Asian Journal of Engineering and Applied Technology
ISSN: 2249-068X Vol.10 No.1, 2021, pp.38-44

Attack in SDN Based Distributed Denial of Service

S. Selvakani[1], K.Vasumathi[2], T. Vijayalakshmi[3] and A. Kavitha[4]
[1]Assistant Professor and Head, PG Department of Computer Science
[2]Assistant Professor and Head, Department of Computer Applications
[3&4]PG Scholar, PG Department of Computer Science
[1,2,3&4]Government Arts and Science College, Arakkonam, Tamil Nadu, India
E-mail: sselvakani@hotmail.com, kulirmail@gmail.com, vijayalakshml41020@gmail.com, Kaviyadhava54@gmail.com.

***Abstract* - DOS assaults are executed with the aid of using assault tools, worms and botnets the usage of exclusive packet-transmission techniques and diverse types of assault packets to conquer protection structures. These issues cause protection structures requiring diverse detection techniques to be able to discover assaults. Moreover, DOS assaults can blend their traffics for the duration of flash crowds. By doing this, the complicated protection machine cannot locate the assault site visitors in time. In this challenge a conduct primarily based totally detection the usage of Crowd Correlation Analysis which can discriminate DOS assault site visitors from site visitors generated with the aid of using actual customers. In the Euclidean area to specific as a diagonal matrix proposed can grasp the potential of community machine towards every assault manner and the protection functionality of community machine. Cyber-assault consisting of DDOS assault continues to be the maximum effective assault that disrupts the real customers from having access to the crucial offerings. In software layer-primarily based totally DDOS assault, attacker makes use of different gadget in preference to the usage of his very own IP cope with to flood the focused machine and disrupts the offerings SDN (software program described networks) for value performance and community Application layer allotted denial of provider (DDOS) assaults have turn out to be a extreme hazard to the safety of net servers. These assaults avoid maximum intrusion prevention structures with the aid of using sending several HTTP requests flexibility, however DDOS is one of the maximum released assault on SDN layer. DDOS assault on this kind of surroundings results in machine failure DDoS is one of the maximum released assault on SDN layer. DDOS assault on this kind of surroundings results in machine failure monetary loss, facts theft, and overall performance degradation massive survey has been made to locate and save you DDOS primarily based totally assault in software layer and SDN primarily based totally surroundings. We suggest an powerful protection machine, named Sky Shield, which leverages the caricature facts shape to fast locate and mitigate software layer DDOS assaults. Novel calculation of the divergence among sketches, which alleviates the effect of community dynamics and improves the detection accuracy.**
Keywords: **Distributer Denial of Service, SDN, Application Layer**

I. INTRODUCTION

Denial of provider (DOS) assaults has turn out to be a main hazard to modern pc networks. Early DOS assaults have been technical video games performed amongst underground attackers. For example, an attacker would possibly need to get manage of an IRC channel thru appearing DOS assaults towards the channel owner. Attackers may want to get reputation with inside the underground network thru taking down famous net sites. Because easy-to-use DOS tools, consisting of Trinco (Dmitritch 1999), may be effortlessly downloaded from the Internet, ordinary pc customers can turn out to be DOS attackers as well. They someday co-ordinately expressed their perspectives thru launching DOS assaults towards groups whose rules they disagreed with. DOS assaults additionally seemed in unlawful actions. Denial-of-Service assault is a cyber-assault that makes community assets unavailable to the meant customers with the aid of using disrupting the offerings Distributed Denial-of-Service (DDOS) assault is a big scale denial of provider assault wherein attacker makes use of exclusive IP addresses to the flood the sufferer. Series of net related gadgets managed with the aid of using breaching its protection assault site visitors to simulate valid person conduct software program-described community (SDN) surroundings, that is, valid site visitors that appears similar. Information distance metric is used scribe the versions of site visitors conduct of such events. AL DDoS assault and protection software is proposed to calculate the outcomes of AL-DDoS assault. By evaluating the simulation test facts with the associated technical facts the effectiveness, objectivity, and accuracy of the technique software program described networks.

II. DDOS ATTACKS IN APPLICATIONLAYER

Important thing for customers. DDOS assault on net server is developing hastily and has brought on large financial loss for the sufferer. The site visitors created with the aid of using the flash crowd results in boom within side the distribution of supply IP cope with. HTTP primarily based totally assault is a software layer-primarily based totally DDOS assault. In those forms of assaults, attacker employ attributes of HTTP to hook up with the server in order that they live related till the request is completed. With the aid of using sending incomplete HTTP requests. Either incomplete HTTP header might be found in HTTP GET requests or the duration of HTTP headers content material area might be very large as compared to the message frame of HTTP DDOS assault may be created the usage of the BOTNET that compromise big range of bots. Bots are

managed with the aid of using the attacker that has neither firewall nor antivirus and are used for net relay chat (IRC).

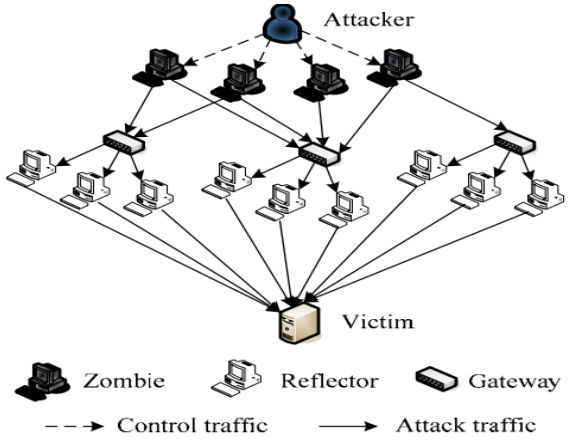

Fig.1 Overview of Denial of Service attack

A. Types of Attacks

1. UDP flood attack
2. SYN flood attack
3. SNMP Reflection attack
4. Single web page attack
5. Main Page Attack
6. Dominant web page attack

III. LITERATURE SURVEY

Various studies have taken place to design systems to defend DDoS attacks. Major concerns of a DDoS attack defense system are: i) System should mitigate the attacks as soon as possible. ii) Quality of Experience (QOE) of user. iii) System should not impose much overhead to legitimate users. iv)DDOS attacks involve huge volume of traffic that these demand an efficient data structure to process the traffic. Filter-based approaches using deployed filters [2], [3] are used to block unwanted traffic. A frame work called Kill-bots [4] which provides authentication using graphical passwords is an approach to capture Denial of Service attacks mounted by professionals using botnets Admission control is provided as a function of total load to ensure the consistent service of server

Stand-alone system for detecting network intruders in real-time by passively monitoring a network link over which the intruder's traffic transits. We give an overview of the system's design, which emphasizes high-speed (FDDI-rate) monitoring, real-time notification, clear separation between mechanism and policy, and extensibility. To achieve these ends, Bro is divided into an “event engine” that reduces a kernel filtered network traffic stream into a series of higher level events, and a “policy script interpreter” that interprets event handlers written in a specialized language used to express a site's security policy[1]. Event handlers can update state information, synthesize new events, record information to disk, and generate real-time notifications via syslog. And discuss a number of attacks that attempt to subvert passive monitoring systems and defenses against these, and give particulars of how Bro analyzes the four applications integrated into it so far: Finger, FTP, Port mapper and Telnet. The system is publicly available in source code form.

Intrusion detection which classifies the attacks on the Internet from usual behavior of usage on the Internet [5]. Here intrusion detection systems are vital tool in the cluster environment fight to keep its computing resources secure .It is an unavoidable portion of the information security system. Emerging variety of network behaviors and the rapid development of attack scenarios, it is vital to develop fast machine-learning-based intrusion detection algorithms with high detection rates and low false positive and false negative -alarm rates with the help of association rule mining. In this course of work a fuzzy class-association rule mining method based on genetic network programming (GNP) for intrusion detection. GNP is an evolutionary optimization technique, which uses directed graph structures leads for enhancing the representation ability .In combination with fuzzy set theory and GNP, the proposed work can deal with mixed database that contains both discrete and continuous attributes and also extract many important class association rule.

With the tremendous growth of network-based services and users of the Internet, it is important to keep the data and transactions in the Internet more secure. Intrusion detection system has emerged as an essential component and an important technique for network security. In this article, an Ad boost algorithm for network intrusion detection system with combination of multiple weak classifiers is proposed. The classifiers such as Bayes Net, Nave Bayes and Decision Tree are used as weak classifiers. A benchmark dataset is used in these experiments to demonstrate that boosting algorithm can greatly improve the classification accuracy of weak classification algorithms [6]. Our approach achieves higher detection rate with low false alarm rates and is scalable for large datasets, resulting in an effective intrusion detection system.

Flooding attacks detection in traffic of backbone networks requires generally the analysis of a huge amount of data with high accuracy F and low complexity. In this paper [7], we propose a new scheme to detect flooding attacks in high speed networks. The proposed mechanism is based on the application of Power Divergence measures over Sketch data structure. Sketch is used for random aggregation of traffic, and Power Divergence is applied to detect deviations between current and established probability distributions of network traffic.

We focus on tuning the parameter of Power Divergence to optimize the performance. We evaluate our approach using real Internet traffic traces, obtained from MAWI Trans Pacific wide transit link between USA and Japan. Our results show that the proposed approach outperforms

existing solutions in terms of detection accuracy and false alarm ratio.

This is the age of modern computing, internet is the basic need and the backbone for distributed application software defined networks, internet of things and many more technologies. As internet usage increases the crime rate also increases [2]. These crime causes serious economic damage by flooding internet traffic to a network and stops the essential services. DDoS attacks are threats to the networks. The DDoS attack process has 4 roles: Attacker, Master, Zombies and Victim. The attacker leads the operation remotely by delivering the commands. The master receives the command from the attacker and manages the zombies. Zombies perform the operations that are commanded by the master and attack the victims. Victims are the targeted system simultaneously attacked by several hosts [3].The survey report produced by Kaspersky illustrated that the DDoS attack source which has emerged from 86 nations lasted for 329 hours. The DDoS attack size has increased by 73% and increment in HTTP based application layer attacks, from 8.4% to 9.4%. The WISR published in Q1 in 2017 says application layer is the most targeted, where in 80% on HTTP attack and 81% on DNS. Recently, DDoS attack on web servers and web applications has increased. The attackers are targeting the application layer. Application layer DDoS attack will disrupt the services rather than exhausting network resources. These attacks require less network connections for attacking and are difficult to detect because the traffic look like normal benign traffic [10].

With the rapid development of network technology, the field of network security is facing hacker attacks. Intensity of attacks is gradually increasing, and illegal attackers achieve improper goals. DDoS attacks are the main means. ALDDoS attacks are different from traditional network layer DDoS attacks. It mainly uses existing protocol loopholes, such as HTTP and SMTP, and consumes existing network resources, so that the target server cannot provide conventional services. Intensity and accuracy of this attack are higher, and the threat to security is also greater. Number of attackers and the required attack traffic are much lower than traditional AL-DDoS attacks, which also mean that AL-DDoS attacks are easier to launch, and attackers can accurately attack specific applications, so the attack threat is great measurement of network system security by most of today's methods cannot reach the stage of quantitative calculation. Most security measurement methods rely on a certain technology while relying on the human experience of experts to measure whether it is safe.

Methods are not accurate and objective enough, so people are always looking for a method that can quantitatively, dynamically, and objectively measure network security. Although the network is static, it is always changing. In order to measure attacks more accurately, a network security measurement method that can dynamically describe and warn attacks is needed. Boyer *et al.,* [1] propose a network security evaluation framework based on D-S evidence theory, but this method has some problems such as large calculation. Ramaki *et al.,* [2] propose a network security risk assessment method based on Bayesian network. Although this method has a strong capacity to process a large amount of data, it is inevitably affected by some subjective factors, so the method must be properly trained to obtain relevant parameter.

This paper presents a new distributed approach to detecting DDoS (distributed denial of services) flooding attacks at the traffic flow level. The new defense system is suitable for efficient implementation over the core networks operated by Internet service providers (ISP). At the early stage of a DDoS attack, some traffic fluctuations are detectable at Internet routers or at gateways of edge networks. We develop a distributed change-point detection (DCD) architecture using change aggregation trees (CAT). The idea is to detect abrupt traffic changes across multiple network domains at the earliest time. Early detection of DDoS attacks minimizes the flooding damages to the victim systems serviced by the provider. The system is built over attack-transit routers, which work together cooperatively. Each ISP domain has a CAT server to aggregate the flooding alerts reported by the routers. CAT domain servers collaborate among themselves to make the final decision. To resolve policy conflicts at different ISP domains, a new secure infrastructure protocol (SIP) is developed to establish the mutual trust or consensus.

DDoS attacks at the network layer [1]–[8]. Recently, application layer DDoS (app-layer DDoS) attacks against web servers grow rapidly and bring victims with great revenue losses [9]–[10]. App-layer DDoS attacks attempt to disrupt legitimate access to application services by masquerading flash crowds with numerous benign requests. Flash crowd refers to the situation when many users simultaneously access a popular website, producing a surge in traffic to the website and causing the site to be virtually unreachable [10]. The stealthiest of app-layer DDoS attacks makes most signature-based intrusion prevention systems ineffective. Since most DDoS attacks are launched abruptly and severely, it is desirable to design a defense system that can detect and mitigate app-layer DDoS attacks as soon as possible to minimize the losses [4]. Turing test schemes based on graphical puzzles have been proposed to address the above problem on the cost of additional delays [5], [6]. Unfortunately, since a few milliseconds extra delay may cause users to abandon a web page early [7], [8], applying such mechanism to all users will negatively affect the Quality of Experience (QoE). Therefore, an effective defense system should mitigate app-layer DDoS attacks as soon as possible while posing a limited impact on the access of normal users.

Distributed Denial-of-Service (DDoS) is a prominent issue in Network Security and it is extremely horrible threats for datacenters, made the system unable to serve for two days [8]. In 2000, many media and famous companies were

attacked, such as eBay, CNN, Yahoo and Amazon [7]. Usually, the DDoS attacker attacks such big companies are to make them suffer from financial losses. The losses may range to millions when they are unavailable for a few seconds [3]. In 2010, DDoS attack has done to shut down websites such as Visa, MasterCard, Post Finance, and PayPal. Many Industries and organizations have experienced the similar kind of peril tactics. DDoS dissatisfies on these companies for banning the donations to WikiLeaks [1]. Moreover, there is also evidence of politically driven attack such as the most famous attack on White House Website in 2002 [6]. Also, many governmental websites are shut down during the Gezi Park revolt in Turkey [7]. There are two ways to prevent the DDoS attack, namely, machine learning and Bloom Filter. This survey focuses on Bloom Filter to prevent DDoS attack. Ripon Patgiri, patterns and to identify legal and illegal requests. But, Bloom Filter is unintelligent, hence, it cannot identify patterns and unable to differentiate legal and illegal accesses. Surprisingly, Bloom Filter is used to prevent DDoS attack. Unlike machine learning algorithm, Bloom Filter is very simple data structure that consume a tiny amount of memory. The Bloom Filter (BF) [5] is a probabilistic data structure to check the presence of an element in a set [3]. It is a data structure mostly used for membership filtering. Bloom Filter either returns true or false. The true result of Bloom Filter is classified into two different classes, namely, true positive and false positive. Similarly, the negative class is also classified into two different classes, particularly, false negative and true negatives. The false positive and false negative is the overhead of the filter. AS per our study, all Bloom Filter contains false positive. However, there are a few variants of Bloom Filters contain false negative.

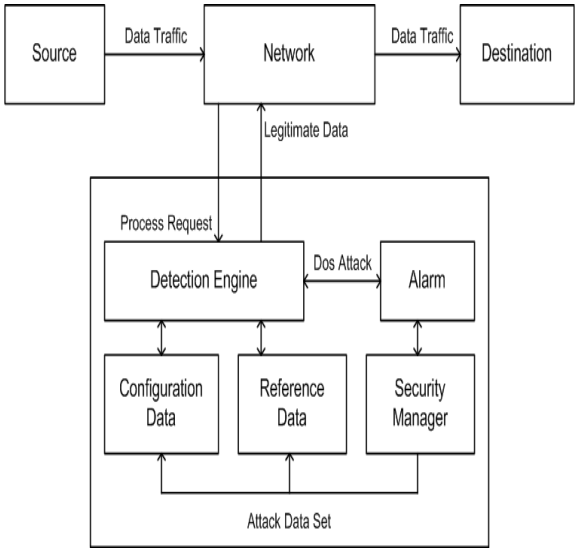

Fig. 2 Architecture Diagram

IV. PROBLEM DEFINITION

Companies would possibly use DOS assaults to knock off their competition within side the market. Extortion thru DOS assaults have been on upward push within side the beyond years (Pappalardo *et al.*, 2005). Attackers threatened on line groups with DOS assaults and asked bills for protection. Known DOS assaults within side the Internet typically triumph over the goal with the aid of using arduous its assets that may be whatever associated with community computing and provider overall performance, consisting of hyperlink bandwidth, TCP connection buffers, software/provider buffer, CPU cycles, etc. Individual attackers also can make the most vulnerability, wreck into goal servers, after which carry down offerings. Because it's miles hard for attackers to overload the goals aid from a unmarried pc, many latest DOS assaults have been released thru a big range of allotted attacking hosts within side the Internet. These assaults are referred to as allotted denial of provider (DDoS) assaults. In a DDoS assault, due to the fact the aggregation of the attacking site visitors may be awesome as compared to the sufferer's aid, the assault can pressure the sufferer to noticeably downgrade its provider overall performance or maybe forestall handing over any offerings.

Attack effect change the network system status

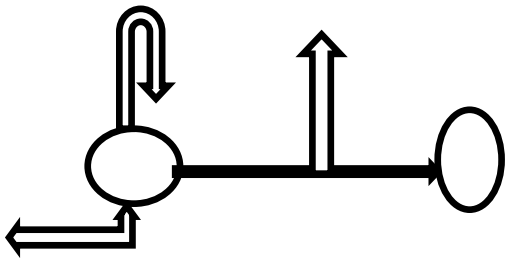

Fig. 3 Attack Effect

V. EXISTING SYSTEM

Generally, it is classified into two main categories: use-based detection systems and anomaly-based detection system. The Sky Shield systems detect attacks by monitoring network activities and looking for matches with the existing attack signatures. The main disadvantage is the large amount of alerts produced.

VI. PROPOSED SYSTEM

In this challenge, a DoS assault detection machine that makes use of Traffic Crowd Analysis (TCA) for correct community site visitors characterization with the aid of using extracting the geometrical correlations among community site visitors capabilities. Our TCA-primarily based totally DoS assault detection machine employs the precept of anomaly-primarily based totally detection in assault reputation. The DoS assault detection machine offered on this paper employs the standards of TCA and anomaly-primarily based totally detection. They equip the detection machine with skills of correct characterization for site visitor’s behaviors and detection of regarded and unknown assaults respectively.

A triangle vicinity approach is evolved to decorate and to hurry up the manner of TCA. A statistical normalization approach is used to put off the unfairness from the uncooked facts. DDoS protection mechanisms deployed on the supply community can forestall assault flows earlier than they input the Internet center and earlier than they mixture with different assault flows. Being near the sources, they could facilitate simpler hint again and research of the assault. Examples of those mechanisms are proposed.

A supply community mechanism has the equal downside because the intermediate community mechanism of detecting the incidence on an assault, because it does now no longer enjoy any difficulties. This downside may be balanced with the aid of using its cappotential to sacrifice a number of its assets and overall performance for higher DDoS detection. However, any such machine would possibly limit valid site visitors from a community within side the case of unreliable assault detection powerful verbal exchange and cooperation among researchers may be completed in order that extra weaknesses of the DDoS area may be identified.

These classifications want to be constantly up to date and improved as new threats and protection mechanisms are discovered. Their fee in accomplishing similarly studies and dialogue is surely big. A subsequent step on this course could be to create units of facts and an experimental test bed so that everyone those diverse mechanisms may be as compared and evaluated. DDoS assaults aren't most effective a critical hazard for stressed out networks however additionally for Wi-Fi infrastructures. Some development has been made to be able to shield Wi-Fi networks towards DDoS assaults.

Propose a conceptual version for protecting towards DDoS assaults at the Wi-Fi Internet, which includes each cooperative technological answers and financial incentive mechanisms constructed on utilization-primarily based totally fees. Further paintings is all even though wished that mixes widely recognized protection drawbacks of Wi-Fi protocols with protection strategies which are already mature in a DDOS assault.

A. Advantages of Proposed System

1. More detection accuracy
2. Less false alarm
3. Accurate characterization for traffic behaviors and detection of known and unknown attacks respectively.

VII. EXPERIMENTAL RESULT

In this paper, we first describe the collection of datasets and then report the extensive evaluation results of DDoS Attack using the real datasets in the SDN Based Distributed Denial of Service Attack Node Formation

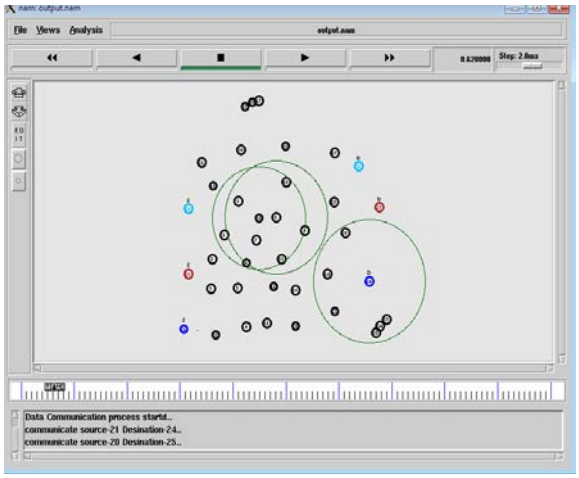

Fig. 4 Node Formation

This screen four Destinations and two sources and sixty eight nodes one node to another node data transmission. Network based on Data communication process start communicate source 21 Destination 24 and communicate source 20 Destination 25 in the node formation.

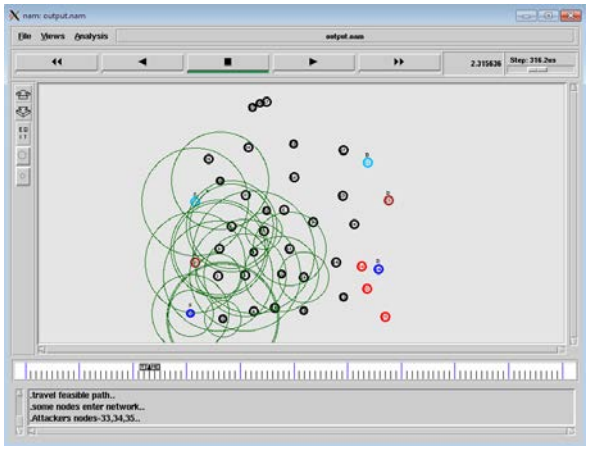

Fig. 5 Node Communication

In the paper one node to another node communicate to the Node Communication. It is data transmission of the Distributed Denial of Service.

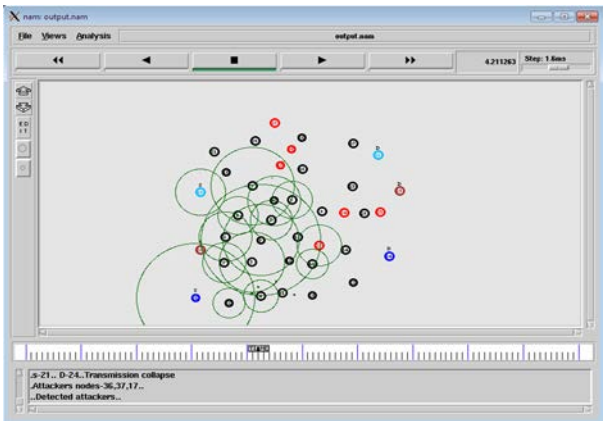

Fig. 6 Network Attack

Many resent Dos attack also called DDos attacks were distributed attacking hosts. A DDos attack is launched in two phases. First an attacker builds an attack network which is distributed and consists of thousands of compromised computers. Then attacking hosts flood tremendous volume of traffic towards victims either under the command of the attacker or automatically.

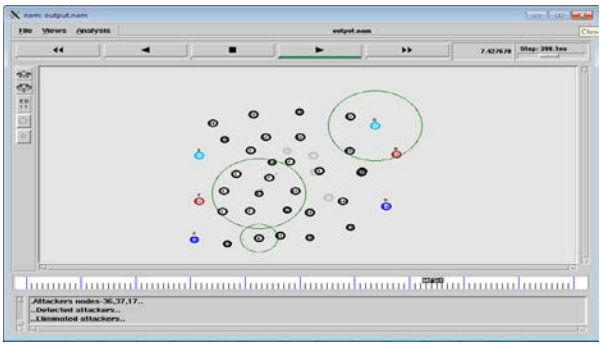

Fig. 7 Attack Detection

DDoS attacks mainly take advantage of the Internet architecture and this is that makes them even more powerful. The Internet was designed with functionality, not security, in mind. Its design opens several security issues that can be exploited by attackers. More analytically

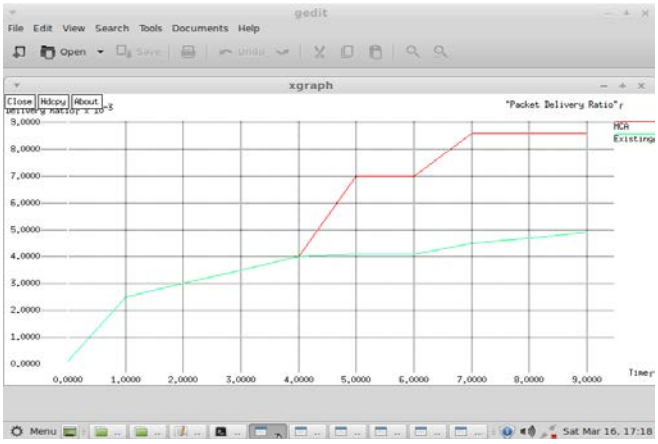

Fig. 8 Throughput Ratio

The analyzing the attack and defence measures used in experiment we can obtain the attack utility value caused. To the application layer of the current network under different attack

IX. FUTURE ENHANCEMENTS

In future, there are numerous techniques used to hit upon and mitigate the impact of DDOS assault. Different techniques have distinct boundaries like criminal customers ought to wait greater time for service, excessive fake positives, and excessive fake negatives, greater time ingesting and complex, require greater reminiscence utilization etc. Mild weight mechanism to server is suggested. The proposed answer is being divided into 3 phase.

1. Identify DDOS assault.
2. Differentiate DDOS assault visitors from everyday visitors.
3. Mitigate the effect of DDOS attack.

X. CONCLUSION

This task has offered a TCA-primarily based totally DoS assault detection gadget that's powered with the aid of using the triangle-place primarily based totally CCA method and the anomaly-primarily based totally detection method. The former method extracts the geometrical correlations hidden in man or woman pairs of awesome functions inside every community site visitor's record, and gives extra correct characterization for community site visitor's behaviors. The latter method allows our gadget in order to distinguish each regarded and unknown DoS assaults from valid community site visitors. In this paper, to begin with we talk approximately the DDoS assault and its effects. Then we've explored the well-known DDoS assaults that has taken region until date. At this factor we numerous kinds and techniques utilized by the attacker to create utility layer and SDN primarily based totally DDoS assault. In addition, we make an intensive survey on DDoS detection the use of numerous techniques in utility layer and software program described networking environment. In this project all of the algorithms were summarized in a table with parameters used to hit upon, DDoS detection degree and overall performance metrics utilized by the ones algorithms. At last, we inspect the actual time troubles created with the aid of using attacker and attempt to save you the ones troubles with proposed structure. The proposed structure will keep away from waft desk overloading technique with the aid of using waft desk sharing approach in SDN. In utility layer, we hit upon the packet is proper or not. If it's far malicious and from attacker, then we are able to terminate the ones packets. These tactics will assist us to face up to the assaults.

REFERENCES

[1] Sini Thankachan, Bibin Varghese Smita, and C. Thomas, "BOTFILTER - An Approach to Defend Application Layer Distributed Denial of Service Attacks," *IJSRD - International Journal for Scientific Research and Development*, No.9, Vol. 6, pp.220-223.

[2] V. Paxson, "Bro: A System for Detecting Network Intruders in Real-Time," *Computer Networks*, Vol. 31, No.23-24, pp. 2435-2463, 14 Dec. 1999.

[3] Harinee, K. Veeramuthu, J. and Han, M. Kamber, "Data Mining Concepts And Techniques," (2nd Edition) Morgan Kaufmann Publishers, 2006,2014.

[4] P. Natesan, P. Balasubramanie, and G. Gowrison, "Improving the Attack Detection Rate in Network Intrusion Detection using Adaboost Algorithm," *Journal of Computer Science*, Vol. 8, No. 7, pp.1041-1048,2021. https://doi.org/10.3844/jcssp.2012.1041.1048

[5] Ali Makke, Osman Salem, Mohamad Assaad, Hassine Moungla, and Ahmed Mehaoua, "Flooding Attacks Detection in Backbone Traffic Using Power Divergence," 2012. ffhal- 0081298.

[6] A.S. Sharan, Dr. K.R. Radhika, "A Survey of DDoS Attacks in Application Layer and SDN Based Environments," *IJCSN Journal*, Vol. 9, No. 2, pp. 51-60, April 2020.

[7] Xiaolin Zhao , Hui Peng ,Xiang Li , Yue Li, Jingfeng Xue , Yaoyuan Liang, and Mingzhe Pei, "Defending Application Layer DDoS Attacks via Multidimensional Parallelotope - Volume 2020 Communication Security in Social net-Oriented Cyber Space's," Special Issue | Article ID 6679304 | DOI: https://doi.org/10.1155/2020/6679304

[8] Yu Chen, Kai Hwang and Wei-Shinn Ku, "Collaborative Detection of DDoS Attacks over Multiple Network Domains," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 18, No. 12, pp. 1649-1662, 2007.

[9] Chenxu Wang, Tony T. N. Miu, Xiapu Luo, and Jinhe Wang, "SkyShield: A Sketch-Based Defense SystemAgainst Application Layer DDoS Attacks," *IEEE Transactions on Information Forensics and Security*, Vol. 13, No. 3, 2018, pp. 559-571.

[10] Ripon Patgiri1, Sabuzima Nayak1, and Samir Kumar Borgohain, "Preventing DDoS using Bloom Filter," *EAI Endorsed Transactions on Scalable Information Systems*, Vol. 5, No. 19 , June 2018.