Current State Of Art And Key Rationales Of Application Layer Distributed Denial Of Service Attacks In Software Defined Networking

Sarabjeet Kaur, Amanpreet Kaur, Abhinav Bhandari

Abstract: Software Defined Networking (SDN) provides the provision of centralized and faster network. It provides the greater control on network traffic by separating the control plane and data plane which is a new network paradigm shift from the traditional network. Although SDN has replaced the traditional networks with its fast and flexible features, yet there are some of the areas where research is being emphasized like reliability, scalability, latency and security. Due to the centralized service based architecture of SDN there occurs various security issues at its different layers like control layer, data layer and application Layer. These issues are unauthorized access to controller, forwarding policy violation or modification, system level security issues, unauthorized access to applications and denial of service etc. Out of these, the DDoS (Distributed Denial Of Service) attack is the most leading issue at present. DDoS attack is interruption in normal traffic flow thereby making the services unavailable to legitimate users by consuming victim’s resources. DDoS attack although has an impact on different layers, yet the application layer DDoS attack has become the most distinguished area of discussion for various researchers. So, in this paper, we have covered the most prominent area of security in SDN i.e. DDoS attack. We are going to present a review of the current state of art on an application layer DDoS attack in SDN. Our study identifies and discusses the different defense approaches, its implementations, an idea behind work done and an outcome of recent related works which is helpful in handling the application layer DDoS attack in the SDN. It gives the clear view to the researchers about the recent updates in defense mechanism of an application layer DDoS attack in the SDN. Also the mapping study highlights the limitations of each research which leads to the research findings and gaps out of present research being done yet. The future scope of this research study is to develop a new mitigation framework after analyzing the research gaps highlighted in research article.

Keywords: Software Defined Networking, Denial of Service, Application layer, Defense Mechanism, Internet of Things.

1 INTRODUCTION

The present state of network measurement and its criticality is inadequate. If we discuss briefly about network behavior and generally its operability, it requires high level of manual involvement. This practice indeed becomes difficult in case of large and complex networks. The traditional network faces many of such problems which are overcome SDN (Software Defined Networking) which is emerging technology in trend [5]. It is the new paradigm that solves the issues of traditional networks by centralizing the control and separating it from data plane. It controls the behavior of network equipment through dynamic software approach. SDN is now considered as vital solution to the complexities of traditional networks as the decision path in SDN is handled by its controller and the forwarding part by the switches. This approach of SDN is considered as its biggest strength. Though the SDN has been adopted in wide spectrum, yet it lacks in some features like reliability, latency, scalability and security. The researchers are working on these issues to increase the performance of SDN. But still the limited work has been done on its security issues.

There are several security threats which either may harm the controller or switches of SDN network. These security threats may distress at application layer, control layer and data layer of SDN architecture. There are number of security issues which harm one, two or all of the layers in network. Some of the security threats are like some unauthorized access, configuration issues, denial of service attacks etc. Due to centralized controller at control plane of SDN, it is much targeted by denial of service attacks [9][28]. These attacks block the network equipment as the attackers send multiple requests to controller or switches thereby making it unavailable [11][26][29]. It finds out the opening for an intrusion to process the attack on server [25]. DDoS attacks become more substantial when generated from multiple resources initiating the distributed denial of service (DDoS) attack [19][20][23]. The DDoS attack is carried out at different layers of network such as transport layer, network layer as well as an application layer which makes the respective protocols inactive [18]. There are different protocols which get affected as per different layer DDoS attacks such as ICMP (Internet Control Message Protocol) in network layer, TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) in transport layer, DNS (Domain Name Service) and HTTP protocols in an application layer. DDoS attack makes the server unavailable for legitimate users [12]. DDoS attacks are becoming more dangerous as per reports of Arbor, McAfee Labs and Kaspersky Labs. The NETSCOUT’s annual Worldwide Infrastructure Security Report (WISR) states there is three times increase in SaaS services attacks from 2017 which was 13% to 2018 which was 41% [37]. The highest record of attack is 1.7 TBPS in size per as per WISR Arbor’s report 2018. McAfee Lab report says that DDoS are the third largest attacks which tend to grow year by year. As per prediction reports of McAfee Labs the attacks will increase on homely devices connected with Internet of Things for

• Sarabjeet Kaur is currently pursuing Ph.D in Computer Applications at Chandigarh University, Gharuan, India, E-mail: mca.sarabjeet@gmail.com
• Dr. Amanpreet Kaur is currently working as Associate Prof. at Chandigarh University, Gharuan, India, E-mail: amansagal.ynr@gmail.com
• Dr. Abhinav Bhandari is currently working as Assistant Prof. at Punjabi University, Patiala, India, E-mail: bhandarinit@gmail.com

IJSTR©2020
monetary gains in 2019 [35]. Likewise the Kaspersky Lab’s report 2018 says that for the enterprises the cost of handling DDoS attacks is rising gradually worldwide [36]. It recorded this cost upto $2M per attack as an average in 2018. So, all these recent records clearly show the criticality of DDoS attacks increasing day by day globally. In this paper, we have reviewed the research work related to an application layer DDoS attacks in SDN. This paper covers the various features, rationales, tools or simulators used and outcome of different research contributions to detection and defense of an application layer DDoS attacks. Also the mapping study highlights the limitations of each research which leads to the research findings and gaps out of present research being done yet. The future scope of this research study is to develop a new mitigation framework after analyzing the research gaps highlighted in research article.

The main contributions of this research paper are:-

- To list various security issues of SDN architectures.
- To study the modus operandi of application layer DDoS attacks in SDN.
- To study the current state of art of detection and rationales of application layer DDoS attacks in SDN.

The remainder of this paper covers the study as follows: Section 2 discusses the security challenges in SDN. Section 3 describes the modus operandi of an application layer DDoS attack in SDN and related research in detail. Section 4 presents the current state of art of detection and rationales of application layer DDoS attacks in SDN. Finally, Section 5 concludes the review.

1. SECURITY CHALLENGES IN SDN

In SDN the traffic is forwarded by the networking elements like switches as per the entries of forwarding tables which is controlled by the centralized controller. There are two different approaches to accomplish the operation i.e. proactive and reactive [4] [21]. In proactive the forwarding rules are set by the controller and only those packets are forwarded whose entry matches into the table [17]. Whereas in reactive approach, the decision is taken by the controller by considering overall view or state of network. Generally, the focus of researchers is to detect the threats on centralized controller of SDN to prevent the failure. The least focused area of research is SDN security. Our study is mainly concentrated on security features of SDN. There are many security issues according to the research study which can be categorized [15] [16]. The table below shows different security features of SDN which may trigger all of the layers by unauthorized access to either controller or to any application of networks. Some of the attacks may access and modify the data by leakage of flow rules or forwarding tables and policies. Another threat is some malicious attack on an application and controller which makes them unavailable [13]. The DOS attack from among other attacks may affect network layers and elements [1]. If we list out, the Denial of Service attack may affect:

- Switch Buffer
- Flow Table
- State Table
- Data Flows or Processes

The most prominent attack is DDoS attack in SDN [14]. There are some positive and negative features as well as weak areas of SDN which makes it either DDoS resolver or Victim [1]. The centralized controller is one of the features that make SDN a DDoS resolver. As it is a software approach, it can easily program the network decisions and updates the network dynamically by separating the logic from infrastructure. In comparison these features also make SDN a DDoS victim due to failure of SDN controller, the slow processing of controller as compare to routers and switches and dumb switches etc. In next section we have covered the impacts of an application layer DDoS attacks in SDN which is main focus of our study in this paper.

![Figure 1: The protocols affected by DDoS attacks at different layers](image)
Table 1: Security Issues in SDN

<table>
<thead>
<tr>
<th>Security Issues</th>
<th>Application Layer</th>
<th>Control Layer</th>
<th>Data Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized Access to controller</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Unauthorized/Unauthenticated Access to an application</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Input Buffer Attack</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Forwarding Policy Violation</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Flow Rule Modification</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Malicious and Compromised Applications</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denial of Service Attack</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Configuration Issues</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>System Level SDN Security</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

2. MODUS OPERANDI OF APPLICATION LAYER DDoS ATTACKS IN SDN

We have discussed in our previous section about criticality of security threats in SDN. The DDoS attack amongst the security threats is most noticeable attack [22]. The distributed denial of service attack exerts the influence on an application layer protocols such as DNS and HTTP, which is of much concern. There are many relevant researches available on an application layer DDoS attack. The study of few has been presented in this paper. As an application layer uses genuine HTTP protocol, the attacker tries to exploit the features of protocol by sending the huge traffic. It is sometimes quite difficult to differentiate between the attacker and legitimate user. As per the study there are many algorithms [3] being available to detect an application layer DDoS attack. It classifies the DDoS attacks into two categories as: at an application level and infrastructure level. To clearly visualize the process of HTTP DDoS attacks in SDN Figure 2 below can be explained. It begins with first type of attack where the attacker sends the HTTP request and the server is connected to it after receiving the request. Attacker keeps on establishing the connection keeping the server busy. Due to this, the server becomes unable to connect any other request [27]. This is Slowloris attack on an application layer [2]. On the other hand if attacker sends the huge number of HTTP requests which makes the server overloaded and unable to handle those requests. This makes the server unavailable and known as HTTP flood attack an application Layer. The major reason of DDoS attack is lack of trusted API's which can be resolved by frequent software updates and securing the components [1].
3. CURRENT STATE OF ART OF DETECTION AND KEY RATIONALES OF APPLICATION LAYER DDoS ATTACKS IN SDN

There are many researches done in past few years on SDN DDoS attack detection and defense. In this paper we have reviewed few related research papers particularly on an application layer DDoS attack in SDN. Although in previous researches, the main focus is shown on volumetric attacks in network and transport layers, yet an application layer has not attained much attention from researchers. The papers in our study are taken from past two year's research work being done by different researches in application layer DDoS attacks in SDN network. The table 2 below shows some of the research features given as per respective papers from past research. The parameters we have focused are like the basics about paper as title, authors, number of citations etc. Apart from this the specific analysis has been done regarding the detection techniques being used in these papers by researchers which are capable of detecting and implementing defense against DDoS attacks. Further study includes the impacts of attacks on SDN network, also the simulators and emulators used to implement work. The rationale of papers in table gives the idea about the aim of work done in these papers and the conclusion highlights the outcome and results achieved in each paper. As per the study of work done by K.Hong and Y.Kim in paper [2], the slow attack done by the attacker sends the incomplete requests to block the server. It uses the NS3 simulator to implement the detection algorithm SHDA being proposed in paper. It detects and mitigates the slowloris and HTTP POST attacks. The outcome in conclusion shows how successfully SHDA has been implemented through timeout detection and updating the flow rules. Another study shows the implementation of EPA-HTTP DDoS, CAIDA 2007 and MLP-GA algorithms are used to solve the problem where it is unable to identify the attacker and genuine or legitimate user of network [3]. Khundrakpam, Johnson Singh and Tanmay De used the features and structure rules of attacks to analyze the behavior of attackers and legitimate users. Next in other research proposed by Ariff Aizuddin, Ahmad & Megat Mohamed the DNS amplification attack has been covered. DNS is one of an application layer DDoS attack domain which has been discussed in this paper [6]. Authors used sFlow with Security Centric SDN detection technique to implement the defense of DDoS attack. The attack affects the DNS server by exploiting the distribution of amplified responses. Authors have used the MININET emulator to conduct the series of test bed experiments which is actual implementation of flexible flow monitoring an application. The paper concluded the proposed research idea showing the increased performance of sFlow based security centric SDN and minimizing the cache overload. Y.Lin, J.Kuo, D.Yang and W.chen proposed an algorithm in their research paper [7] to manage the effectiveness and cost of shuffling the traffic in SDN. They used virtual machine implementation through MININET for Multi Objective Markov Decision process. The other algorithms are also implemented in paper like SDSS, BSA and CSA. These algorithms reduced the frequent shuffling of traffic and

![Figure 2: HTTP DDoS attack process.](image-url)
deployed the defense against HTTP DDoS attacks in SDN and NVF. Another contribution was done by Grigoryan, Garegin & Liu Yaoqing in 2018 in application layer DDoS attack. This paper used LAMP technique to mitigate application layer with programmable data planes. It prevented the server to get exhausted by huge number of GET and POST requests sent by the attacker. The bm2v emulator model has been implemented in MININET for P4 programming language. It provided the solution to directly handle the alerts of attack by new architecture LAMP which is quicker to detect and mitigate the attacks. There are many other researches that are not exactly related to application layer DDoS attack in SDN. But these could be studied as base to understand the concept of DDoS attacks. We have also included one contribution given by Gera, J. & Battula in 2018 which throws the light on this. Many researches actually differentiate the DDoS attacks from flash crowds [31]. This paper used NS2 simulator to use source address entropy and traffic cluster entropy values to detect and differentiate the flash events. In another research done by Kim, S., Lee, S., Cho, G., Ahmed, M. E., Jeong, J., & Kim, H in 2017 the other domain of application layer DDoS attack is discussed. This paper covered the defense against DNS Amplification attacks using the novel scheme [30]. The concept behind was to store the history of DNS queries as an evidence to distinguish normal DNS responses from attack packets. The scheme blocked the network traffic for DNS amplification attack completely and provided a highly scalable and centralized data storage for DNS request using SDN. Again the MININET emulator has been used to implement the scheme experimentally in this research. This section also gives the brief view of key rationales behind the study of application layer DDoS attacks in SDN. The ideas represented by different researchers to cover the area of application layer DDoS attacks in SDN are highlighted in Table 2. First paper in table proposed the technique SHDA which receives the HTTP requests on behalf of server to detect the incomplete and suspicious HTTP requests. It uses timeout based DDoS attack detection to track the slow users [2]. Second paper presents the work to detect the behavior of attackers and legitimate users by analyzing the combination of few parameters like count of GET or POST requests, no of IP addresses within small time span, frame length of protocols and constant mapping [3]. The discussion in third paper emphasized on DNS application data. It used the sFlow to collect the flow traffic data and checks the headers of packets [6]. By matching the query ID sFlow identifies the normal DNS requests or suspicious requests [24]. The technique reduces the cache overload by separately storing the request to normal cache or immediate cache. Fourth paper is based on shuffling of application layer DDoS attack effected virtual machine replicas. It focused the concentration of attackers on few virtual machines by repeatedly resetting the attacked VMs [7]. Fifth paper brought the idea of new framework LAMP. It works by scanning the network for application layer ddos attacks and sending the alert messages. LAMP blocks the suspicious IP addresses to prevent the attacks [8]. The research in sixth paper differentiates the DDoS attacks from flash events. It correlates the packets from different locations to check the general structure. If the packet structure rules are violated it is declared as DDoS attack. The study finds out the source and traffic entropy to detect flash events [10]. The seventh paper in table 2 is based upon novel security framework of SDN to detect the application Layer DDoS attacks. It maps the strict differences [30]. All of these research contributions are discussed below in table along with other features like simulators used, impacts of attacks, detection techniques etc. The study in eighth paper emphasizes on the DNS based DDoS attacks. It makes the network strong so as to prevent the attacks by proposing two hypotheses [32]. One of the hypotheses is based on core network with SDN and another is based on core network without SDN. It is basically representation of previous studies that are applicable in deep packet inspection and DNS of IoT. The study of next paper given by Vishal Gupta and Eklaya Sharma provides the solution to DNS amplification attacks with geographically distributes routers known as Barrier of Routers (BOR) [33] to control the inflow and outflow of network traffic. Lastly, tenth paper is about the solution named KarmaNet [34]. This study uses the Novel DNS response packet routing scheme to prevent the DDoS attacks.

Table 2: Review of Research features of related papers

<table>
<thead>
<tr>
<th>Simulator used</th>
<th>NS3 Simulator</th>
<th>SDN emulator (MININET)</th>
<th>SDN emulator (MININET)</th>
<th>Throughput methods using MININET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limitations</td>
<td>ShDA generally runs on controller and may not be part of other DDoS attack defense process</td>
<td>Improvement is required in detection rate and correlation of false positives and false negatives and in accuracy of detection. Also it is required to differentiate layer DDoS attacks from flash events</td>
<td>More work is to be done to analyze the amplified attack responses</td>
<td>The improved algorithms are required to optimize the cost and effectiveness for handling DDoS attacks</td>
</tr>
<tr>
<td>Impact of Attack</td>
<td>It makes the web server unavailable by sending incomplete requests</td>
<td>Unable to identify the attacker and legitimate user</td>
<td>DNS Server exploitation to distribute amplified traffic responses</td>
<td>Frequent shuffling of traffic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Rationale

It proposed the SHDA technique that handles the attack situation when the incomplete HTTP requests are received by the server increasing the number of open connections. SHDA receives the HTTP requests by itself on behalf of web server as per the flow rules updated by the SDN controller. This makes SHDA to detect and manage the incomplete or suspicious HTTP requests. SHDA uses the timeout based DoS attack detection to find out the requests from slow clients.

In this paper, the behavior of attackers and legitimate clients are analyzed on the basis of few parameters such as count of GET or POST requests, no. of IP addresses within small time span, analyzing no. of open and closed port connections by constant mapping and lastly, the frame length of protocol. These parameters are collectively used to propose the experimental result through classification model execution, which differentiates the attackers from legitimate users.

This paper describes the behavior of HTTP DDoS attacks and also proposes the defense model in SDN/NVF. It identifies the attack types like session flooding, request flooding, asymmetric and slow request/response attacks. The work in this paper is based upon shuffling the replicas of VMs if it is under DDoS attack.

<table>
<thead>
<tr>
<th>Impact of Attack</th>
<th>Limitations</th>
<th>Simulator used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exhales the server by sending huge number of POST and GET requests</td>
<td>The centralized controller is additional overhead and increases the complexity. The performance of LAMP may be affected by differences of P4 and SDN implementation in MININET</td>
<td>bm2 emulator model using MININET for P4 programming language</td>
</tr>
<tr>
<td>Degrades the network performance by occurrence of attacks resembling flash events</td>
<td>It does not implement the true performance of proposed system. The high accuracy is required to detect the low flash crowd attacks.</td>
<td>NS-2</td>
</tr>
<tr>
<td>huge volume of DNS name lookup requests to open DNS servers</td>
<td>Still there is communication delay in proposed system and analysis of memory lookup overhead is to be done.</td>
<td>MININET 2.3.0d1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Paper</th>
<th>Author</th>
<th>Year</th>
<th>References</th>
<th>Detection Technique</th>
<th>Rationale</th>
</tr>
</thead>
</table>

Impact of Attack

Exhausts the server by sending huge number of POST and GET requests
Exhales the server by sending huge number of POST and GET requests
Degrades the network performance by occurrence of attacks resembling flash events
huge volume of DNS name lookup requests to open DNS servers

Limitations

The centralized controller is additional overhead and increases the complexity. The performance of LAMP may be affected by differences of P4 and SDN implementation in MININET
It does not implement the true performance of proposed system. The high accuracy is required to detect the low flash crowd attacks.
Still there is communication delay in proposed system and analysis of memory lookup overhead is to be done.
<table>
<thead>
<tr>
<th>Simulator used</th>
<th>Paper</th>
<th>Author</th>
<th>Year</th>
<th>References</th>
<th>Detection Technique</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>MININET</td>
<td>LAMP: prompt application layer attack mitigation with programmable data planes</td>
<td>Grigoryan, Garegin &amp; Liu, Yaoqing</td>
<td>2018</td>
<td>[8]</td>
<td>LAMP: Application layer Mitigation with programmable data planes</td>
<td>In this paper, the application layer DDoS attack mitigation has been demonstrated with LAMP, a new cooperative framework. The attacker sends the attack against application layer, which is not detected by the network devices and the packets reach up to the end hosts. LAMP detects such attacks by scanning the attempts and sending the alert messages. It then blocks the IP addresses from which the attack has been initiated. LAMP uses the parser, match action tables and control flows for implementation.</td>
</tr>
<tr>
<td>MININET</td>
<td>Detection of spoofed and non-spoofed DDoS attacks and discriminating them from flash crowds</td>
<td>Gera, J. &amp; Battula, B.P. EURASIP</td>
<td>2018</td>
<td>[10]</td>
<td>Detection of spoofed, non-spoofed DDoS attacks and discriminating them from Flash crowds</td>
<td>The research in this paper detects and differentiates the DDoS attacks from flash crowds. This is done by correlating the packets at different places to find out the differences. Due to the DDoS attacks the general structure of packets gets violated to form the disorder of traffic flow. This is known as entropy. The work in this paper firstly identifies the source entropy and traffic entropy. When the packets are send continuously to increase the traffic, the source and traffic entropy is found. When the current source entropy is greater than upper threshold source entropy, the flash events are detected.</td>
</tr>
<tr>
<td>MININET</td>
<td>Preventing DNS Amplification Attacks Using the History of DNS Queries with SDN</td>
<td>Kim, S., Lee, S., Cho, G., Ahmed, M. E., Jeong, J., &amp; Kim, H</td>
<td>2017</td>
<td>[30]</td>
<td>Novel security framework using Software-Defined Networking(SDN)</td>
<td>This study uses the Novel security framework to detect the huge volume of DNS name lookup requests to open DNS servers. The work is done to store the history of DNS queries as an evidence to distinguish normal DNS responses from attack packets. It does one to one mapping of DNS requests and responses.</td>
</tr>
<tr>
<td>Paper</td>
<td>Author</td>
<td>Year</td>
<td>References</td>
<td>Detection Technique</td>
<td>Rationale</td>
<td>Impact of Attack</td>
</tr>
<tr>
<td>-------</td>
<td>--------</td>
<td>------</td>
<td>------------</td>
<td>---------------------</td>
<td>-----------</td>
<td>------------------</td>
</tr>
<tr>
<td>Prevention and Mitigation of DNS based DDoS attacks in SDN Environment</td>
<td>Shail Saharan, Vishal Gupta</td>
<td>2019</td>
<td>[32]</td>
<td>Two hypothesis-network with SDN and network without SDN</td>
<td>In this article the network has made strong enough to prevent the DNS based DDoS attacks. It proposed the two hypothesis i.e SDN based network and without network. It is basically representation of previous studies that are applicable in deep packet hypothesis and DNS of Internet of Things.</td>
<td>Disturbs the normal working of user and internet service provider</td>
</tr>
<tr>
<td>Mitigating DNS Amplification Attacks Using a Set of Geographically Distributed SDN Routers</td>
<td>Vishal Gupta, Eklavya Sharma</td>
<td>2018</td>
<td>[33]</td>
<td>(BOR) Barrier of routers</td>
<td>The study provides the solution to DNS amplification attacks with geographically distributed routers known as Barrier of Routers (BOR). These are used to route the traffic inflow and outflow of network. These barriers scan the traffic to detect the DNS based DDoS attacks.</td>
<td>Degrades the network performance by flooding the large number of DNS requests to DNS servers.</td>
</tr>
<tr>
<td>KarmaNet: SDN Solution to DNS-Based Denial-of-Service</td>
<td>Govind Mittal and Vishal Gupta</td>
<td>2019</td>
<td>[34]</td>
<td>Novel DNS response packet routing scheme</td>
<td>This study uses the Novel DNS response packet routing scheme to prevent the DDoS attacks. It intends the DDoS attacks to destruct itself using IP spoofing. This happens if the path of DNS response packet is same as that of request packet.</td>
<td>Disrupt the network services by DDoS attacks</td>
</tr>
</tbody>
</table>
4. CONCLUSION

The purpose of this paper is to find out the different reviews on HTTP DDoS attack in SDN. We have considered few papers which are very close to our study and are quite relevant. Although not much work has been done in this domain, yet we have found the research proposals by different researchers which may better detect and mitigate the attacks. Also we have studied the techniques and key rationales of these papers. The main security issues as discussed like unauthorized access of application, configuration issues, malicious applications and denial of service attacks are highlighted research problems to be worked on in near future. As our research problem and this article we are working on DDoS attacks on application layer of SDN network. In the future, the work on detection and defense of HTTP DDoS attack in SDN could be considered as serious area of research. New detection techniques and methods need to be developed against attacks. Also, from the study we found the most suitable emulator to be used is MININET for better performance and understanding. A new mitigation framework will be developed in future after analyzing the research gaps highlighted in this research article.

5. REFERENCES:


[22]. N. A. S. Lima and M. P. Fernandez, “Towards an Efficient DDoS Detection Scheme for Software-


[27]. Gabriel IM, Valeriu PV. Achieving DDoS resiliency in a software defined network by Intelligent Risk Assessment based on neural networks and danger theory. 5th IEEE International Symposium on Computational Intelligence and Informatics;319–324. (2014)


[37]. https://www.netscout.com/report/