An Empirical Study of The Impact of DoS, DDoS Attacks on Various Web Servers and Application Servers

Phai Vu Dinh, Viet Hung Nguyen, Nguyen Ngoc Tran, Minh Son Duong

***Abstract*— In recent research, DoS and DDoS attack is a crucial topic where solutions have not been satisfied with the real problem. As a consequence of the fact that the former one mainly focuses on the vulnerabilities of protocols to conduct an invasion, while the latter one utilizes multiple compromised systems for a single target to make the services unavailable for legitimate users. In this paper, we will concentrate on making clear the impact of these attacks on RAM utilization, CPU usage, and network throughput of various Web Servers and Application Servers, which contributes to understanding deeply and constructing effective DoS, DDoS defense systems.**

***Tóm tắt*— Trong các nghiên cứu gần đây, tấn công từ chối dịch vụ DoS và DDoS là một chủ đề thời sự, tuy nhiên có khá nhiều giải pháp chưa thật sự đáp ứng được các vấn đề thực tế. Các tấn công DoS tập trung vào việc khai thác các lỗ hổng giao thức mạng để tiến hành một cuộc tấn công. Trong khi đó tấn công DDoS sử dụng rất nhiều các hệ thống bị thỏa hiệp để tấn công một mục tiêu cố định nhằm ngăn chặn các người dùng hợp lệ sử dụng dịch vụ. Trong bài báo này, chúng tôi tập trung vào làm rõ các ảnh hưởng của các cuộc tấn công từ chối dịch vụ đối với RAM, CPU và băng thông của các máy chủ web và các máy chủ ứng dụng. Các nghiên cứu này góp phần vào việc hiểu sâu hơn ảnh hưởng của tấn công từ chối dịch vụ và việc tạo ra các hệ thống phòng thủ đối với tấn công từ chối dịch vụ một cách hiệu quả.**

***Keywords*: Impact of DoS and DDoS; RAM utilization; CPU usage; Network throughput; Breaking Point System; UFONe.**

***Từ khóa:* Impact of DoS and DDoS; RAM utilization; CPU usage; Network throughput; Breaking Point System; UFONe.**

I. INTRODUCTION

Denial-of-Service (DoS) and Distributed-Denial-of-Service (DDoS) are attacks which hackers want to prevent legitimate users access and use the Internet resources. For instance, when a bank system is in a DoS attack, you can not access to take any transactions as a consequence of a huge of requests as you standing in a queue. As you know, while the DoS appears more early in the 18th century, the DDoS is a type of attack that is developed on a higher level in early 1992 [1]. The difference between DoS and DDoS is the scope of the attack. While the former attack is generated from a computer or a few ones, the latter attack is created from a huge amount of computers. There are two prevalent attack methods. On the first one, attackers send a specific packet that for a sack of creating an error in victim's system such as the error of protocol, software's error and so on. This method depends on the vulnerability of protocol or software. When it comes to the second attack method, there is more popular attack than the first one. As we know, the discipline of DDoS attack based on flooding Internet traffic, bandwidth exhaustion and Internet resource.

No sooner did the first DDoS attack happen in 1992 than there were a huge amount of flooding attacks were deployed to companies, organizations, and governments. Most of the attacks trigger flooding to the host system that is responsible for reducing financial income and increasing the cost of security and insurance. For example, in 2000, the Yahoo network system suffered the first DDoS attack, which made this system stop providing service in 2 hours and affected significantly by their advertisement income. In addition, in December of 2010, the group of people that named "Anonymous" created the several DDoS attacks to stop working website of financial organizations such as Master card, Visa International, Paypal, and Post Finance. In September of 2012, the big attack from a group of attackers "Izz ad-Din AL-Qassam Cuber Fighters" decided to attack nine Banks of America. The kind of attacks is more prevalent, by dint of the

This manuscript is received on March 15, 2018. It is commented on March 20, 2018 and is accepted on April 20, 2018 by the first reviewer. It is commented on March 20, 2018 and is accepted on April 16, 2018 by the second reviewer.

development of technical methods and public attack tools [2].

In terms of the purpose of the attacker, we can divide into five group of DDoS attacks. To specific, while the first one concerns about the financial benefits, the second groups takes care of enemies. The former one usually has an advanced technique with high experience, which jeopardizes to big companies and organizations. This attack wants to obtain financial benefits is the most dangerous attack. It is difficult to defence this attack. The latter group is a few people who victimize to others one. Regarding warfare aspect, the third group one relates to armies, governments or terrorist organizations. The destination of attacks is an organization of governments such as bank systems or Inter-telecoms Corporation group. Moreover, the final one with learning target is young people including teenagers, students from high school and so on. These people increase sharply by virtue of public tools and open sources.

With a view to defending effectively DDoS attack and reducing the influence of this attack, whether research and analysis are necessary to find effective solutions in protecting the system from this attack. There are many questions referrer to involve to the DDoS and DoS attack. For instance, what is the difference between.

II. BACKGROUND

A. DoS Techniques

1. Attack on application layer

Slow HTTP

A Slow HTTP DoS attack referrers to Slow loris attack that make uses HTTP GET requests to occupy all available HTTP connections permitted on a web server. A slow HTTP DoS attack takes advantage of a weakness on the thread-base web server which has to wait for entire HTTP headers to be received before releasing the connection. While some thread-based servers such as Apache use a time-out to wait for an incomplete connection, the timeout, that is set 300 seconds by default, is reset as soon as the client sends additional data.

A situation is generated when attackers could open several connections on a web server by creating an HTTP request but do not close it. By keeping the faking HTTP request open before timeout reaches, the connection will keep until the attacker closes it. To be honest, no sooner do attackers send HTTP request than legitimate users can not to have their HTTP requests processed by this server, thus experiencing a denial of service.

To specify, with CRLF standing for Carriage Return Line Feed, is a non-printable character that is used to denote the end of the line. Similar to a text editor, HTTP request may contain CRLF at the end of a line to start a fresh line, and two CRLF to denote a blank line. The HTTP protocol defines a blank line as a completion of the header. A slow HTTP DoS abuses this by not sending a finish blank line to complete the HTTP header.

HTTP-POST

As we know, a POST request includes a message body in addition to a URL used to specify information for the action being performed. This body can use any encoding, but when web pages send POST requests an HTML form element the Internet media type is "application/x-www-form-urlencoded". The field "Content-Length" in the HTTP header tells the web server how large the message body is, (for instance: Content-Length = 100). Being compromised robots, web servers will obey the "Content-Length" field to wait for the remaining message body to be sent. Then, by waiting for the complete message body to be sent, web servers can support users with a slow or intermittent connection.

In order to attack a web server, attackers have just taken random content data in the body of the message. In addition, conducting to combine multi-processing threads, attackers can be easy to give birth several thousand HTTP POST requests. Recent studies have shown that this attacks can evade Layer 4 detection techniques as there is no TCP error, just like Slowloris above. Unlike Slowloris, there is no delay in sending HTTP header, hence it can disable the function of the Internet Information Service (IIS) defence, making IIS vulnerability too. By virtue of doing random the size, character sets and time intervals, this attack may avoid any recognition of Layer 7 traffic patterns by DoS protection systems.

2. Attack on transport and network layer

TCP-SYN

We are going to consider the three ways handshake of TCP connection. The TCP connection consists of three major steps, a request, an acknowledgement and an agreed upon connection. The initiating host denotes as Initiator, which will request a connection with a target server that denotes by Listener below. The

target server must acknowledge the request. The acknowledgement to the Initiator indicates that the Listener is ready to establish a session, and sets up the bi-directional method of ensuring proper data transmission. The Initiator must acknowledge the receipt of this message and a session will be created.

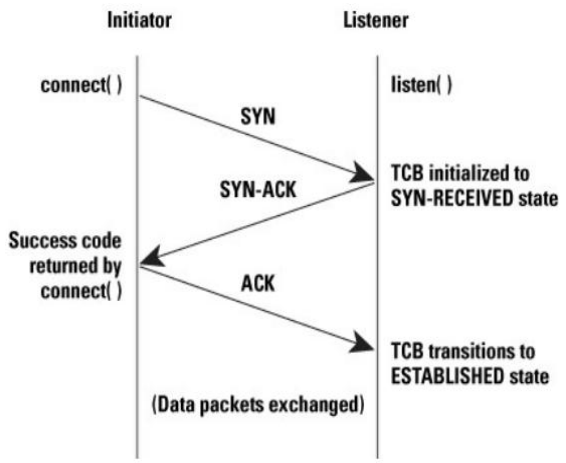

Figure 1. Three ways handshake

In order to conduct a TCP-SYN attack, the attacker starts initiating a connection to the target host but never returning the final acknowledgement of the three-way handshake previously described. The target host, having sent the SYN-ACK packet, is left waiting for the final ACK packet from the attacker. During this waiting period, the host holds the entry in its backlog table until the attempt times out. The attacking host continues initiating connection establishment sessions. We definitely understand the fact that the target host's backlog table will be filled. Thus it can no longer accept a new connection and of course, its service has effectively been denied. To pass to the suspicious of the host, attackers can take spoofing the source IP address.

UDP

UDP Flood attack is simple, common and famous Layer-4 attack DoS attack. UDP Flood vulnerabilities have been discovered during the year 1998-2000. In this attack, a barrage of UDP packets is sent to the victim computer either on selected UDP port or on a random port.

The targeted system processes the incoming datagram to determine which application it has requested on that system by refereeing the port number and in case if the requested application is not present on the system or the requested port was not opened on the targeted system.

ICMP

Internet Control Message Protocol (ICMP) flood attacks have existed for many years. They are among the oldest types of DoS attacks. In ICMP flood attacks, the attacker overwhelms the targeted resource with ICMP echo request (ping) packets, large ICMP packets, and other ICMP types to significantly saturate and slow down the victim's network infrastructure. ICMP attack, relates to the Smurf attack, which will be presented on below.

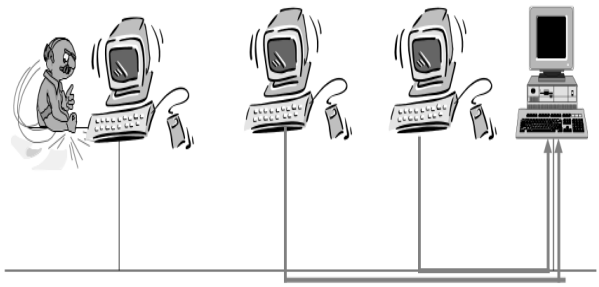

Figure 2. ICMP smurf attack

The Smurf Attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic.

B. DDoS techniques

1. Botnet control mechanisms

Internet Relay Chat

In their infancy, Internet Relay Chat (IRC) was the C&C medium of choice for botnets. IRC is widely deployed across the Internet and several public IRC networks are in existence. It has a simple text-based command syntax and provides almost real-time communication between bots and C&C server. Nevertheless, the use of IRC is not common, particularly in enterprise networks. Also, the message format of the standard implementation of IRC is unique, making IRC traffic easily distinguishable from the normal traffic. Agobot, Spybot, and Sdbot are some prevalent IRC based botnets [3].

HTTP

After the relative success of law enforcement agencies and industry in tackling the issue of IRC botnets [4], the next step in botnet evolution was HTTP C&C communication. In HTTP-based botnets, bots contact C&C server to commands. As a consequence of the fact that blocking of HTTP traffic is not a smart option for most organizations and corporate networks, which is responsible for this botnets' protocol being difficult detection. Besides, HTTP is the most common protocol used on the Internet making it ideal for C&C communication. Use of HTTP as the C&C protocol results in a centralized botnet structure. In the context of large botnets, some strategies must be adopted to keep the C&C server from being overwhelmed if all the bot happen to contact it simultaneously.

Peer-to-peer

In terms of peer-to-peer (P2P) networks, originally developed to facilitate file sharing among peer nodes, have been utilized for botnet C&C communication. Thanks to commands being distributed using any node in the P2P network, its C&C servers makes it difficult to detect. Several protocols are available for P2P-based C&C communication, such as WASTE, BitTorrent, Kademlia, Direct Connect, Gnutella, and Overnet.

2. DDoS Architecture model

Before real attack traffic reaches the victim, the attacker must communicate with all its DDoS agents. Therefore, there must be control channels present in between the agent machines and the attacker machine. This cooperation between the two requires all agents to send traffic based on the commands received from the attacker. The attack network consists of the three components: attacker, agents, and control channels. In attack, networks are divided into three types: the agent-handle model, the IRC-based model and the reflector model [5].

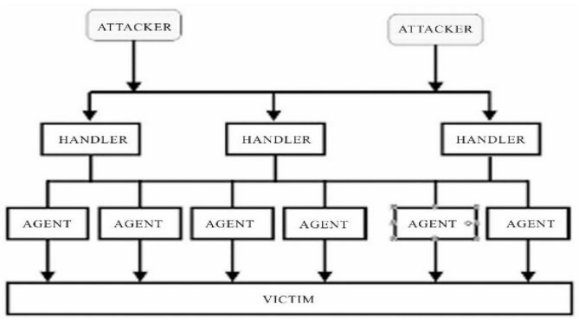

Figure 3. Agent-handler model

The Agent-Handler model of a DDoS attack consists of agents, handlers and client. Figure 3.3 shows the Agent-Handler Model, in which the agent and handler know the each-others identity. The client is the interface where the attacker/mastermind communicates with the rest of the DDoS Components. The handlers are software packages distributed all over the Internet so that it helps the client to convey its command to the agents. The agent software's are vulnerable systems, compromised by the handlers and actually launch the attack on victim's machine. The agent's status and schedule for launching attack can be upgraded by the handler when it is required. Communication relation between agent and handler is either one to one or one to many. Most common way to attack is by installing handler instructions either on the compromised route on network layer or on the network server. This makes it difficult to identify messages exchanged by the client handler and between the handler-agents [6].

III. EXISTING WORK

The DDoS attacks are not new to the world of cybersecurity [9], [10] however the mode of DDoS attacks is changing parallel with the advancement in security solutions. Most of the researches are focusing on how to protect the systems from a DoS and DDoS attack [11-14] while others conduct surveys to show the effectiveness of DDoS attacks [15-17]. Besides, several types of research have created attributes of network traffic from DDoS attacks, which helps the community can generate models to protect their systems from these attacks.

Bin Xiao and Wei Chen have used Bloom filter to generate accurate detection results yet consumes minimal storage and computational resources. This approach can show the false alarm probability of the detection scheme, which is insensitive to false alarms when using specially designed evaluation functions [18]. Moreover, machine learning methods are utilised to solve this problem such as fuzzy estimators [11], RBF Neural Networks [13].

Some approaches relate to generating botnet traffic that the data is captured in the field in terms of the botnet behaviours represented. Fariba Haddadi and A. Nur Zincir-Heywood generated Zeus and Citadel botnet traffic in the sandbox environment and used Tranalyzer flow exporter and HTTP filter with the C4.5 classifier to filter botnet traffic classification. [19-20].

IV. PROPOSED METHODOLOGY

In this section, we are going to represent how to generate network traffic which is utilized to evaluate the impact of DoS and DDoS attacks.

When it comes to the DoS attack, we decide to create a topology which includes two computers such as client and server, respectively. While the former one is used to generate an invasion to the server, the latter one is used to install several web servers and application servers. Doing these experiments, we have just configured directly between the client and server by a switch or router. Then, no sooner do we decide to conduct an invasion from the client to the server then we capture the change of the server in terms of RAM utilization, CPU usage, and bandwidth. The change is compared to the difference between normal and attacked state of the server.

With regarding the DDoS attack, in preparation of evaluating the performance of these DDoS attacks that compare to the Breaking Point System (BPS) on the side of bandwidth, we do three experiments which relate to the DDoS attack. For instance, the first one is the botnet system which is created with five agents and a botmaster on the laboratory. The botmaster can control and launch an attack by the Web interface and it is easy to choose the target and the type of attacks such as TCP, UPD, HTTP GET, HTTP POST and ICMP. On the second attack, we use a real botnet which its agents are the web servers on the Internet that contain the URL redirection abuse. In fulfilment of scanning all of these web servers, we use the UFONet open source. There have more than 2000 agents is found down, before it is used to attack the server. The final attack, we used the BPS to generate a DDoS attack. The three types of attack are captured the network traffic on the servers when these attacks happen.

DDoS via Web Abuse

In order to examine DDoS via Web Abuse, the authors try to use UFONet, "a free software tool designed to test DDoS attacks against a target using "Open Redirect" vectors on third-party web applications like botnets". This open-source botnet is easy to install and run, and it's capable of searching out vulnerable hosts, testing them, cataloguing them, running DDoS attacks, and more [8].

The figure below describes the working principle of UFONet model. Overall, the model has two stages such as selected information and attacking, respectively. For example, in the first step, the UFONet master sends requests to numerous proxy servers to get lists of compromised Web servers which have URL redirection abuse. Next, no sooner does the master UFONet get the list of URL redirection abuse than it can directly conduct a DDoS attack to a target by using sending the request to compromised computers.

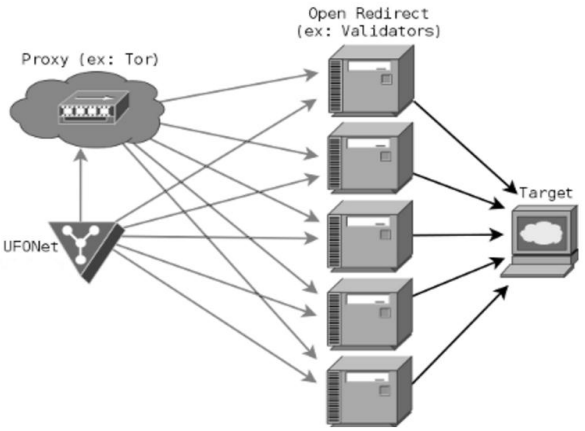

Figure 4. UFONet model

DDoS with 5 agents

With a view to conducting DDoS experiment, we try to give birth 5 zombies. After constructing the zombie's network, we decide to attack the victim with five types of attack such as ICMP, UDP, SYN, HTTP-GET and HTTP-POST. Statistical result is captured from Wireshark software from victim's machine.

Breaking Point System

The Breaking Point System (BPS) which reproduces from IXIA company. This device can help us to develop simulations of enterprise infrastructures, Internet infrastructures, and people interactions, and create 80 tests using the security exploit traffic [7]. Besides, Breaking Point platforms allow us to simulate how millions of people interact and communicate with each other. The most important thing of the BPS system in this paper is that it can help to create a big network traffic flow with maximum 1GB. We are going to conduct an experiment of the BPS to create a DDoS attack.

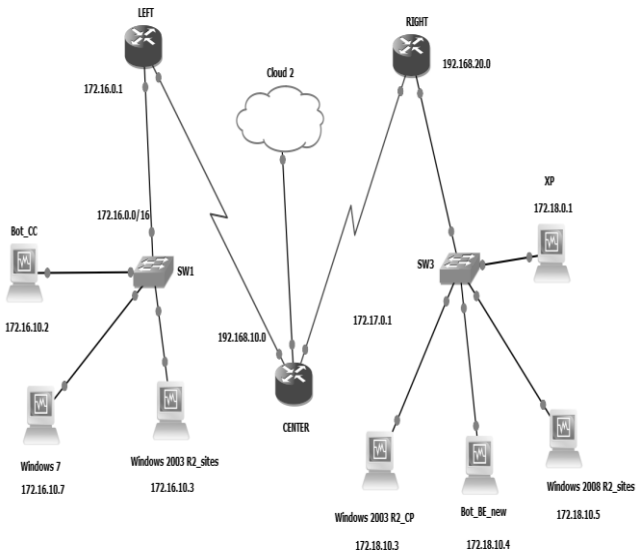

Figure 5. DDoS topology with 5 agents

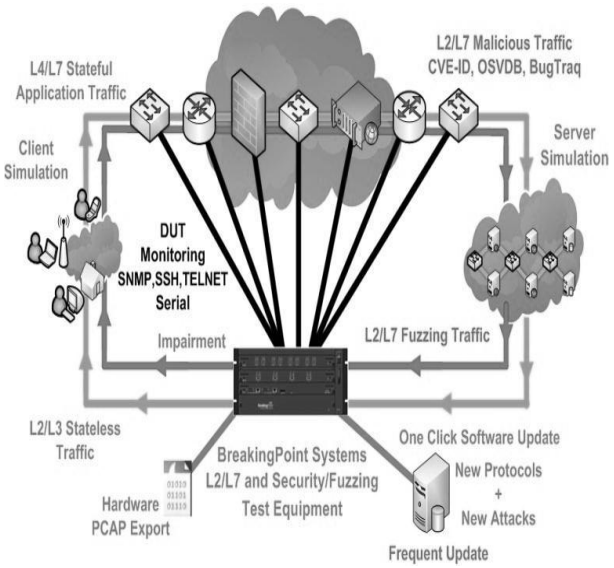

Figure 6. Breaking Point System

In preparation for getting the change of CPU usage, RAM utilization and Network throughput when the DoS attack happening, we use the lib-statgrab library. There an open source that is written in C language. It's written in C and presents a selection of user interfaces which can be used to access key system statistics. The current list of statistics includes CPU usage, memory utilisation, disk usage, process counts, network traffic, disk I/O, and more [21].

V. EVALUATION & RESULTS

A. DoS effectiveness

Table 1 illustrates the impact of DoS attacks on RAM, CPU and bandwidth on the server. Overall, these attacks do not consume much server's resource. However, these can take advantage of vulnerabilities of protocols to attack, which can be responsible for being reducing the performance of the server, even leading to denial-of-service.

TABLE 1. IMPACT OF RAM, CPU, AND BANDWIDTH

	RAM utilization increment (AVG/MB)	**CPU usage increment (AVG/ %)**			**Network throughput increment (AVG)**	
		User CPU	Kernel CPU	Iowait CPU	KB/s	No of Packets/s
HTTP GET	35.92	26.56	11.99	5.21	5.38	40
HTTP POST	86.26	7.84	5.74	2.54	1535.40	11871
TCP	33.80	12.51	5.03	27.89	36.60	645
UDP	22.47	7.47	5.08	2.64	44.71	799

Table 2 describes the time implement of HTTP requests by various protocols on several Web Servers. Generally speaking, the performance of a variety of attacks is different. For instance, when it comes to Apache Server, most of the attacks make the Web Server deny of service and this Web Server spends about 7 seconds responding the request during being attacked.

TABLE 2. TIME IMPLEMENT OF DoS ATTACKS

	Apache (ms)	**Flask (ms)**	**Nodejs (ms)**	**Service API in Java (ms)**
HTTP GET	Time-out	10220	54	32
HTTP POST	Time-out	51	53	30
TCP	Time-out	Time-out	55	47
UDP	6970	2960	52	31

With regard to Flask Web Server, even though the HTTP-POST attack does not affect the performance of this Web Server, other attacks reduce the performance of this server. For example, the server is denied by the server when it is attacked by the TCP and Slowloris. In addition, not only does the server spend about 10 seconds responding a request with HTTP-GET attack but this gets a little bit problem with UDP attack with approximate 3 seconds per request.

In terms of the performance of Nodejs Web Server and API Service on Java, we definitely claim that there is no effect on these server with all of these attacks. It can be explained that the performance of these servers is better than most servers above which are responsible for the number of requests not having enough to deny of service.

Figure 7 depicts the impact of DoS on RAM. The first line-graph show the result of HTTP- GET which can make the memory of server rise about 150 MB on the period attacking. When it comes to HTTP_POST attack, this attack does influence the most on the memory usage to compare with others. No sooner do we conduct a TCP attack than the memory usage go up remarkably from 2000 to 2340 Mb for the first 5 seconds. In the next 5-seconds period witnesses a slight increase of the used memory to the peak at 2350 MB before falling significantly to 2100 MB at second 36. Finally, the line graph of UDP attack illustrates the change in two stages. For example, the first period for the first 70 second experiences a fluctuates of memory usage between 3480 and 3450 MB while the last stage goes up and down from 3530 to 3540 MB.

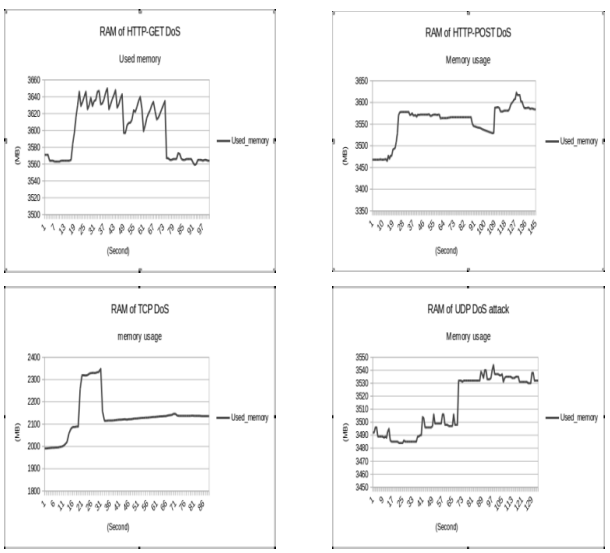

Figure 7. Impact of DoS on RAM

As can be sent from the change of CPU usage of HTTP-GET DoS on Figure 8, no sooner does this attack take place than the CPU usage of the server has increased dramatically. For examples, there is a rocket-increase from 10% to 43% of User CPU usage at the second 20 before this fluctuates slightly at 40% on the period of the attack. This attack triggers the most effective on the server. UDP attack ranks the second position while the remaining two attacks do not consume server's CPU. Strikingly, HTTP-POST may create the most change on a little period about 5 seconds. It can be understood that after the server is denial-of-service, there is no request that is accepted to process.

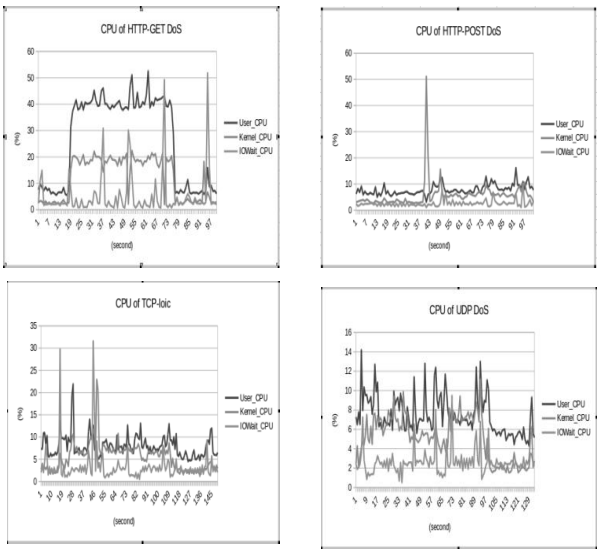

Figure 8. Impact of DoS on CPU

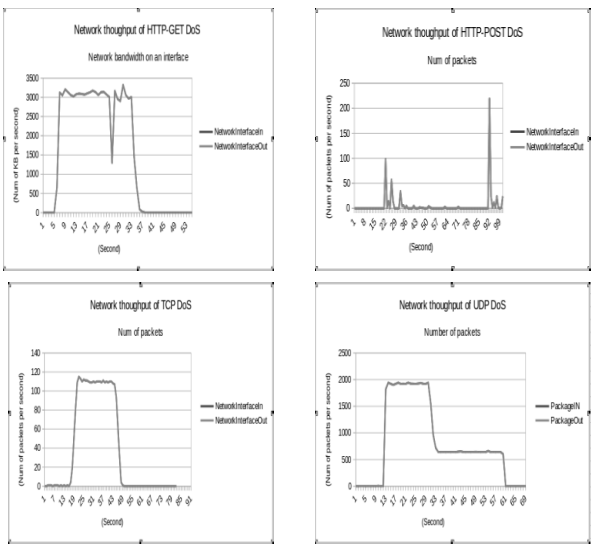

Figure 9. Impact of DoS with Network thoughput

With regarding network throughput, three kinds of attacks such as HTTP-GET, TCP, UDP which make the server's bandwidth consume significantly. However, the last HTTP-POST attack lies on the bottom position of the list since the server is denial-of-service, there is no request that is accepted to process.

B. DDoS performance

Table 3 illustrates the performance of types of DDoS attack. Overall, the impact of types of DDoS attack is not much in terms of bandwidth and average of packets per second with DDoS which is created by 5 agents in the laboratory. For example, the number of average packets per second and average bytes per second is less than the value of the BPS. We can explain that as a consequence of lack of zombies which are responsible for the performance of the DDoS attacks being lower.

TABLE 3. DDoS ATTACKS COMPARISON

Type of Attack	**Num of packets**	**Avg packets / sec**	**Avg bytes / sec**
DDoS - ICMP	45252	245	50491
DDoS - SYN	41601	58	6428
DDoS - UDP	2112	239	9684
DDoS-HTTP GET	7111	29	1837
DDoS-HTTP POST	2090	5	6484
DDoS via Web Abuse	409	7	1098
BPS	123416	128M	1026M

VI. CONCLUSION & FUTURE WORK

In brief, on the first hand, the DoS attack is primarily deployed on the vulnerability of protocols, web servers, and approach services. However, this attack can stop providing services for legitimate users, even though the impact of this attack on CPU usage, RAM utilization, and network throughput is not much. For instance, the value of RAM utilization is less than 100 MB, while the value of CPU usage is always lesser than 30 % in total. Besides, the impact of DoS attack depends on a kind of servers is used. To specify, most of DoS attacks may be successful with Apache and Flask Web Server, while Nodejs Web server and Java API services are influenced not much.

In terms of the final result, the paper shows two methods of DDoS attack. The first one takes advantage of URL redirection for selecting compromised computers. The result of these experiments experiences that the number of zombies is not much with approximately 2000 victims while an invasion may generate its bandwidth about 1 MB. The second experiment we take the BPS for establishing an attack. Its bandwidth of the BPS can be created with maximum 1 GB attacked data and be easy to stop the service of web servers and application servers. Nevertheless, when we conduct some experiments with the model above, its bandwidth of this one can construct with 36 Mbs after 10 seconds selected data.

In the future work, we try to use this research for applying the issue of defence denial-of-service attack. We hope these results can contribute to enhancing the performance of DoS and DDoS detection problem.

REFERENCES

[1]. https://en.wikipedia.org/wiki/Denial of service attack

[2]. Rajkumar, ManishaJitendra Nene, "A Survey on Latest DoS Attacks:Classification and Defense Mechanisms", An ISO 3297: 2007 Certified Organization, Vol. 1, Issue 8, October 2013

[3]. P. Barford and V. Yegneswaran, "An Inside Look at Botnets" in Malware Detection, ser. Advances in Information Security, M.Christodorescu, S. Jha, D. Maughan, D. Song, and C. Wang, Eds.Boston, MA: Springer US, vol. 27, ch. 8, pp. 171–191, 2007.

[4]. T. Cymru, "A taste of http botnets" http://tinyurl.com/9o5chx2, 2008, [Online; accessed 20-December-2011].

[5]. Meghna Chhabra 1 , Brij Gupta 1* , Ammar Almomani 2 "A Novel Solution to Handle DDoS Attack in MANET" Journal of Information Security Vol. 4 No. 3, 2013.

[6]. Shweta Tripathi,Brij Gupta, Ammar Almomani, Anupama Mishra, Suresh Veluru "Hadoop Based Defense Solution to Handle Distributed Denial of Service (DDoS) Attacks" Journal of Information Security, 4, 150-164, 2013.

[7]. https://support.ixiacom.com/support-services/training/breakingpoint

[8]. https://null-byte.wonderhowto.com/how-to/use-ufonet-0174158

[9]. http://en.wikipedia.org/wiki/Cyberspace

[10]. http://www.arbornetworks.com/attack-DDoS

[11]. Stavros N. Shiaeles , Vasilios Katos , Alexandros S. Karakos, Basil K. Papadopoulos, "Real time DDoS detection using fuzzy estimators", computers & security 31 782 – 790, 2012.

[12]. Rui Zhong, and Guangxue Yue, "DDoS Detection System Based on Data Mining", ISNNS '10, Jinggangshan, P. R. China, 2-4, April, pp. 062-065, 2010.

[13]. Reyhaneh Karimazad and Ahmad Faraahi, "An Anomaly-Based Method for DDoS Attacks

Detection using RBF Neural Networks", 2011 International Conference on Network and Electronics Engineering IPCSIT vol.11 IACSIT Press, Singapore, 2011.

[14]. Seyed Mohammad Mousavi and Marc St-Hilaire, "Early Detection of DDoS Attacks against SDN Controllers", 2015 International Conference on Computing, Networking and Communications, Communications and Information Security Symposium

[15]. Vrizlynn L. L. Thing, Morris Sloman, and Naranker Dulay, "A Survey of Bots Used for Distributed Denial of Service Attacks", http://www.doc.ic.ac.uk.

[16]. Rajkumar, ManishaJitendra Nene, "A Survey on Latest DoS Attacks:Classification and Defense Mechanisms", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 8, October 2013.

[17]. Somayeh Soltani, Seyed Amin Hosseini Seno, Maryam Nezhadkamali 1 and Rahmat Budirato, "A Survey On Real World Botnets And Detection Mechanisms", International Journal of Information & Network Security (IJINS), Vol.3, No.2, , pp. 116~127, April 2014.

[18]. Bin Xiao, Wei Chen, Yanxiang He, "A novel approach to detecting DDoS attacks at an early stage", The Journal of Supercomputing, , Volume 36, Issue 3, pp 235–248.

[19]. Fariba Haddadi and A. Nur Zincir-Heywood, "Data Confirmation for Botnet Traffic Analysis".

[20]. Fariba Haddadi, Student Member, "Benchmarking the Effect of Flow Exporters and Protocol Filters on Botnet Traffic Classification", IEEE SYSTEMS JOURNAL, VoL. 10, No. 4, december 2016.

[21]. https://github.com/i-scream/libstatgrab.

ABOUT THE AUTHOR

M.S. Phai Vu Dinh

Workplace: Le Quy Don Technical University

Email: dinhphai88@gmail.com

Research today: He is a Researcher in the Department for Information Security at Le Quy Don Technical University in Vietnam. Since 2013, he has been involved in various research projects and teaching at LQDU. He received his Master's degree in Information Systems from LQDU in 2016. His research interests include network security, wireless security and machine learning.

Dr. Viet Hung Nguyen

Workplace: Le Quy Don Technical University

Email: hungnv@mta.edu.vn

Research today:He graduated with a BA (2006) and a master's degree (2008) from the Moscow University of Technical Physics, specializing in "Neural Computer and Neural Network" and successfully defended the PhD thesis in Russia in 2012, "Systems Analysis, Control and Information Processing". His research interests focus on artificial neural networks and applications; Image and video processing; Parallel computing.

Assoc. Prof. Nguyen Ngoc Tran

Workplace: Le Quy Don Technical University

Email: ngoctn@mta.edu.vn

Research today: He is the Head of Department for Information Security at Le Quy Don Technical University in Vietnam. He received PhD in System analysis, control and information processing from Don State Technical University, Russia. His research interests focus on the pattern recognition, cyber security and artificial intelligence.

BS. Minh Son Duong

Workplace: Brigade 134, Signal Corps, Vietnam Army

Email: dmson1973@gmail.com

Research today: He is the Head of Department of Technique at Brigade 134, Signal Corps. He graduated from Le Quy Don Technical University in 2005 and his research interests focus on circuit design and transmission systems.