1.1 Introduction

Information Technology (IT) Administrators are continuously facing the troubles that are created by the attack in the internet. Nowadays, there is an enormous range of solutions in the market to assist, and protect against such threats, but they are either expensive or complicated to set up, and more complex to construct correctly. The attacks circulating on the internet range from malicious viruses designed to destroy or corrupt data, to robot networks (more generally known as botnets) with intelligent coding that permits them to intercommunicate with each other. The attackers then capture the private data (like bank account numbers, and credit card information) and send them back to the holder of the malware.

It is significant to make efforts to develop a technology, and build new methods of mitigating the attacks that happen on the internet every day. Malware disturbs the vulnerable computers all the time, and the attackers generate the malware by using snippet code (reusable code) continuously. Malware affected victim network is more complicated, and the attackers have the caliber to manage as many computers at a time.

One of the main problems is that the Internet Protocol (IP) is intended to be as lightweight as possible, and generally too late to identify the malicious activities in the network. The proposed work aims at identifying and mitigating the compromised machines (frequently referred to as zombies or bots), especially, those that are used for attacking the web servers and affecting the accessibility services.

These robotic networks are typically controlled by one person such as an intruder. This person has the facility to command the botnet, and creates synchronized attacks pointed at a website to carry the services in offline. Figure 1.1 demonstrates the typical taxonomy of zombies (compromised machines). The victim might be any service from Hyper Text Transfer Protocol (HTTP) to Domain Name Server (DNS).
The Internet comprises of hundreds of millions of computers all around the world. Millions of people make use of the internet every day, taking full benefit of the available services at both personal and professional levels. It is an easy target for malicious users in World Wide Web (WWW) who try to exhaust their resources, and initiate the Denial of Service (DoS) attacks.

A DoS attack is a malicious effort by a single person or a group of people to begin to attack the victim, site, or node to deny the services to its customers. When this effort derives from a single host of the network, it comprises a DoS attack. In contrast, it is also possible that a lot of malicious hosts organize to flood the victim with a large amount of attack packets. Consequently, the attack takes place at the same time from multiple points. This kind of attack is known as Distributed DoS, or DDoS attacks.

Figure 1.1 Typical taxonomy of zombies
1.2 Denial of Service attack (DoS attack)

A Denial of Service (DoS) attack is described as one computer disturbing another to affect the legitimate users services as shown in figure 1.2. There are different ways in which DoS service attacks could be carried out, such as, to flood a network in traffic, the large amount of bandwidth being consumed, and to disturb a specific service based on known flaws. With today’s computing influence on bandwidth resources, it is more and more complex for one single machine to bring down another by exhausting its resources.

![Figure 1.2 Denial of Service (DoS) attack](image)

**Figure 1.2 Denial of Service (DoS) attack**

For example, it is assumed that, one current DoS exploit has been discovered in the web server software httpdx (Jasper, 2009) when processing a request. Since the request could be issued differently from any computer linked to the internet, and does not need a great amount of resources to take it out, it is extremely dangerous and can cause terrible failure with the services. The probability of a server brought offline as an outcome of this type of attack is high, and most software vendors will appear to cancel the vulnerability right away.

1.2.1 Distributed Denial of Service (DDoS) Attack

Distributed Denial-of-Service (DDoS) attacks are generated by a huge number of compromised systems that attack a single target, which cause a Denial of Service for
users. The flood of inward messages to the target system forces it to shut down, which deny the service of the legitimate user. A single compromised system called as DDoS master is used to launch a DDoS attack in the victim network. The intruder recognizes and communicates with other systems that could be compromised through this DDoS master.

The intruder loads various fast tools in the victim environment for generating the DDoS attacks, or occasionally using thousands of compromised systems. By a single command, the attacker creates many flood attacks against a particular target. The malicious users affect the target system by involving numerous victims and all these compromised systems are controlled by the intruder.

DDoS attacks exhaust the victim resources by hundreds of application service requests simultaneously. Figure 1.3 demonstrates the simple Distributed Denial of Service (DDoS) attack. This figure shows that five computers are making a request to the victim every minute. So the victim is in trouble to process these continuous requests.

Each compromised computer affects 5,000 compromised computers every minute in the internet, so that 25,000 requests would be processed by the server. Without DDoS mitigation software or hardware it is probable that the server’s resources (for instance, CPU, Memory or Network Bandwidth) would be entirely exhausted.

Distributed Denial-of-Service (DDoS) attacks pose an enormous threat in the internet, and many defense mechanisms have been proposed to detect the problem. Attackers continuously change their tools to bypass the security systems, and researchers in turn modify their approaches to handle new categories of attacks. The DDoS attacks are rapidly becoming more and more complex in the victim environment. The variety of known attacks creates the impression that the problem space is vast, hard to explore, and address these issues properly.

On the other hand, existing defense systems deploy various strategies to counter the problems. It is difficult to understand their similarities and differences and assess their
effectiveness. DDoS attacks are large-scale coordinated attacks on the availability of services of a victim system or network resources, and are launched indirectly through many compromised computers in the internet. DDoS attacks can seriously weaken the internet service. There have been a number of proposals and solutions to mitigate the DDoS attacks. However, there is still no comprehensive solution which can protect against all known forms of DDoS attacks.

![Diagram of Distributed Denial of Service attack](image)

**Figure 1.3 A simple Distributed Denial of Service attack**

**Types of DDoS**

Basically, DDoS attacks can be divided into two categories namely bandwidth attack and resource attack, as shown in figure 1.4.
- A bandwidth attack simply tries to generate packets to flood the victim’s network. So, the legitimate requests cannot go to the victim machine.

- A resource attack aims to send packets that misuse network protocol or malformed packets to tie up the network resources. So, the resources are not available to the legitimate users.

![Diagram showing types of DDoS attacks]

**Figure 1.4 Types of DDoS attacks**

A bandwidth attack generates a flood in a network with large volume of bogus packets, in order to overwhelm the victim’s network bandwidth. The objective is to consume the network bandwidth of the targeted network, to such an extent that it starts losing the legitimate packets. The loss of legitimate packets cause a Denial of Service to valid users. In general, a huge number of machines are required to generate the volume of traffic to flood a network. This is known as a Distributed Denial of Service (DDoS) attack, which is caused by several machines that combine together to generate the flood traffic.

In addition, the malicious requests are generated by different machines that are a part of different networks to consume the legitimate resources. Hence, a single network cannot either consume or block the resources. In a typical DDoS attack, bogus packets are simple web server requests or other random packets are sent by large number of machines to the target network or machine.
Based on the exhausting processor and memory resources of victim systems, attacks can be considered as TCP-SYN (Transmission Control Protocol Synchronize) attacks and PUSH-ACK (PUSH Acknowledgement) attacks.

**TCP-SYN attacks**

DDoS Resource Depletion Attacks are created by attackers through the sending packets. These attacks target the network protocol communications that congest network resources, and avoids access for legitimate users. In TCP-SYN Attacks as shown in figure 1.5, the TCP process may include a full handshake between a sender, and a receiver before data packets are transmitted. The initiating system broadcasts a SYN request, and the receiving system will respond by returning an ACK along with its own SYN request. Again a sender sends back its own ACK to allow communication between the two systems.

![Figure 1.5 TCP-SYN attacks](image)

The receiving system transmits a SYN packet to the sender but it does not get an ACK. So, the receiver will resend a new SYN packet after sometime. The processor and memory resources at the receiving system, will be kept for TCP-SYN request until a timeout happens. This is known as resource starvation attack. A DDoS TCP-SYN attack will exploit the TCP function, where zombies will send bogus TCP-SYN requests to a
victim server. It efficiently saturates the server processor resources, and avoids processing the legitimate requests.

It predominantly exploits the three-way handshake between the sending system and the receiving system by sending huge volumes of TCP-SYN packets to the victim system with spoofed source IP (Internet Protocol) addresses. Ultimately, when large volumes of TCP-SYN attack requests are sent and repeated, the victim system runs out of memory and processor resources. Therefore, the system is unable to process the legitimate user requests.

**PUSH-ACK attack**

The PUSH-ACK attacks are like a TCP-SYN attacks in exhausting processor and memory resources of victim systems. A PUSH is a one-bit flag marked within a TCP header. In the TCP process, packets that are transmitted to a destination are buffered within the TCP stack. These packets will be proceeded to be sent to the receiving system once the stack is filled. By setting the PUSH bit to one, the sender requests the receiving system to discharge the contents of the buffer before the buffer becomes filled. In order to reduce the processing overhead, TCP stores incoming data in large blocks for routing on to the receiving system. While this process is repeated with several agents, the receiving system may not be able to handle the large volumes of incoming packets and will result in a collapse.

Malformed packet attacks are maintained exactly by zombies, which send incorrectly formed IP packets to victim system so as to crash it. There are usually two different levels of malformed packet attacks. One is the IP address attack, in which the packet holds the same source and destination IP addresses. This complicates the victim operating system and causes it to crash. The other one is IP packet options attack, in which, an altered packet randomizes optional fields within an IP packet, and sets all quality of service bits to one. Thus the victim systems will be compelled to take additional processing time to examine the traffic. When this attack is repeated using several agents, this may lead to a shutdown of the processing ability in victim systems.
1.3 DDoS impact

Distributed Denial-of-Service (DoS) attacks are happening in the network for a long time. In the computer network field, DDoS attacks typically take one of the two forms. The first form uses bugs in network clients or server applications, in an effort to crash the application (and probably the host on which it is running). The second form floods a network server with false traffic, and makes it hard or not possible for the server to get and process the legal traffic. In buffer swarming attacks, a network application sends a huge amount of data which it fails to hold correctly, instead of overwriting critical information with the surplus data.

Some companies do not receive enough security for their systems. They are easily compromised and pose a threat not only to the companies themselves, however, also to anyone else targeted by a hacker. Protecting against DoS attacks involves using safe operating systems such as Unix, which present process protection (to prevent an application crash from crashing the whole system), keeping up-to-date with safety patches and vulnerability alerts (to avoid running applications which are vulnerable to buffer overrun attacks), and also examining and controlling the network traffic (to handle flood attacks).

A DDoS attack creates network flooding. Since, the attack is launched from hundreds or even thousands of hosts simultaneously, rather than appearing as an excess of traffic coming from a single host, a DDoS attack appears as normal traffic coming from a large number of hosts. This makes it harder to identify and control.

Even when an attack has been identified, it is very difficult to trace back to its origin as so many compromised hosts are involved. When there are many hosts involved, the logistical problems of reducing the attack and identifying the real origin are enormous. The programs used by the attackers commonly use 'address spoofing'. It means that they put fake source addresses in the packets that they send out.
In such a case, tracing the attack back involves examining the logs of all of the middle routers, individually, to trace the packets back one hop at a time. This causes the task almost not possible, and still there is no solution to arrest these attacks. Not only these attacks are inflexible to trace back, but there is no comprehensive protection against them. The internet was not designed with these vulnerabilities in mind, and a real solution would engage re-engineering the entire network architecture. This implies that it is dangerous to take preventive measures to decrease the possibility of these attacks and reduce their impact.

1.4 DDoS - Threats

DDoS attacks have caused rigorous damage to servers, and will cause even larger threat to the development of new internet services. Conventionally, DDoS attacks are at the network layer, such as SYN flooding (Synchronize), ICMP flooding (Internet Control Message protocol), and UDP (User Datagram Protocol) flooding, which are said to be Net-DDoS (Network layer Distributed Denial of Service) attacks. The aim of these attacks is to use the network bandwidth, and deny service to legitimate users of the victim systems.

For mitigating these Net-DDoS attacks, many studies have noticed and proposed various schemes (like network measure or anomaly detection) to defend the network, and equip from the bandwidth attacks. It is not as simple as in the past for attackers to initiate the DDoS attacks on network layer. While the simple Net-DDoS attacks are unsuccessful, attackers shift their offensive strategies to Application-layer attacks, and found a more complicated type of DDoS attacks.

The following are the different ways in which the App-DDoS attacks take place.

- Avoiding detection by attacking the victim web servers using legitimate HTTP GET requests (such as HTTP Flooding)
- Pulling large image files from the victim server in overwhelming numbers.
• Attackers running a large number of queries through the victim’s search engine or database query to push the server down.

Application Layer DDoS (App-DDoS) attacks as shown in figure. 1.6. MyDoom worm, and the CyberSlam are all known examples of App-DDoS attacks.

![Diagram of App-DDoS attacks]

**Figure 1.6 App-DDoS attacks**

DDoS attacks persist to threaten networks and computers connected to the internet. Next to proprietary information robbery, DoS attacks cause largest financial setback. CERT (Computer Emergency Response Team) describes the DoS attack as the avoidance of authorized access to a system resource, or the delaying of system operations and functions. While other classifications for DDoS attacks exist, DDoS attacks are
usually separated into two wide classes. One is ‘logic-based’ attacks, which use vulnerabilities in a system’s software to make it unable to respond to valid user requests. The other is ‘flow-based’ attacks, which weaken the available resources, for instance CPU cycles, system storage or network bandwidth.

In the current study, it is suitable to differentiate the class of flow-based DDoS attacks between those that use target resources, and those that use bandwidth. The resource consumption attacks, such as, TCP-SYN attack, weaken the available memory on the target machine by overwhelming the connection requests. The bandwidth consumption attacks, for instance, in the well-publicized 2000 attacks that can take place at any time, a traffic of nearly 3.5 Gigabits per hour is seen to flood the target networks of e-commerce sites, and the legitimate users are denied access to use the available network bandwidth.

A single-source flow-based DDoS attacks are still observed in the internet. DDoS attacks are one in which various traffic generating sources take part in attacking a target system. These attacks usually involve unsuspecting compromised machines or zombies that assist to flood a target machine with traffic. The impact of DDoS attacks has improved progressively in recent years, because more computers are attached to the internet. A growing supply of zombies and target machines, become available to the attackers wishing to launch a DDoS attacks. A current survey estimated that approximately 4000 DDoS attacks per week are active in the internet at any specified time. The DoS and DDoS attack tools have advanced considerably in the recent years, showing the proof of increased sophistication in automation, extension, and secrecy.

1.4.1 Attack tools

Attack tools are easy to utilize. Even hackers with limited coding experience may launch worms, and scripts that cause injure with the help of expert attackers. Some systems use Remote Monitoring (RMON) data to model the network traffic activities, and to notice flow-based, bandwidth DDoS attacks. RMON is a Management Information
Base (MIB) design to employ with the Simple Network Management Protocol (SNMP) that checks the attributes of network devices as shown in figure 1.7.

![Diagram](image)

**Figure 1.7 RMON to detect network traffic**

In the family of RMON MIBs, RMON1 recognizes the attributes of low-level ethernet traffic that will be used to differentiate the network utilization through byte, packet, and error counts. The RMON1 specification is assisted by most enterprise routers manufactured by CISCO and NORTEL, and therefore removes the requirement for the special purpose of DDoS detection hardware. Furthermore, the SNMP management model requires no reconfiguration of the network being monitored. An SNMP network manager occasionally queries an agent for the attributes in SNMP traffic, and it only initiates a small amount of load on the network.

One group of researchers used RMON in order to know when the traffic destination addresses exceeded the expected limits. This study relied upon RMON2 which checks network, and application layers 3 and 4 of TCP/IP traffic. Even though good detection capability can be established using RMON2, it is not universally supported by today’s network traffic devices. RMON2 relies upon variables for DDoS discovery, but it needs a different method for monitoring the indicators of network congestion to point out the anomalous DDoS traffic.
1.5 Authenticity of packet

Token is issued to the client by the overlay network, and it is used to confirm the authenticity of each packet communicated by the client (figure 1.8). The purpose of a token is to improve the necessity to maintain the application or network-level state of any overlay nodes. Even though the attackers use the state dependence to attack the overlay nodes, the network seems to be protected from the DDoS attack.

![Diagram of packet authenticity](image)

**Figure 1.8 Authenticity of packet**

The major challenges should address, related to the scheme’s effectiveness (in terms of performance and latency of the continuous path), resiliency of attacks, quantity of states that requests to be maintained by every overlay node (essential to prevent packet replay or forging attacks), and the removal of communication pinch points on which the attackers will focus their attention. In order to effectively attack the victim network, an attacker will have to subvert or suppress 40% or more of the overlay nodes. So, the network become unusable for all the users. Therefore, the network needs an operational threshold in the order of 40% of the nodes being subverted [1].

When 40% threshold is reached, the users will not observe a significant impact of their connectivity. By a comparison, in the original SOS (Secure Overlay Service) architecture, the user has to discover an Access Point(AP) that is not under attack, which becomes gradually more difficult as well as increases the portion of nodes under attack.
Foremost, DDoS attacks on networks comprises of Authentication Request Flooding (AuthRF), Deauthentication Flooding, Association Request Flooding (AssRF), and Disassociation Flooding. These DDoS attacks affect the network or some of its wireless nodes which are out of services. DDoS attacks against networks become more and more complex. Hence, the researchers have improved their interests, publications on the issues, and gave the solutions for such DDoS attacks. Those publications increase the awareness of DDoS attacks, offer wireless users and network managers with cooperative practices to protect their networks, but still, there are no studies to concentrate on solutions to decide AuthRF and AssRF DDoS attacks. Additionally, there are no investigational studies on the effects of these DDoS attacks on network performance, data integrity, and user experience of time sensitive applications.

1.6 Flash crowd (Application DDoS attacks)

A new special phenomenon of network traffic known as flash crowd, has been observed by the researchers in the past years. On the web, flash crowd describes the state when a very huge number of users concurrently access a popular website (figure 1.9). It makes a rush in traffic to the website, and may cause the site to be nearly unreachable. Since, burst traffic and large volume are the general characteristics of App-DDoS attacks or flash crowds, it is not simple for current techniques to differentiate them merely by statistical characteristics of the traffic. So, App-DDoS attacks might be stealthier, and more risky for the commercial websites than the common Net-DDoS attacks.

Resolving the network Denial of Service (DoS) problem is very hard. Due to the open nature of the internet, the router vendors and network operators are unwilling to operate new potential difficult mechanisms. Overlay based methods such as Secure Overlay Services (SOS) and MayDay, present an attractive alternative. Because, they do not need changes to protocols and routers, which require only minimum collaboration from Internet Service Providers (ISPs), such systems employ wide network nodes, that perform as first-level firewalls, discriminating among legitimate traffic and malicious traffic, based on various kinds of users or end-host authentication.
The adversaries suppress the functionality of network, because attack traffic must be split among all the nodes to disrupt the protected interactions. Indirection based Overlay Network (ION) methods depend on the inability of an adversary, to find out the connectivity information for a given client and the infrastructure. This makes them vulnerable to a variety of easy to launch attacks that are not considered in the standard risk model.

For instance, adversaries might possess real-time knowledge of the specific overlay nodes of a client in routing the traffic through, or might be attacking nodes using a time-based system. It will try to exploit the impact of the attack on clients connectivity. Such attacks will be network-oriented (like TCP-SYN attacks) or application-related targeted attacks or sweeping attacks.

In targeted attacks, an attacker has information about the client communication parameters, and defeat the nodes in the network. When the client realizes (usually after
some timeout period) that the overlay node is impassive and switches to a new node, the attacker also shifts to that new node. Therefore, an attacker will bring down a single node and will make a targeted DDoS for specific clients. Related attacks are exploiting information that should only be available to trusted components of the system. However, an attacker will possibly gain access against almost all anti-DDoS mechanisms.

In sweeping attacks, the attacker employs its power (which is inadequate to bring down the whole ION) to disturb the overlay nodes at a time. This kind of attack targets the application-level state preserved by the client overlay node. Damaging this state, forces the client to restore both network and application-level connectivity, it corrupts the client connection, leading to DDoS for time-critical or latency-dependent applications. Therefore, IONs are affected by vulnerable DDoS attacks.

1.7 DDoS consequences

DoS/DDoS attacks are a dangerous, comparatively new type of internet attacks. The attackers affected the largest web sites owned by the most well-known E-Commerce companies like Yahoo, eBay, and Amazon. They find it difficult to get customers, partners, and users, up to twenty-four hours and several web sites have experienced numerous days of shutdown. Then they try to re-establish the services, and the financial losses are very massive. The report ‘2003: CSI (Computer Security Institute) / FBI (Federal Bureau of Investigation) Computer Crime and Security Survey’, help to know about the impact of DoS/DDoS attacks in America.

The international terrorist organizations employ the DoS/DDoS methods to attack the web sites or internet systems of U.S. Government, and military successfully. It causes the outcome which is terrible and unbelievable. So, for guarding both American national security and commercial security, it is important to detect, prevent and mitigate the DoS/DDoS attacks.

The popularity of networks meets a continuous demand in security against attacks in that networks, and the 2005 study from Computer Security Institute (CSI) and Federal
Bureau of Investigation (FBI) demonstrates that network abuses (like security attacks) are the only growing threat of computer crimes. The network security attacks are categorized into two types. They are crypto attacks and DDoS attacks. The crypto attacks comprises of unauthorized access, man-in-the-middle, masquerading, eavesdropping, replay, tampering and session hijack. In general, security solutions of VPN (Virtual Private Network) and 802.11i provide an effective mechanism to address crypto attacks. Unfortunately, these solutions are not suitable to protect the networks against DDoS attacks.

Meanwhile, to prevent DDoS attacks on networks, 802.11w task group works to protect the management frames and action frames. The mechanisms or protocols to protect these frames are very similar to the protection of data frames using the keys derived for TKIP (Temporal Key Integrity Protocol) or CCMP (Counter mode with Cipher block chaining Message authentication Protocol). However, there are some limitations in the draft version of 802.11w. First, all management frames sent or received by a station before keys are derived. Secondly, 802.11w does not mention how to protect and prevent Authentication Request Frame (AuthRF) and Association Request Frame (AssRF) DDoS attacks.

A Denial of Service (DoS) attack is an attack, with the purpose of preventing legitimate users from using a specified network’s resources such as a website, web service, or computer system. A Distributed Denial of Service (DDoS) attack is a coordinated attack, on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems. The services under attack are called ‘primary victim’, while the compromised systems used to launch the attack are often called ‘secondary victim’.

By being anonymous, the secondary victim in a DDoS attack provides the attacker with the ability to pursue a much larger and more disruptive attack. The secondary victim actually performs the attack making it more difficult for the network forensics to track down the real attackers. Attacks against a variety of companies provide an anti-spam
service. These attacks caused many of them to shut down their services. DDoS attacks are relatively new and not well understood.

1.7.1 DDoS attacks on network services

Denial of Services (DoS) attacks aimed at disrupting the network services by simple bandwidth exhaustion attacks, and those targeted at flaws in commercial software (COTS - Commercial Of The Shelf). These types of attacks are not new, and have produced overwhelming effect to prevent normal operation of the victim sites. Historically, these attacks by hacktivists and extortionists alike have targeted companies as diverse as eBay and Microsoft, the Recording Industry Association of America (RIAA) and Shanghai Corporation Organization (SCO), and a plethora of online gambling companies.

Attackers have not exploited the full range of vulnerabilities present in many online services. Particularly, attacks aimed at the application and data processing layer. With the rise of increasingly targeted and motivated attacks, these application level DDoS attacks will be exploited certainly for immoral gains.

Conceptually, DDoS attacks are intended to prevent legitimate users, customers or clients of a site from accessing it successfully. Traditional DDoS attacks have been aimed at consuming resources or disrupting the services at the network or operating system level. Typical examples are server based attacks such as SYN floods and bandwidth exhaustion attacks that attempt to saturate the victim’s internet connection with illegitimate traffic. With remedy measures for Network DDoS attacks, adversaries change their strategy to be offensive on the application layer services provided by the internet server such as, mail services, social network communication, blog and forum initiatives.

The application service attacks are generated to the victim web servers by HTTP GET requests (like HTTP Flooding) and POST requests, frequent access of large sized files from the victim servers. DDoS attackers initiate more number of repeated queries on
target application search engine and transactional query to deny the regular service being carried out by the server. These types of DDoS attacks are specified as application layer attacks.

Recent researches worked on application layer DDoS attacks such as flash crowd which cause massive problem in internet application servers. As very large number of users simultaneously access a popular website, a surge in traffic is caused to the website which probe the application services to spend most of its services. Burst traffic and high volume data traffic are major characteristics of App-DDoS attacks and flash crowds which is not easy to identify from conventional DDoS attack resistance filters.

Normal App-DDoS attacks (like Flood) are resisted by enhancing the resistance mechanism for Network DDoS attacks, by verifying HTTP request rate, HTTP session rate, and duration of users access. However, App-DDoS attacks target at popular websites with increasing bandwidth flooding to more stealthy attacks hidden in the application volume of data traffic flow. These data traffic flow may be carried out in wired and wireless network initiatives.

1.8 Proposed work to mitigate DDoS attack

The nature of data traffic flow from wired network is extremely different from wireless network. Therefore, the DDoS application service attacks from the wired ones are produced as IP frame, and wireless ones from Media Access Control (MAC) frame. The variant in the frames motivates the requirement of enhanced resistive mechanism for Application DDoS attacks for internet application servers enabled with both wired and wireless networks. An Application Service Network Request Identification (ASNRI) technique is used for the wired and wireless access in internet application services. An ASNRI technique first identifies the type of data stream frame, and inputs to the IHBCM (Integrated Hidden Markov Model and Bayes Packet Classifier with Gaussian Distribution).
In IHBCM, the separated data frames are verified for the malicious characteristic to filter out the malicious frames. Simulations are carried out to evaluate the performance of ASNRI against the conventional App-DDoS attack resistance schemes based on the rate of true positive and true negative data frames, and the malicious attack resistance rate at different traffic volumes.

The Bayes packet classifier performs major role in IHBCM technique. The Gaussian factor, and ASNRI technique have been used to improve the quality of input by segregating the input streams. It leads to significant improvement in the accuracy of the Bayes technique. Integrated Hidden Markov Model (HMM) and Bayes Packet Classifier based Gaussian distribution factor is used to detect, and respond to App-DDoS attacks if they occur during a flash crowd event for both dynamic and stationary objects.

1.9 Literature review

The various scenario of DDoS attacks detection methods can be classified as four kinds. They are Net-DDoS attacks against steady backdrop traffic [2], Net-DDoS attacks against flash crowd (such as burst background traffic), App-DDoS attacks against stable background traffic, and App-DDoS attacks against flash crowd. The initial two scenarios have been well examined, and may be handled by most existing DDoS detection methods. The other two groups are fairly different from the earlier ones [3]. Moreover, the flooding attack pattern, App-DDoS attacks might focus on consuming the server resources such as sockets, memory, CPU, I/O bandwidth, and disk/database bandwidth.

In [4] authors introduced a categorization of Denial-of-Service attacks in accordance with the kind of the target (like web server, firewall, router), a source attack uses the network bandwidth, TCP/IP stack, and the used susceptibility of bugs or overload. This categorization concentrates more on the real attack phase, whereas this research involved in looking at the whole attack method in order to emphasize features that are exact to dispersed attacks. In [5] categorize brute-force DDoS attacks based on number of agent machines generate the attacks, and whether the attack was replicated or not.
In [6] and [7], Howard suggests classification of computers and network attacks. This classification concentrates on computer attacks in common, and does not adequately emphasize features specific to DDoS attacks. CERT is at present taking the proposal to develop a comprehensive classification of computer incidents as part of the plan of general incident data format and replace actions. However, unfortunately results are not thus far available. Business Branding Network (BBN) is also working on the protection of DDoS attack impression, however its results are not so far released [8].

The work in [9] offered an important discussion of the DDoS troubles, and of some security methods. A solid team of work on categorization survives in the area of Intrusion Detection Systems [10, 11, and 12], and presented useful reading for researchers in the DDoS protection field. With growing computational difficulty in internet applications and enhanced network bandwidth, access to the server assets might become restricted. Therefore, the App-DDoS attacks might cause more severe problems in the internet.

1.9.1 App-DDoS attacks

The initial feature of App-DDoS attacks is that the Application layer needs originating from the legal hosts are identical from those created by legitimate users. Contrasting the Net-DDoS attacks, App-DDoS attacks do not essentially rely on insufficiency in the fundamental protocols or operating systems. They may be increased with valid requests from legitimately associated network machines. App-DDoS attacks use the fault facilitated by the standard practice of opening services like HTTP and HTTPS (TCP port 80 and 443) via the majority of firewalls to initiate the attack [13]. Lot of protocols and applications, both legitimate and illegitimate, may employ these openings to channel via firewalls, over a standard TCP port 80 (such as Code Red virus) or in Secure Socket Layer (SSL) tunnels.

Attack requests intended at these services might pass through the firewall without being discovered. In addition, attackers might demand services to the point where other
trade are not capable to finish their transactions, or troubled to the point where they sacrifice.

While considering App-DDoS attacks vs stable background traffic, the following four problems are to be taken into account.

- Net-DDoS attack detection techniques are not capable of gathering sufficient unpleasant signals for noticing the App-DDoS attacks, since, they belong to dissimilar layers correspondingly.
- TCP anomaly detection techniques may hardly recognize the App-DDoS attacks launched by HTTP requests based on valid TCP connections.
- In order to create the TCP link, as the attackers have to employ the valid IP addresses and IP packets, the anomaly detection techniques find it hard to identify the original IP packets.
- App-DDoS attacks might imitate the access behaviors of regular users. So most of the present detection techniques, do not succeed in differentiating the characteristics of DDoS attack traffic from that of usual traffic. Though, the background traffic of this scenario is specified to be stable, some App-DDoS attacks (like Flood) still may be checked by enhancing previous methods of Net-DDoS attacks, such as, concern HTTP session rate, the HTTP request rate, and duration of users admission for detecting.

The next feature of App-DDoS attacks is that, the attackers aspiring at some particular websites are gradually moving away from bandwidth flooding to more stealthy attacks that mimic as (or hide in) usual flash crowds of the websites [14]. Because, such websites become more and more for the rising demands of information transmit, and electronic commerce, network security has to face a new trouble of how to discover, and react to the App-DDoS attacks if they happen during a flash crowd event.

As a consequence of flash crowd and App-DDoS attacks, the traffic becomes unbalanced, bursty and enormous. The attack nodes might assemble their cruel web
traffic to imitate the usual one by HTTP artificial tools [9]. Consequently, the malicious requests vary from the legitimate ones in intention but not in traffic characteristics. Most of the present detection mechanisms (such as those based on traffic features) become invalid.

Attack nodes use a huge number of extensive resources that belong to recognized clients. So, it is difficult to connect these resources to regular clients. Therefore, they cannot be removed from the IP prefix. Other previous protection methods might be those based on operate–machine communication, such as passwords, puzzles, and the CAPTCHAs. As [15] and [16] have pointed out, those methods are not efficient for the DDoS attacks detection, because, they can annoy users and initiate extra service delays.

The Application layer DDoS attacks in contrast with conventional attacks with respect to the utilization of resources like memory, CPU, and database, might not require consuming a lot of network bandwidth. Consequently, the conventional DDoS detection methods for bandwidth consuming attacks become unsuccessful.

In [17, 18] employed the cross-correlation investigation has been discussed to detect the traffic patterns, and to find out where and when a DDoS attack probably arises. A DDoS attack is different from that of a concurrent network attack on a victim (for example, a web server or a router) because in the case of DDoS attack, attacks are received from a huge number of cooperated hosts, which might be dispersed among dissimilar, self-governing networks. By merely, using the irregularity existing between network wide resources and local facilities of a victim, a flooding based DDoS attack may increase a predicted congestion very rapidly at an attacked target [19].

The internet routing communication, which is stateless and established mostly on destination addresses, is susceptible to such large-scale synchronized attacks. DDoS attacks could not be noticed and stopped, since, bogus source addresses and other complicated methods have been used to hide attack sources [18, 20]. DDoS flooding attacks may get a victim network off in the internet, even without using specific susceptibilities in network protocols or weaknesses in system plan, completion, or
arrangement. Security patches might avoid attacks against protocol or system susceptibilities. Congestion-inducing DDoS attacks cause a real limitation in the internet design, and therefore present a severe risk to internet stability.

In [21], irregularity of two-way packet rates is exploited to recognize attacks in edge routers. A flash crowd is a rush in traffic to a specific web site that affects the site to be practically unreachable. The conventional work has introduced a model of flash crowd events and evaluates the performance of several multi-level caching methods appropriate for managing these events. Usage of essential caching methods leads to considerable reduction in client reply times, as well as server, and network loads during flash crowd in the network. Even more savings will be recognized with sensible choice of substitute algorithms and assignment of proxies.

After that, a technique for proactive discovery of DDoS attack by categorizing the network position to be used in the discovery stage has been presented. More specially, the two-stage DDoS architecture, the control phase and the attack phase have been illustrated. Afterward, the events of DDoS attacks to choose the attribute variables that are significant in recognizing the DDoS attacks have been examined, because they are to be unusually changed every time the attack occurs.

In Net-DDoS attacks, opposition results filter the bandwidth consumption attacks. Though particular application service attacks are generated by DDoS, the conventional techniques are not capable of mitigating these attacks, because of the difference of attack intensities. Additionally, reasonable and deployment complicacy limits the change of building network based methods. Opponents having capability of eavesdropping messages swap by the applications, to start attacks to application service ports.

In [22, 23], a port-hopping method has been initiated to prevent the DDoS attacks by various application service ports. The suggestion in [24] focuses on the statement between two parties, modeled as sender and recipient. The recipient sends back an acceptance for every message established from the sender, and the sender employs these acceptances as the signals to alter the destination port numbers of its messages. Because
this protocol is acknowledgment based, time management is not essential. However, the acknowledgment may be misplaced in the network, and this might remain in the two parties using a sure port for a long time. If the attacker obtains the port number in this time, then a directed attack can be sent under which the communication can hardly endure.

To manage the above said situation, a solution that reinitializes the protocol is offered in [25]. The final solution depends on clocks that have similar rate.

In [26, 27] the authors also introduce a meticulous model, and analysis of the difficulty of probable DoS to applications (ports) by an adaptive opponent. The analysis, in addition to the parts that engage the port-hopping protocols introduced, also comprises a part examining the effect of adversary’s dissimilar methods for launching blind attacks.

There is a client-transparent method presented in [28] which is somewhat similar to port hopping. This technique uses draft to establish verification code into the TCP/IP layer of the networking stack. Hence the messages with unacceptable verification code will be restricted by the server’s firewall. In order to protect the DoS attacks, the verification code alters occasionally. There is a confront server in charge of issuing keys, controlling the number of clients linked with the server, and matching the clients with the server too. Because, this technique relies on the confront server, the defense of the confront server is fairly vital.

As a result of its popularity and helpfulness, the internet is accessed by malicious users as well as users who are not aware of DoS attacks. Both these users will not depart on their own. Certainly, current studies have demonstrated a large number of DoS attacks happening continually during the internet [29, 30].

SOS [31] first recommended the notion of using an overlay network preferably to route traffic from valid users to a stealthy node (that can modify over time). All other traffic is limited at the ISPs, which in the majority of cases has sufficient capability to hold all attacks and legitimate traffic (the bottleneck is classically in the secluded server’s
access link). Because the routers do white-list filtering, the overhead of the system is insignificant. In the unique SOS technique, permission to the overlay was completed based on public-key (or, more generally, cryptographic) verification, requiring prior information of the set of valid users.

WebSOS [32] reduces the restrictions through adding a Graphic Turing Test to the overlay, which permits the system to distinguish between normal users and attack zombies. MOVE [33] removes the dependency on network filtering at the ISP routers by maintaining the present location of the secret server, and using process relocation to go away from targeted locations.

Mayday [34] discovers independently for the two main aspects of the SOS architecture, such as filtering and overlay routing, with numerous substitute methods considered. It is shown that in some cases, the different safety properties obtainable by SOS may still be preserved using methods that are simpler and more expected. Though, some second order properties, for example, the ability to quickly reconfigure the architecture or in reaction to break the filtering identity (like recognizing the secret servlet) are negotiated.

An analysis of several security or performance design tradeoffs in IONs happens in [35]. In [36] an online network simulator is used to examine the resistance of proxy networks (such as SOS) versus simple DoS attacks. The resistance of a proxy network to flooding attacks is found to augment linearly with its size. Though, the users may immediately detect the attacked ION nodes, and change to new ones with zero overhead, a statement that did not hold for any ION architecture has been recognized.

In [37] the first scheme is to generate stateless flow filtering by having every router add ‘capabilities’ to packets that cross them. The receiver of these packets is after that dependable for sending these abilities to its peers, which will permit the traffic at superior rates (privileged traffic). Poor traffic is restricted to a part of the accessible bandwidth. Therefore, a DoS attack can avoid new links from being recognized (by overloading the control channel employed to converse these capabilities), existing links
will be safe. Estrin et al. initially proposed a ‘capability’ like method for network packets in [38, 39].

In [40] the purpose of a server that may create tickets at line speeds has been proposed. Clients should attain a ticket from the server before they are permitted to read a protected service. The method is mainly geared towards application level DoS defense. In [41] a comparable system for utilization in the network layer of an internet has been proposed. Then, the architecture has been designed with a fresh slate, considering a secluded token server architecture, and rate-limiting or filtering traffic on routers by these tokens.

1.9.2 App-DDoS attacks in IP and MAC frame

Literature survey points out that researchers try to discover DDoS attacks from three dissimilar layers that is., TCP layer, IP layer, and application layer [42]. From all of these viewpoints, researchers are examining different methods to differentiate normal traffic from the attack one. The majority of DDoS related studies concentrate on the IP layer [43]. These methods try to discover attacks by examining particular features, such as, arrival rate or header information. For instance, [19] employed the management information base (MIB) data that comprise parameters that point out dissimilar packet, and routing statistics from routers to attain the early discovery.

Different methods have been recommended to resist the DDoS attacks. Traceback schemes [44] attempt to find the real source of the attack whereas overlay networks try to assure the safe flow of information by certification. Autonomous systems employ ingress and egress traffic filtering to filter the false traffic. The other method is to construct traffic aggregates by categorizing the traffic. Therefore, the traffic with the uppermost probability of being malicious will be filtered out. Two essential methods namely, signature finding and anomaly finding [45, 46] survive based on this idea.

In the signature finding method, the inward traffic is scanned for recognizing signs of DDoS attacks (the permanent TCP sequence numbers employed by the DDoS tool
Shaft). A database of signatures is constructed by hand a priori [47]. As the signatures are extremely good indicators of nasty traffic, human expert knowledge is used to remove them. Such a solution will not resist new attacks without human interference. Making these signatures takes a large amount of skill. Therefore this technique presents no quick protection against previously unknown (Zero-Day) attacks.

Anomaly detection does not employ permanent signatures but contrasts the present traffic to a baseline profile [48]. Different methods have been introduced to achieve this. They comprise statistical methods like a Chi-Square-Test on the entropy values of the packet headers [49], covariance analysis [50], and clustering and feature space modeling [50]. Various methods taken from pattern analysis and machine learning like Wavelets, Genetic Algorithms [52], Markov Models [53], Artificial Neural Networks (ANN) [54], [55] and Bayesian Learning [56] have also been discussed.

In [57] current DDoS detection mechanism has been reviewed. Only a small number of solutions on near target DDoS mitigation have been proposed in [58], [59]. In [60] a method called History based IP Filtering (HIF) has been introduced, which keeps track of formerly seen hosts, and it is found to be efficient in large scale attacks. In [61] the thought of modeling historic traffic has been employed, but this method has been enhanced with clustering observed traffic, and building a restricted number of Access Control Lists (ACL) heuristically. This method is very compute intensive, and consequently limited to a small historic time span.

In [62] a technique to mitigate DDoS attacks based on experimental data has been presented. The scheme does not aspire at the discovery of such attacks, however at the automatic formation of filter rules for IP firewalls like iptables, nf-HiPAC or Cisco ACLs that can permit the server to persist serving legitimate users even while under a large scale DDoS attacks.

In contradiction of all previous methods, [63] relies on an accurate statistical framework of Bayesian decision theory. This permits, to extract from the implementational details, the theoretical predictions about performance, and decision
rules which are best in the selected scenario. Statistical framework [64] is introduced for mitigating DDoS attacks based on Bayesian decision theory to deduce optimal rules.

Adaptive History Based IP Filtering (AHIF) [65] reduces security damage (blocking legal users) during near target DDoS mitigation. Contrasting other methods, this method will be used to arrange certain filter rule sets before a DDoS attack takes place. Not examining IP traffic [66] during an attack to mitigate, it has the following advantages.

- The mitigation will happen immediately once an attack has been noticed
- The resources of the firewall system will be employed entirely for attack packet filtering
- Rules may be transmitted to distributed firewalls in order to filter out DDoS traffic at the limits of an ISP core network (edge router)

In [67] a naive Bayesian classifier is applied to traffic categorization. Considerably, the simple classifier determines each of the variables for describing an object. The data, drawn from preceding hand classification work, has shown substantial redundancy, and important interdependence among features describing every flow; this will considerably decrease the accuracy of classification [68]. Obviously, a technique that integrates dependence, such as the Bayesian neural network, might give a more robust and efficient classifier. The feature of network data traffic may get abnormally changed whenever the attack happens.

As the internet scenario is comprised of both wired IP packet transmission and wireless MAC packet transmission, demarcation of these streams is essential to efficiently resist the App-DDoS attacks. Only some of the works listed on discovering wireless MAC frame application attacks, include sybil attacks, grey hole, and black hole attacks. These attacks require special filtering methods compared to that of wired filter methods.
To overcome this, in the proposed work, Bayes packet classifier method has been used to classify the status of network data traffic for each phase of the DDoS attacks. The HMM is improvised to eliminate the unwanted features for the DDoS application attack resistance. It provides a mapping element of the ISP data traffic, which describes the period of packet transfer in a network. The Gaussian distribution factor is applied to resist gradually changing anomalous DDoS attacks with flexible adjustment of feature variables. To defeat the attack discrepancy on wired and wireless scenario of App-DDoS attacks, in the proposed work, an Application Service Network Request Identification (ASNRI) technique has been introduced to filter out the application service denials effectively on hybrid network streams.

1.10 Network simulator- 2

NS (version 2) is an object-oriented, discrete event driven network simulator developed at UC Berkely written in C++ and Object Oriented Tool command language. NS is primarily helpful for simulating local and wide area networks.

As shown in figure 1.10, in a simplified user's view, NS is Object-oriented Tcl (OTcl) script interpreter that has a simulation event scheduler, network component object libraries, and network setup (plumbing) module libraries (actually, plumbing modules are implemented as member functions of the base simulator object). In NS, the user should write the program in OTcl script language. Simulation and analysis has been carried out using NS2 simulator tool.

![Figure 1.10 Simplified user's view of NS](image)

31
1.11 Problem definition

With the growth of information networks, the number of network attacks have increased. Distributed Denial of Service (DDoS) attacks pose an enormous threat to the internet. Attackers run a massive number of queries through the victim’s search engine or database query to bring the server down, and it is called App-DDoS attacks.

Simple App-DDoS attacks (like Flood) could be monitored by using HTTP session rate, HTTP request rate, and duration of user’s access. But burst traffic and high volume data traffic are major characteristics of App-DDoS attacks. The flash crowd cannot be easily identified by the conventional DDoS attack resistance filters.

The nature of data traffic flow from wired network is highly different from that of wireless network. So the DDoS application service attacks from the wired ones are generated as IP frames and wireless ones as MAC frames. The variant in the frames motivates the requirement for enhanced resistive mechanism for App-DDoS attacks in hybrid network streams.

1.12 Objectives of the proposed research work

The objective of the proposed work is to develop a counter mechanism to mitigate the potency of the application traffic DDoS attacks and evaluate the efficacy. Integrated HMM and Bayes Classifier Model (IHBCM) have been presented to improve the attack resistance rate of legitimate clients against App-DDoS attacks. Gaussian distribution factor has been introduced, to improve the resistance scheme for better detection rate of App-DDoS attacks. To conquer facts of attack discrepancy on wired and wireless scenario of App-DDoS attacks, Application Service Network Request Identification (ASNRI) technique is presented to filter out the application service denials effectively on hybrid network streams.

The various techniques used in this proposed research work are given below.

- An access matrix to capture the spatial-temporal patterns of a normal flash crowd.
• Anomaly detector based on Hidden Markov Model (HMM) has been proposed to describe the dynamics of Access Matrix (AM), and to detect the App-DDoS attacks.

• Bayes packet classifier method has been applied to classify the status of network data traffic for each phase of the DDoS attack.

• The HMM has been improvised to eliminate the unwanted features for resisting the Application layer DDoS attacks.

• Integrated HMM and Bayes Classifier Model (IHBCM) have to improve the attack resistance rate of legitimate clients against App-DDoS attacks.

• Gaussian distribution factor has been introduced, for improving the resistance scheme to have better detection rate even for stationary object in the App-DDoS attacks.

• Application Service Network Request Identification (ASNRI) technique has been proposed to filter out the application service denials effectively on hybrid (wired and wireless) network streams.

• In ASNRI, resistance filters are activated to restrict the Denial of Service attacks in the respective platforms of wired or wireless.

1.13 Organization of the thesis

This thesis is organized as follows.

Chapter 1 provides an introduction and analyzes the issues related to Denial of Service attacks (DoS) faced by administrators. It also describes the detailed overview of the related work that has been made in this field, and also the detailed classification of the attacks and different mitigation methods.

Chapter 2 provides the overall methodology involved in this work.
Chapter 3 presents the Trust and Access Matrix (AM) based HMM Models to mitigate the App-DDoS attacks which detains the spatial-temporal patterns of a normal flash crowd event, and detects the Application DDoS (App-DDoS) attacks.

Chapter 4 describes Integrated HMM model and Bayes Packet Classifier model (IHBCM). This section discusses this method to recognize whether the surge in traffic is caused by App-DDoS attackers or by normal web surfers.

Chapter 5 discusses the technique of Application Service Oriented Network Request Identification (ASNRI), for resisting DDoS attacks in IP and MAC Frames. It develops counter mechanism to mitigate the influence of the resource attacks, and evaluates the efficacy. ASNRI technique provides a clear discrimination of wired service and wireless services request.

Chapter 6 provides performance evaluation of ASNRI to mitigate DDoS attacks. This section presents the results obtained by implementing the proposed solution, and analyzes the credibility of results from simulations. The detection results are measured in several experiments involving the DDoS detection models.

Chapter 7 contains the conclusion of this work and lists some suggestions for future research work in this field.