A Denial of Service Attack Method for an IoT System

[1]Lulu Liang, [2]Kai Zheng, [2]Qiankun Sheng, [2]Xin Huang
[1]China Information Technology Security Evaluation Center
Leung.bjtu@gmail.com
[2]Department of Computer Science and Software Engineering,
Xi'an Jiaotong-Liverpool University, China,
Kai.Zheng14@student.xjtlu.edu.cn, Qiankun.Sheng 11@student.xjtlu.edu.cn, Xin.Huang@xjtlu.edu.cn

***Abstract*—In recent years, Internet of things (IoT) is widely used in various domains. However, the security of the IoT system becomes a challenge. If the IoT system is attacked, a great property loss will happen. In this paper, a denial of service (DoS) attack to an IoT system is shown. The attack tool is Kali Linux, A Denial of Service (DOS) attack is launched by using 3 different methods. The comparison between the 3 DoS attack methods is also given.**

Keywords— Internet of things (IoT), Denial of Service (DOS) attack, Kali Linux.

I. INTRODUCTION

The Internet of Things (IoT) is a novel paradigm that is rapidly gaining ground in the scenario of modern wireless telecommunications [1]. The IoT can be described as connecting everyday objects together automatically to enable new functions [2]

The IoT enables us to collect rich real-time data such as temperature and radiation. According to the collected data, the monitoring and control of all kinds of system can be improved. Due to the advantages of IoT, this technique is used in various domains such as environmental monitoring, smart building, disaster management system and healthcare monitoring system, [3-6]. In recent years, many countries have their plans for developing IoT [7] and the number of IoT devices is fast increasing.

However, the cyber-attack for IoT will bring great loss to residents and industries. According to [8], the IoT system is vulnerable to some cyber-attack like Denial of Service (DoS) attack, selective forwarding, bogus routing information and eavesdropping. Among the cyber-attack, DOS attack is a widely used method [9]. Due to the threat of cyber-attack, the security analysis of IoT system is essential.

For the security of IoT system, there are many related works. In [10], a tool for DoS attack on IoT is designed. In [11, 12], security of frameworks of IoT is introduced. In [13-17], a security framework of intelligent building networks are introduced. In this paper, these related works are also helpful for the experiment

In this paper, a DoS attack method for IoT system is designed and implemented. A DoS attack is launched to attack the target IoT system with different methods, while the experiment results can help to analyze the effect of cyber-attack methods. The contribution in this paper is shown as following:

- Launch a DoS attack on the simple IoT system in by using Kali Linux with different methods.
- The time for attacking, CPU utility, memory utility and the success rate of attacking is given.
- The comparison of different DoS attack methods is shown and the factors influence the performance of attack are analyzed.

The paper is organized as follows. Section II introduces the experiment platform. Section III shows the process of DoS attack. Section IV is the conclusion part.

II. THE EXPERIMENT PLATFORM FOR DOS ATTACK

A. DoS Attack

A Denial-of-Service attack is an attack which can be used to influence the connection of network, making it inaccessible to its intended users. DoS attack is realized by flooding the target with traffic, or sending it information to triggers a crash [18]. It is one of the most popular cyber-attack methods in security of network. Victims of DoS attack are often the web servers of high-profile organizations such as banking, commerce and media companies

B. The Framework of Experiment Platform

The framework of our experiment platform is shown in Figure 1, the attacker is also included.

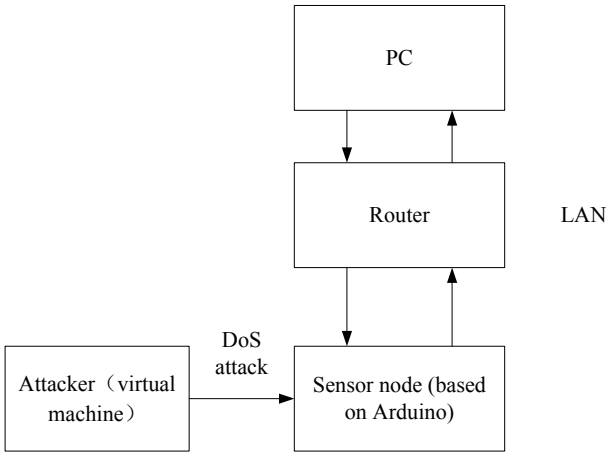

Fig.1.The framework of our IoT system

The experiment platform consists of the following components:

978-1-5090-3906-7/16 $31.00 © 2016 IEEE
DOI 10.1109/ITME.2016.154

- **PC:** The PC can get the data abstained by sensor node, and provide the data to the users by using some applications.
- **Router:** The router connects the PC, sensor nodes and the virtual machine as a LAN(local area network)**.** The router can give IP addresses to the PC, virtual machine and Arduino. In normal case, the connection between sensor node and PC is unobstructed.
- **Sensor node (based on Arduino):** The sensor node is based on Arduino, which can record the data of surrounding environment such as temperature and humidity.
- **Attacker (Kali Linux):** The attacker is Kali Linux, which is installed in a PC as a virtual machine.

In normal case, the sensor records the data and transfer the data to the PC via router. The applications in PC will show the data to the users. The communication between PC and sensor node is also unrestricted. However, the attacker (Kali Linux) can launch a DoS attack at the sensor node, which will influence the connection between PC and sensor node.

C. *The Experiment Equipment in The Lab*

The equipment in the lab is shown in Figure 2.

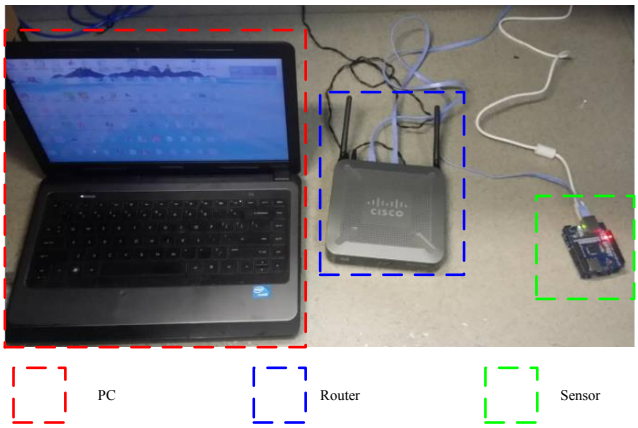

Fig. 2. The equipments in the lab

The red box stands for the PC, the blue box stands for the router, and the green box is the sensor node. The sensor node is connected to the LAN via the router.

D. *Kali Linux*

The attack tool is Kali Linux, which is installed in the PC as a virtual machine. Kali Linux is a Debian-derived Linux distribution which can be used for digital forensics and penetration testing [19]. Kali Linux is preinstalled with over 300 penetration-testing programs, including Armitage (a graphical cyber-attack management tool), nmap (a port scanner), Wireshark (a packet analyzer) and so on.

The tools which are used in this experiment are the terminal of Kali Linux and Wireshark. The terminal of Kali Linux is use to launch DoS attack. Wireshark is a packet analyzer to analyse the DoS attack.

III. THE PROCESS OF DOS ATTACK EXPERIMENT

A. *The Preparation for The Experiment*

The PC and sensor node are connected to the LAN via router, and the router gives IP address to PC, virtual machine and sensor nodes. Firstly, the IP addresses of different components should be found out. The components and their IP addresses are shown in Table I.

TABLE I. THE IP ADRESSES OF DIFFERENT COMPONENTS

Device	IP Address	MAC Address	Role
PC	192.168.1.175	20:10:7a:61:67:82	Server
Virtual Machine on PC	192.168.1.197	08:00:27:5f:01:f9	Attacker
Arduino development board	192.168.1.177	de:ad:be:ef:fe:ed	Victim
Cisco router	192.168.1.1	ac:f2:c5:97:3a:02	Local Network Gateway

We first use ping command to check the connection between sensor node and PC. The PC send a ping command to the sensor node, IP address of this sensor node is 192.168.1.177. For both initial status and sending ping command status, the response time of sensor node, CPU utility and computer memory utility of the PC are tested. The experiment results are shown in Table II.

TABLE II. EXPERIMENT RESULTS FOR INITIAL STATUS AND SENDING PING COMMAND STATUS

Status	CPU utility	Memory utility	Response time(average)
Initial status	13%	54%	/
Sending ping command status	18%	61%	9.8ms

Finding. For the 2 status, the CPU utility of the PC is low, and the memory utility of the PC is not high. The response time for ping command is very short. This means that the connection between PC and sensor node is unrestricted.

The response time for 10 packets is shown in Figure 3:

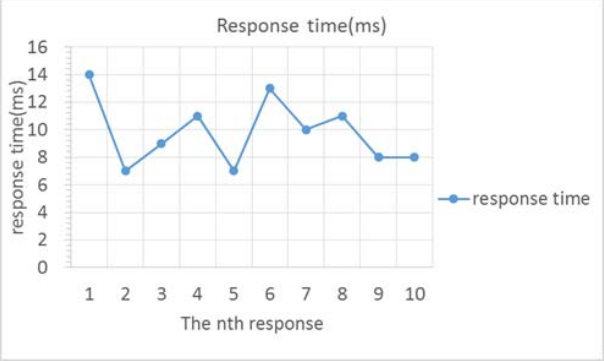

Fig.3. The response time of the sensor node

Finding. Figure 3 shows that the response time is fluctuating, but overall the response time is very short, which also means that the connection between PC and sensor node is unrestricted.

B. DoS Attack Using Hping3 With Random Source IP

In the Kali, open the terminal and input the command "hping3 –c 10000 –d 1200 –S –w 64 –p 6633 –flood –rand-source targetIP". "targetIP" would be filled with the victim IP address. "hping3" means the program command. "-c 10000" means the number of packets to send is 10000. "-d 1200" means the size of each packet that was sent to target machine is 1200 bytes. "-S" means sending SYN packets only. "-w 64" means the TCP window size. "-p 6633" means the destination port. "-flood" means sending packets as fast as possible, without taking care to show incoming replies. "-rand-source" means using random source IP address to hide the track.

In this set of experiments, the sizes of packets which are sent by the attackers are different. The packets are 600 bytes, 1200 bytes and 1800 bytes, which is realized by changing the value of "-d" in the command. After the DoS attack is launched, the ping command is also used to verify the connection between sensor node and PC. The time for attack when first packet lost (time for success of attack), the packet loss rate of different attack methods, memory utility, CPU utility are shown in Table III. Around 150 packets are sent by PC. The packet loss after attack can be calculated. The time for success of attack means the time when first packet loss occurs.

TABLE III. EXPERIMENT RESULTS FOR DOS ATTACK USING HPING3 WITH DIFFERENT SIZE OF PACKETS

Size of packets	CPU utility	Memory utility	Time for success of attack	packet loss rate
600 bytes	79%	63%	42s	48.2%
1200 bytes	90%	65%	16s	90.3%
1800 bytes	93%	67%	14s	93.2%

Finding. Table III shows that CPU utility of the computer is proportional to the size of packets. The change of memory utility is small when the size of packets changes. When the size of packets increases, the times for success of attack decrease while the packet loss rate increase. In another words, the effect of DoS attack is better with the increasing of packet size.

The response time for 10 packets is shown in Figure 4:

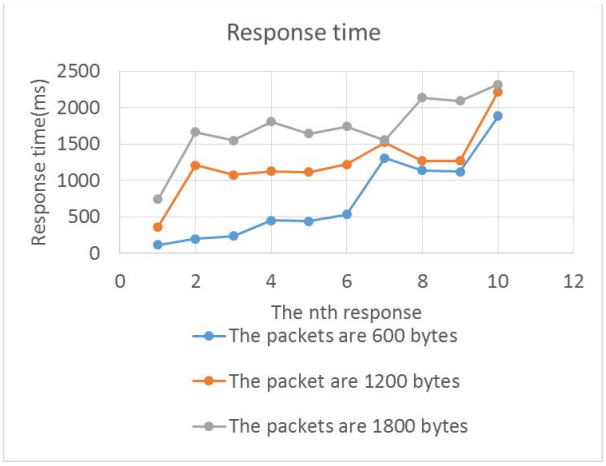

Fig.4.The response time of the sensor node when the size of packets increases

Finding. In Figure 4, the response time is proportional to the size of packets. The increasing of response time means the better attack performance. It can be concluded that the larger packets are, the better attack performance. The DoS attack can be analyzed in Wireshark, which is shown in Figure 5.

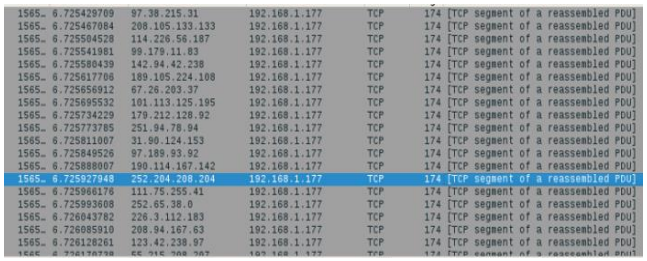

Fig.5 The experiment result in Wireshark

Finding. It can be seen from the Figure 5 that the attacker continue to send packets to the victim by using random IP addresses, which means that the DoS attack is successful.

C. Simple SYN Flood With Sproofed IP

Another command also can be used to launch a DoS attack to the simple IoT system. Compared with formal one, the destination port number is not necessary to be known.

The command is "hping3 –S –P –U –flood –V –rand-source targetIP". The meaning of "hping3",-S", "-flood" and "–rand-source" are same with formal command. "-P" means the packets were marked with PUSH. "-U" means the packets were marked with URG.

D. TCP Connect Flood

Then a SYN flood combined with TCP connect was tested. The command is "nping –tcp-connect –rate=90000 –c 9000000 –q targetIP". "Nping" means the program executed to DOS attack. "–tcp-connect" means unprivileged TCP connect probe mode. "-rate = 90000" means the rate of attacking is 90000. "-c

900000" means that stop the attack after 9000000 rounds. "-q" means decrease verbosity level by one.

E. Compareation of The 3 DoS Attack Methods

The time for success of attack, the packet loss rate, memory utility, CPU utility of the 3 DoS attack methods are shown in Table IV. Around 150 packets are sent by PC and the packet loss rate is calculated. DoS attack using hping3 with random source IP is method 1, simple SYN flood with proofed IP is method 2, TCP connect flood is method 3.

TABLE IV. EXPERIMENT RESULTS FOR THE THREE DOS ATTACK METHODS

3 DoS attack methods	CPU utility	Memory utility	Time for success of attack	packet loss rate
DoS attack using hping3 with random source IP(1200bytes)	90%	65%	16s	90.3%
Simple SYN flood with proofed IP	79%	64%	19s	19.5%
TCP connect flood	93%	90%	20s	28%

Finding. In Table IV, the comparison between the 3 DoS attack methods are shown. The CPU utility of method 1 and method 3 is very high. The memory utility of method 3 is much higher than others. The difference of time for success of attack is small. For the packet loss rate, method 1 have the highest packets loss rate, which means the method 1 has the best attack performance.

The response time for 10 ping command of the 3 different methods are shown in Figure 6.

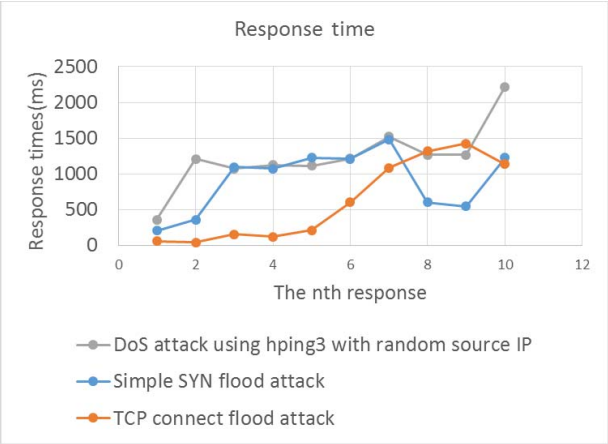

Fig.6. The response time of sensor node by using different DoS attack method

Finding. Figure 6 also shows that method 1 has the best performance because the response time increases quickly. For method 2 and method 3, the performance of method 2 is better.

IV. CONCLUSION

In this paper, an IoT system is set up as a target system. A DoS attack is launched by using Kali Linux with 3 different methods. The experiment results show that the DoS attack influenced the connection between the sensor node and PC. For method 1, the experiment results show that the larger size of packets, the better performance of the attack. The comparison between the 3 methods is also given. The experiment results show that method 1 has the best performance, the performance of method 2 is better than method 3.

In further study, more attack methods will be studied and the effect of the attack methods will be analyzed.

ACKNOWLEDGED

This work has been supported by the XJTLU research development fund projects RDF140243 and RDF150246, as well as by the Suzhou Science and Technology Development Plan under grant SYG201516, and Jiangsu Province National Science Foundation under grant BK20150376.

This work was supported in part by the Natural Science Foundation of China under Grant No. 61401517,in part by the National High Technology Research and Development Program("863"Program) of China under Grant No. 2015AA016001

REFERENCES

[1] K., "The Internet of Things: A survey," Computer Networks, vol. 54, pp. 2787-2805, 2010.

[2] M. Grabovica, S. Popić, D. Pezer, and V. Knežević, "Provided security measures of enabling technologies in Internet of Things (IoT): A survey," in Zooming Innovation in Consumer Electronics International Conference, 2016.

[3] M. Navarro, T. W. Davis, G. Villalba, Y. Li, X. Zhong, N. Erratt, et al., "Towards Long-Term Multi-Hop WSN Deployments for Environmental Monitoring: An Experimental Network Evaluation," Journal of Sensor & Actuator Networks, vol. 3, pp. 297-330, 2014.

[4] S. Saha and M. Matsumoto, "A framework for disaster management system and WSN protocol for rescue operation," in TENCON 2007 - 2007 IEEE Region 10 Conference, 2007, pp. 1 - 4.

[5] V. Vaidehi, M. Vardhini, H. Yogeshwaran, G. Inbasagar, R. Bhargavi, and C. S. Hemalatha, "Agent Based Health Monitoring of Elderly People in Indoor Environments Using Wireless Sensor Networks," Procedia Computer Science, vol. 19, pp. 64–71, 2013.

[6] R. Xu, X. Huang, J. Zhang, Y. Lu and G. Wu. "Software Defined Intelligent Building". International Journal of Information Security and Privacy (IJISP), 9(3): 84-99, 2015.

[7] L. Linlu, "Comparative Study on the Development of IOT(Internet of Things)Policy in China and European Union—— Based on and," Sci-Tech Information Development & Economy, 2014.

[8] K. Zhao and L. Ge, "A Survey on the Internet of Things Security," in International Conference on Computational Intelligence & Security, 2013, pp. 663-667.

[9] S. Alanazi, J. Al-Muhtadi, A. Derhab, and K. Saleem, "On resilience of Wireless Mesh routing protocol against DoS attacks in IoT-based ambient assisted living applications," in International Conference on E-Health Networking, Application & Services, 2015.

[10] C. Bao, X.Guan, Q.Sheng, K. Zheng, and X. Huang, " A Tool for Denial of Service Attack Testing in IoT " presented at the 1st Conference on emerging topics in interactive systems, Suzhou, 2016.
[11] N. Xue, X. Huang and J. Zhang. “S2Net: A Security Framework for Software Defined Intelligent Building Networks”. The IEEE International Conference on Trust, Security and Privacy in Computing and Communications. Tianjin, China, 2016.
[12] Nian Xue, Lulu Liang, Xin Huang, Jie Zhang. POSTER: A Framework for IoT Reprogramming. 12th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2016), Guangzhou, China, 10-12 October, 2016.
[13] X. Huang, P. Craig, H. Lin and Z. Yan. “SecIoT: a security framework for the Internet of Things”. Security and Communication Networks, 2015.
[14] Yiwen Wang, Xin Huang, Guanglei Cong, He Zhu, Shuangyuan Yu, Tingting Zhang. Privacy and security aware home sensor system. 2010 Cross-Strait Conference on Information Science and Technology, Qinhuangdao, China, 2010.
[15] Weihan Bo, Yiling Zhang, Xianbin Hong, Hanrong Sun, Xin Huang. Usable Security Mechanisms in Smart Building. In Proceeding of 2014 IEEE 17th International Conference on Computational Science and Engineering (CSE), pp.748-753, 19-21 Dec. 2014.
[16] Xin Huang, Weihan Bo, Yiling Zhang, Na Gong. I-Lock: A Phone-Based Access Control System. International Conference on Computing and Technology Innovation (CTI 2015), Luton, UK, May 2015
[17] Nian Xue, Lulu Liang, Jie Zhang, Xin Huang. An Access Control System for Intelligent Buildings. Accepted by The 9th EAI International Conference on Mobile Multimedia Communications (MOBIMEDIA 2016), Xi'an, China, June 18–19, 2016
[18] S. Alanazi, J. Al-Muhtadi, A. Derhab, and K. Saleem, "On resilience of Wireless Mesh routing protocol against DoS attacks in IoT-based ambient assisted living applications," in International Conference on E-Health Networking, Application & Services, 2015.
[19] J. A. Ansari, "Web Penetration Testing with Kali Linux," 2015.