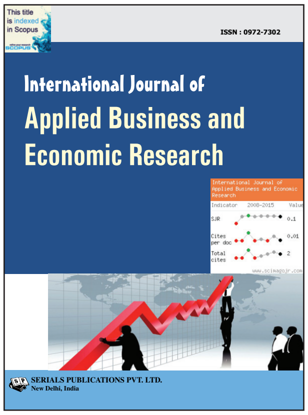

International Journal of Applied Business and Economic Research

ISSN : 0972-7302

available at http: www.serialsjournals.com

© **Serials Publications Pvt. Ltd.**

Volume 15 • Number 22 • 2017

Performance Monitoring of Virtual Host During DDoS Attack In Cloud

B. S. Kiruthika Devi[a] K.V. Mahesh Babuand[a] and T. Subbulakshmi[a]

School of Computing Science and Engineering, VIT University Chennai - 600127, Tamil Nadu, India. Email: kiruthikadevi.bs2015@vit.ac.in, venkata.maheshbabu2015@vit.ac.in, subbulakshmi.t@vit.ac.in

ABSTRACT

The advent of the cloud technology in business and IT industries for the best utilization of resources has made a socio-economic impact on the internet community. The growing use of this cloud computing is visible as most of the web servers are grouped into cloud data centers. However, the level of vulnerability exposed to the virtual machine and the potential risk that leads to malicious attacks like Denial of Service (DoS) and Distributed Denial of Service (DDoS) are unexplored. This type of attacks can be done by using tools like Tribe Flood Network, Golden Eye Toolkit, Low Orbit Ion Canon, High Orbit Ion Cannon, hPing, Slowloris, UDP Flooder, RUDY, Pyloris, OWASP Switchblade and DDoSIM. Specialized DDoS attack tools have developed to target multiple platforms, rendering DDoS attacks more dangerous for targets and much easier for hackers to carry out. It becomes very difficult for us to differentiate between legitimate users and unauthorized users. So, to detect and reduce the effect of DDoS attacks the network-based performance metrics are evaluated to study the effects of attack in cloud. Based on the anomalies attack sources are blacklisted to take appropriate actions and protect the cloud server.

Keywords : DDoS; DDoS Attack Tools; monitoring; performance metrics; cloud computing.

1. INTRODUCTION

Cloud computing provides the accessing of services, resources and applications over the web.This model has changed the idea of organizations and industries away from the deploy mentand day to day working of their IT services by providing an self-service, on-demand, and pay as you use business model. Cloud computing has changed the organizations and industries to a different level and continued to increase its popularity in recent times.

The National Institute of Standard and Technology (NIST)characterizes the essential characteristics of cloud computing as on demand self service, resource pooling, rapid elasticity and measured service (Melland Grance, 2011). The service model can be broadly divided into (Figure. 1), Platform-as- a-Service(PaaS), Software-as-a-service(SaaS) and Infrastructure-as-a-Service (IaaS) [41].

1.1. Software-as-a-Service

Software as a service is a packaged service in which the application, data, runtime, middleware, operating system virtulization, servers, storage and networking is managed by the vendor and provided as a web browser. We can use those services and certain permissions are given to the users like creating, deleting and quering. SaaS mainly focusses on the application level where the users are away from the platform details and infrastructure. The service provider usually controls virtually everything about the application. In many cases, this will limit any customization that can be done. But depending on the implementation, you may beable to request that the user interface (UI) or the look and feel of the application be modified slightly. Some of the examples are Outlook.com, Google Drive, Salesforce.com, etc.

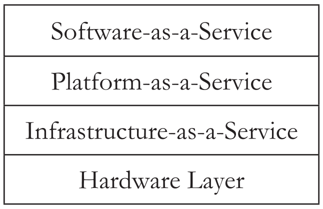

Figure 1: Cloud Services

1.2. Platform-as- a-Service

PaaS implementations allow organizations to build and deploy Web applications without having to build their own infrastructure. PaaS offerings generally include facilities for development, integration, and testing, here the users can manage the application and data. The remaining services are managed by the provider. In a PaaS environment, the data will be stored at the provider site. the customer is generally responsible for everything above the operating system and development platform level. user willbe responsible for installing and maintaining any additional applications that user will need. This includes application patching and application monitoring. Thedatabase platform may be supplied for the user, but the customer will have direct access to itIf there are any problems with the data. Some of the examples are Windows Azure, Google App Engine, Engine Yard and Force.com.

1.3. Infrastructure-as-a-Service

IaaS provides core services such as computing power, storage, networking and operating systems. You can then build your environment on top of theseresources. An IaaS provider may provide user with hardware resources such as servers. These servers would be housed in the provider's datacenter, but the user will have direct access to them. users can then install whatever they needed toonto the servers. This can be costly, though, because the provider would not be able to make use of multitenancy or economies of scale. Therefore, customers would have to absorb all the costs of the systems themselves. IaaS providers are really picking up steam in the marketplace. This isn't just due to demand. There is also the fact that IaaS platforms such as CloudStackand OpenStack have been developed to make automation and orchestrationeasier. some examples of IaaS providers are Amazon EC2,S3,Go Grid and Rackspace.

There are some other service models like Database as a Service, Desktop as a Service, Storage as a Service, Security as a Service, etc. These service models are deployed onapublic, private, community or hybrid cloud (Tsaietal., 2010).

1.4. Public Cloud

In this the services are managed and provided by organizations like Google, Microsoft and Amazon to the general public. Public clouds provide services to multiple users and clients. The services will be provided over the internet and the users have to pay what they used. Some of the attributes of public cloud are cost of building the data center on service consumer has no initial cost, operation and maintainance cost is low with respect to the data center size, size of the data center can be 50000 servers, infrastructure has limitted configuration controllability and flexibility, the level of trust is lowest and infrastructure location is off-premise.

1.5. Private Cloud

In this the cloud serviceare provided and managed by an organization or third party srvice providerfor the use of the organizations private use. This cloud provides services only to this particular organization. It provides data protection and servive level issues. some of the private clouds are Open Stack, Eucalyptus, Opennebula, etc. some of the attributes of the private cloud are High initial cost of the buildind the datacenter on service consumer, operation and maintainance cost is high with respect to the data center size, the size of the datacenter may be 50000 servers, It has full control over the hardware and software of the infracture, the level of trust is higher, on-premise infrastructure location and the organization is the owner of the private cloud.

1.6. Hybrid Cloud

Hybrid cloud is the combination of both public and private clouds. Some of the attributes of hybrid cloud are: it has medium initial cost for building the datacenter, operation maintainance is weighted average of the public and private cloud, size of the data center is less than the private cloud, full control over the infrastructure of private cloud and limited for public cloud, hybrid cloud location can be on-premise or off-premise.

1.7. Community Cloud

The Community cloud shares infrastructure and services with several organizations from a different community with common concerns like compliance, security,flexibility etc. it is managed by the users or third part service providers. Some of the attributes of community cloud are: cost of the building depends on the number of cooperatives, operation and maintainance is similar to private cloud but the cost is divided on the participants, size of the servers can be 15000 more than private cloud but less than public cloud, High controlability over the infrastructure but limited by the community policies, high trust and the location of the community cloud is within the cooperative facility.

While cloud computing provides various benefits tousers, there a real sounder lying security and privacy risks (Quickand Choo, 2014; Wayne, 2011; Christofetal., 2009; Gonzalezetal., 2012). For example, resource, poolingmulti-tenancy and share ability features can be exploited by attackers. That will lead to the DDoS attack.

2. DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS)

DDoS stands for "Distributed Denial of Service [42]." A DDoS attack is a malicious attempt to make an online service unavailable to users, usually by temporarily interrupting or suspending the services of its hosting server.Unlike a Denial of Service (DoS) attack, in which a single Internet-connected device is used to flood targeted resource with packets, a DDoS attack is launched from numerous compromised devices, often distributed globally in what is referred to as a botnet.

Distributed Denial of Service attacks are comprised of one or more malious packets which are controlled by an attacker to flood the predetermined target. These attacks engage thepower of more number of coordinated Internethosts to exhaust the critical resource at thetarget and deny the services to legitimate users(Choi etal., 2013).The traffic is usually so aggregated that it is difficultto distinguish legitimate packets from attackpackets. Moreover, the attack packets are greater in number that a system can handle. The user have to take special care or else a DDoS attack can occur. The attacked victim face a damage of shutdown, filecorruption and total or partial loss of service from the server.

3. TYPES OF DDOS ATTACKS

DDoS attacks can be broadly divided into three types [42]:

3.1. Volume Based Attacks

These includes TCP floods, UDP floods, ICMP floods, and other spoofed-packet floods. The attack's goal is to drench the bandwidth of the attacked website, and magnitude is measured in Bits per Second.

3.2. Protocol Attacks:

This includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more. This type of attack consumes actual server resources, or those of intermediate communication equipment, such as firewalls and load balancers, and is measured in Packets per Second.

3.3. Application Layer Attacks

This includes low-and-slow attacks, GET/POST floods, attacks that target Windows, Apache and linux vulnerabilities. Comprised of seemingly legitimate and innocent requests, the goal of these attacks is to crash the web server, and the magnitude is measured in Requests per second.

4. SPECIFIC DDOS ATTACKS TYPES

Some of the popular DDoS attacks include [43]:

4.1. User Datagram Protocol (UDP) Flood

This DDoS attack damages the User Datagram Protocol (UDP), a sessionless networking protocol. This type of attacks can be seen in a remote host with numerous UDP packets, this attack uses the host to repeatedly check for the applications listening at that port, and if there is no application found on destination. They reply with an ICMP Destination Unreachable packet. This process drains host resources, and can ultimately lead to server failure.

4.2. Internet ControlMessage Protocol (ICMP) Flood

Similar in principle to the UDP flood attack, an ICMP flood overwhelms the target resource with ICMP Echo Request (ping) packets, generally sending packets as fast as possible without waiting for replies. This type of attack can consume both outgoing and incoming bandwidth, since the victim's servers will often attempt to respond with ICMP Echo Reply packets, resulting a significant overall system slowdown.

4.3. Synchronization (SYN) Flood

A SYN flood DDoS attack exploits a known weakness in the Transfer Control Protocol connection sequence (the three way handshake), here a SYN request to initiate a TCP connection with a host must be answered by a SYN-ACK response from that host, and then confirmed by an ACK response from the requester. In a SYN flood scenario, the requester sends multiple SYN requests, but either does not respond to the host's SYN-ACK response, or sends the SYN requests from a spoofed IP address. Either way, the host system continues to wait for acknowledgement for each of the requests, binding resources until no new connections can be made, and ultimately resulting in Denial of Service.

4.4. Ping of Death (PoD)

A ping of death attack involves the attacker sending multiple malicious pings to a computer. The maximum packet length of an IP packet with header is 65,535 bytes. However, the Data Link Layer usually poses limits to the maximum frame size for example 1500 bytes over an Ethernet network. In this case, a large IP packet is split across multiple IP packets, and the recipient host reassembles the IP fragments into the complete packet. In a Ping of Death scenario, following malicious manipulation of fragment content, the recipient ends up with an IP packet which is larger than 65,535 bytes when reassembled. This can overflow memory buffers allocated for the packet, causing denial of service for legitimate packets.

4.5. Slowloris

Slowloris is a highly-targeted attack, enabling one web server to take down another server, without affecting other services or ports on the target network. Slowloris does this by holding as many connections to the target web server open for as long as possible. It accomplishes this by creating connections to the target server, but sending only a partial request. Slowloris constantly sends more HTTP headers, but never completes a request. The targeted server keeps each of these false connections open. This eventually overflows the maximum concurrent connection pool, and leads to denial of additional connections from legitimate clients.

4.6. Network Time Protocol (NTP) Amplification

In NTP Amplification the attacker exploits publically accessible Network Time Protocol (NTP) servers to overcome the targeted server with User Datagram Protocol (UDP) traffic. In an NTP amplification attack, the query-to-response ratio is anywhere between 1:20 and 1:200 or more. This means that any attacker that obtains a list of open NTP servers can easily generate a high-bandwidth, high-volume DDoS attack.

4.7. Hyper Text Transfer Protocol (HTTP) Flood

In HTTP flood DDoS attack the attacker exploits apparently legitimate HTTP GET or POST requests to attack anapplication orweb server. HTTP floods do not use malicious packets, spoofing or reflection techniques, and require less bandwidth to bring down the targeted website or server. The attack is most effective when it forces the server or application to allocate the maximum resources possible in response to each single request.

4.8. Zero-day DDoS Attacks

"Zero-day" are simply unknown attacks, exploiting vulnerabilities for which no patch has yet been released. The term is well-known amongst the members of the hacker community, where the practice of trading Zero-day vulnerabilities has become a popular activity.

5. DDOS ATTACK CLASSIFICATION

Due to increased growth in internet services there are many number of possible ways to attack these services. DDoS attack is one of the highest occurrence attack over the past decade. Many internet service providers and users have seriously affected from these attacks. DDoS flooding attack incidents have increased rapidly in the frequency and the size of the targeted networks and computers over the past years.machanisms have been proposed in literature to address the DDoS flooding attacks.

DDoS attack is a common extension of DoS attacks in which the attacking power is increased with numerous attacking sources which are under attacker's control. The DDoS attacks are categorized into different categories based on the location where they are implemented:

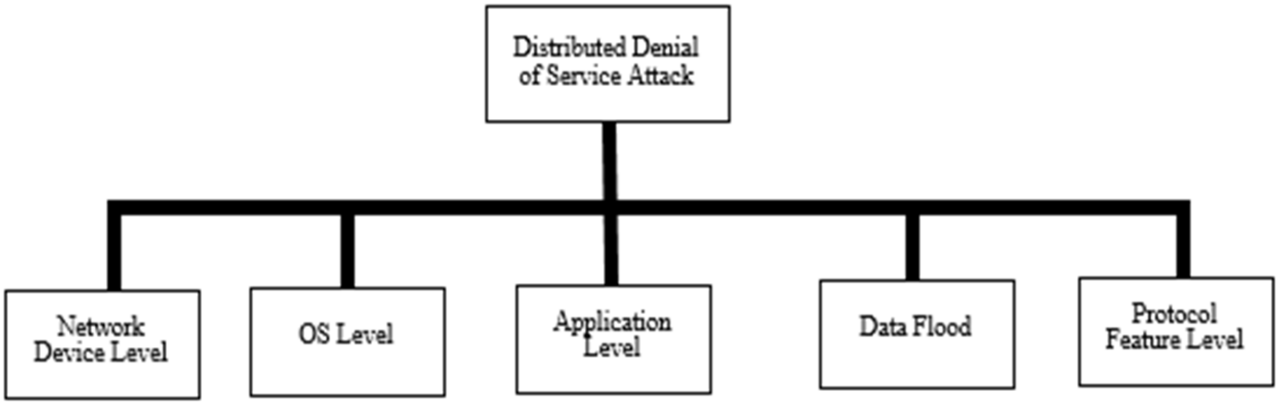

Figure 2: DDoS attack categories classification

In above classification as in Figure 2 [1], Network Device Level attack exploits a router's weak point. OS Level attack exploits OS vulnerability. Application Level attack determines application's vulnerability through port scanning. Data Flood refers to flooding a network or server's connection points to deny services for legitimate clients. This is achieved by sending huge traffic (data packets) towards victim. The protocol feature attack exploits some protocol's weak point such as the requirement of final acknowledgement from client by the server in TCP's three-way handshake.

DDoS attacks have gained challenge in the recent years because attackers are becoming more sophisticated and organized. DDoS attacks against customers are increasingly the most commonly experienced security threat as in Figure 3. The percentage seeing these attacks reached a new high of 77 percent; this exceeds last year's result by four percentage points. DDoS attacks targeting service infrastructure were seen by a lower proportion than last year, in contrast to an increase in those seeing bandwidth saturation (*e.g.*, due to streaming, over-the-top services, unique events, flash crowds, etc.). Interestingly, we are once again seeing a declining trend in those experiencing infrastructure outages due to equipment failures or misconfiguration. The percentage has fallen steadily over the past few years from 60 percent, to 55 percent, to 53 percent and finally 49 percent this year.

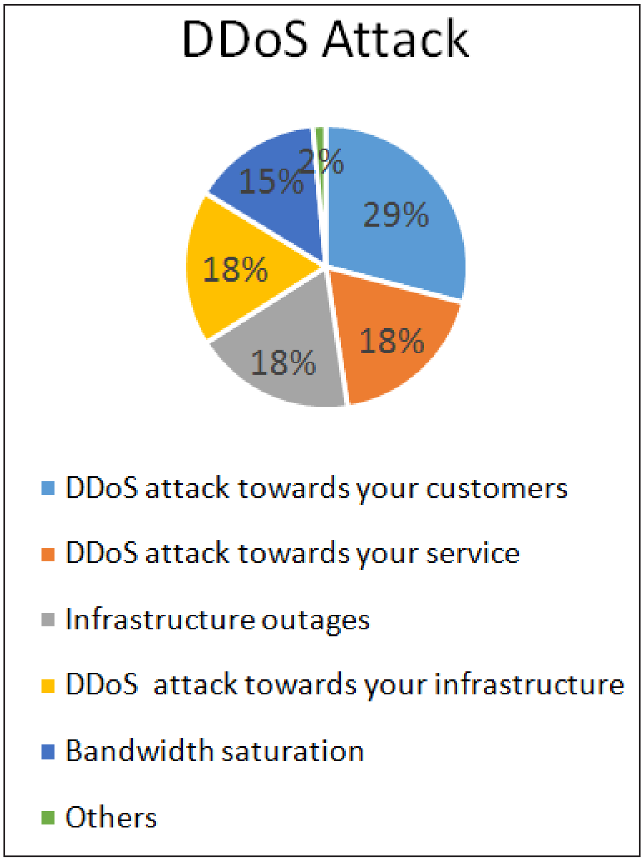

Figure 3: Service Provider Experienced Threats [2]

As per the world wide infrastructure report [4] the largest single DDoS Attacks observed per survey year in Gbps are as shown in Fig. 4. In this paper the performance metrics of the defense framework against the Distributed Denial of Service attacks has been explained. The methodology mainly concentrates on the performance metrics which measure the defense framework's effectiveness, cost and security.

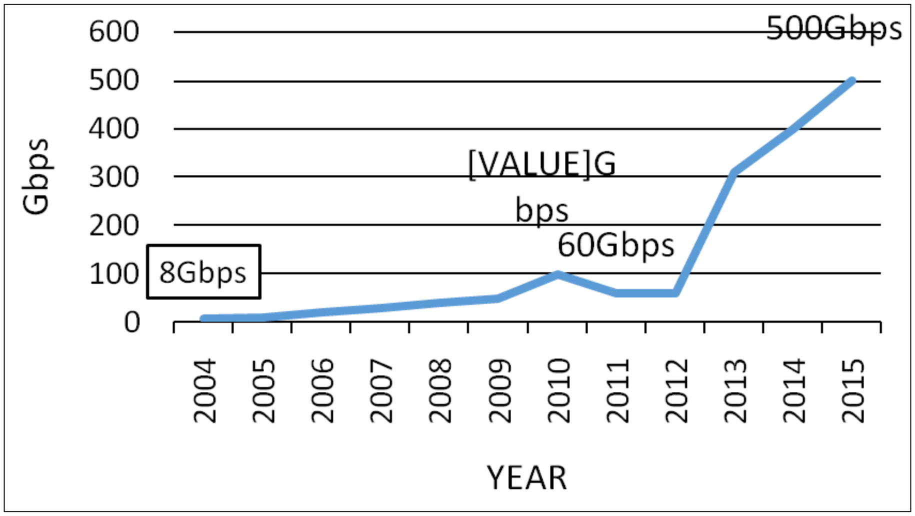

Figure 4: Year wise statistics of Attack Strength of DDoS Attacks [4]

There are many recent solutions to detect bandwidth attacks in literature. However they becomes less effectivewhen the attack traffic sources are highly distributed. The detection of DDoS attacks becomes more difficult as the distance to the victim increases. The reason is that the attack traffic is spread across multiple links, which makes it more diffuse and harder to detect. Basically, there are two challenges for detecting bandwidth attacks. The first one is how to detect malicious traffic close toits source. This is a difficult task when the attack is highlydistributed, since the attack traffic from each source may bevery small compared to the normal background traffic. Thesecond one is to detect the bandwidth attack as soon as possiblewithout raising a false positive alarm, keeping the falsenegative rate low, so that the victim has more time to takeaction against the attacker.A successful attack prevents the victim from providing desired services to its legitimate users. Themost commonly attacked type of service denial is the flooding based attacks which intended to overwhelm a limited targets. Such flooding attacksattempt to perform continued resource exhaustion at awell-provisioned target.

6. EXPERIMENTAL SETUP

The proposed system will be implementedin a private cloud build up on Linux machines and virtual interfaces. By considering those results, we will provide sufficient bandwidth for the legitimate users during DDoS attacks. The attacks will be detected and mitigatedusing an experimental testbed. Firstly, the system will differentiate the attacks based on the network-based performance metrics and host metrics under normal condition and after the attack by using DDoS monitoring tools. The major causes of the degradation of virtual machines will be investiagted. These results can be used to find the robustness and security of the VMs in modern virtualization systems.

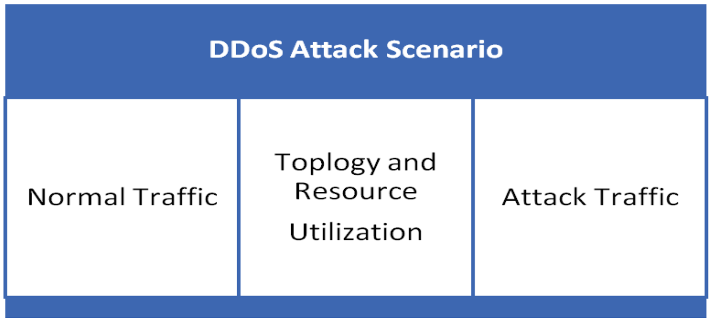

Figure 5: DDoS Attack Scenario

There are some basic terms which must be taken into consideration while measuring/evaluating the DDoS Mitigation Framework. Some of the common elements of DDoS attack scenario are shown in Fig. 5. Legitimate traffic constitutes of the packets sent from source to destination by the normal/legitimate users. During the attack scenario both legitimate and attack packets compete for the same resources and major goal of the attacker is to win the race by the attack traffic over legitimate traffic. Metrics can be defined which measure how much of the legitimate traffic is being dropped while the attack is going on. Attack traffic constitutes of packets generated by the number of attackers at different locations over the Internet with the aim of denying the service to the normal users who are accessing a service. Network topology is the overall arrangement of the nodes, links, intermediate routers and victim. Victim may be a server or any other computer. Resources may include the resources of the server being victimized, intermediate routers' resources like memory and attackers' resources. Attackers are smart enough to generate attack that can fully utilize the resources.

Usually by the time a DDoS flooding attack is detected, there is nothing that can be done except to disconnect the victim from thenetwork and manually fix the problem. DDoS flooding attackswaste a lot of resources (*e.g.*, processing time, space, etc.) on thepaths that lead to the targeted machine; hence, the ultimate goalof any DDoS defense mechanism is to detect them as soon aspossible and stop them as near as possible to their sources.

7. TYPES OF DDOS TOOLS

Some of the DDoS attacking tools present in internet are Tribe Flood Network, Golden Eye Toolkit, Low Orbit Ion Canon, High Orbit Ion Cannon, hPing, Slowloris, UDP Flooder, RUDY, Pyloris, OWASP Switchblade, Trinoo, DDOSIM, TFN2K, Shaft, Trinity and Knight. Attackers use these tools to attack on the organizations, online retailers and users. Some of the DDoS monitoring tools are Nagios, Cacti, Icinga, Snort, Wireshark, Corero, Net Flow Analyzer, Floodlight, EC2West, Flow Visor and Cloud flare. As an Internet user, you should also take care of your system. Hackers can use your system as a part of their zombie network. So, always try to protect your system. Always keep your system up to date with the latest patches. Install a good antivirus solution. Always take care while installing software. Never download software from un-trusted or unknown sources. Many websites serve malicious software to install Trojans in the systems of innocent users.

8. PROPOSED WORK

A virtual host monitoring system deployed in the testbed is to get traffic results from the network. After collecting the traffic results the legitimateuser traffic is observed and performance metrics like CPU usage, Memory usage, Latency, Packet loss, Throughput andLink utilization are measured. Once the performance metrics are measured during attack there is need to rate limit the attack traffic, so that the legitimate users are not affected. Rate limiting enables user to assign a bandwidth restriction to a category of traffic such as TCP, UDP, ICMP, or specific connection types. DDoS monitoring tools are used to reduce the attack traffic so that legitimate users can send their packets without any congestion.The implementation is carried out on an experimental testbed. Instead of simulation.Real-time results can prove that the DDoS monitoring tools reduce the DDoS attacks in the network. By doing real experiments in the lab assure better understanding on the performance of the proposed methods.

The major categories of DDoS defence mechanism are as follows:

1. DDoS Monitoring and Detection
2. DDoS Mitigation

8.1. DDoS Monitoring and Detection

The system can be monitored by performing intrusion detection. Intrusion detection has been used by everyone to monitor the host computer network. This system detects the DDoS attack either by using known database signatures or by considering the abnormalities in the network.A scalable network can be monitored my using DDoS monitoring tools that are present in the internet like Nagios, Cacti, Icinga, Snort, Wireshark, Corero, Net Flow Analyzer, Floodlight, EC2West, Flow Visor and Cloud flare. They can easily detect the DDoS attack and can be monitored according to the user requirements.Some other metrics that need to monitor the DDoS are detailed in the section. The system will be deployed in the victim network for the effective detection and filtering of cloud DDoS attack traffic.

1. Memory usage
2. CPU usage
3. Packet Loss
4. Latency
5. Link utilization
6. Throughput
7. Good put
8. Attack Traffic Filtering Percentage (ATFP)
9. Request Response Delay (RRD)
10. Transaction Duration (TD)
11. Collateral Damage (CD)

8.2. Memory Usage

During flooding kind of attack the memory available at the victim system decreases as the attack intensity raises drastically. As time increases, the physical memory is completely eaten up thus denying service to legitimate clients.

8.3. CPU Usage

Host based metric CPU Usage is analyzed here to see the impact of DDoS attacks which describes how much the processor is utilized at most. DDoS creates a large spike in CPU Usage. The victim is overloaded and when flooding type of attack takes place in test bed CPU Usage consumption goes up to 100 percent. At that time, incoming pings and echo requests were all blocked during DDoS flooding attack.

8.4. Packet Loss

Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. It measures the discarded packet in a network when a router or other network device is overloaded. With the help of online network monitoring. Ideally a defense system should minimize the loss to zero for the legitimate traffic. It tells the presence of congestion in the network due to DDoS flooding attacks. It does not suite for the attacks which do not cause congestion in the network normally called pulsing attack in these days. Loss can be calculated as under:

$$\text{Loss} = \left(\frac{\sum \text{PL}}{\sum \text{PS}}\right) \times 100$$

Where PL is the Packet lost and PS is the total number of packets sent towards the destination.

8.5. Latency

It is the time taken for a packet to travel from a host to another. Before attack the response time for each request should be similar. Once an attack has been launched, Ping response. Latency indicated an unbearable load. So increase in response latency indicates that DDoS attack is happening.

$$\text{Average Latency} \quad = \quad \frac{\sum_{i=1}^{N}(T - TR)}{N}$$

Where T is the time at which a transaction begins and TR is the time at which it gets the response and N is the total number of transactions.

8.6. Link Utilization

It is the percentage of capacity currently being consumed by aggregated traffic on a link or path. Without attack maximum link utilization at the observed network was high. During attack the legitimate user link utilization drops to low due to the presence of high volume of attack traffic.

8.7. Throughput

It is defined as the number of bytes transferred per unit time from source to destination. The DDoS defense mechanism ideally increases the throughput for the legitimate users. It is measured in packets per second.

$$\text{Throughput} \quad = \quad \frac{\text{Packet delivered}}{\text{Packet arrial - packet start time}}$$

8.8. Goodput

It is also defined as the number of bytes transferred per unit time from the source to destination but it does count the retransmitted bytes [13]. Ideally a defense framework should maximize the goodput for the legitimate sources. Throughput and Goodput metrics are relevant to the TCP based traffics which respond to the congestion by lowering the sending rate and capture the presence of the congestion in the network. These metrics can't be used for the delay sensitive applications as they depend on the volume and timing of the individual transactions as well as on the network conditions.

8.9. Attack Traffic Filtering Percentage (ATFP)

It givesthe overall percentage of traffic filtered after the detection of the attack. It can be obtained as:

$$\text{ATFP} \quad = \quad \frac{\text{Attack traffic filtered}}{\text{Total traffic}}$$

8.10. Request Response Delay (RRD)

It is defined as the time lapse between when a request is first sent and complete response is received from the destination [16]. Ideally a defense framework should reduce the RRD for a particular legitimate source who is initiating the data transfer.

$$\text{RRD} = T_Q - T_R$$

Where T_Q is the time at which a request is first sent and T_R is the time for getting complete response

8.11. Transaction Duration (TD)

It is defined as the time between the start and end of the data transfer between a source and destination [16] [17]. Ideal defense mechanism should minimize the transaction duration for a specific legitimate source.

$$\text{TD} = T_S - T_E$$

T_S is the time at which transaction starts and T_E is the time at which a transaction ends.

8.12. Collateral Damage (CD)

Collateral Damage is defined as the damage done by the defence mechanism on the legitimate user traffic by falsely considering it as attack traffic and filtering it. Packet Loss metric can be used to measure the collateral damage by calculating the loss of the legitimate traffic packets by the defence mechanism. A perfect mitigation must have zero collateral damage which is not possible to achieve. So the main aim of the defence mechanism is to minimize the collateral damage.

And there are also some other metrics but these are the important metrics considered for implementation in the experimental testbed.

8.13. DDoS Mitigation

It is impossible to stop or prevent DDoS attack completely. So, only the attack severity can be reduced after deploying some mitigation techniques. To mitigate a network, we have to consider the Fault tolerance and Quality of service of a network.

Fault tolerance: It is well known research area where the designs are built on most critical infrastructures. The fault tolerance can be applied in three levels namely Hardware, Software and System. The idea of fault tolerance is that by duplicating the network servicesand diversifying its access points, the network can continue offering its services when flooding traffic congests one network link.

Quality of Service: QoS describes the assurance the network to deliver good results for certain type of applications traffic. Many QoS techniques have been developed to mitigate DDoS attacks. Integrated and Differentiated services are used as principle architectures [26]. Integrated services use the Resource Reservation Protocol (RSVP) to coordinate the allocation of resources allocation along the path that a specific traffic flow will pass. The link bandwidth and buffer space are assured for that specific traffic flow. Differentiated [27, 28] services are an aggregate class based discrimination framework. Differentiated services makes use of the type-of-service byte in the IP header and allocates resource based on the TOS of each packet.

Queuing techniques are also used to prevent DDoS attacks. There are many queuing techniques. The oldest and most widely applied queuing technique is Class-based queuing (CBQ). Traffic shaping used to set different traffic queues for different type of service packets. A certain amount of outbound bandwidth can then be assigned to each of thequeues. Class-based queuing has shown tomaintain QoS during a DDoS attack on clusters of webserver s [29].

Using the techniques deployed in Quality of Service regulation Garg and Reddy [30]proposed a defensive approach against DDoS attacks by reducing resource consumption in the system.They suggest that resource regulation can bedone at the flow level, where each flow gets a fairshare of the resource much in the same way asround robin scheduling in CPUs. There is a chance to mount a Denial of Service attackby having a large number of hosts systems connecting tothe server where each server make use of the resource, thus causing resource starvation, same as the dining philosophers problem. Their aim is to extend resource control to the network subsystem. They categorised network traffic into classes based on resource consumption. Other different mechanisms for regulating traffic includeACK pacing, firewalling, etc.

Resource pricing is another different approach that was proposed by T. Znati et al., in order to mitigateDDoS attacks. T. Znati et al., [31].Some other architectures like XenoService [32] infrastructure, Pushback architecture [33], Cooperative Intrusion Traceback and Response Architecture (CITRA) [34] and Throttling [35] provide mitigation from DDoS attacks.

8.14. DDoS Deployment Location

Based on the DDoS deployment location, we provide mitigation to the victim network or the source network.

Victim network mechanism: Mostly DDoS attacks mitigation occur at the victim side. Here most of the damage is done by the DDoS attacks to the victim which results in degradation of performance of the network and high usage of resources. The victim requires more security and defence. Some of the examples of these systems are Event Monitoring Enabling Responses to Anomalous Live Disturbances(EMERALD) [36] and Protocol Security Mechanism [37, 38]. These mechanisms helps a victim's ability to recognize that it isthe target of an attack, and it tries to gain more time torespond.

Source Network Mechanism: DDoS mitigation deployed at the source network can prevent attack flows before they get into the systems core and before they try to attack the victim's network. If the defence mechanismis close to the sources, they can provide easier trace back and detection of the attack. Some of the examples of these mitigation mechanisms are proposed in [39, 40]. A source network mechanism has a disadvantage of detectingthe occurrence on an attack, since it does not experience any difficulties. This disadvantage can be reduced by its mechanism to lose some of its resources and performance for better DDoS detection. This results in restricting the legitimate traffic from a network in thecase of malicious attack detection.

9. DDOS DIRECT ATTACK SCENARIO

In direct DDoS attacks Fig. 6, attacker proceeds with instructions to Handlers which perform Command & Control operations to control VMs. Moreover, zombie VMs directly attack victims and also pass the information to handlers [2]. The machines on targeted victim's network is flooded with huge amount of traffic (IP packets).

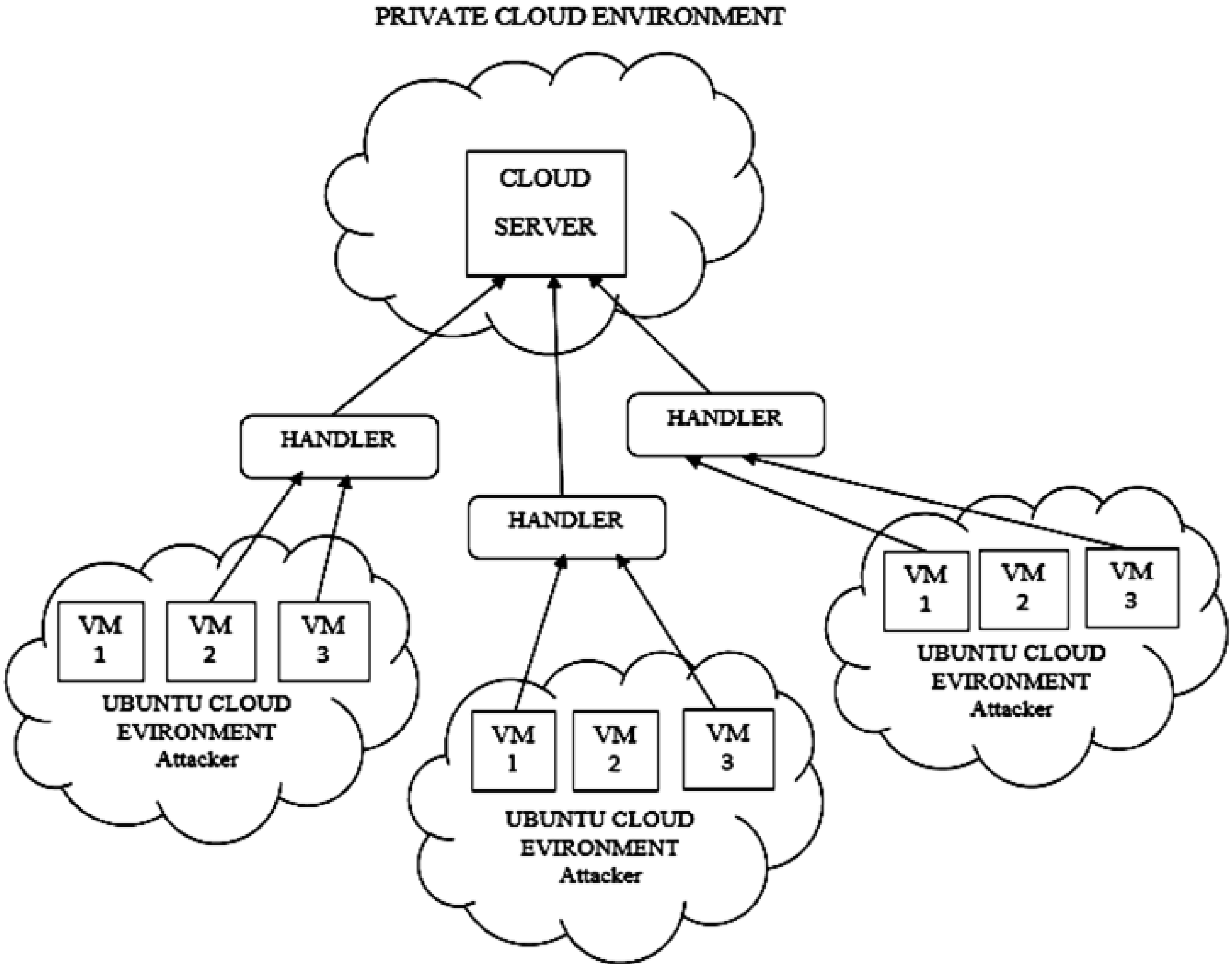

Figure 6: DDoS Direct Attack Scenario

10. TESTBED ENVIRONMENT FOR CLOUD

The private cloud environment using Ubuntu eucalyptus on Linux machines with required number of VMs is setup for monitoring the DDoS attack and the variants of DDoS attacks will be executed. The performance metrics and the degradation of the server functionality is considered for further research.

10.1. Hardware Specifications

1. **Operating system:** Linux mint or Fedora
2. **Ram:** 16gb DDR-3
3. Intel Xenon E5-2630 *v*2 Six core processor 2.6 GHz
4. **Storage:** 1TB hard drive with 16 Mb cache

10.2. Software Specifications

1. Oracle VM Virtual Box
2. Ubuntu 10.04.4-Server-i386 ISO file

10.3. Private Cloud

1. Ubuntu Eucalyptus

10.4. DDOS Attack Tools

1. LOIC (Low Orbit Ion Canon)
2. XOIC

10.5. DDOS Monitoring Tools:

1. SNORT
2. WIRESHARK

11. CONCLUSION AND FUTURE WORK

The propsoed system is designed to detect and mitigate the DDoS attacks in the cloud compuitng environment by analyzong the detoraition in the preformance aspects both on the network and host level. The quality of service is assured by using efficient queueing methods and the potential damage to cloud services is reduced. An experimental testbed is setup bu configuring ubuntu private cloud for analyzing the effects of virtual hosts. The optimization of the detection and mitigation techniqueswill be extended in further research.

References

H. J. Kashyap,M. H. Bhuyan,J. K. Kalita andD. K. Bhattacharyya, "Detecting distributed denial of service attacks: methods, tools and future directions," The Computer Journal, vol. 57, no. 4, pp.537-556, 2013.

Abliz M, "Internet denial of service attacks and defense mechanisms," University of Pittsburgh Technical Report, no. TR-11-178,pp. 1-50, 2011.

P. Zaroo, "Survey of DDoS attacks and some DDoS defense mechanisms," 2003.

"Annual Worldwide Infrastructure Security Report (WISR)",in 2016.

S. Dietrich, N. Long and D. Dittrich, "Analyzing distributed denial of service tools: the shaft case," In Proceedings of the fourteenth systems administration conference, pp. 329-339, 2000.

A. S. Vijayan,B. K. Joshi andB. Joshi, "Securing Cloud Computing Environment Against DDoS Attacks," In proceedings of the International Conference on Computer Communication and Informatics, pp.1-5, 2012.

T. Sivakumar, G. Aghila andT. Karnwal, "A Comber Approach to Protect Cloud Computing against XML DDoS and HTTP DDoS attack," In proceedings of the IEEE Students Conference on Electrical, Electronics and Computer Science, pp.1-5,2012.

S. Malliga andE. Anitha, “A Packet Marking Approach To Protect Cloud Environment Against DDoS Attacks,” In proceedings of the International Conference on Information Communication and Embedded Systems, pp.367 -370, 2013.

J. B. Hong and D. S. Kim, “Assessing the Effectiveness of Moving Target Defenses using Security Models,” IEEE Transactions on Dependable and Secure Computing, vol.13,no.2, pp.1, 2015.

D. Yau andF. Liang, “Using Adaptive Router Throttles against Distributed Denial-of -Service Attacks”, International Journal of Software, vol.13, issue. 7, pp. 1120-1127, in 2002.

D. Cheriton andK. Argyraki, “Active Internet Traffic Filtering: Real-Time Response to Denial-of-Service Attacks”, USENIX, in 2005.

B. Wilson,S. Fahmy, A. Hussain, J. Mirkovic, P. Reiher, R. Thomas and S. Schwab, “Automating DDoS Experimentation”, in the DETER workshop, on August 2007.

E. Arikan,P. Reiher , S. Wei,J. Mirkovic, R. Thomas andS. Fahmy, “Benchmarks for DDoS Defense Evaluation”, in MILCOM, 2006.

P. Reiher andJ. Mirkovic, “A Taxonomy of DDoS Attacks and Defense Mechanisms”, ACM SIGCOMM Computer Communications Review, vol. 34, issue.2, pp.39-54, April 2004.

S. Bellovin, R.Mahajan, S. Floyd, S. Shenker and V. Paxson, “Controlling High Bandwidth Aggregates in the Network”, ACM Computer Communications Review, vol.32, issue.3, pp. 62-73, July 2002.

F. Liang, J.C. Lui, D.K.Yau and Y. Yam, “Defending against Distributed Denial-of-Service Attacks with Max-Min Fair Server-Centric Router Throttles. ACM Transaction on Networking”, vol. 13, issu-1, pp.29- 42, February 2005.

Xueping Wang, Yinan Jing, Gendu Zhang andXiaochun Xiao, “Defending Against Meek DDoS Attacks By IP Traceback-based Rate Limiting”, Global Telecommunications Conference, ‘06. IEEE, in December 2006.

J. Xu andM.Sung, “IP Traceback-based Intelligent Packet Filtering: A Novel Technique for Defending against Internet DDoS attacks”, in IEEE ICNP, Paris, France, December 2002.

M. Weber, J. Maier andF.Kargl, “Protecting Web Servers from Distributed Denial of Service Attacks”, in 10th International World Wide Web Conference, May 2001.

Kang, L. Barolli,J. H. Park and Y. Jeon, “Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks,” International Journal of Network and Computer Applications, vol.34, no 4, pp-1097-1107, 2011.

Opeyemi Osanaiye, “Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework”, Journal ofNetworkandComputerApplications67(2016)147–165, 2016.

Malvinder Singh Bali, “Performance Analysis of Cloud Computing under the Impact of BotnetAttack”, ELSEVIER,2015.

B. S. Kiruthika Devi and T. Subbulakshmi, “A Comparative Analysis of Security Methods for DDoS Attacks in the Cloud Computing Environment”, Indian Journal of Science and Technology**,** *Vol 9(34), DOI: 10.17485/ijst/2016/v9i34/93175, September 2016.*

Muhammad Aamir, “Study and Performance Evaluation on Recent DDoS Trends of Attack & Defense”, *I.J. Information Technology and Computer Science,* 2013, 08, 54-65 Published Online July 2013 in MECS (http://www.mecs-press.org/).

Abhinav Bhandari and A.L Sangal, “Performance Metrics for Defense Framework against Distributed Denial of Service Attacks”, ACEE, International Journal of Network Security, vol.6, April, 2014.

D. Olshefski, W. Zhao, H. Schulzrinne, Internet Quality ofService: an overview, Columbia Technical Report CUCS-003-00, 2000.

D. Black, S. Blake, M. Carlson, E. Davies, Z. Wang, W.Weiss, An architecture for differentiated services, in: IETF,RFC 2475, 1998.

G. Xie, M.B. Geoffrey, A feeedback mechanism formitigating Denial of Service attacks against differentiatedservices clients, in: Proceedings of the 10th InternationalConference on Telecommunications systems, Monterey, CA, October 2002.

M. Weber, J. Maier, F. Kargl: Protecting web servers fromDistributed Denial of Service attacks, in: Proceedings ofthe Tenth International Conference on World Wide Web,Hong Kong, May 1–5, 2001, pp. 514–524.

A.L.N. Reddy, A. Garg, Mitigating Denial of serviceAttacks using QoS regulation, in: Proceedings of the TenthIEEE International Workshop on Quality of Service, 2002,pp. 45–53.

T. Znati, C. Sangpachatanaruk, S.M. Mankins , R. Melhem,D. Moss, Proactive server roaming for mitigatingDenial of Service attacks, in: Proceedings of 1st InternationalConference on Information Technology Researchand Education (ITRE), Newark, NJ, USA, August 10–13,2003.

S. Early, J. Yan, R. Anderson, The XenoService adistributed defeat for Distributed Denial of Service, in:Proceedings of ISW 2000, in: Proceedings of ISW 2000,IEEE Computer Society, Boston USA, 2000.

S.M. Bellovin, J. Ioannidis, Implementing pushback:router-based defense against DDoS Attacks, in: Proceedingsof Network and Distributed System Security Symposium,NDSS02, San Diego, CA, 2002, pp. 6–8.

K. Djahandari , D. Sterne, B. Wilson, B. Babson, D.Schnackenberg, H. Holliday, T. Reid, Autonomic responseto Distributed Denial of Service attacks, in: Proceedings ofRecent Advances in Intrusion Detection, 4th InternationalSymposium, RAID 2001 Davis, CA, USA, October 10–12,2001, pp. 134–149.

F. Liang, D.K. Yau, J.C.S. Lui, Defending againstDistributed Denial of Service attacks with max–min fairserver-centric router throttles, in: Proceedings of the TenthIEEE International Workshop on Quality of Service(IWQoS), Miami Beach, FL, 2002, pp. 35–44.

P.A. Porras, P.G. Neumann: EMERALD: event monitoringenabling responses to anomalous live disturbances, in:Proceedings of the Nineteenth National Computer SecurityConference, Baltimore, MD, October 22–25, 1997, pp.353–365.

J. Leiwo, P. Nikander, T. Aura, Towards network denial of service resistant protocols, in: Proceedings of the 15thInternational Information Security Conference (IFIP/SEC2000), Beijing, China, Kluwer, Dordrecht, 2000.

C. Meadows, A formal framework and evaluation method for network Denial of Service, in: Proceedings of the 12th IEEE Computer Security Foundations Workshop, IEEE.

G. Prier, J. Mirkovic, P. Reiher, Attacking DDoS at thesource, in: Proceedings of ICNP 2002, Paris, France, 2002,pp. 312–321.

M. Poleto,T.M. Gil, MULTOPS: a data-structure forbandwidth attack detection, in: Proceedings of 10th UsenixSecurity Symposium, Washington, DC, August 13–17,2001, pp. 23–38.

Mohammed M. Alani, “Securing the Cloud: Threats, Attacks and Mitigation Techniques”. Journal of Advanced Computer Science and Technology, 3 (2) (2014) 202-213.

Christos Douligeris, Aikaterini Mitrokotsa: “DDoS attacks and defense mechanisms: classification and state-of-the-art”. ELSEVIER, Computer Networks 44 (2004) 643–666.

Internet: popular DDoS attacks in recent trends.