Denial of Service Attack in IPv6 Duplicate Address Detection Process

An Impact Analysis on IPv6 Address Auto-configuration Mechanism

Shafiq Ul Rehman, Selvakumar Manickam
National Advanced IPv6 Centre (NAv6)
University of Science Malaysia
Penang, Malaysia

***Abstract*—IPv6 was designed to replace the existing Internet Protocol, that is, IPv4. The main advantage of IPv6 over IPv4 is the vastness of address space. In addition, various improvements were brought to IPv6 to address the drawbacks in IPv4. Nevertheless, as with any new technology, IPv6 suffers from various security vulnerabilities. One of the vulnerabilities discovered allows Denial of Service Attack using the Duplicate Address Detection mechanism. In order to study and analyse this attack, an IPv6 security testbed was designed and implemented. This paper presents our experience with the deployment and operation of the testbed, and discussion on the outcome and data gathered from carrying out DoS attack in this testbed.**

***Keywords*—Duplicate Address Detection; Denial of Service; IPv6; Address autoconfiguration; Security; Internet Protocol**

I. Introduction

Internet protocol version 6 (IPv6) [1], was introduced not only to overcome the limitations of an existing Internet protocol version 4 (IPv4) [2] but also be future oriented due to the rapid growth of Internet technologies. Thus, IPv6 is also known as a next generation Internet protocol. In December 1998, Internet Engineering Task Force (IETF) defined this new Internet protocol. In addition, to provide large address space, new features were introduced in IPv6 such as; simpler header format, mobility functions, extension header, as well as address autoconfiguration [1].

One of the main features of IPv6 protocol is address autoconfiguration [3], which means IPv6 host(s) can obtain IP address automatically. Therefore, autoconfiguration can simplify addressing assignment among IPv6 hosts in link local communication as hosts can generate addresses without any intervention. Even though it has eased IP addressing assignment, improper configuration can raise serious security issues. Studies [4-6] have proven that autoconfiguration mechanism is susceptible to security threats like denial of service (DoS) attacks during address autoconfiguration process.

This paper focuses on the impact analysis of denial of service (DoS) attack [7] on duplicate address detection (DAD) [6] process during address autoconfiguration in IPv6 link local network and its consequences. The rest of the paper is organized as follows.

Section II of this article describes the concept of denial of service (DoS) attack and its classifications. Section III explains the address autoconfiguration process in IPv6 link local network, including duplicate address detection (DAD) process and the denial of service attack attempts during DAD process in respective subsections. Section IV presents the design and implementation of testbed setup based on DoS-on-DAD attack. Section V depicts the outcome obtained from the experimental setup. Finally, Section VI concludes this article with future work.

II. Denial of Service Attack and its Classification

Denial of service (DoS) attack is one of the major security threats to the IPv4 and IPv6 networks [7]. In DoS attacks, a victim host(s) can be denied from the services by wasting its resources and disrupt its communication with other neighboring hosts on same link. A targeted device is unable to process such large amount of network traffic and becomes unavailable or out of service.

Moreover, when DoS attack is being attempted from large networks or systems then it is known as Distributed Denial of Service (DDoS) attacks [7, 8]. In order to perform DDoS attack, an attackers uses various resources such as network nodes and Internet services which are distributed around the globe considered as botnets. Later, these botnets are used to launch the DDoS attack against the targeted victim.

A. Denial of service attacks on IPv6 network

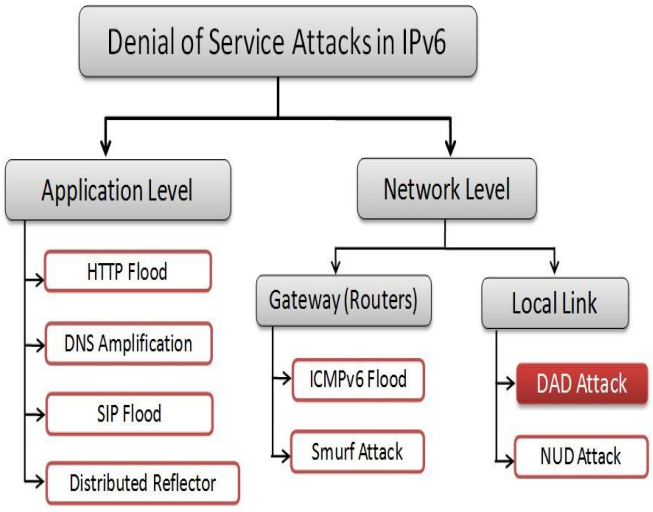


Fig. 1. Taxonomy of DoS attacks in IPv6 network

Denial of Service (DoS) attacks in IPv6 network can be broadly classified into two main categories based on the attacked level such as; application level and network level. Further network level DoS attacks can be subdivided into gateway (router) and local link levels respectively. Figure 1 depicts the taxonomy of DoS attacks in IPv6 network.

During address autoconfiguration in IPv6 link local network, Internet control message protocol (ICMPv6) [9] message types are used by the hosts to communicate with neighboring hosts within a local link. However, studies [10, 11] have shown that ICMPv6 messages are vulnerable to denial of service (DoS) attacks, especially during duplicate address detection (DAD) process while host(s) attempts to configure its own generated interface identifier (IID).

Therefore, an attacker can take an advantage of it and can fabricate these ICMPv6 messages. Later, attacker can exploit these modified messages to generate denial of service (DoS) attacks in a number of ways; either by spoofing the messages, Man-in-the-Middle form or simply sending excessive numbers of bogus ICMPv6 packets to the target host on the local link. Thus, an attacker can disrupt the IPv6 hosts to obtain their interface identifier (IID).

III. Address Autoconfiguration in IPv6 Link Local Network

In IPv6 Link local network, IPv6 host can communicate with other neighboring hosts by using five types of ICMPv6 messages also known as Neighbor Discovery Protocol (NDP) [12] messages are as follows:

- Router Solicitation (RS) message type 133, is send by IPv6 hosts to discover the presence of a neighboring router(s) on local link.
- Router Advertisement (RA) message type 134, is sends by router(s) in reply to a RS message or periodically advertises the RA messages.
- Neighbor Solicitation (NS) message type 135, is send by IPv6 nodes to resolve IPv6 address to its link-layer address (MAC address) or to verify IPv6 node reachability or to perform duplicate address detection.
- Neighbor Advertisement (NA) message type 135, is send by IPv6 nodes in response to a NS message or to advertise a link-layer address change.
- Redirect message type 137, is send by routers in IPv6 Link local communication to advertise better route for a destination.

Neighbor discovery [12], as the name suggests, in IPv6 networks allow the hosts to find the presence and link local addresses of other hosts on the same link. Also, it provides other functionalities such as address resolution, neighbor unreachability detection, router discovery, redirect method for routers to inform IPv6 hosts about the most appropriate router available on the same link and resolve duplicate address detection on the same link .

A. IPv6 Address Autoconfiguration Process

When a new host joins an IPv6 local link network, it goes through a number of operations to configure its own Interface identifier (IID). As IPv6 host connects to local link network, it sends a Router Solicitation (RS) message to a link local router to get the network prefix information. In response, link local router replies with a Router Advertisement (RA) message by sending network prefix. Once the host has gathered that network prefix can now generate its interface identifier (IID) [3].

Afterwards, the host combines the subnet prefix with the IID to form a complete 128 bits IPv6 address which is enough for hosts to communicate within a same link [3]. Finally, an autoconfiguration process verifies its uniqueness on a link by performing a Duplicate Address Detection process [6] that will be discussed in Subsection B. Figure 2 depicts new host address autoconfiguration process in IPv6 link local network.

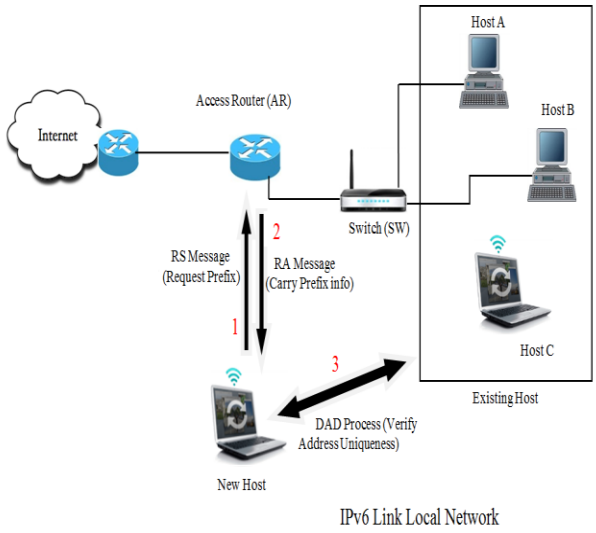


Fig. 2. IPv6 address autoconfiguration process

B. Duplicate Address Detection Process

Duplicate address detection is a mechanism ensuring that all the IPv6 hosts have unique IP addresses by verifying their uniqueness on the same link. Every host must execute DAD process before specifying an address to an interface [6]. When host(s) generate new IP addresses, after generating an interface identifier host(s) ascertain that no other neighboring host(s) already possesses that generated address on the same link to avoid the IP address conflict.

DAD process is being performed by sending Neighbor Solicitation (NS) messages multicast to all neighboring hosts within a same link. These NS messages carry the tentative IP address that the host(s) has generated and would like to assign as its interface identifier. If the tentative address is already assigned by any other neighboring host within a same link, then that neighboring host will send a Neighbor Advertisement (NA) in reply. Hence, new host generates a

new tentative address. In next attempt, if a new host does not receive any response to its NS messages from the neighboring nodes; it indicates that the newly generated address is unique and no other neighboring host is using this address. Thus, a host can use that generated address as preferred address as an interface identifier [6]. Figure 3 illustrates the DAD process.

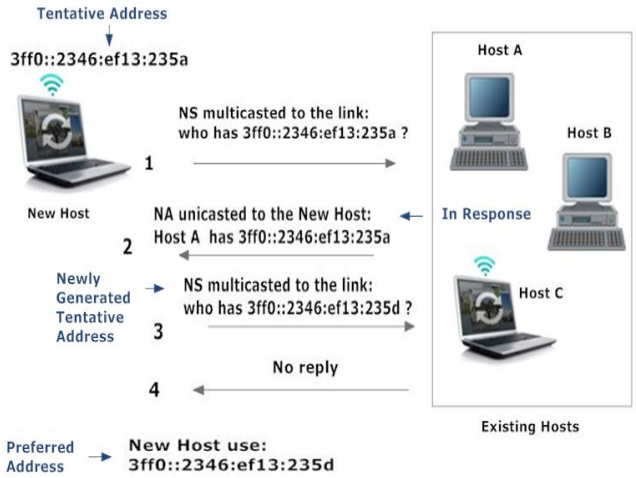


Fig. 3. Duplicate address detection process

C. Denial of Service Attack on DAD Process

During the DAD operation, an attacker can disguise the victim host while attempting to verify its address uniqueness in IPv6 link local communication by using the specific address and responds to every detection message. Thus, it the victim host may be unable to configure its IP address such type of attack is known as DoS on DAD attack. During this attack an attacker can respond to every duplicate address detection attempts made by a newly joining host in IPv6 link local communication. In case an attacker claims addresses, the other host(s) on a same link will never be able to configure an IP address [6]. Figure 4 illustrates the DoS on DAD attack.

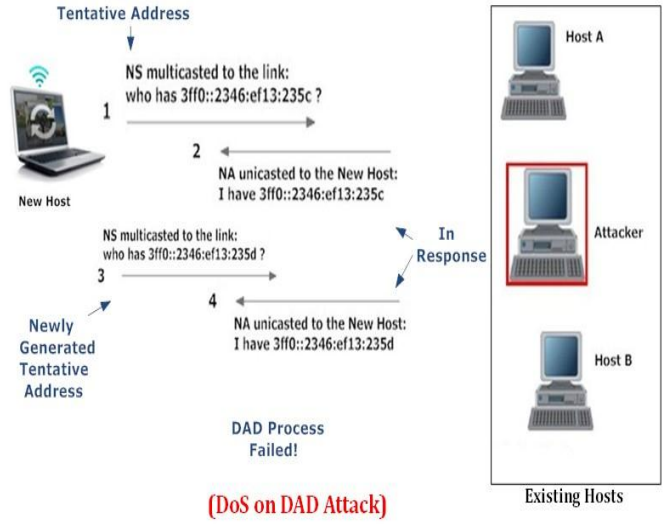


Fig. 4. Denial of service attack on DAD process

IV. Design and Implementation of Testbed Setup

Beginning with the assumptions this section describes the design and implementation of testbed setup scenario for the experiment required. In order to conduct the test on DoS-on-DAD attack in IPv6 networks; a closed IPv6 network setup environment has been deployed at the National Advanced IPv6 Center (NAv6) research Institute, University Sains Malaysia (USM).

A. Assumptions

In order to design and implement the proposed testbed, the following assumptions have been considered to conduct the experiments successfully such as:

- IPv6 local network comprises of at least one gateway router, an ethernet switch, a new host, existing hosts and an attacker host.
- IPv6 address in the local network is obtained from SLAAC mechanism instead of using DHCPv6 server.
- The number of attacker hosts in an IPv6 local network are less than the number of legitimate hosts

Based on the assumptions the required hardware and software specifications for testbed setup environment are presented in Tables 1 and 2, respectively.

The hardware and software specifications have been selected based on the availability and support for IPv6 environment at NAv6 research institute to conduct the experiment successfully.

TABLE I. Details on Hardware Required for the Experiments

Hardware		Details
Computer Hardware	CPU	Intel® Core™ i7 3770 / 3.40GHz
	Memory	8 GB Ram
	Motherboard	IntelQ77 Express Chipset
	Network Interface Card	Intel® 82579LM Gigabit1 Ethernet LAN 10/100/1000
Other Network Devices	Network Patch cables	Digitus UTP Cat5e
	Switch	Cisco Catalyst 2960 Fast Ethernet
	Gateway Router	Cisco Router C7200

TABLE II. DETAILS ON SOFTWARE REQUIRED FOR THE EXPERIMENTS

Operating System		Role	Tools
Microsoft Windows	Windows 7 Ultimate 64-bit	Monitoring/ Victim Host	Wireshark
	Windows Vista Home Premium 64-bit	Victim Host	-
Linux Distributions	Ubuntu 14.04 LTS-desktop-amd64	Victim Host	-
	Fedora 3.17.4.x86_64	Victim Host	-
	Kali Linux 3.18.0-amd64	Attacker PC	THC IPv6 Attack Toolkit 2.7

Testbed setup environment comprises hosts (Host A, Host B, Host C and Host D) based on Windows as well as Linux Operating Systems so that to run the experiment on both the platforms in order to analyses the impact of DoS-on-DAD attack as the design and implementation of IPv6 stack in these Operating Systems differ slightly in some manners [13].

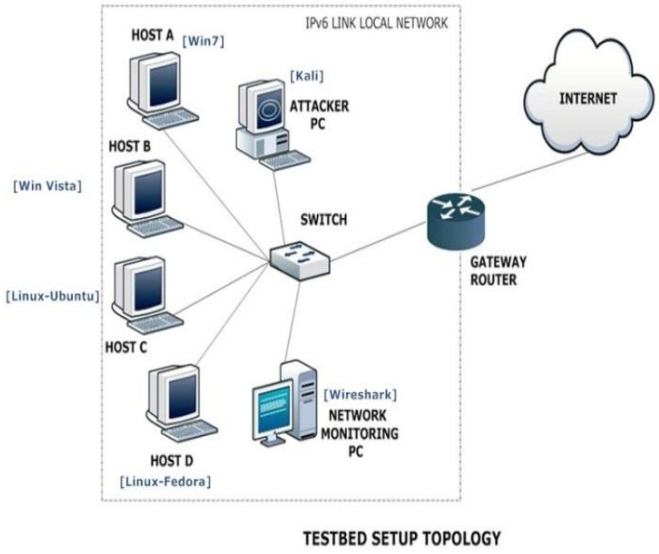


Fig. 5. Testbed setup environment

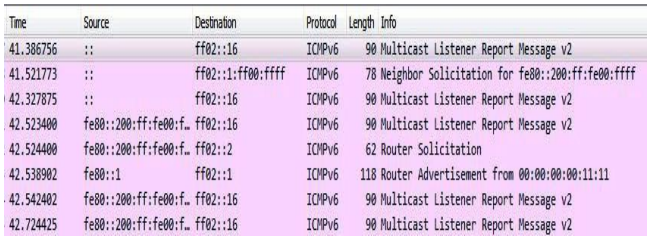
The Hackers Choice (THC) attacking toolkit [14] provides a set of tools that can enable the user to explore weaknesses in existing IPv6 implementations. One of the tools, called dos-new-ip6, can be used to run the DoS attack on DAD process in IPv6 local link network. Kali is a Linux-based open source system; it has built-in THC-IPv6 attacking toolkit support. Therefore, Kali have been used as an Attacker PC to exploit the testbed setup environment.

In order to monitor and capture the network traffic Wireshark [15, 16] network analyser tool has been used to analyse the captured network traffic. Cisco router C7200 has been used as a gateway router for the network and Cisco catalyst 2960 fast ethernet switch has been used to connect all the hosts in IPv6 link local network. Figure 5 depicts the testbed setup environment.

A. Senario Based testbed Setup

Based on the deployed IPv6 testbed setup environment, two experimental scenarios have been conducted such as: Normal Scenario and Attacking Scenario.

- Normal Scenario: In case of normal scenario, a default DAD process during address autoconfiguration in IPv6 link local communication has been analysed by capturing the ICMPv6 message types like RS, RA, NS and NA in Wireshark network analyzer tool as shown in Figure 6.



Time	Source	Destination	Protocol	Length	Info
41.386756	::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
41.521773	::	ff02::1:ff00:ffff	ICMPv6	78	Neighbor Solicitation for fe80::200:ff:fe00:ffff
42.327875	::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
42.523400	fe80::200:ff:fe00:f…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
42.524400	fe80::200:ff:fe00:f…	ff02::2	ICMPv6	62	Router Solicitation
42.538902	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from 00:00:00:00:11:11
42.542402	fe80::200:ff:fe00:f…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
42.724425	fe80::200:ff:fe00:f…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2

Fig. 6. ICMPv6 packets traffic analyses

In order to investigate the DAD process on various platforms, address autoconfiguration process has been performed on hosts with different Operating Systems such as Windows (Win7, Win Vista) and Linux (Ubuntu, Fedora) on a deployed IPv6 Testbed setup. After successful DAD process hosts are able to configure their preferred IPv6 link local addresses. Figure 7 depicts the Windows host after configuring its IPv6 link local address.

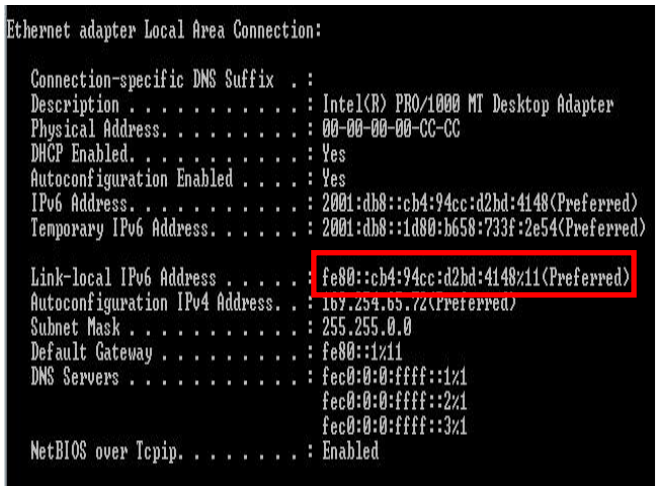


Fig. 7. Snapshot of Window's host IPv6 address autoconfiguration.

Likewise, Figure 8 shows that Linux based host after successful DAD process configured its link local address in IPv6 network.

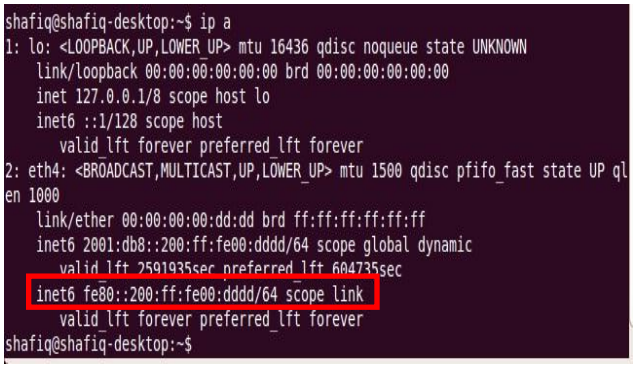


Fig. 8. Snapshot of Linux host Address Autoconfiguration

- Attacking Scenario: In attacking scenario, an attempt of DoS-on-DAD attack during address autoconfiguration in IPv6 link local communication has been examined by capturing the ICMPv6 message types like RS, RA, NS and NA in Wireshark network analyser tool as shown in Figure 9.

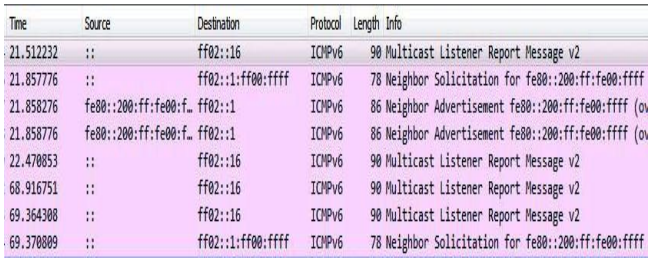
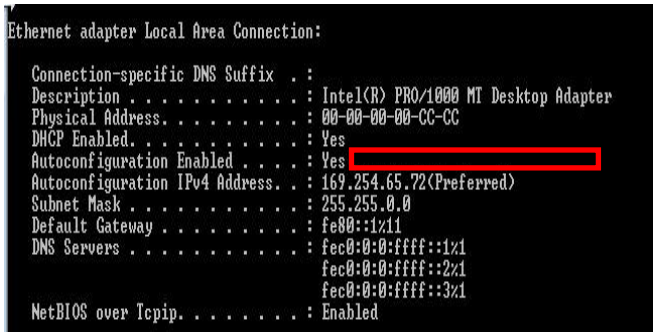


Fig. 9. Screenshot of DoS-on-DAD attack.

In order to test the scenario, Kali as an attacker (PC) have been used to run the DoS on DAD attack with the help of THC-IPv6 attacking toolkit during address autoconfiguration process in IPv6 link local network. During the attack, it has been noticed that Windows-based hosts, that is, Host A and Host B are unable to configure IPv6 link local addresses as depicted in Figure 10.



While ongoing DoS attack, IPv6 hosts cannot obtain the IP addresses as the attacker PC claims that all the IP addresses are already being obtained by it during the attempts of DAD process in IPv6 link local network as shown in Figure 13.

Fig. 10. Host unable to configure IPv6 link local address

Likewise, Linux Hosts such as; Host C and Host D are able to generate tentative IP address but fails to perform DAD process. Thus, due to the DAD process failure hosts are unable to verify the uniqueness of the generated (tentative) IP address. Since, only the preferred IP address after successful DAD process can allow host(s) to communicate with other neighboring hosts within the same link. Therefore, new host(s) cannot communicate with existing hosts in the IPv6 link local network as shown in Figure 11.

Fig. 11. Snapshot of DAD process failure

V. Testbed Outcome

In this study, dos-new-ip6 attacking tool was used to examine the impact of DoS attack during DAD process on Windows and Linux based hosts on deployed IPv6 testbed setup environment as depicted in Figure 12.

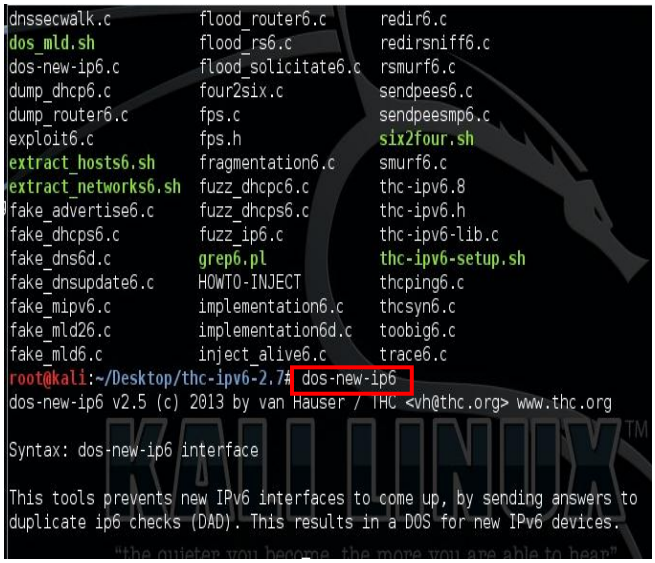


Fig. 12. Snapshot of attacker attempting DoS-on-DAD attack

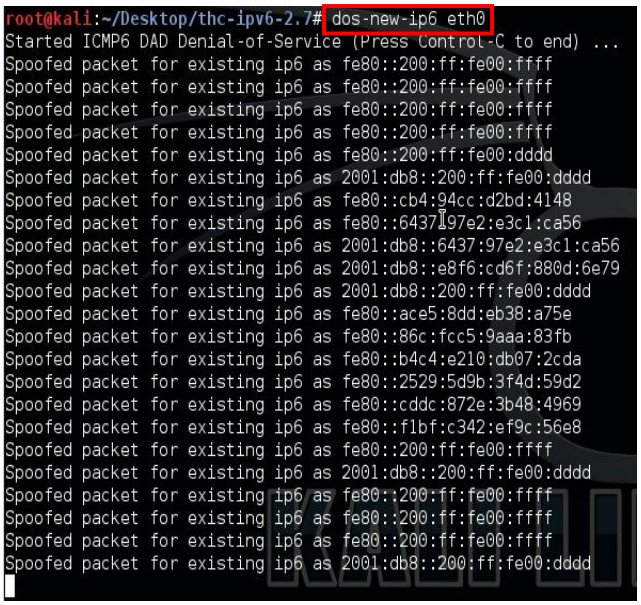


Fig. 13. Snapshot of DoS-on-DAD attack

Since, the attacker disrupts the IPv6 hosts to obtain preferred IP addresses by causing DAD process failure. As a result, the new hosts are unable to communicate with their neighboring hosts on the same link. Figure 14 and 15 depicts the outcome of the experiment conducted on both Windows and Linux OS platforms respectively.

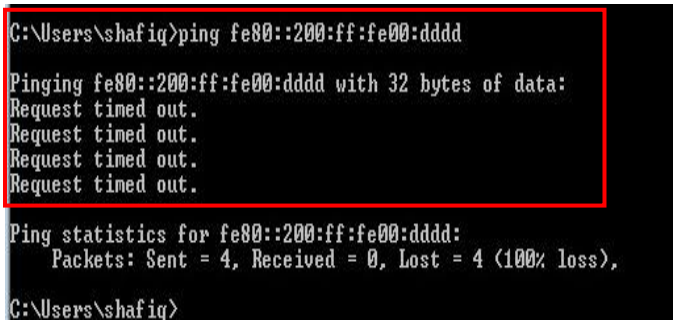


Fig. 14. Snapshot of Window's host communication disruption.

Fig. 15. Snapshot of Linux host communication disruption.

VI. CONCLUSION AND FUTURE WORK

The purpose of this paper was to analyse the impact of DoS on DAD attack and its outcome. In pursuant to this, an IPv6 testbed has been designed and implemented to carry out the attacks on multiple OS platforms. The testbed outcome has shown that during DoS-on-DAD attack IPv6 hosts are unable to obtain IPv6 addresses due to DAD process failure. There are existing mechanisms and approaches that, to some length, address this issue but have drawbacks in terms of efficiency and complexity. Thus, a more effective security mechanism is required to secure DAD process during address autoconfiguration in IPv6 link local network.

Therefore, our future work will be to propose a security mechanism which ensures a secure DAD process during address autoconfiguration in IPv6 link local communication by preventing denial of service (DoS) attack with reduced overhead.

ACKNOWLEDGMENT

This research was supported by National Advanced IPv6 Centre (NAV6), Universiti Sains Malaysia (USM).

REFERENCES

[1] K. Batiha, K. Batiha, and A. AbuAli, THE NEED FOR IPv6, International Journal of Academic Research, vol. 3(3), 2011.

[2] E. Durdaugi and A. Buldu, IPV4/IPV6 security and threat comparisons, Procedia-Social and Behavioral Sciences, vol. 2(2): pp. 5285–5291, 2010.

[3] AlSa'deh, H. Rafiee, and C. Meinel, IPv6 stateless address autoconfiguration: balancing between security, privacy and usability, in Foundations and Practice of Security, Springer, pp. 149–161, 2012.

[4] H. Rafiee and C. Meinel, Privacy and security in IPv6 networks: challenges and possible solutions, in Proceedings of the 6th International Conference on Security of Information and Networks, pp. 218–224, 2013.

[5] J. Ullrich, K. Krombholz, H. Hobel, A. Dabrowski, and E. Weippl, IPv6 security: attacks and countermeasures in a nutshell, in Proceedings of the 8th USENIX conference on Offensive Technologies, pp. 5–5, 2014.

[6] S. U. Rehman and S. Manickam, Significance of Duplicate Address Detection Mechanism in Ipv6 and its Security Issues: A Survey, Indian Journal of Science and Technology, vol. 8(30), 2015.

[7] L. Prudente, E. Aguirre, A. F. M. Hdez, and R. J. Garcia, DoS Attacks Flood Techniques, International Journal of Combinatorial Optimization Problems and Informatics, vol. 3(2): pp. 3–13, 2012.

[8] S.T. Zargar, J. Joshi, , and D.Tipper: A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks, Communications Surveys & Tutorials, IEEE, 15 (4): pp. 2046-2069, 2013.

[9] S. Ahmed, R. Hassan, and N. E. Othman, Improving security for IPv6 neighbor discovery, 2015 International Conference on Electrical Engineering and Informatics (ICEEI), pp. 271–274, 2015.

[10] Conta, S. Deering, and M. Gupta, Internet Control Message Protocol (ICMPv6) for the Internet Protocol version 6 (IPv6), RFC 4443, March 2006.

[11] R.M.Saad, S. Ramadass, and S. Manickam, A study on detecting ICMPv6 flooding attack based on IDS. Australian Journal of Basic and Applied Sciences, vol.7: pp. 175-181, 2013.

[12] R.K.Murugesan, and S.Ramadass: REVIEW ON IPV6 SECURITY VULNERABILITY ISSUES AND MITIGATION METHODS, International Journal of Network Security & Its Applications, 4 (6), 2012.

[13] S. S. Mohamed, A. Y. M. Abusin, and D. Chieng, Evaluation of IPv6 and comparative study with different Operating Systems, Third International Conference on Information Technology and Applications, ICITA 2005, vol. 2: pp. 665–670, 2005.

[14] THC-IPv6 attack toolkit 2015-04-19. Available from: https://www.thc.org/thc-ipv6/.

[15] V. Ndatinya, Z. Xiao, V. R. Manepalli, K. Meng, and Y. Xiao, Network forensics analysis using Wireshark, International Journal of Security and Networks, vol. 10(2): pp. 91–106, 2015.

[16] Qadeer, Mohammed Abdul, Mohammad Zahid, Arshad Iqbal, and MisbahurRahman Siddiqui. Network traffic analysis and intrusion detection using packet sniffer. Second IEEE International Conference on Communication Software and Networks, (ICCSN'10). pp. 313-317, 2010