Indonesian Journal of Electrical Engineering and Computer Science
Vol. 19, No. 1, July 2020, pp. 505~512
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v19.i1.pp505-512

Impact analysis of SYN flood DDoS attack on HAProxy and NLB cluster-based web servers

Subhi R. M. Zeebaree[1], Karwan Jacksi[2], Rizgar R. Zebari[3]
[1]Duhok Polytechnic University, Iraq
[2]Computer Science Department, University of Zakho, Iraq
[3]Information Technology Dept. Duhok Polytechnic University, Iraq

Article Info

Article history:

Received Jul 23, 2019
Revised Nov 17, 2019
Accepted Jan 29, 2020

Keywords:

DoS
NLB
SYN flood DDoS
Attack HAProxy
Web server

ABSTRACT

In recent, the high available internet service is the main demand of most people. However, online services occasionally become inaccessible due to various threats and attacks. Synchronization (SYN) flood distributed denial of service (DDoS) is the most used and has a serious effect on public network services. Hence, the outcome of this attack on the commonly utilized cluster-based web servers is systematically illustrated in this paper. Moreover, the performance of Internet Information Service 10.0 (IIS 10.0) on Windows server 2016 and Apache 2 on Linux Ubuntu 16.04 server is evaluated efficiently. The performance measuring process is done on both network load balancing (NLB) and high available proxy (HAProxy) in Windows and Linux environments respectively as methods for web server load balancing. Furthermore, the stability, efficiency, and responsiveness of the web servers are depended on the study evaluation metrics. Additionally, average CPU usage and throughput of both mechanisms are measured in the proposed system. The results show that the IIS 10.0 cluster-based web servers are more responsiveness, efficiency and stable with and without SYN flood DDoS attack. Also, the performance of the IIS 10.0 web server is better than of Apache 2 in terms of the average CPU usage and throughput.

Corresponding Author:

Rizgar R. Zebari,
Duhok Polytecgnic University,
61 Zakho Road, Mazi Qr.
Email: rzgarz11@gmail.com

1. INTRODUCTION

Information and Communication Technology made deep effects on human life. Nowadays, most of the daily life routines can be achieved by using Internet services and more specifically by depending on the World Wide Web (WWW) [1–3]. Also, Internet users are on a continuous increase, where in June 2018 the users of the Internet reached 3.95 billion [4]. The dramatic increase of the global network users over time and their dependency on the WWW has drastically increased the load of the web servers [5, 6]. However, the most attractive and granular web server is the one that responds to client requests in fast [7].

Providing high availability of web services and a more responsiveness system to customers can be achieved by using server load balancing [8]. Furthermore, using server load balancing can get acute advantages such as security, scalability, and availability of web services. A cluster-based web server is the most used and popular type of web server load balancing [9]. On the other hand, the cluster is a set of interconnected stand-alone computers working together as an integrated and a single computing resource. This style is suitable for small, medium and large internet servers. Additionally, the user's requests or traffic load is distributed among multiple servers to reduce latency, increase throughput and to attain maximum performance [10].

A load-balancing cluster-based web server is usually consisting of the load balancer and the webserver farm behind it. The load balancer is responsible for accessing clusters, receive end-user requests and redistributing the requests of clients to a set of servers that are offering services [11]. Furthermore, layer 4 or layer 7 of the open systems interconnection (OSI) Model are used for load balancers to work at. IP addresses and transport ports information is used for decision making on the layer 4 load balancing. While on layer 7 more specific decisions can be used. The cluster resource is accessible to Clients by IP associated with the load balancer network interface known as virtual IP address (VIP). Rather than the real IP address of the interface, the VIP is set additionally [10].

Despite the advantages of the public network, there are some drawbacks or weaknesses, and network security has been the main challenge to the security community [12]. Due to the fact, there is some vulnerability present in transmission control protocol (TCP) layers in which some attacks can be launched on the internet [13]. The most serious and harmful attack is the denial of service (DoS) and its extension distributed denial of service (DDoS). DoS appeared in 1980, while the first report of DDoS appeared in 1995 [14, 15]. Generally performing a DoS attack is simple and can be initiated on a solitary framework [16]. While for initiating DDoS attack many zombies systems are used by the attacker. A larger number of malicious packets is generated and sends on the infected systems to the victim so that accessing its services becomes difficult [17]. Also, the main goal of Dos and DDoS is to overload the web servers by superabundance the resources of the victim by abnormal requests. Hence, fulfilling all client requests becomes out of the targeted system capability [18, 19]. As a result, the customers' requests will fail and webservers resources become inaccessible. Also slowly accessing web servers has a negative impression on customers, as 32% of users give up on accessing slow websites [20]. Therefore, visitors of the hosted web sites on the victim web servers will reduce that has a direct impact on the page ranking. When the number of users who request a web site reduced, the page ranking automatically reduced and become unvisible by the search engines because of low ranking [21].

The purpose of this paper is to determine the most responsiveness, efficiency and stable approach of clustering web servers' methods under the effect of the TCP SYN flood DDoS. Therefore, the performance of the two most used web servers according to the survey from NETCRAFT [22] in October 2018 in the cluster-based structure is systematically analyzed. The HAProxy on Linux Ubuntu 16.04 and NLB on Windows server 2016 are used as techniques of web server load balancing. The performance of the proposed systems indicates that using IIS 10.0 NLB clustering web servers on the Windows server 2016 achieves better results with and without DDoS attack compared to the existing researches.

2. RELATED WORK

Over the most recent years, some researchers analyzed the performance of different web servers. Also, several other researchers evaluated the impact of the DDoS attack on web servers' performance. The summary and review of some of them are presented in this section. In [23], R. Zebari et al. analyzed and evaluated the impact of the Hypertext Transfer Protocol (HTTP) and SYN flood DDoS attacks on the Apache 2 and IIS 10.0 web servers. In their evaluation study, they used the Apache-JMeter tool for generating legitimated users and measuring the performance of the web servers. Moreover, they depended on hping3 and high orbit cannon (HOIC) tools for creating HTTP and SYN flood attacks. The test results demonstrated that the IIS 10.0 web server's presentation was better during the HTTP attack. While the stability and responsiveness of the Apache 2 webserver was more and attained greatly efficiency during an SYN attack.

In [24], T. Bezboruah and A. Bora performed the evaluation performance of Apache web server in a load-balancing cluster-based and none cluster-based architecture in the Linux platform. They used the Mercury Load Runner tool for virtual users creating and measuring the performance of webserver and the evaluation key metrics were average response time and throughput. Their results were shown that the response time of the cluster-based web server was greater than that of none cluster-based and throughput also was less. However, the load-balanced cluster-based had more stability and handled more web service users.

In [25], S. S. Kolahi et al. evaluated the effect of the user datagram protocol (UDP) flood DDoS attack on the performance of a web server on Linux Ubuntu 13. They used Hping3 on Backtrack R3 for generating attack and Webstress server tool used to generate legitimate traffic. Moreover, they depended on round-trip time and CPU usage as the main metrics for performance analysis. Furthermore, they evaluated the performance of the web in NLB with the attack. The results indicated that the round trip time of web server with 10 HTTP requests was only 0.621ms without the attack, 26.469ms with the attack and 26.487ms in NLB with the attack. Also, CPU usage was 0.5% before the attack, 24.90% with attack and 18% in NLB with the attack.

In [26], K. Treseangrat et al. analyzed the performance of the webserver on Linux Ubuntu 13 and Windows server 2012 with and without the UDP flood DDoS attack. They depended on round-trip time and

CPU usage as main metrics for performance evaluation. Furthermore, they analyzed the performance of the web in NLB with the attack. They used Hping3 on Backtrack R3 for generating attack and Webstress server tool used to generate legitimate traffic. The results denoted that the round trip time of the webserver on Ubuntu was 0.621ms without, 26.422ms with attack and 26.487ms in NLB with the attack. Also, the round trip time of the webserver on Windows server 2012 was 0.99ms without the attack, 27.384 with the attack and 28.973ms in NLB with the attack. The CPU usage of the webserver on Windows server 2012 was 1% without, 24% with the attack and 18% in NLB with the attack. While the CPU usage of Linux Ubuntu 13 webserver was 0.7% without the attack, 24.9% with the attack and 18% in NLB with the attack.

In [11], J. M. Cruz de la Cruz, J.E.C. and C.A.R. Goyzueta designed a system to provide high availability in a cluster-based web server in Linux platform, they depended on HAProxy as a load balancer and Domain Name Service (DNS) to handle clients load among cluster nodes. Moreover, they used a round-robin algorithm to distribute HTTP requests for both HAProxy and DNS. The results indicated that the proposed system was simple, easy to use, and could accomplish a high availability of 99.905%.

In [27], R. Papadie and I. Apostol evaluated the effect of different DDoS attacks such as Slowrise and HTTP flood on IIS and Apache web servers' performance. On the other hand, they analyzed some techniques which were software defense mechanisms against those attacks on both Linux and Windows servers. They have used the high orbit ion cannon (HOIC) tool for creating flood attacks and Slowrise for Slowrise attacks. However, they used the Apache-JMeter tool to generate simulation users or legitimated traffic. Besides, they depended on response time as a key metric in normal and under attacks condition. Their results indicated that the response time in normal mode was very short in both web servers, but in attacks condition, the response time was very long.

3. EXPERIMENTAL SETUP

To analyze the performance of web servers and to get precise and right outcomes, both cluster-based web servers were implemented and configured in a real installation network. Moreover, the specification, system, and the number of used computers in the study are illustrated in Table 1. Also, the used network was installed in 1Gbps Ethernet and shown in Figure 1. Two nodes of computers are grouped as active/active clustered web servers in the Windows environment. Furthermore, the NLB feature has installed and configured in both cluster nodes which is provided by Windows Server 2016. The unicast operation mode is selected for allowing periodic communication of cluster hosts from heartbeat messages. HTTP traffic is directed to the VIP address. NLB driver identical copy is run in parallel on each cluster node to concurrently detect incoming traffic.

In the Linux platform, HAProxy is installed on a separate server as a load balancer. For that reason, the efficiency and the flexibility of the HAProxy have been used in the professional environment with a large number of customers. Moreover, it has the ability to provide high availability services for the real servers; therefore, it is configured to work in the frontend of real web servers. In addition, it is configured to work at the transport layer (layer 4 of the OSI model) to speedily distribute requests through web servers (Backend servers). The end-users' requests are directed to the HAProxy IP address and then redistributed among the backend part which consists of two Apache 2 web servers. Round robin is used as the load balancing algorithm in this installation.

Apache-J Meter 3.3 [28] is used as a load testing tool for analyzing and measuring the performance of both web servers in cluster-based construction. In order to generate multiple clients' HTTP requests for (stress and then analyze the performance of the web servers), Apache-JMeter distributed testing is utilized. The remote testing consists of one JMeter graphical user interface (GUI) workstation (i.e. client) and ten slave Jmeter-servers (i.e. slaves) as command-line hosts, and all of them are configured on Linux Ubuntu 16.04 LTS. Because of that this tool is a pure Java application and it requires java development kit (JDK) to work properly, therefore the JDK-8 is installed in all Jmeters (GUI and command-line).

In order to evaluate the SYN flood DDoS attack impact on the web servers in cluster-based and also on both platforms, the Hping3 command [29] is used. Hping3 command exists within backtrack R5 and has the ability to send a massive number of malicious transmission control protocol (TCP) packets to the victims. Moreover, to generate DDoS type of SYN flood attack the Hping3 command is configured in two workstations so that to send a huge size of the malicious TCP packet to the web servers during the legitimated HTTP requests.

Linux environment provides System Activity Report (SAR) which is a part of the Sysstat package in Linux. SAR has the capability to report, collect, and save system activity information [30]. SAR is being used to monitor system performance such as the utilization of Memory (RAM), CPU Usage, and activities of Input/output (I/O) due to its ability to take system snapshots. The average CPU usage of Apache 2 web server on the Ubuntu 16.04 LTS has been measured by this command. Windows OS provides a PowerShell

environment command called Get-Counter which can directly get real, live and real-time data counter-performance. In order to measure the average CPU utilization of the IIS 10.0 web server on the Windows platform, the Get-Counter is used [23].

Table 1. Workstations specifications

Task	No.	Hardware	CPU	Memory	NIC
Web Servers	4	Dell OptiPlex	Intel Core I3, 3.3 GHz	4 GB	1Gbps
Load Balancer	1	Dell OptiPlex	Intel Core I3, 3.3 GHz	4 GB	1Gbps
Clients	11	HPPro Desk 400	Intel Core I7, 3.4 GHz	4 GB	1Gbps
Attackers	2	Dell OptiPlex	Intel Core I3, 3.3 GHz	4 GB	1Gbps

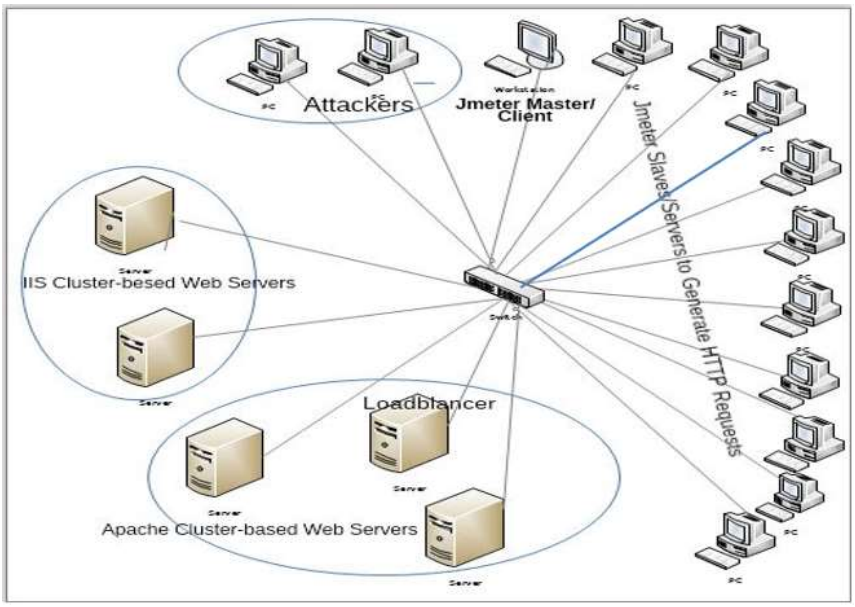

Figure 1. Test network

4. RESULTS AND PERFORMANCE EVALUATION

The performance of Apache 2 and IIS 10.0 cluster-based web servers is analyzed under high concurrent traffic load. Six tests (50000, 100000, 150000, 200000, 250000 and 300000) of HTTP requests were performed and directed to the web servers. Moreover, 1000 malicious packets of TCP were generated and targeted load balancer of each cluster-based web servers separately with the normal HTTP request to evaluate the impact of SYN flood DDoS attack. Furthermore, the test time was 120 seconds and to attain more accurate results each test was repeated more than 5 times. Additionally, analyzing and evaluation key metrics were average response time, average CPU usage, error rate, standard deviation, and throughput.

4.1. Performance analysis of apache 2 and IIS 10.0 cluster-based web servers without SYN Flood DDoS attack

The average response time, standard deviation and error rates of Apache 2 and IIS 10.0 cluster-based web servers is illustrated in Table 2. The IIS 10.0 web servers average response time was 1ms in all tests. Though, the average response time of the Apache 2 web servers was 2ms in the first and second tests. Also, it was 3ms in the third test then increased sharply to 7005ms, 7168ms, and 23996ms in the last three tests. This indicates that the IIS10.0 web servers outperformed Apache 2 web servers in responsiveness.

The error rates of IIS 10.0 web servers were zero from the first test to the last test. Also, the Apache 2 cluster-based web servers' error rates were zero in the first three tests, but in the last three tests, the percentages were 1.49%, 1.66%, and 11.94% respectively. This proves that the efficiency of IIS 10.0 web servers is greater than of Apache 2 web servers.

The IIS 10.0 cluster-based web server's standard deviation values were 0.41ms, 0.47ms in the first and second tests and then increased to 0.48ms in the third and fourth tests, and 0.49ms in the fifth test finally reached to 0.52ms. Nonetheless, the standard deviation values of the Apache 2 clustered web servers were

0.57ms, 0.77ms, and 1.2ms in the first three tests and then rapidly increased to 19459.87ms in the fourth test, after that the value continued on increasing to reach 19706.31ms in the fifth test and reached peak 43848.84ms in the last test. Therefore, the IIS10.0 web servers are more stable compared to Apache 2 web servers.

The average CPU usage of one node of each cluster-based web server is shown in Figure 2. The amount of CPU usage consumed on the IIS 10.0 web server is less than on the Apache 2 web server. The average CPU usage on IIS 10.0 web server is ranged (4.1% → 12.6%) in the first test to the last test but on Apache 2 webserver it ranged (6.2% → 18.2%) in all tests. The throughput of both cluster-based web servers without Attack is illustrated in Figure 3. The throughput of the IIS 10.0 cluster-based web server is 9.66 KB/Sec in the first test and then linearly increased to reach 57.94 KB/Sec in the last test. But the throughput of Apache 2 cluster-based web server is 7.07 KB/Sec in the first test and then slowly increased in the rest tests to be 30.59 KB in the last test.

Table 2. Apache 2 and IIS 10.0 cluster-based web servers average response time, standard deviation and error rates without attack

Requests	Average Response Time (ms)		Standard Deviation		Error Rates	
	Apache	IIS	Apache	IIS	Apache	IIS
50000	2	1	0.57	0.41	0 %	0%
100000	2	1	0.77	0.47	0 %	0%
150000	3	1	1.2	0.48	0 %	0%
200000	7005	1	19459.87	0.48	1.49%	0%
250000	7168	1	19706.31	0.49	1.66%	0%
300000	23996	1	43848.84	0.52	11.84%	0%

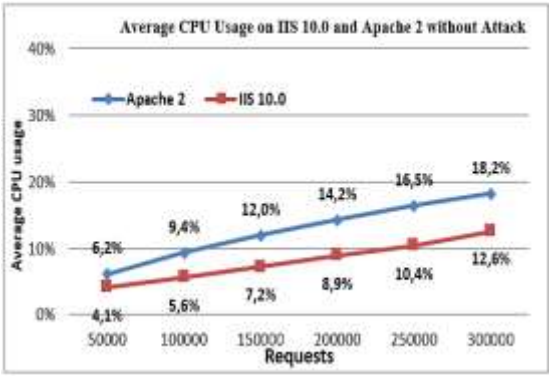

Figure 2. Average CPU Usage on Apache 2 and IIS 10.0 cluster-based web servers without attack

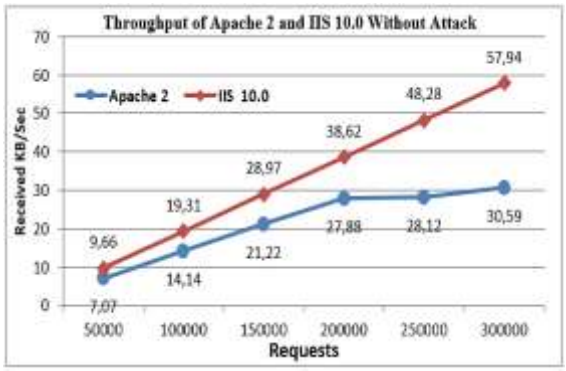

Figure 3. Throughput of Apache 2 and IIS 10.0 cluster-based web servers without attack

4.2. Performance analysis of apache 2and IIS 10.0 cluster-based web servers with SYN Flood DDoS attack

Table 3 illustrates average response time, standard deviation and error rates of both Apache 2 and IIS 10.0 cluster-based web servers. The average response time of the IIS 10.0 was only 6ms in all tests. However, the Apache 2 average response time is 14ms and 15ms in the first two tests and increased to 2980ms in the third test, while in the fourth and fifth tests it was dramatically amplified to 25300ms and 38402ms respectively, in the last test it reached to 45894ms. This shows that the SYN attack increased Apache 2 web servers' response time radically. The standard deviation values of IIS 10.0 cluster-based web servers ranged (2.04ms→2.35ms). Nevertheless, the standard deviation values of the Apache 2 cluster-based web servers ranged (15.15ms → 59457.03ms). Therefore, the stability of the IIS10.0 web servers is better than of the Apache 2 web servers.

The IIS 10.0 error rates were 0% from the first test to the last; hence the attack did not cause error rate problems to HTTP requests on the IIS 10.0 web servers. Also, the Apache 2 cluster-based web servers' error rates were zero percentages in two first tests, became 0.04% in test three, and then increased to 12.38% and 21.42 in the fourth and fifth tests. However, it became worst in the last test at 29.19%.

Table 3. Apache 2 and IIS 10.0 Cluster-based web servers average response time, standard deviation and error rates during attack

Requests	Average Response Time (ms)		Standard Deviation		Error Rates	
	Apache	IIS	Apache	IIS	Apache	IIS
50000	14	6	15.15	2.04	0.00%	0.00%
100000	15	6	18.53	2.05	0.00%	0.00%
150000	2980	6	6134.28	2.06	0.04%	0.00%
200000	25300	6	43701.03	2.06	12.38%	0.00%
250000	38402	6	54466.03	2.06	21.42%	0.00%
300000	45894	6	59457.01	2.35	29.19%	0.00%

The average CPU usage on both platforms during the attack is shown in Figure 4. The IIS 10.0 web servers' average CPU usage ranged (12.74% → 23.051%) but on Apache 2 web servers the average CPU usage ranged (7.25% → 18.17%) from the first to the last test. Thus, the attack impact was more on the IIS10.0 web servers compared to Apache 2 web servers in terms of CPU usage. The throughput of both cluster-based web servers in all tests during the SYN flood attack is illustrated in Figure 5. The IIS 10.0 clustered web server's throughput ranged (12.4 KB/sec → 57.94 KB/sec). However, the throughput of the Apache 2 cluster-based web servers ranged (7.07 KB/sec → 26.63 KB/sec). The SYN flood attack affected more on the Apache 2 web servers in compared with IIS 10.0 web servers.

The overall performance of the proposed system (IIS 10.0 NLB cluster-based webserver) along with the existing researches is compared and illustrated in Table 4. The average response time of the existing researches: [23] is 29 ms, [24] is 11112 ms, [25] is 26.487 ms, [26] is 28.973 ms and for [27] is 70000 ms, while for the IIS 10.0 NLB cluster-based web server part of the proposed system is only 6 ms. Hence the proposed technique is the most responsiveness method of the web servers even under the impact of the DDoS attack. Also, the efficiency of the proposed system and the research [23] was similar because both techniques have zero rates of error (percentage of failed HTTP requests) but for the research [24] the rate is 80.45% and others researches did not measure this key metric.

Moreover, the IIS 10.0 NLB cluster-based web server achieved better stability compared to the existing researches where the standard deviation value of the proposed approach is only 2.33 but for the research [23] the value is 5.1. The throughput of the researches [24] and [27] is 8.5 and 8 KB per second respectively but for our system is 57.94 KB per second. Additionally, the CPU usage for the proposed system is only 6.2%, while for the research [23] is 7.6% and for both [25] and [26] researches is 18%. In the above comparison, the proposed approach attained better performance regarding all key metrics under high concurrent workload (300000 HTTP requests) with and without DDoS attack.

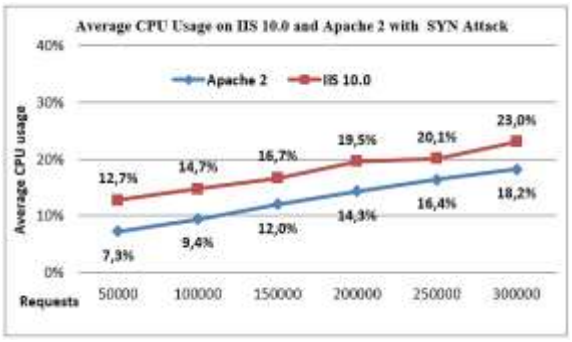

Figure 4. Average CPU Usage on Apache 2 and IIS 10.0 Cluster-based Web Servers with SYN DDoS attack

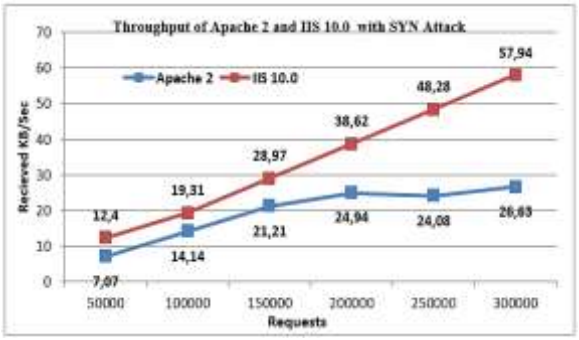

Figure 5. Throughput of Apache 2 and IIS 10.0 Cluster-based Web Servers with SYN DDoS attack

Table 4. Performance comparison of the proposed system and existing researches

	Average Response Time	Error Rates	Standard Deviation	Throughput	CPU Usage
R. Zebari et al. [23]	29	0%	5.1	-	7.6%
T. Bezboruah and A. Bora [24]	11112	80.45%	-	8.5	-
S. S. Kolahi et al. [25]	26.487	-	-	-	18%.
K. Treseangrat et al. [26]	28.973	-	-	-	18%.
R. Papadie and I. Apostol [27]	70000	-	-	8	-
Proposed System	6	0%	2.35	57.94	6.2%

5. CONCLUSION

To perform systematic impact analysis of DDoS attack, and to get accurate and correct results, the proposed system was implemented in the 1Gbps real network. Also, the system was installed and configured on the utmost modern operating systems. The depended web servers were prepared on the NLB Cluster-based web servers in Windows and Linux platforms. The analyzing was performed with and without the SYN flood DDoS attack in six tests of HTTP requests. The study mainly based on the responsiveness, efficiency and stability, also the average CPU utilization and throughput are measured as metrics of the evaluation process with a heavy load. In Cluster-based construction without attack, the experimental results illustrated that IIS 10.0 is more responsiveness compared to the Apache 2 web server. The average CPU usage on Apache 2 web server is greater than that of the IIS 10.0. Also, IIS 10.0 has better standard deviation value; therefore, IIS 10.0 is more stable. The throughput of IIS 10.0 cluster-based webservers is much greater than that of Apache 2 web servers. Moreover, IIS 10.0 Efficiency is better than that of Apache 2 because IIS 10.0 has no error rates, while Apache 2 suffered from error rates. The experimental results indicated that the SYN DDoS attack impact was more on the performance of Apache 2 web servers. Where, the average response time, standard deviation and error rates dramatically increased. Also, the throughput of Apache 2 cluster-based web servers reduced during the attack. Therefore, the IIS10.0 is more responsiveness, stable and has better efficiency during the attack. However, the average CPU usage of the Apache 2 clustered web servers did not affect by the SYN attack.

REFERENCES

[1] K. Jacksi and S. M. Abass, "Development History of the World Wide Web," *International Journal of Scientific & Technology Research (IJSTR)*, vol. 8, no. 9, pp. 75-79, 2019.

[2] K. Jacksi, S. R. M. Zeebaree, and N. Dimililer, "LOD Explorer: Presenting the Web of Data," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 9, no. 1, pp. 45-51, 2018.

[3] K. Jacksi, "Design and Implementation of E-Campus Ontology with a Hybrid Software Engineering Methodology," *Science Journal of University of Zakho*, vol. 7, no. 3, pp. 95-100, 2019,

[4] Stevens, J., "Internet Statistics & Facts (Including Mobile) for 2019," *HostingFacts.com*. [Online]. Available: https://hostingfacts.com/internet-facts-stats/. [Accessed: 30-Nov-2019].

[5] P. Srivani, S. Ramachandram, and R. Sridevi, "A survey on client side and server-side approaches to secure web applications," in *2017 International conference of Electronics, Communication and Aerospace Technology (ICECA)*, vol. 1, pp. 22–27, 2017.

[6] Z. N. Rashid, S. R. Zebari, K. H. Sharif, and K. Jacksi, "Distributed Cloud Computing and Distributed Parallel Computing: A Review," *presented at the 2018 International Conference on Advanced Science and Engineering (ICOASE)*, pp. 167–172, 2018.

[7] Q. Fan and Q. Wang, "Performance comparison of web servers with different architectures: a case study using high concurrency workload," in *2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*, pp. 37–42, 2015.

[8] O. H. Jader, S. R. Zeebaree, and R. R. Zebari, "A State of Art Survey for Web Server Performance Measurement and Load Balancing Mechanisms," *International Journal of Scientific & Technology Research (IJSTR)*, vol. 8, no. 12, pp. 535-543, 2019.

[9] M. A. Saifullah and M. M. Mohammed, "Scalable load balancing using enhanced server health monitoring and adimission control," in *2015 IEEE International Conference on Engineering and Technology (ICETECH)*, pp. 1–4, 2015.

[10] P. López and E. Baydal, "Teaching high-performance service in a cluster computing course," *Journal of Parallel and Distributed Computing*, vol. 117, pp. 138–147, 2018.

[11] J. E. C. de la Cruz and C. A. R. Goyzueta, "Design of a high availability system with HAProxy and domain name service for web services," in *2017 IEEE XXIV International Conference on Electronics, Electrical Engineering and Computing (INTERCON)*, pp. 1–4, 2017.

[12] S. R. M. Zeebaree, R. R. Zebari, K. Jacksi, and D. A. Hasan, "Security Approaches for Integrated Enterprise Systems Performance: A Review," *International Journal of Scientific & Technology Research (IJSTR)* vol. 8, no. 12, pp. 2485-2489, 2019.

[13] S. Akbar and A. D. Wibawa, "The impact analysis and mitigation of DDoS attack on local government electronic procurement service (LPSE)," in *2016 International Seminar on Intelligent Technology and Its Applications (ISITIA)*, pp. 405–410, 2016.

[14] S. Bravo and D. Mauricio, "Systematic review of aspects of DDoS attacks detection," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 14, pp162-176, 2019.

[15] B. Singh, K. Kumar, and A. Bhandari, "Simulation study of application layer DDoS attack," in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, pp. 893–898, 2015.

[16] S. R. Zeebaree, K. H. Sharif, and R. M. M. Amin, "Application Layer Distributed Denial of Service Attacks Defense Techniques: A review," *Academic Journal of Nawroz University*, vol. 7, no. 4, pp. 113–117, 2018.

[17] S. Daneshgadeh and N. Baykal, "DDoS attack modeling and detection using smo," in *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pp. 432–436, 2017.

[18] M. Semerci, A. T. Cemgil, and B. Sankur, "An intelligent cyber security system against DDoS attacks in SIP networks," *Computer Networks*, vol. 136, pp. 137–154, 2018.
[19] B. Prabadevi and N. Jeyanthi, "A Review on Various Sniffing Attacks and its Mitigation Techniques," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, no. 3, pp. 1117–1125, 2018.
[20] M. N. Vora and D. Shah, "Estimating effective web server response time," in *2017 Second International Conference on Information Systems Engineering (ICISE)*, pp. 37–44, 2017.
[21] A. Saravanan, S. SathyaBama, S. Kadry, and L. K. Ramasamy, "A new framework to alleviate DDoS vulnerabilities in cloud computing," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, pp. 4163–4175, 2019.
[22] "Netcraft | Internet Research, Cybercrime Disruption and PCI Security Services." [Online]. Available: https://news.netcraft.com/. [Accessed: 30-Nov-2019].
[23] R. R. Zebari, S. R. Zeebaree, and K. Jacksi, "Impact Analysis of HTTP and SYN Flood DDoS Attacks on Apache 2 and IIS 10.0 Web Servers," in *2018 International Conference on Advanced Science and Engineering (ICOASE)*, pp. 156–161, 2018.
[24] T. Bezboruah and A. Bora, "Performance evaluation of hierarchical SOAP based web service in load balancing cluster-based and non-cluster-based web server," *International Journal of Information Retrieval Research (IJIRR)*, vol. 5, no. 4, pp. 19–30, 2015.
[25] S. S. Kolahi, K. Treseangrat, and B. Sarrafpour, "Analysis of UDP DDoS flood cyber attack and defense mechanisms on web server with Linux Ubuntu 13," in *2015 International Conference on Communications, Signal Processing, and their Applications (ICCSPA'15)*, pp. 1–5, 2015.
[26] K. Treseangrat, "Performance analysis of defense mechanisms against UDP flood attacks," Master's Thesis, 2014.
[27] R. Papadie and I. Apostol, "Analyzing websites protection mechanisms against DDoS attacks," in *2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, pp. 1–6, 2017.
[28] M. A. Putri, H. N. Hadi, and F. Ramdani, "Performance testing analysis on web application: Study case student admission web system," in *2017 International Conference on Sustainable Information Engineering and Technology (SIET)*, pp. 1–5, 2017.
[29] P. M. Ombase, N. P. Kulkarni, S. T. Bagade, and A. V. Mhaisgawali, "DoS attack mitigation using rule based and anomaly-based techniques in software defined networking," in *2017 International Conference on Inventive Computing and Informatics (ICICI)*, pp. 469–475, 2017.
[30] A. G. Chekkilla, *"Monitoring and Analysis of CPU Utilization, Disk Throughput and Latency in servers running Cassandra database: An Experimental Investigation,"* 2017.

BIOGRAPHIES OF AUTHORS

Subhi Rafeeq Mohmed Zeebaree is the Director of Culture and Student Activities Center at Duhok Polytechnic University. He got his BSc, MSc and PhD Degrees from University of Technology-Baghdad-Iraq at 1990, 1995 and 2006 respectively. He started teaching and supervising post-graduate courses (PhD and MSc) since 2007 and until now. He has joint PhD supervisions with UTM (Malaysia), Firat University (Turkey), and EMU (Cyprus). He was the Chairman of Scientific and Research Advices Committee of DPU for five years. He is a member of IEEE Iraq-section.

Karwan Jacksi obtained a B.Sc. in Computer Science from the University of Duhok, in 2007. In 2011, he obtained a M.Sc. in CS at Uppsala University, Sweden. He earned his Ph.D. degree in CS from the University of Zakho (UoZ) and Eastern Mediterranean University in a split-site program, in 2018. He has been an active member for several national and international Journals, conferences, and workshops. More information about Dr. Jacksi can be found from his personal website: www.KarwanJacksi.net.

Rizgar Ramadhan Zebari obtained a B.Sc. in Computer Science from the University of Salahaddin, in 2006. Also, he obtained M.Sc. in Information technology at Duhok Polytechnic University (DPU), in 2018. He is a lecturer at the department of Information Technology, DPU. His areas of interest include Computer Network, DoS, Data Mining and information retrievals, search engines. He has authored and co-authored 5 papers in international journals and conferences.