SECURITY THREATS IN COMPUTER SYSTEMS AND INTERNET WEB SERVICES

Sobana S[1], Krishna Prabha S[2], Seerangurayar T[3], Sudha S[4]

[1]*Adithya Institute of Technology, Coimbatore, Tamil Nadu, India*

[2]*P.S.N.A College of Engineering and Technology, Dindigul, Tamil Nadu, India*

[3]*Bannari Amman Institute of Technology, Sathyamangalam, Tamil Nadu, India*

[4]*SSM Institute of Engineering and Technology, Dindigul, Tamil Nadu, India*

Abstract: *An investigation on the latest procedures in manipulating Distributed Denial of Service (DDoS) intrusions is conferred in this work. Distributed denial-of-service (DDoS) attacks are the most profound attacks of today's cyber-intrusions that cause devastating consequences on the internet cloud computing. The foremost intent of a DDoS attack is to devastate the resources of the user or public network connections and thriving vulnerabilities adopting malicious packet. Numerous counteractive actions have been intended by assorted investigators. This article presents a meticulous scrutiny of different DDoS intrusions and detection and fortification techniques. Finally, some essential research trends in the vicinity of future to endow with the security against DDoS attacks are delineated.*

Keywords: Attack, Network security, Application layer, Cyber attacks, Security threats, Hactivism, DDoS

1. INTRODUCTION

The rapid development of internet technology makes human more dependent on the development of cloud services and the accessibility of network competent mobile devices[1, 2].Organizing a huge amount of data in cloud services increases the design complexity and computational complexity that leads insecure data processing. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks are the most serious threats that steal sensitive information. DoS is the most dangerous as well as simple security fright to present Internet services [3]. The attacker floods unnecessary requests thereby overload the victim's resources and prevent them to process their own legitimate requests[4].Thus DoS permanently or temporarily blocks the injured system's network resources thereby interrupts their network activities.

Distributed Denial of Service (DDoS) is a variation of DoS attack which is capable of flooding malicious attacks from different attackers at the same time. The main intention of DDos attack is to control the cloud services and access the customer's web servers to perform online transactions or credit card transactions without the knowledge of the customer [5]. Though the victim is unaware of the attack

of Trojan or a backdoor program, the device memory is accessed by the hacker and sometimes the intruder intimidate the victims through activism and blackmails [4].The DDoS intrusions are in many ways such as controlling display of their personal data, ceasing their online systems and retrieving industrial sensor information, etc.,[6]. As concluded by Riquet, Grimaud [7], the DDoS attacks cannot be detected using security software such as intrusion detection system (IDS) and Firewall. The DDoS intrusions are categorized as direct attack and indirect attack by Fernandes, Soares [8]. The direct attack deals with encoding the victim network's security mechanism and accessing its resources and information. The indirect attack deals with refusing the connection requests received from the legal network services. The DDoSintrusion affects both the network as well as the victim resources [9] and introduces network performance degradation by flooding malicious packets [10].

Therefore, this article presents review of classification of DDoS attack and its detection and organized as follows; section 2 describes the motivation of DDoS attack. Section 3 explains the basics, phases, and classification of DDoS attacks and their classifications. Finally, section 4 discusses the different types of DoS detection techniques to avoid DDoS intrusion.

2. MOTIVATIONS BEHIND DDOS

Identifying and analyzing the motivation behind the occurrence of the DDoS attack in today's network environment becomes more difficult. For the past three decades, news headlines are covered with illegal cyber activities and efforts has been taken in detecting and preventing these activities. The growth in number of mobile and network users has been increased the DDoS attack in real time network applications [11].

Cohen and Felson [12] reported that the hacker control and access the computers or network systems and perform their attacks from a remote hidden place. Organizations must know about the origin and causes of these intrusions and identify the solution to tackle their effects. Identifying motivation behind the attack is a difficult process hence the reasons for DDoS attack occur from the assumptions of a small amount of evidence. A DDoS attack depends on either financial or nonfinancial motivations [13].They may include blackmail or extortion, political or ideological disputes, revenge, to damage the organization/person's good name, an effort to achieve a competitive benefit in a business competition and theft of personal and official information. Some of the common reasons for the DDOS attacks are:

2.1 Financial motivations

The DDoS attackers implement this type of intrusions against an organization or individual person for achieving some financial benefits [14]. They perform their hacking activities in three different ways such as data breach, financial demands, and anticompetitive business practices. In the data breach

approach, the hackers theft the identity proves of property details, credit card details and health information of the victim. The hacking team chooses a market place for the hackers and sell the stolen information to commit illegal activities. In the financial demands approach, hackers attack the laptops or mobile phones of the victims and access their details without their knowledge to threaten them to satisfy their financial demands. Criminals also send fake emails from well-known companies, especially from bankers to the victim and reveal their personal information. In the anticompetitive business practices, the hacker attacks the competing company's websites and interferes with service provided by the target servers. The hacker then demands a large sum of money to end up the attacking process. In some places, the hacker threatens the victim's for money before they initiate their attacks. The hackers involved in these illegal attacks are highly experienced technicians. Thus, it is difficult to identify the hackers and stop their attacks [15].

2.2 Nonfinancial motivations

Sometimes for politically or socially motivated purposes, the hackers try to access the computer systems or personal information. The aim of this hactivism is to introduce their own techniques or tools in the market. The attackers (technically lowered skill person) involve in hactivism for revealing their dominations. Hacktivists involve in DDoS attack when they are not agreeing with the activities of opponent companies. Terrorists or people who do not like to support the Governments and political bodies utilize this attacking mechanism to stop their normal activities[16].

Other than these illegal activities, hackers also introduce the DDoS attack for some intellectual challenges**.** Here, the attacker who has a little knowledge of internet can also be capable of downloading and running a program that performs DDoS attack. Hence, an average computer users can able to hack a large company's network or others personal computer to scarify their vengeance [17].

3. ATTACK DETECTION

3.1 Attack strategies

The DDoS attack makes the victim system to shutdown or run at dangerous conditions. The hacker attack the DNS servers and control the banking, medical,air travel services, and etc. The basic structure of the DDoS attack contains three phases and four components [18]. The sequence of DDoS attack is depicted in the figure 1. Attacker, control masters, slaves, agents or zombies and victim server are the basic four components. The phases are categorized according to the functions performed during a DDoS attack.

(1) *Recruiting attack armies (Phase I):* The attacker first identify the devices which have poor security mechanism and consider these devices as master devices. The master devices then flood the attack to other devices in the network and control them[19]. The malicious code is then installed into the master devices and the master's flood the codes to the slave devices. This attacking army is generated by a random scanning technique, hit list scanning technique, topological scanning technique, local subnet scanning technique and permutation scanning technique [20].

(2) *Propagation (Phase II):* Propagation phase propagates the malicious attack codes and commands information to the slave network devices through the master devices. The attack code includes details about the victim IP address, time of attack, and duration of the attack, etc. The way of propagation may be a central source or back chaining or autonomous propagation [21, 22].

(3) *Attack (Phase III):* The attacker commands the master devices to initiate and carry out their attacks against the slave devices. Attackers use spoofed IP address in order to hide their location and personal information. Thus, the victim devices are unable to identify these malicious software's [3].

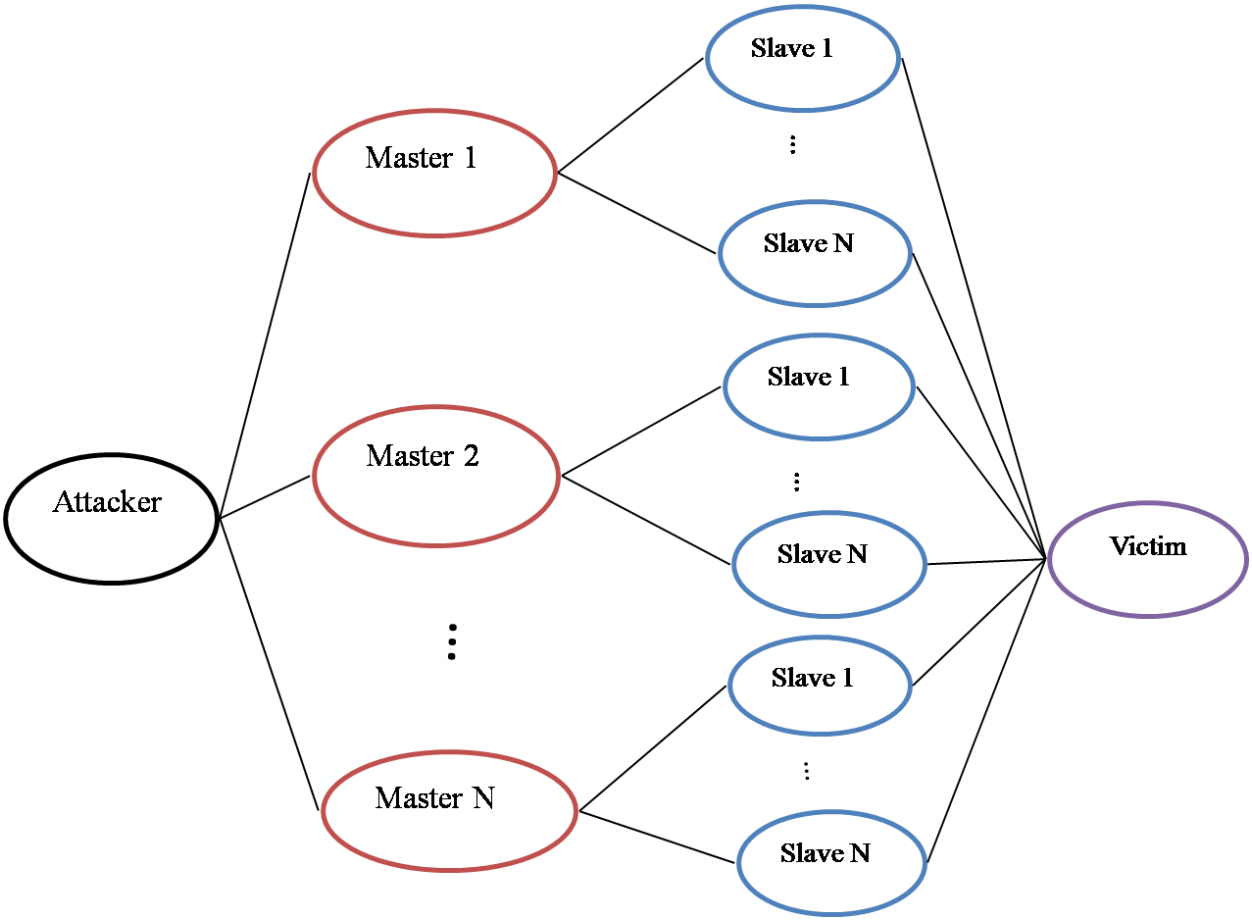

Figure 1. DDoS attacks Structure

3.2 Attack scenarios

Manual attack, Agent-handler attack and automatic attack are the three attack scenarios that set the different DDoS phases and their implementation.

(1) ***Manual Attack*****:** In this scenario, the attacker manually finds out the security loopholes and controls the victim machines. The manual attack consumes a longer time period to initiate malicious attacks.

(2) ***Agent–handler attack*****:** This attack includes both automatic and manual procedures to flood the attacking codes. Thus, it comes under a semiautomatic attacking process. Here, supervisor and agents communicate together through some manual process. This communication includes details about categories, time period and victims of the attack. However, recruiting, handling and utilizing the administrator networks is an automatic process. The administrator network, machine and the representatives may either directly or indirectly communicate with each other.

i. In the *direct communication* method, the agent identifies the supervisor's IP address with the help of compromised agent machine and combines the IP address with their attack code for their later communications. This communication is widely used to inform the availability of the agents to the supervisors. This communication is easy to identify and the DDoS attack can be easily revealed by backtracking method.

ii. In the *indirect communication* method, the supervisor uses some internet chat programs, for example, internet relay chat (IRC) channels which is used to control the activities of the agents. The legitimate service and the distributed nature of the IRC make it difficult to reveal malicious communication.

(3) ***Automatic attack*****:** In this scenario, all the essential communications and steps to flood the DDoS attacks are automatic. Attack code loaded in the compromised machine contains all the essential details needed for the attack and it executes the codes to initiate the required attack. At any time the attacker can attack the victim without the supervisor's and the agent's knowledge[23].

3.3 Mechanisms involved in different attack phases

The three different phases involved in the DDoS attack contains different techniques to spread the DoS attack. They are as follows:

(1) ***Recruiting attack armies (Phase I):*** In this phase, the attacker uses some self-propagating programs to generate botnet [19]. This type of attack only concentrates on victim systems which has poor security services [24]. The followings are some of the frequently used attacking methods used to discover the victim systems[20].

i) Random scanning: Each affected victim systems probes an IP address randomly from local or global address spaces and introduce infection. The Worm Code-Red (CRv2)method is the

best example for random scanning [25]. The basic assumption of this method is that the connected systems are assumed to be in dissimilar networks and also there is no synchronization between the attacking hackers. Thereby a heavy traffic load and more duplicate data transmission occur when the number of infected systems are more in a network[26].

ii) *Hit-list scanning:* An attacker generates a hit-list externally, which includes details about the list of vulnerable systems. Then it propagates some worms using the victim systems, thereby a minimum of 30 seconds is enough to spread the DDoS attack throughout the network [24]. If the Hit-list is prepared using portscan known as stealthy scanning it needs a longer duration. Sometimes the hit-list was prepared by an already infected system known as a distributed scanning process. Web-crawling and public survey are some of the widely used methods to generate hit list well in advance. The hit-list probably occupies a high volume of traffic.

iii) *Permutation scanning:* Self-coordination among the victims is used to stop the propagation of same IP address in multiple times. The vulnerable systems share a common pseudorandom permutation list of IP addresses having any 32-bit block chipper [27]. A compromised host frequently scans the occurrence of new target devices and makes a decision to finalize the ending point of probing when it encounters sequencing a predefined number of systems. The infected compromised system randomly chooses the next system from the list and infects it. After reaching the stopping point, a new permutation key is generated and a new scanning process takes place. This mechanism reduced the possibility of reinfection of the same target. This leads to a huge dropin duplicate infection and increases in infection rate.

iv) *Partitioned permutation scanning:* Hit-list scanning and permutation scanning are combined together to introduce a new DDoS spreading mechanism known as partitioned permutation scanning mechanism. In this scanning method, the attacker generates a permutation list and spread DDoS attacks until it finds a new target. If it finds a new target it split the list into two halves and the old user and new user spread the attack separately to their corresponding permutation list. As the length of the list reduces below a predefined value the partitioned permutation scanning is turned to a single permutation process [22].

v) *Topological scanning:* Topological scanning is the modification of the Hit-list scanning process. The compromised system is responsible for identifying a new victim system and spreading a worm. This type of infection may be either peer-to-peer based infection or web-server based infection. In Peer-to-peer based infection, information about the list of victim

systems for their upcoming attack is with the infected system itself. In the web server–based infection, the worms itself spreads like a transmittable disease without the help of an infected system and infect the victim systems [28].

vi) *Local subnet scanning:* In this method, the network is divided into sub-networks and the compromised system identifies the new victim devices from its sub-net and flood DoS attack. In practice, this method must be combined with any one of the above said methods.Eventhough the subnet have firewall protection this scanning method can infect the victim systems in the same subnet [29].

(2) ***Propagation (Phase II):***Recruiting attack armies initiate the DDoSintrusion process during Phase I. Then, in Phase II the attacking army propagates the attack codes to the victim networks. To initiate the propagation attacking army needs the victim's IP address, duration of the attack and time of the attack. The propagation may take place in any one of the following ways.

i. *Central source propagation:* In Central source propagation, the attack code is propagated with the help of central server as shown in Figure 2(a). Since the central server generates a huge amount of traffic and this attack can be easily discoverable. If the central server is identified and removed from the network of interest, then we can stop this DDoS attack.

ii. *Back-chaining propagation:* The attacker first establishes a connection with the victim network to propagate the attack codes as depicted in figure 2 (b). The general protocol used for connection establishment is File Transfer Protocol (FTP)[22]. Using FTP the victim network directly downloads the attack code from the attacker.

iii. *Autonomous propagation:* This propagation mechanism does not need any prior connection with the server system or with the victim system. So if the attack has its attack code it can propagate to the corresponding victim system (Figure 2 (c)). The duration of the direct linkbetween the attacker and the victim is for a limited period; hence it is more difficult to discover this attack.

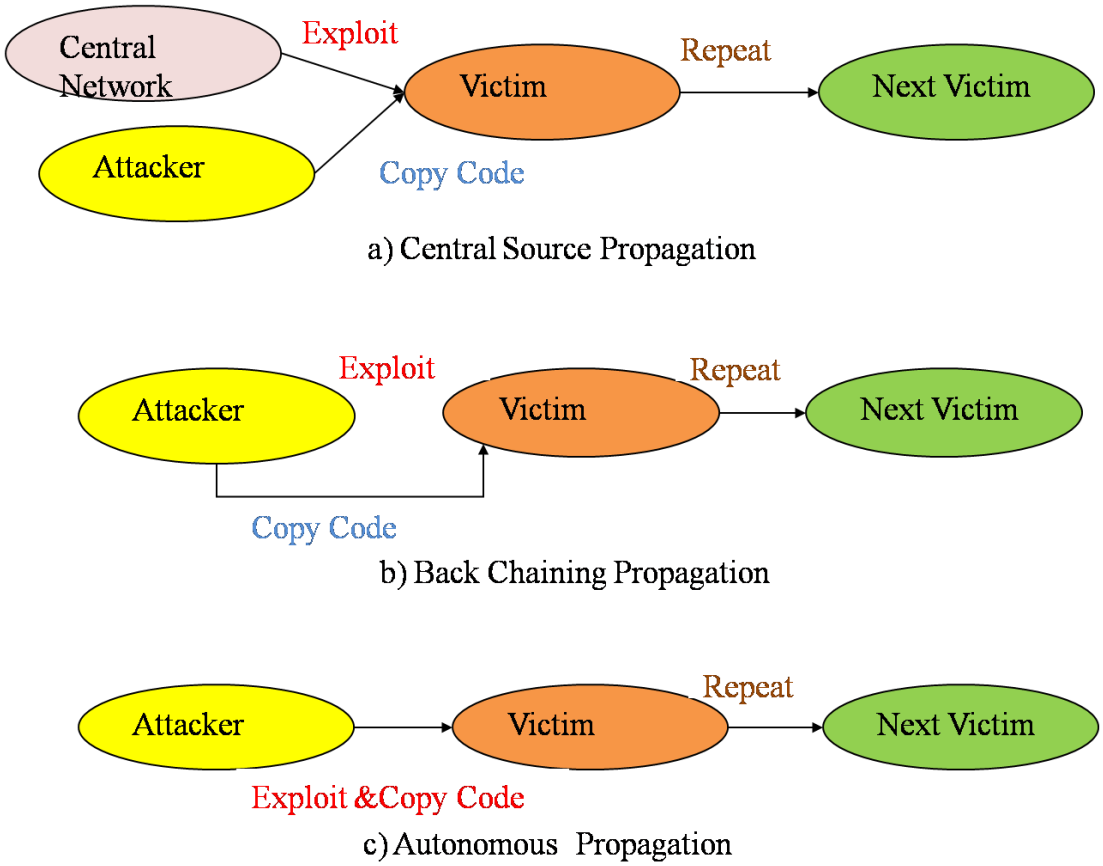

Figure 2. Attack Mechanisms involved in Phase II

(3) ***Phase III - attack:*** In this attack, the root location of the attacker is hidden by a spoof IP address. The attacker only control and directs the victim systems to start and carry out their attack. Use of spoofed IP address does not allow the victim to identify the malicious software thereby makes it difficult to locate the attacker location [3]. During this phase, the network takes more time period to open and execute the required files. Similarly, this makes accessing of web content as a difficult process and in sometimes it makes it difficult to find out the required web pages.

4. CLASSIFICATION OF DOS ATTACK

The DoS attack aims to occupy and exploit the victims network asserts and limit them from accessing their own network resources. Figure 3 demonstrates the basic types of DoS attack and their subtypes in networks.

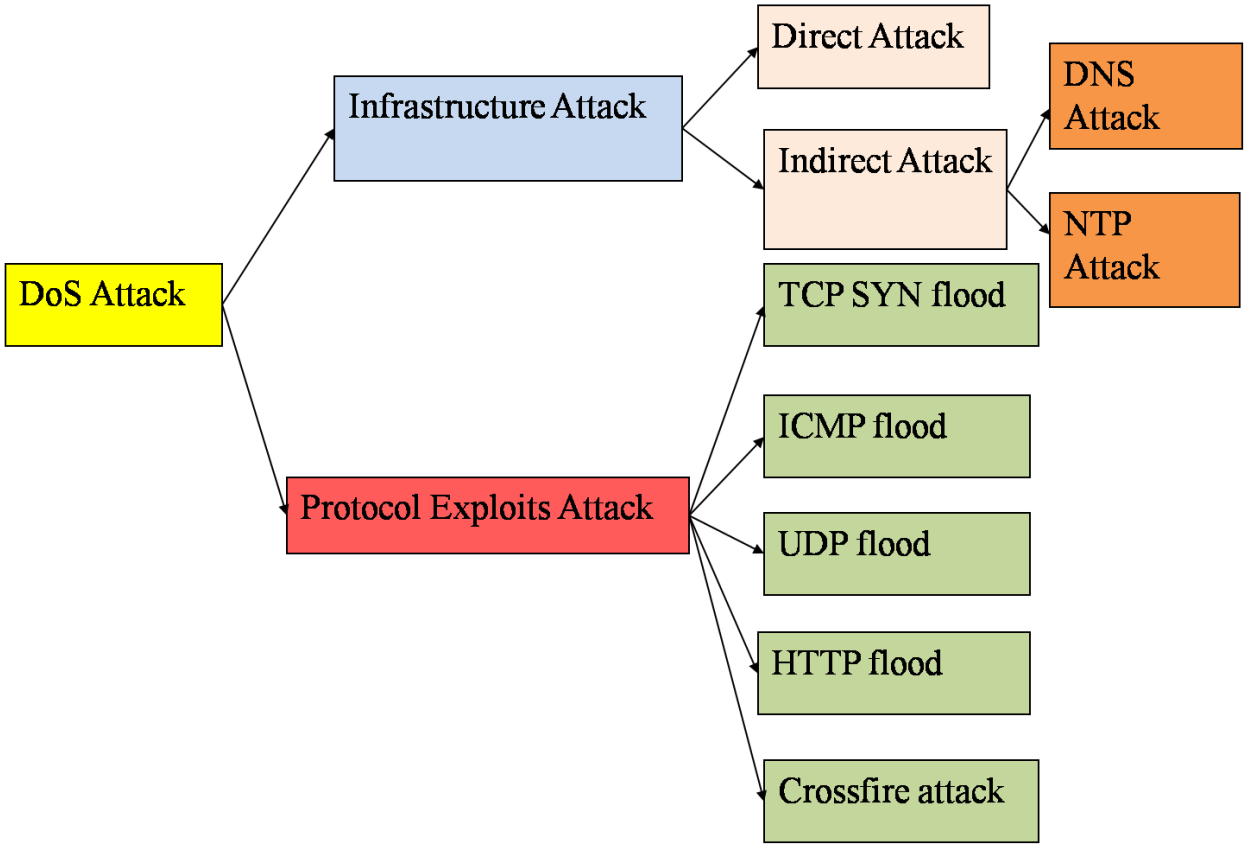

Figure 3.Classification of DoS Attack

4.1 Infrastructure level attacks

Network infrastructure comprises of computing resources, routing equipment and bandwidth. In this attack, the attacker propels a huge amount of fake requests to the victim system thereby overwhelm the resource capacity. Overwhelming the victim resources leads performance degradation and system damages. Some of the widely used infrastructure level attacks are listed below [30].

i. *Direct Attack:* A direct Denial-of-Service attack is described as a basic attacking method to prevent the utilizationof resources from an authorized victim [29]. A Distributed Denial-of-Service attack transfers a large size of packets to a victim system from multiple attackers. Victim's key resources are thus occupied by these packets arrays. Processing of packet array is very difficult when compared with real-time application packets.

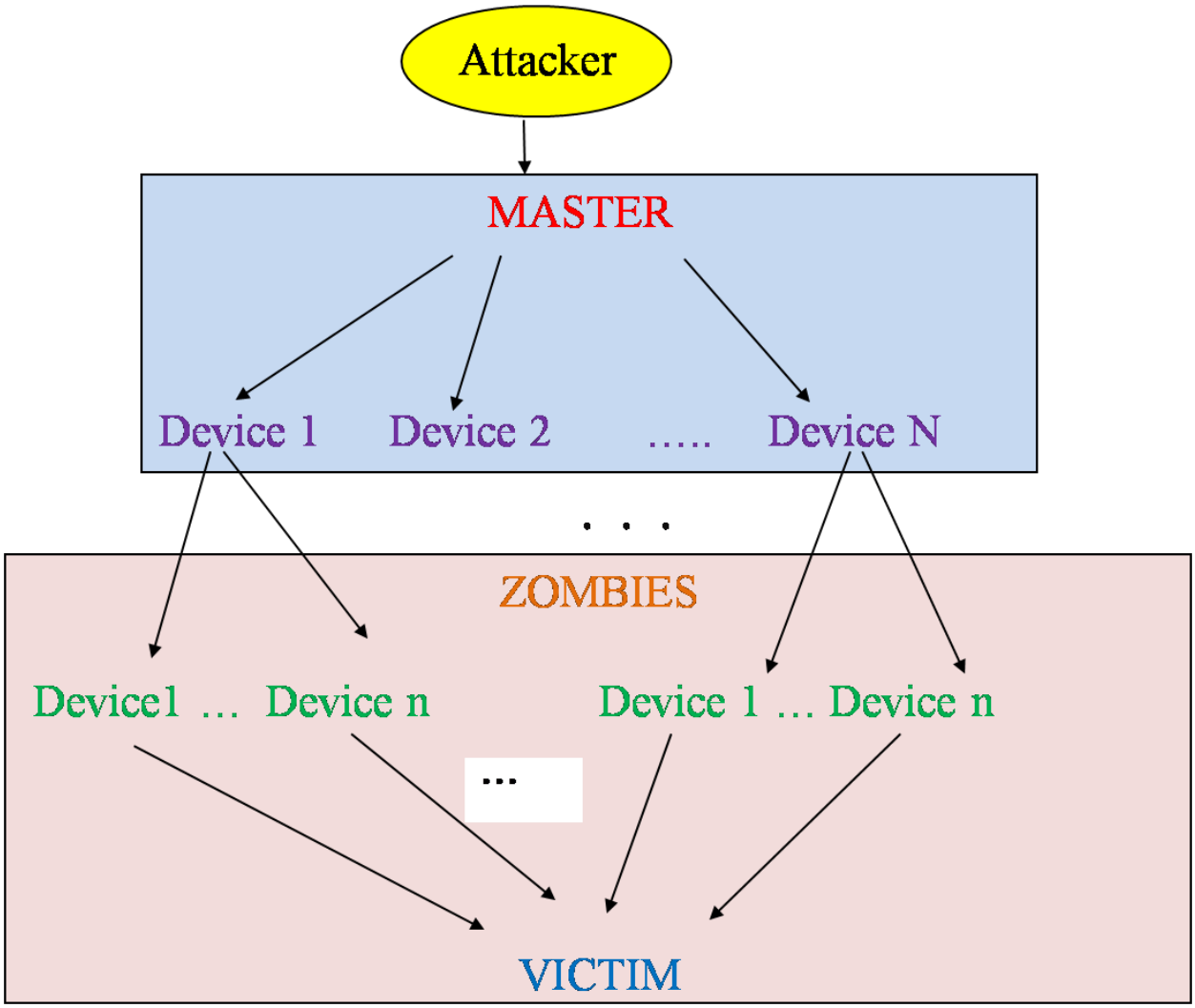

Figure 4.Direct DDoS Attack

ii. *Indirect Attack:* The compromised network receives a burst of requests from the attacker and reflects these requests to the specified victims'systems.Some of the widely used reflection mechanisms are discussed below[30].

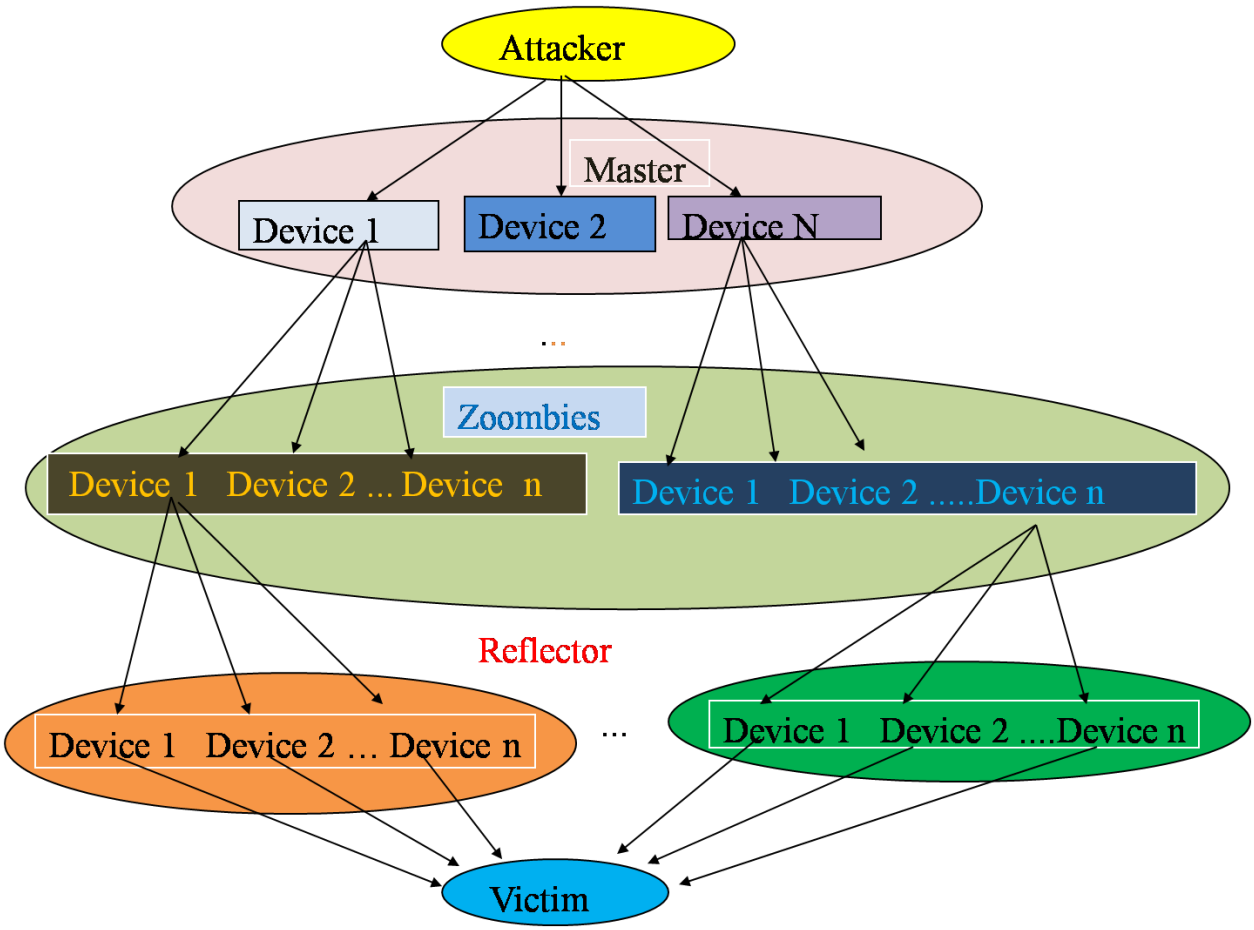

Figure 5. Indirect DDoS Attack

a. *DNS amplification attack:*Its aim is to spread DoS vulnerabilities as much as possible. DNS servers perform this type of attack by floodinga massive UDP packet to the victim networks. The increase in the number of packets increases data traffic, whichintroduces severe catastrophic effect. Thus the attacker occupies the resourceof the spoofed source IP address[31]. It is difficult to identify this type of attack in an earlier stage and the attacker employs less effort to introduce this DoS attack.

b. *NTP (Network Time Protocol) amplification attack*: This attack follows the same concept of DNS amplification attack[32]. NTP synchronizes the clocks of the machines which are connected between the client and the server [33]. MON_GETLIST command is frequently sent from the attacker to the server. The server sends a bunch of response messages that is approximately 19 times more than the query messages[32]. These amplified response messages, thusslow down the data transmission amongthe legitimate users and the server.

4.2 Protocol exploited attacks

The objective of the protocol exploited attacks is to attack the layer protocols of the victim server thereby tries to utilize its total memory. Some of the transport, network, and application layer protocols are affected by these attacks include Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), Session Initiation Protocol (SIP) andHypertext Transfer Protocol (HTTP). Zargar, Joshi [14] compared and analyzed the effects of different types of attacking protocols.They are as follows:

i. *TCP SYN attack:* TCP connection establishment is enabled with the help of a three-way handshaking process. In three-way handshaking, the server is responsible for preserving the data until a connection establishment or timeout. The attacker floods a fake connection request and forces the server to reject the connection requests from valid and legitimate users. The attacker also tries to establish an incomplete connection by spreading some non-surviving IP addresses and a lot of SYN packets. The compromised network disregardthe SYN+ACK packets obtained from the victim networks and flood the spoofed SYN packets from the attackers [30].

ii. *UDP flood attack:* A very common DDoS attack is the UDP flood attack. On UDP flood attack a massive amount of UDP packets is sent from the attacker armies to random ports on the intendedvictim networks. After receiving the UDP packet the victim tries to identify the application type of packet appeared in its port. If the victim network is unable to identify the type of the packet, then the server is responsible for sending ICMP response packet [30].

iii. *Smurf attack:* Smurf attack, also known as an ICMP flood attack, is a ping-based DoS attack. The attacker propels a huge number of ICMP_ECHO_REQUEST packets to a victim's server. The attacker uses ping message packet to identify the availability of the remote victim host. Then it sends the ICMP packet to the victim server IP address as a broadcast message. The host devices connected to this broadcast network will send their ICMP_ECHO_REPLY packet to the spoofed target source IP address. In the meantime, the attacker uses an intermediate network to breakdown the TCP/IP stack on the server network and force it to reject the requests received from the genuine users and stop responding to incoming TCP/IP requests. Thus, it controls the total bandwidth of the victim's network[34].

iv. *Crossfire Attack:* The controller of botnet attacker first identifies a groupofspoofed IP addresses and the advertised routes crossing the same link. A massive amount of request packets is then sent from the attacker in order to inhabitthe bandwidth of the victim network [35].

v. *HTTP flood attacks:* HTTP flood attack is the second most common application layer protocol attack. In this attack, the attacker spreads tremendous amount of HTTP GET and POST packets to the victim web servers and consume their resources [30]. Thus the victim server is unable to accept the requests from the legitimate servers. Among the other protocol attacks, the HTTP flood attack has the highest resolution,thereby it is intractableto detect and mitigate this type of attacks.

5. DETECTION TECHNIQUES

The basic idea about various detection techniques of DDoSattackare reported by Carl et al, 2006. The detection techniques are introduced to discriminatethe malicious data packets from the legitimate data packets. In a recent network scenario, Activity profiling, Sequential Change-Point detection, and Wavelet analysis are the most commonly used DDoS detection techniques.

5.1 Activity profiling

In this detection process, the header network flow is monitored frequently and based on the results an active profile iscreated. The network flow is measured by identifying the number of consecutive packets havingindistinguishableheader fields and the average packet rate is the elapsed time between these successive packets. The total network flow includes the ratio between the sum of packet rates and the average packet rates of all incoming and outgoing network flows. If the size of the network is too large to manage then clustering of networks is done [36] to detect DDoS attack. The data communications having similar characteristics are grouped into one cluster. The network flow is now calculated for the individual cluster and their summation indicates an increase or decrease attack rate[37].

The modification of active profiling is known as trace-back processing where the server sends only less frequent packets over the internet. The different methods of trace backing detection techniques are as follows.

5.2 IP Trace-back Technique

This technique uses IP spoofing for detecting and protecting against DDoS attacks. The main process here is to identify the original source IP address of the packet [38]. In a network scenario, multiple sources initiate their attacks at the same time [39],thus it is difficult to discoverthe original source IP address. Proactive and reactive approaches are the most widely used IP trace-back techniques.

(i) *Reactive approach*: Reactive approach responds to an attack after they have happened. In a reactive approach, a stimuli-response mechanism is used to execute the trace-back process. Depending upon the use of an Intrusion Detection Scheme (IDS),the reactive approach is classified into IDS and Non-IDS assisted approaches. The IDS based reactive approach is the most common

detection technique used in recent scenario and Network based IDS and Host based IDS schemes are the basic types of IDS assisted scheme[40].

(ii) *Proactive approach*: In the proactive approach, attacks are eliminated before they have a chance to appear. This is done by recording and monitoring the traffic packets as they flow through the network. These records indicate the legitimate user to the victim network thereby provides timely response on the occurrence of DDoS attack. The trace-back packets in the network are then used for identification and reconstruction of the attack path [41, 42]. If the trace-back information is sent within the data packet then the information is known as in-band information.Ifthe informationis sent as a separate trace-back packet thenitis called as out-of-band information.

The drawbacks of trace-back techniques include minimum scalability, high storage cost, and poor router performance.

5.3 Packet Marking Technique

This detection method is coming under a proactive approach with in-band detection approach. The routers in the networks mark the packets when they cross them [43]. Either probabilistic packet marking (PPM) or deterministic packet marking (DPM) is employed to mark the packets [38]. The injured systemthen reconstructs the attack path using inbuilt trace-back information.

(i) *Probabilistic packet marking (PPM):* In PPM, the IP header contains a 16-bit IP identification field to hold the route marking information [44]. Krishan Kumar, Sangal [38]stated that approximately 677 attackers try to give wrong information about the packet marking information. The marking is done either as node marking or edge marking. In node marking the router and IP address is used for forwarding the attacking packets whereas in edge marking the IP address of the edge of the paths is used.

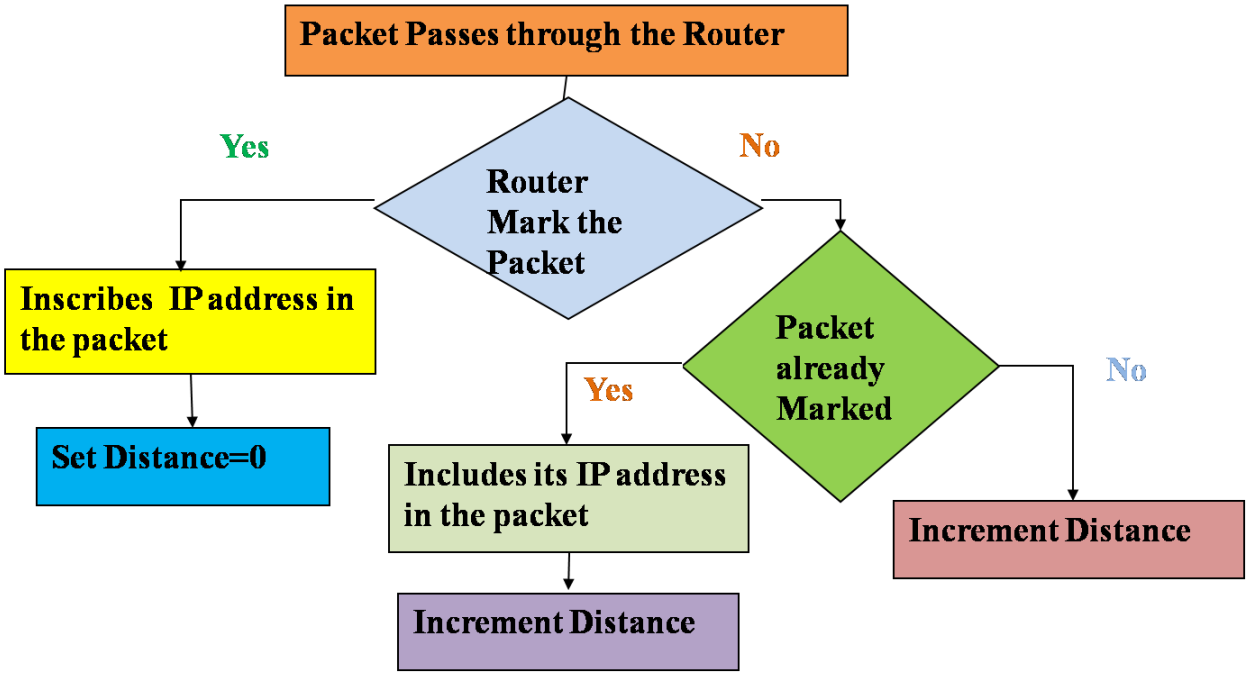

Figure 6.PPM algorithm

(ii) *Deterministic packet marking (DPM)*: In DPM, the router marks and assigns its IP address to every packet passes through it. The main advantages of DPM algorithm are it converges quickly, the overhead needed is less and the computation complexity is less [38].

(iii) *Entropy Variation:* Random variation in the flow of packets through a particular router is termed as Entropy variation. The router detects and analyzes the characteristics of the network data traffic dynamically. If the network entropy variation falls below a certain threshold value, the LAN router makes an alarm and the router discards the DDoS packets received from the attackers before [45]. The router thus avoids the DDoS attack before it happens.

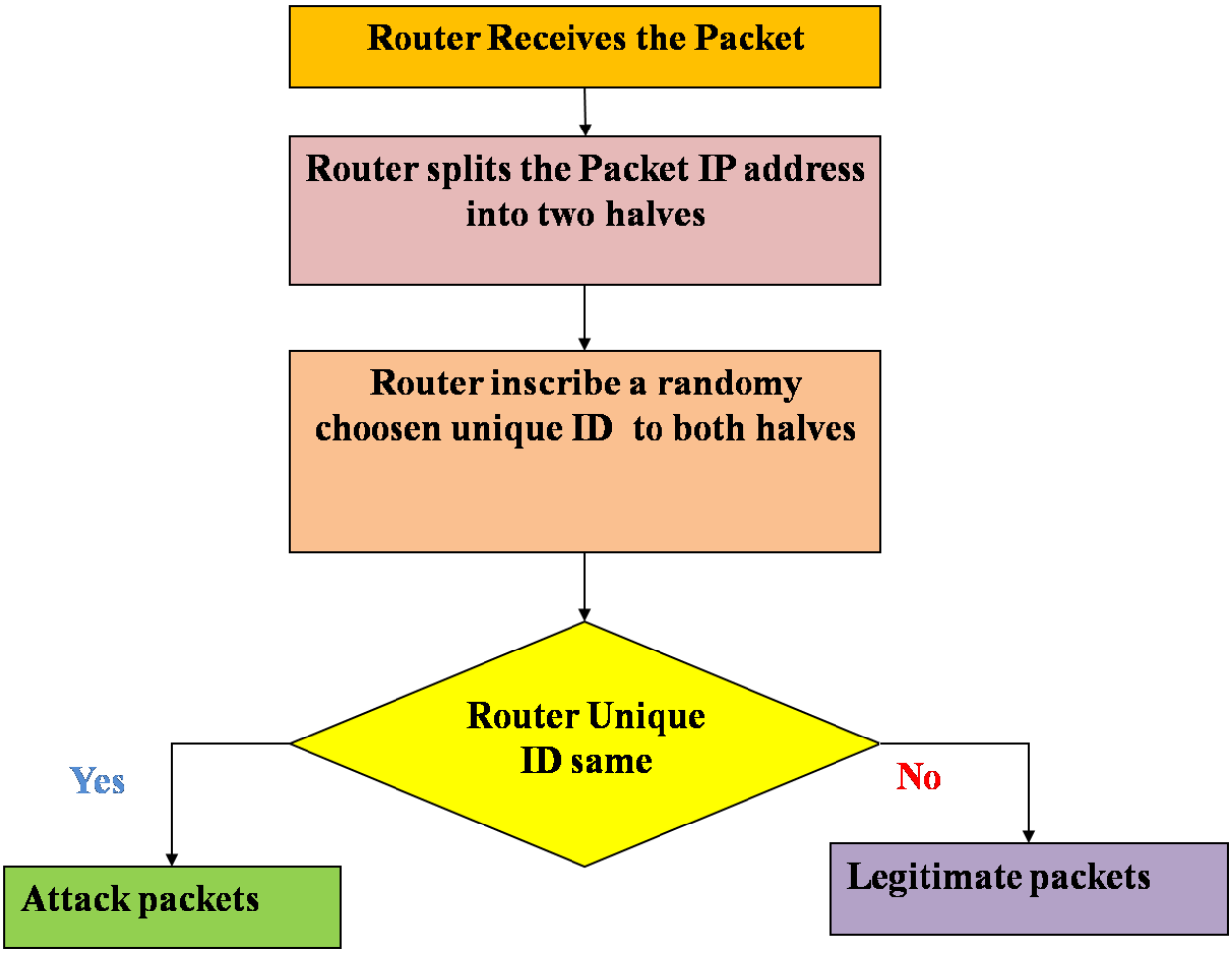

Figure 7.DPM algorithm

5.3 Sequential Change-Point Detection Technique

The network local agents use the parameters such as port details, IP address, and type of protocol as a filter to detect the attackers [36]. The router calculates these filtering parameters after a particular duration of time continuously.

(i) *Intrusion Detection and Prevention System (IDS/IPS):* The local agent uses Intrusion Detection and Identification Protocol (IDIP) to monitor the uncertain incidentsand inform it to the boundary router. The router then takes the necessary action according to the IDIP message received from the local agent. The IDIP message is generated by techniques such asanomaly detection, signature-based detection etc[46].

(ii) *Signature-Based Detection:* In signature based intrusion detection, the users are differentiated by an individual signature. The router uses the signature only if the data traffic exceeds some

predefined high load threshold (HLT) to differentiate the spurious packets and block the doubtful users. If the traffic load is in between the low-level threshold (LLT) then the hesitantusers are not permitted to cross the network [47].

(iii) *Anomaly (or behavioral) Detection:*This technique is used to detect the network's abnormal activity. Abnormality is measured by periodic monitoring and statistical analysis of packer parameters. Existing techniques include statistical modeling, hidden Markov modeling and data mining [48].

5.4 Misuse detection

Misuse detection uses some of the signature-based detection techniques such as Realsecure, Snort and CISCO'S NetRanger[49] to monitor the performance of the network. The network monitor has some well-defined patterns of malicious packets and then looks out for occurrences of such patterns and not allowing them to enter into the network.

In general, the objective of the IDPS is to investigate differentincidents of the network, collecting data regarding them, generate reports and decide to block abnormal events.

(i) *Host-based IDS (HIDS) approach:* HIDS aims to monitor and collects data in the low-level network operations on a single PC. It monitors system call attempts, files, logs and setting information then alert if any unwanted access, detection, modifications and copying of files happened. It also replaces the altered files and maintains integrity [50].

(ii) *Network-based IDS (NIDS) approach:* NIDScollects and monitors data flow in the network level. Sensors are located in the network to monitor and capture the network traffic. The captured values are compared with a set of predefined attack patterns. NIDS devices perform this comparison process for each and every data packets they encounter and try to avoid malicious DDoS attack packets [50].

(iii) *Hybrid agents IDS approach:* This approach is thecombination of host-based agent approach and network-based sensor approach. Thus it is possible to analyze the network traffic addressed to a network as well as a single host in the network [51].

5.5 Wavelet Analysis

The wavelet analysis is accomplished by spectral components rather than statistical components.Wavelet analysis separates the irregular malicious packets by analyzing the spectral energy. Mirkovic and Reiher [29]used this analysis to detect attacks, flash crowds, measurement failure and network failures.

5.6 Support Vector Machine (SVM) based framework

This method aims to ensure detection accuracy in a dynamic environment. The SVM correlates virtual machine (VM) application parameters with original resource traffic load parameters. This comparison helps to detect the occurrence of DDoS attack as well as the compromised VM which occupies more bandwidth [52].

5.7 Probability-based Malicious Request Detection (PBMRD)

Hidden Markov Model (HMM) is used in PBMRD to detect the probability of a given request to be malicious. High probability, average probability, and lower probability are the three different cases occurred in this analysis. High probability ensures the occurrence of DDoS attack and stops receiving requests from the particular attacker. In an average-valued probability condition, the XML Vulnerability Detector is responsible for further analysis of the request. If the network has a lower probability, then Request Scheduler is responsible for further processing. The HMM shows only the output and the states are hidden. The current state of the process is determined by the HMM's Forward-Backward formula [53].

$$P(X_t|Y_{1:t}) = \frac{P(Y_t|X_t)\cdot P(X_t|Y_{1:t-1})}{\sum\left(P(Y_t|X_t)\cdot P(X_t|Y_{1:t-1})\right)} \quad (1)$$

6. CONCLUSION

DDoS attacks will turn out to be the most significant predicament on the network hustles in future as the intensity of onslaught computerization has widened enormously. This paper wrangles to accomplish a vital expertise of DDoS attacks along with the categorization of these onslaughts and also propose an updated outlook of spotting the DDoS attack in assorted encompassment. The foremost confront pinpointed in this revisit is to catalogue the DDoS attacks ensued in different network layers and accomplish an acceptable success rate in perceiving the attacks. The paper expounded some research attempts for perceiving DDoS attacks where there is no sensible authentication across different network environments. The annexe of this review embraces deploying a test-bed to interpret the concert of various revealing techniques. The endurance of the network reckon on the success rate of DDoS attack detection. It is vital to prevent the manifestation of DDoS attack instead of revealing the occurrence.

REFERENCES

1. Kumar, G., K. Kumar, and M. Sachdeva, *The use of artificial intelligence based techniques for intrusion detection: a review*. Artificial Intelligence Review, 2010. **34**(4): p. 369-387.
2. Nsfocus. *Introduction to DDoS attack*. 2014 [cited Retrieved July 28, 2014; Available from: https://en.nsfocus.com.
3. Mahjabin, T., et al., *A survey of distributed denial-of-service attack, prevention, and mitigation techniques.* International Journal of Distributed Sensor Networks, 2017. **13**(12): p. 1550147717741463.
4. *DoS* 2019.
5. Bonguet, A. and M. Bellaiche, *A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing. Future Internet*, 2017. **9**(3): p. 43.
6. NCSC. *National Cyber Security Centre: Understanding denial of service (DoS) attacks*. 2018; Available from: https://www.ncsc.gov.uk/guidance/
7. Riquet, D., G. Grimaud, and M. Hauspie. *Large-scale coordinated attacks: Impact on the cloud security*. in *Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*. 2012. IEEE.
8. Fernandes, D.A., et al., *Security issues in cloud environments: a survey.* International Journal of Information Security, 2014. **13**(2): p. 113-170.
9. Somani, G., et al., *DDoS attacks in cloud computing: collateral damage to non-targets.* Computer Networks, 2016. **109**: p. 157-171.
10. Antunes, J., N.F. Neves, and P.J. Veríssimo. *Detection and prediction of resource-exhaustion vulnerabilities*. in *19th International Symposium on Software Reliability Engineering, 2008. ISSRE 2008*. 2008. IEEE.
11. Arushi Arora, Sumit Kumar Yadav, and K. Sharma, *Denial-of-Service (DoS) Attack and Botnet: Network Analysis, Research Tactics, and Mitigation*, in *Handbook of Research on Network Forensics and Analysis Techniques*. 2018, IGI Global. p. 117-141.
12. Cohen, L.E. and M. Felson, *Social Change and Crime Rate Trends: A Routine Activity Approach (1979)*, in *Classics in Environmental Criminology*. 2016, CRC Press. p. 203-232.
13. Jayanthi, M.K., G. DileepKumar, and M. Singh, *Network Security Attacks and Countermeasures*, in *Security and Forensics for 2019*. 2016, IGI Global
14. Zargar, S.T., J. Joshi, and D. Tipper, *A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks.* IEEE communications surveys & tutorials, 2013. **15**(4): p. 2046-2069.
15. Sikkanan, S. and M. Kasthuri, *Denial-of-Service and Botnet Analysis, Detection, and Mitigation*, in *Forensic Investigations and Risk Management in Mobile and Wireless Communications*. 2020, IGI Global. p. 114-151.
16. Sharma, K. and B. Gupta, *Taxonomy of distributed denial of service (DDoS) attacks and defense mechanisms in present era of smartphone devices.* International Journal of E-Services and Mobile Applications (IJESMA), 2018. **10**(2): p. 58-74.
17. Yadav, S.K., K. Sharma, and A. Arora, *Security Integration in DDoS Attack Mitigation Using Access Control Lists*, in *International Journal of Information System Modeling and Design*. 2018, IGI Global. p. 56-76.
18. Liu, J., et al., *Botnet: classification, attacks, detection, tracing, and preventive measures.* EURASIP journal on wireless communications and networking, 2009. **2009**(1): p. 692654.
19. Sun, B., et al., *Self-propagating mal-packets in wireless sensor networks: Dynamics and defense implications.* Ad Hoc Networks, 2009. **7**(8): p. 1489-1500.
20. Weaver, N., *Warhol worms: The potential for very fast internet plagues*. 2001.

21. Mirkovic, J., et al., *Internet denial of service: attack and defense mechanisms (Radia Perlman Computer Networking and Security)*. 2004.
22. Patrikakis, C., M. Masikos, and O. Zouraraki, *Distributed denial of service attacks.* The Internet Protocol Journal, 2004. **7**(4): p. 13-35.
23. Gupta, B., R.C. Joshi, and M. Misra, *Distributed denial of service prevention techniques.* arXiv preprint arXiv:1208.3557, 2012.
24. Staniford, S., V. Paxson, and N. Weaver. *How to Own the Internet in Your Spare Time*. in *USENIX security symposium*. 2002.
25. Moore, D. and C. Shannon. *Code-Red: a case study on the spread and victims of an Internet worm*. in *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment*. 2002. ACM.
26. Gu, Q. and P. Liu, *Denial of service attacks.* Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications, 2007. **3**: p. 454-468.
27. Weaver, N., *Potential strategies for high speed active worms: A worst case analysis.* Whitepaper, UC Berkeley, 2002.
28. Chen, Z. and C. Ji, *Optimal worm-scanning method using vulnerable-host distributions.* International Journal of Security and Networks, 2007. **2**(1-2): p. 71-80.
29. Mirkovic, J. and P. Reiher, *A taxonomy of DDoS attack and DDoS defense mechanisms.* ACM SIGCOMM Computer Communication Review, 2004. **34**(2): p. 39-53.
30. Deka, R.K., D.K. Bhattacharyya, and J.K. Kalita, *DDoS Attacks: Tools, Mitigation Approaches, and Probable Impact on Private Cloud Environment.* arXiv preprint arXiv:1710.08628, 2017.
31. Peng, T., C. Leckie, and K. Ramamohanarao, *Survey of network-based defense mechanisms countering the DoS and DDoS problems.* ACM Computing Surveys (CSUR), 2007. **39**(1): p. 3.
32. Graham-Cumming and John, *Understanding and mitigating NTP-based DDoS attacks*, in *Cloudflare, Inc*. 2014.
33. Mills, D.L., *Computer network time synchronization: the network time protocol on earth and in space*. 2016: CRC Press.
34. Amiri, I.S. and M.R.K. Soltanian, *Theoretical and Experimental Methods for Defending Against DDoS Attacks*. 2015: Syngress.
35. Kang, M.S., S.B. Lee, and V.D. Gligor. *The crossfire attack*. in *Security and Privacy (SP), 2013 IEEE Symposium on*. 2013. IEEE.
36. Carl, G., et al., *Denial-of-service attack-detection techniques.* IEEE Internet computing, 2006. **10**(1): p. 82-89.
37. Alenezi, M. and M.J. Reed, *Methodologies for detecting DoS/DDoS attacks against network servers*, in *Proceedings of the Seventh International Conference on Systems and Networks Communications—ICSNC*. 2012.
38. Krishan Kumar, A. Sangal, and A. Bhandari. *Traceback techniques against DDOS attacks: a comprehensive review*. in *2nd International Conference on Computer and Communication Technology (ICCCT)*. 2011. IEEE.
39. Sivabalan, S. and P. Radcliffe. *A novel framework to detect and block DDoS attack at the application layer*. in *IEEE 2013 Tencon-Spring*. 2013. IEEE.
40. Prasad, K.M., A.R.M. Reddy, and K.V. Rao, *DoS and DDoS attacks: defense, detection and traceback mechanisms-a survey.* Global Journal of Computer Science and Technology, 2014.
41. Bhale, K.M., *Botnet Detection Tools and Techniques: A review*. 2016, Centre for Cyber Security Institute for Development and Research in Banking Technology.
42. Menezes, J.P. *The botnet menace*. 2007; Available from: https://www.itworldcanada.com/article/the-botnet-menace-and-what-you-can-do-about-it/8454, itworldca.

43. Law, T.K., J.C. Lui, and D.K. Yau, *You can run, but you can't hide: an effective statistical methodology to trace back DDoS attackers.* IEEE Transactions on Parallel and Distributed Systems, 2005. **16**(9): p. 799-813.
44. Savage, S., et al., *Network support for IP traceback.* IEEE/ACM transactions on networking, 2001. **9**(3): p. 226-237.
45. Kamboj, P., et al. *Detection techniques of DDoS attacks: A survey*. in *International Conference on Electrical, Computer and Electronics (UPCON), 2017 4th IEEE Uttar Pradesh Section* 2017. IEEE.
46. Yu, S., et al., *Can we beat DDoS attacks in clouds?* IEEE Transactions on Parallel and Distributed Systems, 2014. **25**(9): p. 2245-2254.
47. Patcha, A. and J.-M. Park, *An overview of anomaly detection techniques: Existing solutions and latest technological trends.* Computer networks, 2007. **51**(12): p. 3448-3470.
48. Pimentel, M.A., et al., *A review of novelty detection.* Signal Processing, 2014. **99**: p. 215-249.
49. Douligeris, C. and A. Mitrokotsa. *DDoS attacks and defense mechanisms: a classification*. in *Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (IEEE Cat. No. 03EX795)*. 2003. IEEE.
50. Sharma, M., *Network intrusion detection system for denial of service attack based on misuse detection.* International Journal of Computational Engineering & Management, 2011. **12**(4): p. 19-23.
51. Sobh, T.S., *Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art.* Computer Standards & Interfaces, 2006. **28**(6): p. 670-694.
52. Abusitta, A., M. Bellaiche, and M. Dagenais, *An SVM-based framework for detecting DoS attacks in virtualized clouds under changing environment.* Journal of Cloud Computing, 2018. **7**(1): p. 9.
53. Modi, K. and A. Quadir, *Detection and Prevention of DDoS Attacks on the Cloud using Double-TCP Mechanism and HMM-based Architecture.* International Journal of Cloud Computing and Services Science, 2014. **3**(2): p. 113.
54. *S. Sikkanan, M. Kasthuri, Denial-of-Service and Botnet Analysis, Detection, and Mitigation, in: Forensic Investigations and Risk Management in Mobile and Wireless Communications, IGI Global, 2020, pp. 114-151.*