ISSN 2278-3091
Volume 8, No.4, July – August 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse88842019.pdf
https://doi.org/10.30534/ijatcse/2019/88842019

A Review of Technique to Self-Generate DDoS Dataset

Ghafar A. Jaafar[1], Shahidan M. Abdullah[2], Saiful Adli [3]
[1,2,3] Razak Faculty of Technology and Informatics,
Universiti Teknologi Malaysia (UTM) 54100 Kuala Lumpur, Malaysia.
[1] afastars@gmail.com
[2] mshahidan@utm.my
[3] saifuladli@utm.my

ABSTRACT

Application Layer Distributed Denial of Service (DDoS) attacks are very challenging to detect and the most common and renowned application layer attack is HTTP flooding. There several approaches adopted by past studies to acquire the dataset such publicly download from and Internet and self-generate by utilizing attack script. Use of old dataset should be prevented as it led to meaningless result. The current available application layer DDoS dataset is obsolete. Furthermore, the latest dataset is not publicly available due to security issue. Hence, DDoS researchers have to move to other atmosphere in order to obtain the latest dataset for DDoS attack execute at application layer. A few attack scripts publicly available which allow researcher to utilize. The attack script requires to work together with actual devices such as a set of computers, web server and other related network devices to create experimental lab. Execution of the attack script also need to pay attention as different attack script utilize different command to run. This paper reviewed 12 techniques utilize by prior studies to self-generate dataset. A summary of each technique is summarized in table view, along with in-depth critical analysis, for future studies to self-generate dataset in conducting DDoS experiment.

Key words: Dataset, DDoS, Application Layer DDoS, HTTP DDoS.

1. INTRODUCTION

A web-based application requires a client to utilize web browser to access a content of the web server. This transaction requires TCP handshake operated at the network layer to successfully establish before the client can reach application layer located at stage seven in Open Systems Interconnection (OSI). During the occurrence of DDoS TCP handshake unable to establish due to massive traffic received at the network layer. Most of the DDoS attack launch at transport and network layer to gain bandwidth and to disrupt services [1]. Mazur, Ksiezopolski [2]. DDoS attacked execute at the network layer by flooding several services, which result to network failure and the attack type publicly known as ICMP flood, SYN Flood and UDP Flood.

DDoS detection at the network layer has emerged year by year. Academician has established sophisticated approach in detecting the attack which makes the attack not really relevant to execute as it can be recognized. Due to this, an attacker changes their attention to execute the attack at the application layer. Yi and Shun-Zheng [3] explained attacker launch DDoS at the application layer when the attack failed to execute at the network layer. DDoS attacks at the application layer capable to mimic the genuine request which makes the attack pattern similar with authentic packet [4-6]. Occurrence of DDoS at the application layer due to settings related to application and function, which allow an attacker to target CPU, memory and network [7, 8]

Numerous approaches produced by past studies to provide solutions in dealing with DDoS. The solution provided by prior studies requires research dataset as the medium to commonly perform as analysis and comparison. However, lack of existence DDoS dataset leads to difficulty for research community to execute research regards to DDoS. This paper presents the review of technique to self-generate dataset for DDoS and highlights several recommendations for future research. Many studies as raise issue pertaining to DDoS dataset, however, none of them provide review regard to technique to self-generate dataset. The self-generate dataset requires technical knowledge as it involve actual equipment to create the experimental lab to generate the dataset. To the best of the authors' knowledge, no recent review has been produced regarding this topic area. The rest of the paper is organized as follows: Section 3 describes DDoS dataset. Section 4.0 until section 4.3 explains the technique to self-generate dataset done by past studies. Section 5.0 until section 5.5 provides a critical analysis regard to DDoS dataset, and lastly the paper is concluded in Section 4.5.

2.DDoS DATASET

A lot of research regards to DDoS has emerged nowadays either to detect the attack at network or application layer. However, the existence of both dataset for research community is very tiny. The atmosphere pertaining to lack of availability DDoS dataset need to be resolved to ensure feature studies provide the meaningful results which possibly will contribute to industry in fighting DDoS. Usage of obsolete dataset should be prevented as it contains

meaningless and ancient data [7], while acquiring actual cutting-edge attack dataset is difficult as they are unavailable publicly [9].

Lack of availability DDoS dataset lead to formation of self-generate dataset. Although some of the dataset are presented the age of the dataset very old. The use of old dataset for benchmark become meaningless, and many studied adopt old dataset and use university or organization web logs [7]. Behal and Kumar [10] highlight prior study utilizes obsolete data and creates self-generate almost similar with real dataset by using network topologies is needed. Behal and Kumar [11] explained most of the existing DDoS dataset capture from network layer and conceal application layer info. Security reason is one of the issues the real dataset is not available for research community [11]. Conducting research related to DDoS lead to complexity due to issue of dataset hence study by [12] utilize simulation software to mimic attack pattern.

The name of old dataset for relates to DDoS attack has been stated by several studies such as [11, 13, 14]. Table 1 shows the old dataset and summary of dataset that utilized by prior studies located at section 2.14.8.

Table 1: DDoS Old Dataset

No	Dataset Name		
1.	KDD Cup Dataset 1999	4.	DARPA DDoS attack dataset 2009
2.	CAIDA DDoS Attack Dataset 2007	5.	Clarknet 1995
3.	Environmental Protection Agency (EPA) HTTP dataset 1995	6.	NASA 1995
7.	MIT Lincoln Laboratory LLSDDoS Dataset 1998	9.	UCLA Dataset 2001
8.	Waikato Internet Trace Storage Project Dataset 2009	10.	TUIDS DDoS Dataset 2012
11.	Booter DNS Dataset 2014	12.	WorldCup 1998

3. TECHNIQUE TO SELF-GENERATE DATASET

This section explorer approach adopted by past studies to self-generate DDoS dataset to validate their proposed solution. This section comprises of three sections such as dataset formulate from simulation software, real attack and regenerate existing dataset.

3.1 DATASET FORMATION - SIMULATION SOFTWARE

Alzahrani and Hong [15] adopt simulation software known as OMNET++ to build normal and attack traffic. According to this researcher's dataset generate from simulation can be utilized to recognize the different type of DDoS attack. The study created a scenario to simulate the occurrence of HTTP DDoS by having a victim web server located at Africa and comprise of two clients to acquire normal and attack traffics. Liao, Li [16] employ existing dataset known as ClarkNet-HTTP to analyst pattern for genuine access. The researchers explained the dataset consisted of plenty of data, hence specific time and date need to select to shrink the scope to constitute self-generate dataset. Since the dataset is huge and replicate, redundant objects were eliminated. The clean dataset from ClarkNet-HTTP is combined with attack dataset which generate from simulation by using software named as MATLAB. Figure 1 shows the architecture.

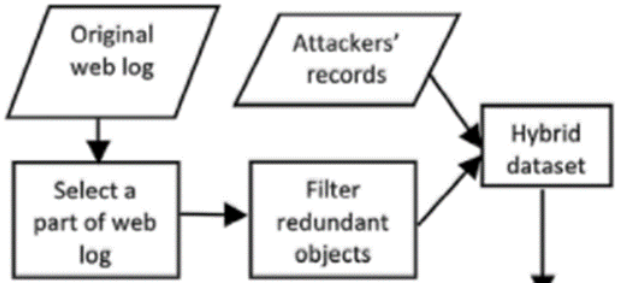

Figure 1: Step to generate hybrid dataset by [16]

3.2 DATASET FORMATION – REAL ATTACK

This section explained about method utilize by prior studies to self-generate dataset by using actual devices. The architecture, devices and attack script to build the dataset is also mentioned throughout this section.

Sree and Saira Bhanu [17] construct authentic dataset from normal browsing activities while adopt the actual attack script for HTTP DDoS to generate attack dataset. The studies utilize publicly known dataset named as HOIC, HTTP DDoS, Hulk. The self-generate dataset is created based on test cases where the attack script is executed individually and combine. The test case and attack script indicated by table 2 while figure 2 shows the architecture.

Table 2: Dataset Test Case

Test Case	Attack Script
1	HOIC
2	HTTP DDoS
3	Hulk
4	Hulk, HTTP DDoS
5	Hulk, HOIC, HTTP DDoS

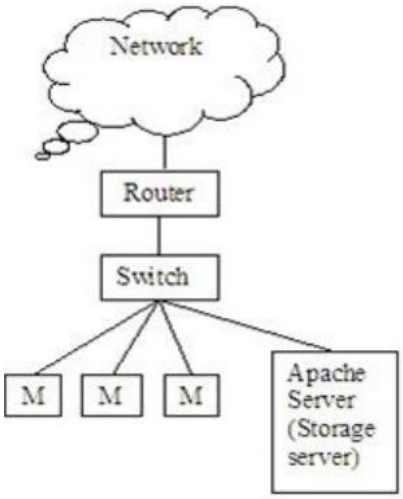

Figure 2: Dataset architecture

Studies by [9] build lab environment consist of a number of machines acted as genuine and attacker and one victim web server. The studies design the lab environment to produce authentic and attack traffic. The attack traffic is generated from the actual attack script publicly known as LOIC and Golden Eye Master. In order to create meaningful HTTP DDoS data, set the studies perform extraction for selected feature comes from normal and attack dataset, which generates at earlier stage. Figure 3 indicates the lab architecture while figure 4 shows the process of dataset formation.

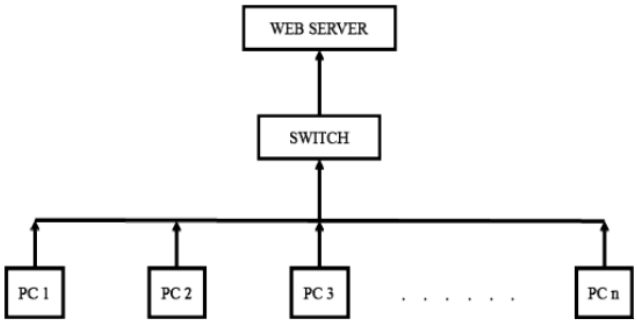

Figure 3 : Lab Architecture by [9]

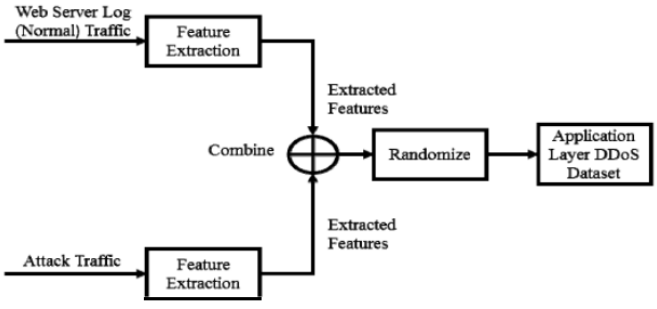

Figure 4: Dataset formation Proses by [9]

Bravo and Mauricio [18] use technique to directly execute the attack script known as LOIC OWASP DOS HTTP POST and GoldenEye. This method also adopt by [19] and execute attack script publicly known as HOIC,HTTP DDoS, HULK, GoldenEye and HULK. Both researches employ actual equipment to execute the attack scripts. Figure 5 shows architecture develop by [19]

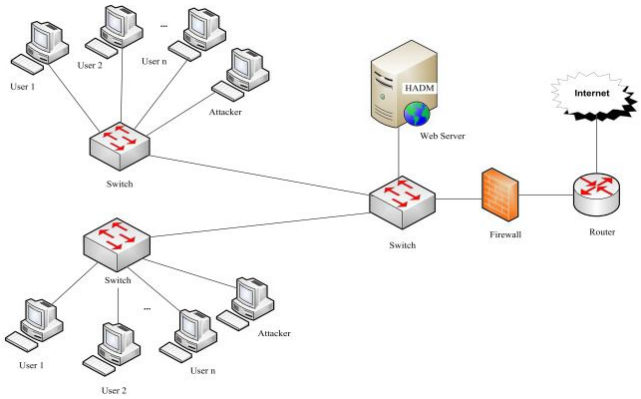

Figure 5 : Dataset formation by [19]

Wang, Liu [20] employs university sub web site and execute attack script known HOIC to create attack dataset. The pattern for normal access is acquire through browsing activity from web site access logs. The studies utilize virtualization technology to have one server and twenty nodes of botnet to launch the attack. This method also was applied by [21] they use virtual apache web server, client and router to architect the environment. Figure 6 demonstrate the architecture.

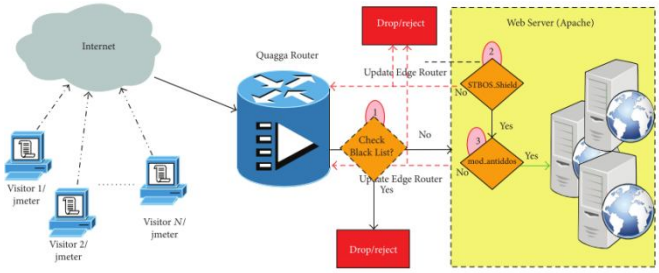

Figure 6 : Dataset formation by [21]

Subbulakshmi, BalaKrishnan [22] elaborate technique to create dataset for DDoS attack occurs at network and application layers. The studies use several machines operate as attacker and authentic users to attack a web server through the Internet as illustrate by figure 7. Attack against a web server is simultaneously launch with the genuine user access to a web server. The studies execute the attack script which requires them to specify the number of attackers, time and victim IP address. A list of type DDoS attack is covered this research such as ICMP flooding, UDP flooding, TCP flooding, Smurf flooding, Land flooding, Port scan, HTTP flooding, Session flooding and IP flooding. The selected attack scripts will produce file based on type of attack and each attack type will separately every thirty minutes. 14 attribute focus by the researchers as shows by table 3.

Table 3: Attribute in Dataset

No.	Attributes		
1.	protocol_type	8.	Service
2.	src_bytes	9.	dst_bytes
3.	Flag	10.	Land
4.	Count_ip	11.	HTTP request rate
5.	Session rate	12.	Packet length
6.	Number TCP packets	12.	Number of TCP src_ports
7.	Number of TCP dst_ports	14.	Number of TCP fin flags

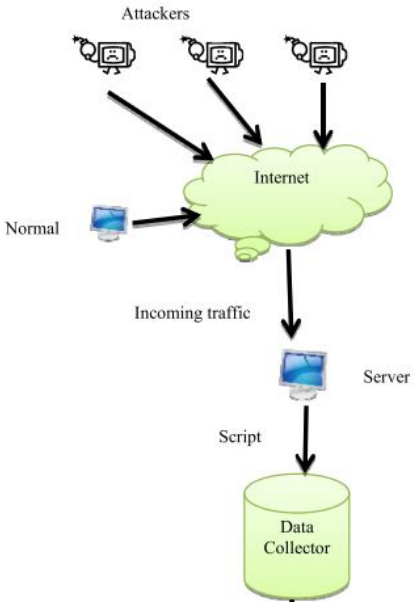

Figure .7: Architecture to Create Dataset

Ghorbani, Habibi Lashkari [23] opted to select various attack types such as Brute Force FTP, Brute Force SSH, DoS, Heartbleed, Web Attack, Infiltration, Botnet and DDoS to construct self-generate dataset. The researchers select specific time and day to execute the attack such as Tuesday morning and afternoon, Thursday and Friday respectively. Dataset for DDoS is generated through variety of attack scripts publicly known as LOIC, HOIC, Hulk, GoldenEye, Slowloris, and Slowhttptest. The architecture to self-generate dataset comprise of victim network and attack network. The victim network is protected by security equipment such as firewall, router and switches. Three server and six clients reside in the victim network while four attack devices to launch the attack are located at the attack network. The self-generate dataset is executed through the Internet. Figure 8 present the architecture to self-generate dataset.

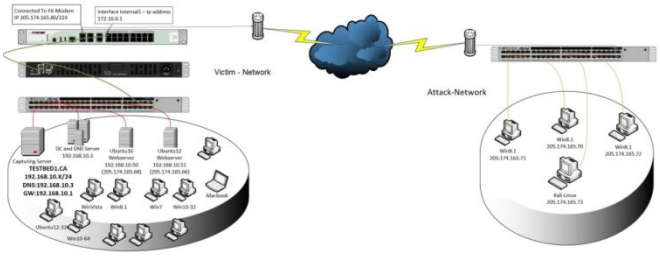

Figure 3.8: Architecture to self-generate dataset

4.DATASET FORMATION - REGENERATE EXISTING DATASETS

Dhanapal and Nithyanandam [13] explained the approach to utilize existing dataset publicly known as FIFA World Cup 1998. According to the researcher's usage of the dataset as it contains diverse GET request from multiple servers. The study employs recreate tool to turn the dataset into the readable format. The technique introduces by this study to regenerate dataset consist of three modules known as HTTP request filtering module to collect web server logs, Client Identifier to Source IP Address Mapping Module to provide various IP addresses to singlet network card to simulate variety IP address comes from HTTP DDoS and HTTP Requests Formatter Flooding Module responsible for mapping IP address after received input from Identifier to Source IP Address Mapping Module. Figure 9 present the steps.

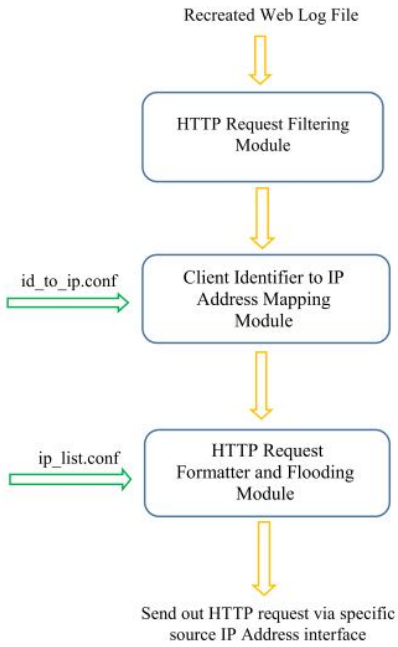

Figure 9: Flow to Regenerate HTTP DDoS Dataset

Studies by [24] employ available dataset due to this formation method for dataset is not presented. Comparison with pass studies indicate all studies employ their architecture.

5. CRITICAL ANALYSIS

This section critically analysis regards to approaches utilize by past studies to self-generate HTTP DDoS dataset. 5 section of critical analysis explain about equipment, configuration, mix dataset, network architecture, and attack script.

5.1 CRITICAL ANALYSIS – EQUIPMENT

This section explains about equipment utilize by prior studies to self-generate dataset. Section 3.2 until section 3.4 reveal all studies employ different hardware, which indicates there is no specific hardware to adopt in order to design isolated lab to self-generate HTTP DDoS dataset. The use of a device as done by [9, 20] like network switch is sufficient to emulate DDoS occurs at the application layer. Besides that, the purpose of academic research is only to acquire dataset and existence of other devices like firewall and web application firewall becomes meaningless. However, for certain circumstance the use of a security device as mention above become meaningful to observe the capability of the attack bypass standard security configuration which commonly utilizes by many organizations to protect their asset. Sree and Bhanu [19] use three equipment like router, firewall and switch while [21] only use router and [17] adopt two equipment known as router and switch. Table 4 shows the summary of equipment use by past studies.

Table 4: Actual equipment employ by past studies

No.	Past Studies	Devices
1.	[17]	Router, Switch
2.	[20]	Switch
3.	[19]	Router, Firewall, Switch
4.	[21]	Router
5.	[9]	Switch

5.2 CRITICAL ANALYSIS – CONFIGURATION

The used of actual hardware require configuration, especially for device like firewall and router. Explanation pertaining to devices configuration provided benefits for another researcher to replicate the same approach and encourage them to perform real experimental rather than simulation as perform by [15, 16]. Furthermore, common practice to configure lab environment for experimental research will facilitate future researchers to conduct experiment lab. Real experiment provides advantages as it close to chances to be deploy in production environment compare then simulation might have compatibility issues. However, for those researcher tents to utilize simulation, they also require providing better explanation pertaining to settings use by them to conduct the simulation to generate dataset or evaluate their proposed work. By doing this method, knowledge sharing among research is improved by providing idea to other studies to conduct research.

5.3 CRITICAL ANALYSIS – MIX DATASET

In actual environment of DDoS attack, genuine and false traffic are mixed up. Mix dataset lead to difficultly to segregate as researchers require more time to spend during the segregation process to ensure dataset is properly segregated. However, this approach only applicable to utilize when it comes to dataset adopt for analysis. To fasten the process to acquire clean dataset which separately contains attack and genuine traffic the generation of dataset should create separately. Utilize public dataset also contain mix traffic hence it is strongly suggested that to self-generate dataset on par with real attack. Dhanapal and Nithyanandam [13] utilize FIFA World Cup 1998 dataset and use recreate tool to turn the dataset into readable format. ClarkNet-HTTP dataset is huge and replicate hence specific duration is needed to turn it into dataset as required [16].

5.4 CRITICAL ANALYSIS – NETWORK ARCHITECTURE

Actual DDoS attack occurs through the Internet hence for an academician who wants to conduct real self-generate dataset they will be facing challenge. Actual self-generate dataset involves many entities such as university network which commonly is the location the research lab located. The university network may receive the impact of the attack which will result to network speed reduces. DDoS attacks consumes resources like bandwidth [25]. Hence special line for this purpose is needed in order to ensure the university network is not jeopardized by experimental work. Besides the university network another entity involves is Internet Services Provider (ISP) although university capable to utilize dedicated line for experiment purpose, the network still requires going through ISP to route the traffic to the Internet to reach a web server that located in somewhere.

Considering this impact most of the past studies as explained at section 3.3 [9, 18-20] utilize the local network architecture where the generated traffic is not passed through to the Internet. Involvement of actual DDoS attack with malicious traffic route to the Internet needs to be caution as the traffic will block by ISP and will jeopardize the creation of dataset. Based on architecture provided by prior studies two studies in this review route the traffic to the Internet [21, 22]. However, these studies did not reveal the duration of the attack is executed. Creation of experiment lab for self-generate dataset by using isolated network and traffic go through internet has difference as illustrated by table 4.

Table 4: Dataset Comparison Generate at Isolated and Through Internet

No.	Generate Dataset Through Isolated Lab	Generate Dataset Through Internet
1.	Attack duration can be more logger as it will not impact user accessibility	Attack duration cannot be longer as the traffic possibly been block by ISP or other third parties.
2.	Minima equipment is sufficient like single switch with several machine comprise of attacker and genuine user.	If the lab is setup from scratch and closely similar with production environment it requires additional hardware like router, firewall to allow user to connect to internet via ISP in order to access Internet.
3.	All utilized devices are fully controlled by the owner.	Devices partially control by the owner as other devices like firewall at ISP is control by them.
4.	Complete attack traffic as all traffic is unblock	Several attack traffic might be block by ISP which will result to self-generate dataset is not fully complete and jeopardize research output

5.5 CRITICAL ANALYSIS – ATTACK SCRIPT

Attacks script utilizes by past study are still uncertain as some of the studies reveal the utilize attack scripts. Attack script to launch HTTP DDoS attack is publicly available. However, it requires technical knowledge to execute the script to launch DDoS attack at the application layer of network layers. Most of the publicly attack script available utilize by prior studies [9, 17-20, 23] as shows by table 5.

Table 5: attack script

No.	Attack Script
1.	HOIC
2.	HTTP DDoS
3.	Hulk
4.	LOIC
5.	Golden Eye Master

Technical knowledge is one of the challenges facing by academician as the actual attack script requires experiment lab to set up machine acted as the authentic and attack machine. Apart from that, academicians require multi discipline knowledge such as security and network practically to successfully design, configure and execute the real attack. Therefore, some of the prior studies [15, 16] tent to utilize simulation approach as develop experiment is time consuming, besides require actual hardware and technical knowledge. This study found that research requires dataset mainly for analysis of attack traffic. Utilize the existing dataset to evaluate propose detection to recognize HTTP DDoS is still unclear. Self-generate dataset for analysis and rerun the execution of attack in real environment is the best option to be opted.

6.0 RECOMMENDATION FOR FUTURE RESEARCH

Future research supposed to consider conducting research for DDoS by adopting real equipment. Due to lack of DDoS dataset presented publicly as explain at section **Error! Reference source not found.**, self-generate dataset is strongly suggested. Besides self-generate dataset, evaluation of the proposed work by using real equipment also provides several advantages such as the outcome of the research has higher possibility to utilize in a production network environment as the proposed work had been programmed to be running in the real device. Hence this section provides a suggestion for architecture, and settings can be done by future research to utilize real hardware on generating self-generate dataset and for evaluation. Suggested solution to combat DDoS are academic interest and only a few execute in real time [10, 26]

6.1 GENERATE DATASET FOR ANALYSIS PURPOSE

Usage of security equipment should be prevented to ensure all attack pattern delivery precise without block by the device. The architecture to self-generate dataset is simple as one network switch, server and machine are sufficient. Besides that, this design does not require details configuration on the network level compare than mimic production environment, which had firewall and requires proper. Figure 10 illustrate the possible architecture to self-generate dataset for analysis purposes.

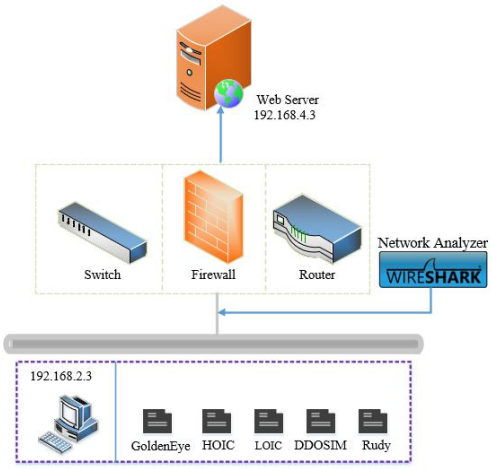

Figure 10: Architecture to self-generate dataset

6.2 GENERATE DATASET FOR EVALUATION PURPOSE

The propose work must be existed either source-end, core-end and victim-end. Beitollahi and Deconinck [6] explained defense against DDoS can be located as stated above. Figure 11 illustrate the architecture.

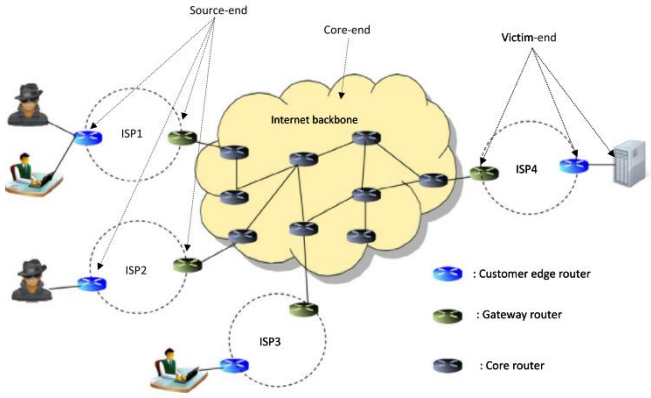

Figure 11: DDoS Defense Location

Future research can implement Victim-End defense and utilize the reactive approach. According to Beitollahi and Deconinck [6] the reactive approach utilizes victim resources. Combination of Victim-End and reactive result to formation of lab experiment where the propose solution will be placed at in front of the web server, and administrator has full control against usage of the equipment use in experiment lab. Figure 12 illustrate the possible architecture to implement in research lab.

- **i)** Propose Solution > (Firewall or Switch or Router) > Web Server
- **ii)** (Firewall or Switch, or Router) > Propose Solution > Web Server
- **iii)** Propose Solution > (Firewall, Switch, Router) > Propose Solution > Web Server

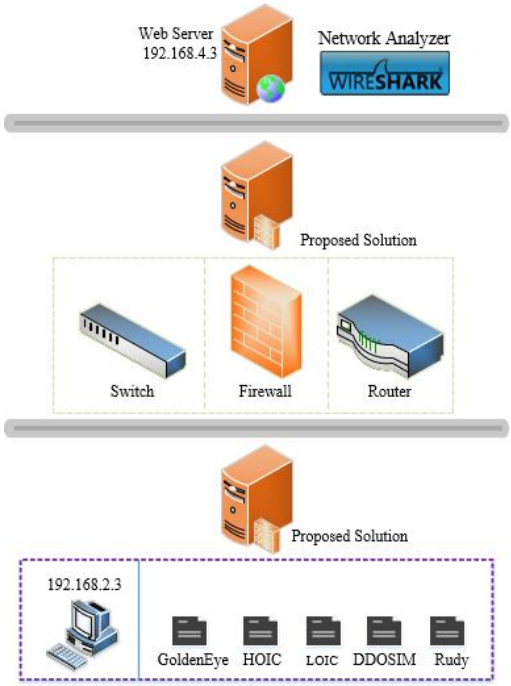

Figure 12: Suggest architecture for evaluation

The last option provides redundant filter due to cater miss detection occurs at first defense will be covered by second filter. During the occurrence of DDoS detection device will overload due to higher traffic received hence malicious traffic might be able to bypass detection device. Due to this circumstance second filter will be the last defense to filter incoming traffic before reach a web server. Future research also can placed propose work on either

6.3 IP ADDRESS CONFIGURATION AND NETWORK ROUTING

Both architecture (Architecture Analysis & Evaluation) requires IP address. The IP address for client and server can be setup static and use class C network such as 192.168. X.X. To facilitate experiment lab both machine (client and server) require same network segment otherwise network routing need to be configured, which require another hardware like firewall and router.

6.4 WEB SERVER CONFIGURATION

Future research can utilize Windows Server operating system trial version which available to download for free. The windows server will be acted as host to manage the client requests to obtain the content of the web server. A simple HTML page can be created as simulation. Usage of windows server is strongly suggested as it provide easy configuration, however usage of open source operating system like Ubuntu and Fedora also provides capabilities to host HTML page.

6.5 ATTACK SCRIPT AND PROGRAMMING SKILL

To self-generate DDoS data set attack script is one of the essential components need to be consider. Usage of the most adopted attack script is much suggested as it is proven that the attack contains DDoS pattern. Attack script that publicly available has a specific name, for instance, HOIC, LOIC, Hulk, Rudy, DDOSIM, Bonesi, PyLoris, XOIC, and Slowloris, highlighted and adopted by earlier researchers [27-30]. Some of the attack script stated also utilizes by prior research as reveal by section 5.5. Future researcher can utilize the script as stated above to self-generate dataset which directly will reduce dependency on publicly available dataset which had issues as discuss at section 3.0.

Besides that, most of the attack script that has capabilities to execute DDoS attack is written in python programming languages. Hence learning the programming language provides advantages as more info can acquire such as the researcher to explorer about the possible attack strategy can be executed, and deeper understanding can be acquired especially on how the attack works to overwhelmed server or network.

6.6 NETWORK RESOURCES AND ATTACK SCALE

Use of devices as a cyber army such as smart phone, camera, television is the possible approached can be taken by future research to create DDoS dataset. Aside from that, generate the dataset by adopting 5G network is the alternative need to be explore by future research. The 5G network provides higher speed for smart phone and other devices [31]. DDoS attacks also can be executed at cloud and it comprises several levels such as application bug level, infrastructure level, direct attack, network and transport layer, application layer and reflector as stated by [32]. Hence self-dataset can be generated by choosing one of the levels to acquire verity attack pattern generated from DDoS.

6.7 ATTACK DURATION

Attack duration is one of the critical factors to decide. For the purpose of the experimental one-minute time frame consider sufficient as one TCP connection allows to deliver multiple GET request [32]. Launch the attack more than one minute had specific drawbacks such as plenty GET request generated introduce to delay in filtering the traffic when it comes to analysis process. Besides that, DDoS attacks are continuously sent in high rate and repeatedly the patterns. Execution of the attack in longer time result to be meaningless as the purpose only to gain attack pattern. The one-minute time duration to execute the attack considers appropriate to be utilized as all patterns are delivered in high rate.

7.CONCLUSION

This paper presents a review of the technique to self-generate DDoS dataset. Researches against DDoS attack have acquired much attention nowadays. However, lack of availability of the research dataset become challenges as adopted old data set result to meaningless result as it shows the proposed solution only capable of to work with old attack pattern. Fresh data set for DDoS is not publicly available hence researchers are strongly suggested to self-generate the data set. The self-generate dataset allow researcher to understand the attack code which will directly to understand the attack strategy. Besides that, researchers had full control against devices and attack scripts that utilize to constitute the data set. The critical analysis has highlighted several points that need attention and recommendation has outlined several points would provide

ACKNOWLEDGEMENT

This research paper was compiled at University Technology Malaysia (UTM).

REFERENCES

1. Zolotukhin, M., et al. *Increasing web service availability by detecting application-layer DDoS attacks in encrypted traffic*. in *Telecommunications (ICT), 2016 23rd International Conference on (pp. 1-6). IEEE*. 2016. IEEE. https://doi.org/10.1109/ICT.2016.7500408
2. Mazur, K., B. Ksiezopolski, and R. Nielek, *Multilevel Modeling of Distributed Denial of Service Attacks in Wireless Sensor Networks.* Journal of Sensors, 2016. **2016**: p. 1-13.
3. Yi, X. and Y. Shun-Zheng, *Monitoring the Application-Layer DDoS Attacks for Popular Websites.* IEEE/ACM Transactions on Networking, 2009. **17**(1): p. 15-25.
4. Subramanian, K., P. Gunasekaran, and M. Selvaraj, *Two Layer Defending Mechanism against DDoS Attacks.* International Arab Journal of Information Technology (IAJIT), 2015. **12**(4).
5. Yuan, X., C. Li, and X. Li. *DeepDefense: Identifying DDoS Attack via Deep Learning*. in *Smart Computing (SMARTCOMP), 2017 IEEE International Conference on*. 2017. IEEE. https://doi.org/10.1109/SMARTCOMP.2017.7946998
6. Beitollahi, H. and G. Deconinck, *Analyzing well-known countermeasures against distributed denial of service attacks.* Computer Communications, 2012. **35**(11): p. 1312-1332.
7. Singh, K., P. Singh, and K. Kumar, *Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges.* Computers & Security, 2017. **65**: p. 344-372.
8. Ni, T., et al., *Real-Time Detection of Application-Layer DDoS Attack Using Time Series Analysis.* Journal of Control Science and Engineering, 2013. **2013**: p. 1-6.
9. Yadav, S. and S. Selvakumar. *Detection of application layer DDoS attack by modeling user behavior using logistic regression*. in *Reliability, Infocom Technologies and Optimization*

(ICRITO)(Trends and Future Directions), 2015 4th International Conference on. 2015. IEEE. https://doi.org/10.1109/ICRITO.2015.7359289

10. Behal, S. and K. Kumar, *Detection of DDoS attacks and flash events using novel information theory metrics.* Computer Networks, 2017. **116**: p. 96-110.
11. Behal, S. and K. Kumar, *Trends in Validation of DDoS Research*, in *International Conference on Computational Modeling and Security (CMS 2016)*. 2016, Elsevier. p. 7-15.
12. Wang, J., et al., *HTTP-SoLDiER: An HTTP-flooding attack detection scheme with the large deviation principle*. Science China Information Sciences, 2014. **57**(10): p. 1-15.
13. Dhanapal, A. and P. Nithyanandam. *An effective mechanism to regenerate HTTP flooding DDoS attack using real time data set*. in *2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*. 2017. IEEE.
14. Singh, K., P. Singh, and K. Kumar, *User behavior analytics-based classification of application layer HTTP-GET flood attacks.* Journal of Network and Computer Applications, 2018. **112**: p. 97-114.
15. Alzahrani, S. and L. Hong, *Generation of DDoS Attack Dataset for Effective IDS Development and Evaluation.* Journal of Information Security, 2018. **09**(04): p. 225-241.
16. Liao, Q., et al., *Application layer DDoS attack detection using cluster with label based on sparse vector decomposition and rhythm matching.* Security and Communication Networks, 2015. **8**(17): p. 3111-3120.
17. Sree, T.R. and S.M. Saira Bhanu, *Investigation of Application Layer DDoS Attacks Using Clustering Techniques.* International Journal of Wireless and Microwave Technologies, 2018. **8**(3): p. 1-13. https://doi.org/10.5815/ijwmt.2018.03.01
18. Bravo, S. and D. Mauricio. *DDoS attack detection mechanism in the application layer using user features*. in *2018 International Conference on Information and Computer Technologies (ICICT)*. 2018.
19. Sree, T.R. and S.M.S. Bhanu, *HADM: detection of HTTP GET flooding attacks by using Analytical hierarchical process and Dempster-Shafer theory with MapReduce.* Security and Communication Networks, 2016. **9**(17): p. 4341-4357.
20. Wang, Y., et al. *A novel approach for countering application layer DDoS attacks*. in *2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*. 2017.
21. Saleh, M.A. and A. Abdul Manaf, *A Novel Protective Framework for Defeating HTTP-Based Denial of Service and Distributed Denial of Service Attacks.* ScientificWorldJournal, 2015. **2015**: p. 238230.
22. Subbulakshmi, T., et al. *Detection of DDoS attacks using Enhanced Support Vector Machines with real time generated dataset*. in *2011 Third International Conference on Advanced Computing*. 2011. IEEE.
23. Ghorbani, A.A., A. Habibi Lashkari, and I. Sharafaldin, *Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization*, in *Proceedings of the 4th International Conference on Information Systems Security and Privacy*. 2018. p. 108-116.
24. Sreeram, I. and V.P.K. Vuppala, *HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm.* Applied Computing and Informatics, 2017.
25. Singh, K., K.S. Dhindsa, and B. Bhushan, *Distributed Defense: An Edge over Centralized Defense against DDos Attacks.* International Journal of Computer Network & Information Security, 2017. **9**(3).
26. Behal, S., K. Kumar, and M. Sachdeva, *Characterizing DDoS attacks and flash events: Review, research gaps and future directions.* Computer Science Review, 2017. **25**: p. 101-114. https://doi.org/10.1016/j.cosrev.2017.07.003
27. Kumar, V. and K. Kumar. *Classification of DDoS attack tools and its handling techniques and strategy at application layer*. in *Advances in Computing, Communication, & Automation (ICACCA)(Fall), International Conference on (pp. 1-6)*. 2016. IEEE.
28. Johnson Singh, K., K. Thongam, and T. De, *Entropy-Based Application Layer DDoS Attack Detection Using Artificial Neural Networks.* Entropy, 2016. **18**(10).
29. Singh, K.J. and T. De, *MLP-GA based algorithm to detect application layer DDoS attack.* Journal of Information Security and Applications, 2017. **36**: p. 145-153.
30. Shiaeles, S.N. and M. Papadaki, *FHSD: An Improved IP Spoof Detection Method for Web DDoS Attacks.* The Computer Journal, 2014. **58**(4): p. 892-903. https://doi.org/10.1093/comjnl/bxu007
31. Amin Salih Mohammed, et al., *Analysis of Mobile IP Wireless Networks in 5G.* International Journal of Advanced Trends in Computer Science and Engineering, 2019. **Volume 8, No.1.2, 2019**: p. 1-4.
32. Ziyad R. Al Ashhab, et al., *Detection of HTTP Flooding DDoS Attack using Hadoop with MapReduce : A Survey.* International Journal of Advanced Trends in Computer Science and Engineering, 2019. **Volume 8, No.1, January – February 2019**: p. 1-7.