2018 9th International Conference on Information Technology in Medicine and Education

Evaluation of Several Denial of Service Attack Methods for IoT System

Yumeng Cui, Qianli Liu, Kai Zheng, Xin Huang
Department of Computer Science and Software Engineering,
Xi'an Jiaotong-Liverpool University, China,
Yumeng.Cui16@student.xjtlu.edu.cn, Qianli.Liu16@student.xjtlu.edu.cn
Kai.Zheng@xjtlu.edu.cn, Xin.Huang@xjtlu.edu.cn

***Abstract*— Recently, the online cheating and attacking posed a threat to net safety. As an important component of the development of the information era, the Internet of Things (IoT) would cause serious property losses once it is attacked. This experiment is to use 3 devices to simulate the principle of the Denial of Service (DoS) attack. The attack is launched by Kali Linux in different ways. Furthermore, this paper lists the changed variables of the experiment and shows how the influence can be caused.**

Keywords*— *Denial of Service (DoS) attack, Kali Linux, Internet of Things (IoT).

I. Introduction

In the past decades, Internet of Things was proposed as a innovative technology which have a dramatic impact on human life. The aim of Internet of Things is to integrate the physical and digital worlds in one single ecosystem [1]. However, it has become a widely concern that these innovative theory may cause safety issues. To avoid the potential risk that civilian may divulge their private information, it is essential for the users to comprehend the principle of the different attack techniques to eavesdrop the citizen's information, among which the DoS attack is regarded as one of the most popular attacking methods.

The definition of DoS attack focuses on out-of-order, which attempt to make a device unavailable to its intended users. There are several ways to achieve the attack. It commonly consists of efforts to temporarily or indefinitely interrupt or suspend services of a host [2]. Before taking an experiment on the DoS attack, there are necessities prepared in advanced. The necessities contain one PC computer, one Router, one Sensor node and one attacker based on the virtual machine that is based on the Kali-Linux system. The Kali-Linux is developed by the Debin's release version of Linux system, which preassembles numerous penetrations testing software, such as nmap, Wireshark and Ettercap [3]. It supports programs that Windows system does not support and thus suitable for the experiment.

The contribution of this paper is listed as follows:

- Change and compare different variables to find the lowest standards to launch a successful attack (packets' sizes and packets' amount).
- Analyze the performance of the DoS attack (success time and loss rate).
- Detect the impact on the attacker (CPU utility and Memory utility of the attacker PC).

In section II, some related works are listed so as to serve as a comparison, thus, to enhance the intention of the paper. Section III will demonstrate the preparation and the principle of the experiment. Section IV will discuss the results of the experiment and at section V, a conclusion will be given.

II. Related work

In this section, a brief overview of related works will be provided in order to make comparisons between several works focusing on variables and indicators.

A. Overview of Related Work

Among the related works researching in the DoS attack, [4] fixed their main context on attacking efficiency under different packet size, transmit frequency and qualified the attacking methods on NTP and ICMP. [5] focused on SYN flooding attack and TCP connect flooding attack. In their paper, sending ratio and packet size were chosen as variables. [6] took success time of attack, packet loss rate, CPU utility and Memory utility of the PC as four key parameters describing the efficiency of hping3 and SYN flood attack.[7], supported by their experiment, introduced two novel attacking methods—sleep disturbance attack and channel disturbance attack as new threaten to IoT system. [8] analyzed the Internet Control Message Protocol flood with different packets size.

B. Comparison

The comparison, as shown in the following table, listed main differences among related works. Though some works may share part of the context, different variables were chosen. For instance, sending ration and transmit frequency are two novel variable that may influence the attacking efficiency. During the experiment, our group detected that the amount of packets sent will lead to the change of attacking performance. As several works proposed, packet size Is a vital variable for different attacking methods. Hence, in our experiment, packet size was discussed. Additionally, to apply the optimal indicator of attacking performance, our team introduced more indicators than other team, including the condition of hardware and data related to responding.

TABLE I. Comparison With Related Works In Accordance With Changing Variables And Different Methods

	Changing packets' size	Changing packets' amount	Attacker numbers

2474-3828/18/$31.00 ©2018 IEEE
DOI 10.1109/ITME.2018.00179

[4]	Yes	No	1
[5]	Yes	No	1
[6]	Yes	No	1
[7]	No	No	1
[8]	Yes	No	1
Our work	Yes	Yes	1/2/3

III. System Design

The DoS attacking is described as the flood attack because the mean to broke the targeted machine by transmitting superfluous requests in order to overload the system [9]. In addition, the legitimate requests from the users are prevented. The experimental equipment can be observed in the Figure 1 [6]. As shown in the figure, PC performs as a platform permits user putting data and installing software, router connects PC, Sensor nodes and the virtual machines, sensor node can retrieve data from PC and Kali Linux launching an attack.

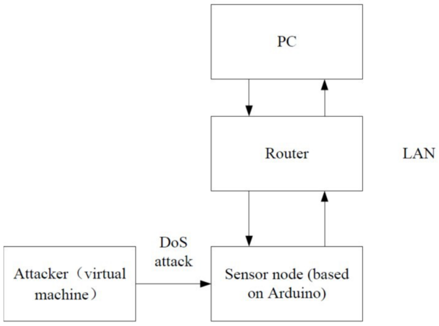


Fig. 1. The Principle of DoS Attack [6]

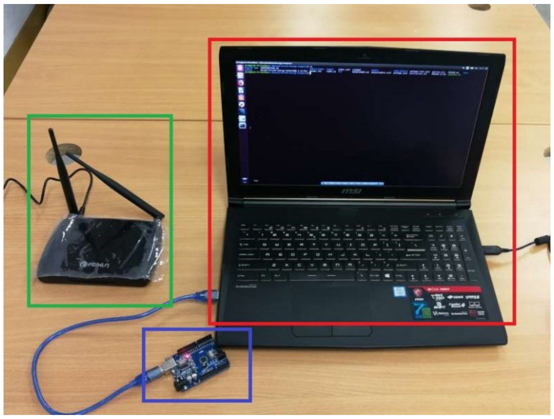
IV. The Experiment Platform For DoS Attack

A. The Experiment Platform for DoS attack

The experiment platform is composed by the following components:

- **PC:** The PC connected to the Router can obtains the information from the sensor node, and it permits user putting data and installing software.
- **Router:** The function of Router is acting as a connector, which can establish a LAN (local area network) by connecting the PC, Sensor nodes and the virtual machines.
- **Sensor node (based on Ardunio):** The sensor node depends on Arduino can be regarded as a recorder that recodes the data from the PC and the Kali-Linux system. In our experiment, the expansion board is not used, because there is Wi-Fi modules on the sensor, which could also make the sensor connected with Ethernet.
- **Attacker (Kali Linux):** The attacker is the Kali-Linux system installed in the PC.

B. The Experiment Equipment in the Lab



🟥 **PC** 🟦 **Sensor** 🟩 **Router**

Fig. 2. The Experiment Equipment

As shown in the Figure 2, the whole set of equipment entails a PC, a router, and a sensor node. Notably, the sensor node is connected to the LAN via the router.

V. The Process Of DoS Attack Experiment

A. The Preparation For The Experiment

In order to attack the sensor node, PC should send a large amount of packets to the sensor node. Hence, sensor node and PC should be connected to the LAN which is provided by router, and the IP addresses of PC, virtual machine and sensor nodes would also be assigned to the router [6]. IP addresses of devices are extremely significant because they are the logical addresses of every device on the network, and every PC on the Internet needs its unique IP address to communicate properly. Initially, the IP address of each experiment device should be investigated clearly. As shown in Table II, the equipment and their IP addresses were listed, additionally, the MAC addresses and the roles are also shown accordingly.

TABLE II: The Ip Address Of Different Devices

Device	**IP Address**	**MAC Address**	**Role**
PC	192.168.1.100	B8-81-98-08-4E-A5	Server

Virtual Machine on PC	192.168.56.1	0A-00-27-00-00-08	Attacker
Arduino development board	192.168.1.160	0xDE, 0xAD, 0xBE, 0xEF, 0xFE, 0xED	Victim
TP-LINK router	192.168.1.1	Fe80::53c:d4b9:78db:73b2%2	Local Network Gateway

Before attacking the sensor node, we input ping command to the PC to check the connection between PC and the sensor node. PC will send a test packet to the sensor node according to the ping command. The ping command requires the feedback of the sensor node which contains the packet with same size. For both initial status and sending ping command status, the average response time of the sensor node, CPU utility and memory utility of PC will be tested. Table III shows the test results.

TABLE III: Test Result For Initial Status And Sending Ping Commend Status

Status	**CPU utility**	**Memory utility**	**Average Response time**
Initial status	9%	49%	/
Sending ping command status	10%	51%	7ms

Finding. Both in these two conditions, the CPU utility is low and the memory utility is not high. In terms of average response time, it is very short. Hence, the connection between the PC and the sensor node is smooth and unrestricted.

Figure 3 gives the response time of the first ten packets, and the horizontal axis represents the nth response and the vertical axis represents the response time (ms).

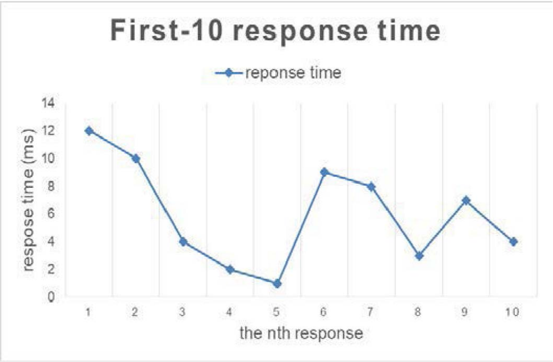


Fig. 3. The Response Time of the First Ten Packets

Finding. Even though the response time of the first ten packets is undulant and floating, generally the response time is very short which means the connection between PC and the sensor node is smooth and unrestricted.

B. DoS Attack Using Hping3 With Random SourceIP

Launch the hping3 command in the terminal of Kali Linux ”hping3 –c 1000 –d 10 –S –w 64 –p 80 —flood —rand-source targetIP”. “targetIP” stands for the victim IP address. “hping3” is the name of the application binary. “- c” means the number of packets to send and “-c 1000” means there are sending 1000 packets. “-d 10” stands for the size of each packet is 10 bytes that was sent to target machine. “-S” means the attacker only send SYN packets. “-w 64” stands for TCP window size. “-p 80” is the destina- tion port and 80 is the HTTP port. “—flood” is the flood mode which means sending packets as fast as possible, without taking care to show incoming replies. “—rand- source” stands for using random source IP addresses to at- tack victim IP addresses withoutexposing.

During those experiments, packets size and packets amount were chosen as variable. CPU and memory utility, in addition to success time and lose rate were set to be the indicator reflecting the attacking efficiency.

TABLE IV: Experiment Result For DoS Attack Using Hping3 With Different Size Of Packets

Size of packets(bytes)	CPU utility (%)	Memory utility (%)	Time for success of attack(s)	Packet loss rate(%)
5	32	43	119.12	16
10	41	44	72.61	22
15	51	47	58.23	25

Finding. Table IV demonstrates that the memory utility changes in a narrow range. As the size of packets increased, the time for success of attack will reduce while the packet loss rate increased as well. In conclusion, within certain range, the bigger packet size it sends, the more remarkable efficiency DoS attack will have.

TABLE VII: Comparison Of Other Related Works

	[6]	Our work
Packet Size	600 bytes	15 bytes
Packet Amount	10000	2000
CPU utility	79%	59%
Memory utility	63%	48%
Time of success attack	42s	47.91s
Loss Rate	48.2%	36%

Finding. As shown in Table VII, the experiment indicates that, the DoS attack can be conducted with packet with rather small size and littleamount.

TABLE V: EXPERIMENT RESULT FOR DOS ATTACK USING Hping3 WITH DIFFERENT AMOUNT OF PACKETS

Amount of packets (15bytes)	CPU utility (%)	Memory utility (%)	Time for success of attack(s)	Packet loss rate (%)
1000	51	47	58.23	25
2000	59	48	47.91	36

Finding. The further experiment implies that the amount that packets being sent also have an impact on the response time. Within certain range, the larger the amount of packets is sent, the less successful time it has.

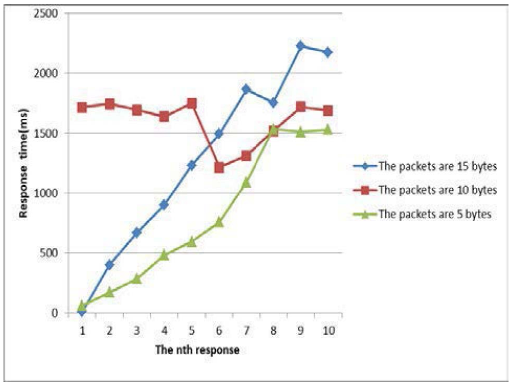


Fig. 3. The relation between response time and packet size

Finding. Figure 3 implied that, by changing the packets with increased size, the response time will increase, which indicates the DoS attack may have a more efficient performance.

C. *Multiple Computers Attack One TargetSimultaneously*

The number of attacker is another factor may affect the attacking performance. To enhance the attacking efficiency, multiple attackers can be applied to one target. The experiment demonstrated the result of attack when the amount of attacker changed. CPU and memory utility coupled with loss rate and success time was chosen as indicators.

TABLE VIII: CPU AND MEMORY UTILITY RESULT FOR MULTIPLE ATTACKERS USING Hping3 WITH SIZE 5 AMOUNT 1000

CPU/Memory Utility	Initial state	Apply one attacker	Apply two attackers	Apply three attackers
Attacker1	7%/79 %	27%/80 %	29%/80 %	29%/80 %
Attacker2	6%/80 %	N/A	27%/80 %	28%/80 %
Attacker3	6%/79 %	N/A	N/A	23%/89 %

Finding. As shown in Table VIII, the attacking process may lead to the increase of CPU and memory utility. However, the relation between attacker numbers and CPU and memory utility remain unclear. In a word, the number of attacker may not have a detectable impact on CPU and memory utility.

TABLE IX: LOSS RATE AND SUCCESS TIME RESULT FOR MULTIPLE ATTACKERS USING Hping3 WITH SIZE 5 AMOUNT 1000

	Apply one attacker	Apply two attackers	Apply three attackers
Loss rate	15%	27%	35%
Success time	108.56s	61.49s	43.26s

Finding. As shown in Table IX, within certain range, the attacking efficiency can be improved when the number of attacker increased. With the number of attacker increased, the loss rate may increase and the success time may shorten.

V. CONCLUSION

The report demonstrates the process how three types of attack commenced by Kali Linux achieved its purpose to paralyze an IoT system. The result indicates that within certain range, the increasing size of packets and greater amount of packets will expedite the attacking process. Moreover, the number of attackers may also affect the attacking result. The result suggested that more attackers may result in a better attacking performance for its less success time and increased loss rate. However, CPU and memory utility do not has an obvious relation with attacker amount. Further experiment is needed either to preclude usability of these indicators or to find deeperrelations.

ACKNOWLEDGEMENT

This work was supported by the XJTLU research development fund projects under Grant RDF140243and Grant

RDF150246, in part by the National Natural Science Foundation of China under Grant No. 61701418, in part by Innovation Projects of The Next Generation Internet Technology under Grant NGII20170301, in part by the Suzhou Science and Technology Development Plan under Grant SYG201516, and in part by the Jiangsu Province National Science Foundation under Grant BK20150376

References

[1] Y. Al-Halabi et al., *Study on access control approaches in the context of Internet of Things: A survey*. 2017 International Conference on Engineering and Technology (ICET), pp. 1-7, 2017

[2] D. Yin et al., *A DDoS Attack Detection and Mitigation with Software-Defined Internet of Things Framework*. IEEE Access, pp. 1-1, 2018.

[3] R. Gaddam and M. Nandhini, *An analysis of various snort based techniques to detect and prevent intrusions in networks proposal with code refactoring snort tool in Kali Linux environment.* 2017 International Conference on Inventive Communication and Computational Technologies *(ICICCT)*, 2017, pp. 10-15.

[4] Ming Cheng, Yichao Xu, Kai Zheng, Xin Huang. A Denial of Service Attack for IoT System. 2018 Symposium on Information Technology and Education (SITE2018), Suzhou, China, Suzhou, China, 2018.

[5] Yuexuan Li, Kun Wang, Qiankun Sheng, Xin Huang. A Denial of Sleep Attack Against IoT System. 2018 Symposium on Information Technology and Education (SITE2018), Suzhou, China, Suzhou, China, 2018.

[6] K. Zheng et al., *A Denial of Service Attack Method for an IoT System*. 2016 8th International Conference on Information Technology in Medicine and Education (ITME), pp. 360-364, 2016.

[7] Liang L, Zheng K, Sheng Q, et al. A Denial of Service Attack Method for IoT System in Photovoltaic Energy System[C]// International Conference on Network and System Security. Springer, Cham, 2017:613-622.

[8] Zhiyong Liu, Kai Zheng, Xin Huang. Analysis of the Impact of ICMP Flood Attack in IoT System. 2018 Symposium on Information Technology and Education (SITE2018), Suzhou, China, Suzhou, China, 2018.

[9] N. Tripathi et al., How Secure are Web Servers? *An Empirical Study of Slow HTTP DoS Attacks and Detection. 2016 11th International Conference on Availability, Reliability and Security (ARES)*, pp. 454-463, 2016.