For details pl refer to paper by Mirkovic and Reiher (152).
1.2.1.1 High-Rate based Flooding Attacks

Flooding based attacks or brute force attacks are the oldest and most common of the DDoS attacks. These attacks have the ability to cause maximum damage and are most difficult to distinguish from legitimate traffic. These attacks fill up the bandwidth of the victim server or consume all the available resources with the server and as a result the server fails to provide its services. Now-a-days these attacks are launched with the help of bots. Bots are compromised machines that send large number of packets to a target machine on receiving launch signal from the master attacker. Because there are numerous number of computers that are always hooked in the internet and all of them are not always well configured therefore the hackers exploit the vulnerabilities of these computers and install special programs on these machines. These programs are activated on receiving request from the attacker and launch timed attack on the victim servers. The three common types of flooding-based DDoS attacks are:

1. **UDP Datagram Flooding Attacks:** User Datagram Protocol a.k.a UDP is transport layer connectionless protocol being used for packet communication in IP networks. It is heavily used by internet users in multimedia applications, DNS queries, network management and routing protocols. Being a connectionless protocol the sender does not have to wait for an acknowledgement. The UDP flooding is the simplest of the flooding attacks because there is no pre-launch work required to be carried out by the attacker in order to ensure the success. The attackers send very large number of UDP packets generally of maximum segment length to the victim and inundate the server. The main objective of these attacks is to consume the network bandwidth and affect the legitimate services. These days direct UDP flooding is not possible because of constraint in the operating systems on the maximum number of UDP packets that can be received from a particular user. But combined with other flooding attacks UDP flooding can prove lethal.

2. **ICMP Datagram Flooding Attacks:** Internet Control Message Protocol a.k.a ICMP is network management protocol. It is used by the network admin-
administrators to handle network operations like packet drops, congestion etc. During an ICMP datagram based flooding attack large number of \textit{ICMP.ECHO} datagrams are sent to the victim. In order to the \textit{ICMP.ECHO} request the victim has to reply with \textit{ICMP.REQUEST} datagrams. Generation and sending of \textit{ICMP.REQUEST} datagrams consumes the resources of the victim. Flooding of ICMP datagrams therefore makes the victim server ineffective in handling the legitimate requests. By blocking the inflow of ICMP datagrams the flooding can be handled. \textit{Smurf} attacks are one of the famous ICMP datagram based flooding attacks.

3. **HTTP Datagram Flooding Attacks:** Hyper Text Transfer Protocol a.k.a HTTP is the application layer protocol that is used to fetch data from web pages. Web based applications being a great success these days has resulted into exploitation of HTTP messages. HTTP uses \textit{GET} and \textit{POST} methods to fetch the data to the client from the web server. A \textit{GET} request includes static pieces of information like images etc whereas \textit{POST} requests are the data that includes input field values. During an HTTP based flooding attack the \textit{bots} are used to send large number of HTTP \textit{GET} or \textit{POST} requests. The server has to allocate resources for processing of these requests and in the face of huge traffic of HTTP requests the server caves in.

4. **TCP SYN Datagram Flooding Attacks:** The most famous of the flooding based attacks is the Transmission Control Protocol a.k.a TCP SYN flooding attacks. The attackers exploit the design flaw in the TCP three-way handshake required for connection establishment by the TCP clients and servers. This requires a small explanation. As shown in the Figure 1-5 in a normal TCP connection establishment request, a SYN packet is sent by the client to the server. The server receives the request, checks its resources so as to fulfill the request and if everything is ok then replies with a \textit{SYN ACK} packet. This \textit{SYN ACK} datagram is received by the client and the client sends an \textit{ACK} datagram as part of the three-way handshake. On receiving the \textit{ACK} datagram
the connection is established between the client and the server.

During TCP SYN datagram based flooding attacks large number of TCP SYN requests are sent by the *bots*. The server on receiving the requests blocks its resources for the client and waits for the ACK from the client. It is called half open connection. The attacker smartly fails to send the ACK to the server. As a consequence the TCP buffers get filled up and the server fails to service the legitimate requests. The designers of TCP have given the provision of time-period to handle half open connections but during flooding the rate of flood packets is so high that time-period fails to provide the support.

**1.2.1.2 Low-rate based DDoS Attacks**

It is no hidden fact that hackers are always looking out for more lethal and stealthier attacks to cause damages to internet services. Shrew attacks popularly know as Low Rate Denial of Service (LDoS) attacks are one such stealthy attacks. First reported by Kim et. al. in (165), a series of their variants, namely, LDoS, PDoS, distributed PDoS, stealthy LDoS (165), (207), (145), (208), (209), (210), etc., have cropped up
in the recent years. This thesis considers these attacks as Pulsating Denial of Service.

Low-rate Denial of Service attacks were first introduced by Kizmanovic in 2003 (145). They were called *Shrew Attacks*. They used Active Queue Management (AQM) techniques to detect and mitigate these attacks. These attacks introduced a new dimension in the area of Denial of Service attacks generation, detection and mitigation mechanisms. LDoS attacks exploited the vulnerability of Transmission Control Protocol (TCP) mainly responsible for carrying the internet traffic. A. Kuzmanovic used small data pulses to inundate the victim in a way so that when TCP’s congestion window is in its additive increase phase it experiences heavy traffic and as a result shrinks its congestion window. As a result the user services get affected. With time these attacks have become more lethal. Over the years various other variants of LDoS attacks have been discovered.

Luo and Chang named low-rate DoS attacks as Pulsating Denial-of-Service (PDoS) attacks (207). A PDoS attacker generates a sequence of false congestion signals to a TCP sender using attack pulses, so that the senders congestion window is constrained to a low value. Therefore, that could seriously degrade the throughput of TCP flows. LDoS attacks are termed as one of important examples of Reduction of Quality (208). RoQ is an attack that exploits system dynamics, i.e., the characteristics of a systems transient behaviour as opposed to its limited steady-state capacity, to achieve the adversarial goals. The PDoS attacks are highly complex and cause more damage than the contemporary flooding-based attacks. The primary reasons for investigating these attacks are:

1. **Tough Tracing:** Traditionally denial of service attacks are detected based on average increase in the data flow because of the attacks but pulsating denial of service attacks have low average rate of flow and hence the old anomaly detection techniques fail in tracing these attacks.

2. **Hacker’s favourite:** To launch a successful distributed denial of service attack the attackers generally use the slave nodes or the bots. These bots or zombies are compromised machines present in the internet and hence the automatic pulse
generating softwares are installed on these machines through malware malfunc-
tions. At some instant in time these bots send small untraceable pulses to the
victim node and bring it down. Because of low individual rate of these pulses
they cannot be identified easily and therefore they are a hacker’s favourite.

3. **Stealthy nature:** Pulsating denial of service attacks the victim node by ex-
ploting the TCP’s weakness in congestion control. Since the congestion control
mechanism is dependent on RTT and henceforth on RTO the pulses impact
the victim in such a way so that the victim shrinks its window and therefore
the amount of outgoing data in the link. As a result the network link receives
less number of packets and therefore its busy bandwidth reduces. Now these
attacks can be used to grow and consume the unused bandwidth and become
more lethal in their attack.

![Figure 1-6: PDoS attack flow parameters. Source: Kuzmanovic et al. (145)](image)

Figure 1-6 shows the parameters for single PDoS attack flow in which the attack-
ing node sends pulses of duration $L$ and rate $R$ in a deterministic on-off pattern with
period $T$. A successful PDoS attack therefore requires rate $R$ that is large enough
to induce loss, of duration $L$ of scale RTT and time period $T$ of scale RTO so that
whenever a legitimate flow tries to come out of timeout it is faced with another loss
of packets. The period $T$ is computed by the estimated RTO timer implementations
using above equations at the legitimate users. During the burst with a peak rate $R$,
the PDoS pulses create a severe congestion on the links to the TCP victim server.
Depending upon the attack period $T$ and length of the pulse one can have variable
nature of the attack flows. Figure 1-4 shows distributed PDoS (PDDoS) attack. By using zombies the attacks can be launched as distributed attacks with lower traffic rates and longer time periods, thereby making their detection even more difficult.

1.2.2 DDoS ATTACK TARGETS

A DDoS attack may have an application like world wide web, an end-system host, core network, or network infrastructure as its target for damage. In the case of application-based DDoS attack the loss incurred is in terms of quality of service being provided as well as goodwill of the service provider resulting in loss of revenue whereas in the case of end-system host based the vulnerabilities of the end-systems are exploited. For example, by exploiting bugs in the particular algorithms, CPU utilization, memory allocation, authentication and authorization protocols etc., the attackers can hack the systems and can then use these compromised systems in launching attacks. The traffic from host-based DDoS attacks is low but damage is done in terms of system crash or consumption of large amount of system resources thus affecting the services of legit users. The most damaging ones are still the core-network based and infrastructure-based DDoS attacks. In these type attacks the damage is done by consuming the bandwidth of bottleneck links and denying the services of the servers to legit users. The loss is in terms of goodwill as well as revenue. Out of all the possible DDoS attack targets our thesis work is focused on development of detection techniques against flooding based DDoS attacks that target the core-networks and applications at the end-systems. Figure 1-7 shows the three attack target locations of DDoS attacks:

1.2.2.1 DDoS Attacks Targeting Core Networks

The Core Networks have limited amount of infrastructure like routers, switches, network links, servers etc. These equipments have fixed buffer sizes and bandwidths. The network-based DDoS attackers exploit this weakness of the Core Networks. DDoS attacks of this type target to bring down the data carrying links by sending mass junk data messages that cause buffer overloading at the end-systems or depletion of
network bandwidths. Typically, *ICMP_ECHO* packets are used for flooding but these days any other type of packets like UDP, TCP, IGMP, VoIP, etc., can be used to launch an attack. With the help of *bots* and *spoofed* IP packets the attackers can not only attack stealthy attacks but can hide their identities as well. TCP based SYN flooding, ICMP based smurf flooding, UDP flooding are few such examples.

### 1.2.2.2 DDoS Attacks Targeting End-System Applications

End-system Application Layer DDoS attacks are a new breed of DDoS attacks that are sophisticated in their approach and do not require mechanisms like flooding. The important reason of their success is *bots* and the high-speed internet access. These attacks exploit the weakness of the firewalls due to the fact that application layer protocols like HTTP, DNS etc. do not provide security in terms of users of these protocols and therefore the firewalls cannot distinguish between the legit and the illegitimate user. HTTP GET requests, DNS queries as well as SIP INVITEs are request-flooding application attacks. Similarly, asymmetric attacks with large amount of data for processing by the web server leading to resource consumption and repeated one-shot attacks with high workload of large number of TCP sessions resulting into degrading of the services also fall in the category of application-based DDoS attacks. SQL injections, hidden-field manipulations, cookie-poisoning etc. are another case of application-exploit DDoS attacks. DNS amplification attacks are an example of this type of attacks.

### 1.2.3 DDoS ATTACK DEFENSE

Although a number of tools and techniques have been proposed in the last two decades, it is still very difficult to detect these attacks due to the large number of bots and spoofed IP addresses. DDoS attacks come in various forms and sizes and are like an albatross around the neck of internet service providers. Detecting DDoS attacks quickly and accurately in network traffic is therefore an important area of study in the current field of research (20), (24), (33), (37), (40), (41).
1.2.3.1 DDoS Defense at the Source End

DDoS defense mechanisms are placed near the sources of the DDoS attack. Their main objective is to disallow the generation of DDoS attacks in the network. These mechanisms are deployed at the routers of the Autonomous Systems (ASes) of the edge-networks. Traditionally, the defense mechanisms have been placed near the source ends. Two of the famous defense mechanisms in this category are D-WARD (25) and MULTOPS (26).

Although source-based defense mechanisms successfully detect the DDoS attacks at the source end and are quite effective in mitigating the attacks but they have few failure points as well. These mechanisms fail when the source of the attacks is distributed along different domains and all the attack sources use IP spoofed addresses. These mechanisms also fail because at the source end the volume of attack traffic packets to the normal traffic packets is small and hence distinguishing the malicious packets from the regular packets is not easy. Moreover, internet applications are dependent on ISPs and not everyone can be made to agree to take responsibility of maintaining and updating these algorithms at the edge networks.

1.2.3.2 DDoS Defense at the Victim End

In the DDoS defense mechanisms deployed at the victim end the detection and mitigation of DDoS attacks is done at the victim server. These mechanisms are installed either at the edge network routers of the victim end or on the access routers of the victim servers. Some of the popular DDoS defense mechanisms at the victim end are IP Traceback mechanisms (27), (28); Management Information Base (MIB) (29) and Packetscore (30). The challenge faced by these mechanisms is that by the time an attack is detected it is in full swing. Therefore, these mechanisms are required to be fast and accurate in detecting attacks. They also suffer from the problem of deciding whom to stop, because at the victim server stopping all the incoming and outgoing packets immensely affects the QoS of the server. But they have an important advantage over the source based mechanisms in a way that these mechanisms need to
be deployed at access routers only and since victim servers are always the interested party, therefore their deployment responsibility is easily taken up by them.

1.2.3.3 DDoS Defense in the Core Network

Core network DDoS defense mechanisms are placed inside the routers of the first-level AS domains. These mechanisms if deployed successfully are considered to be the most effective ones in handling packet drops due to congestion caused by DDoS attacks. Some of the common ones amongst them are route-based packet filtering (31), and detecting and filtering malicious routers (32) (e.g., Watchers). But they suffer from the two most challenging problems of storage and scalability. The mechanisms need to be installed at all routers for effectiveness and this increases the cost of deployment. Moreover maintaining and updating of these mechanisms also requires co-ordination amongst all routers which in practical scenarios is difficult to achieve.

![Figure 1-7: Different Target Locations for DDoS Attacks](image)

All three of the mechanisms have their advantages and disadvantages with respect to strength of the attack and goodwill of the service provider. No single one of
them can be considered the best over the others. We, however choose DDoS defense mechanism for the victim end for two main reasons. Firstly, the need of deployment at the access router only makes it a favourable candidate and secondly, our detection mechanism is dependent on measuring the variability in self-similar behaviour of the network traffic and their characteristic can be best captured at the server end only. The details of the literature surveyed for this are given in chapter 2.

1.3 THESIS OUTLINE

The thesis has been organized into eight chapters. The necessary details pertaining to fundamental concepts, state-of-the-art research done in the area, proposed scheme, received results, analysis and conclusions have been covered and chapterized as follows:

The first Chapter is the introduction chapter and fundamentals of the internet and its vulnerabilities have been explained along with definitions of anomalies, anomaly detection and how DDoS attacks fit in as network-traffic based anomalies. Brief explanation on various types of DDoS attacks and necessary background on current and traditional varieties of DDoS attacks has been covered in the chapter. Since self-similarity is locus of our detection methodology therefore the relation between self-similarity and DDoS attacks has also been explained.

In Chapter 2, the chapter provides state-of-the-art research that has been conducted in the field of DDoS attack detection and mitigation. The comprehensive review of supporting literature on self-similar aspects of the computer network traffic and detection of DDoS attacks based on self-similarity estimation techniques is given. In the chapter we highlight the limitations of each of the defense techniques and in accordance to the identified shortcomings, proper justifications have been provided that associate to our research issues. The chapter also draws attention to the role of visualization techniques in detection of anomalous events in the network traffic and presents summary of various visualization tools. Later, identified knowledge gaps and problem statement formulation have been covered.
Chapter 3 is a prelude to the later chapters. It explains the concepts of self-similarity, presence of self-similarity in the computer network traffic and key characteristics of self-similar processes. The chapter also presents briefing on Hurst estimation to measure self-similarity and details of wavelets based estimation of Hurst parameter. Descriptions of fast-pyramid algorithm and role of multiresolution analysis in diagnosis of fractal behaviour has also been provided.

Chapter 4 presents our proposed generic detection methodology- Multi Scale Network Anomaly Detection (MS-NAD) and pre-test experiments. There are four phases of MS-NAD, namely, filtering of the computer network traffic, computation of wavelet coefficients, Hurst estimation and plotting of Multi Resolution Outlier (MRO) map. Details of the four phases are covered in depth in the chapter. Two pre-test experiments for measuring presence of self-similarity in synthetically generated traces of web-traffic using PackMIME and for measuring the self-similarity on a publicly available dataset and their findings have also been discussed in the chapter.

In Chapter 5, the focus was to study the behaviour of traditional flooding-based DDoS attacks and distinguishing them from other anomalies in the network traffic. Different network traces have been generated and analyzed for DDoS flows ranging from low to high intensity in scenarios consisting of varying types of protocols. The second part of Chapter 5 is devoted to distinguishing between flooding-based DDoS attacks and flash crowds (FCSs). FCSs are sudden increase in traffic due to spontaneously created curiosity in the web users. The sources of flash crowds are spread across Tier-3 networks, send legitimate HTTP GET requests and the flash crowds converge to one point because of the users interest in one web page only. The detailed discussion of results has also been done.

In Chapter 6, we firstly provide background on PDoS attacks, different types of PDoS attacks and how they are different from each other followed by the basic congestion control mechanism of TCP and how exploitation of the TCP’s Timeout Phase can be done by PDoS attacks. The chapter covers in detail modeling of PDoS attacks. Aforesaid attacks are primarily dependent upon three variables, namely, length of the attacking pulse, rate of the attack and duration of the attack. The
network traffic trace was also checked for presence of self-similar behaviour using the logscale plots. The chapter covers visuals generated by the *MRO map* as well. The results for all kinds of observations for detection of attacks have been covered later in the Chapter.

Chapter 7 presents an evaluation of our algorithm on real traces of KDD Dataset. The KDD dataset has attacks divided into four different categories with DoS attacks being one such category. There are six types of attacks under DoS namely, *Smurf, Neptune, Teardrop, Ping-of-Death, Back* and *Local Area Network Denial*. The detection results based on Hurst values, logscale plots and MRO maps have been discussed in the chapter.

Finally, conclusions and future work is given in Chapter 8 followed by references, author’s publications and synopsis at the end.