# Defence Mechanisms Evaluation against RA Flood Attacks for Linux-Victim Node

Samad S. Kolahi * and Bashar Barmada * and Keysha Mudaliar *
* Department of Computer Science, Unitec Institute of Technology, Auckland, New Zealand
E-mail: bbarmada@unitec.ac.nz

***Abstract*— This research evaluates the performance of different defence mechanisms used in IPv6 networks to protect against router advertisement (RA) flood attacks that rely in ICMPv6 Router Advertisement messages to flood the network. Three types of RA flood attacks are considered: the default RA flood attack, RA flood attack with fragmented packets and RA flood attack with extended header packets. The victim machine is considered to be Linux Debian operating system. The defence mechanisms analysed here are: Access Control Lists, Disable Router Discovery, RA Guard, Validate Source MAC and VLAN. The performance is measured according to TCP throughput, TCP round-trip time (RTT) and CPU utilisation.**

## I. INTRODUCTION

IPv6 is developed to replace IPv4, overcome its weakness and improve the performance. However, IPv6 is susceptible to threats such as Denial of Service (DoS) attacks [1, 2, 3]**.** Neighbour Discovery Protocol (NDP) in IPv6 uses Internet Control Message Protocol (ICMPv6) Router Advertisement messages to find neighbouring routers and to enable computers to generate IPv6 addresses for themselves (link-local IPv6). The former process is called router discovery (RD) and the later process is called Stateless Address Autoconfiguration (SLAAC) [4, 5]**.** Since Router Advertisements do not use authentication, they can be misused to launch link-local DoS attacks called Router Advertisement (RA) flood attacks, which stop victim nodes from functioning and might cause the entire network to cripple.

Many solutions relying on other advanced security techniques are proposed to protect against NDP attacks. A Secure Neighbour Discovery protocol was developed to protect the neighbour discovery packets from any attack, such as modification or replaying and providing mechanisms to authenticate the routers [6]. In [7] a proposal was presented to map and bind between IPv6 addresses, MAC addresses and public keys of the network nodes. The mechanism prevented IP address spoofing, which is often used in DoS attacks. A monitoring protocol to compare the packet contents to database entries and discard any mismatch was presented in [2]. [8] developed an IPv6-Plugin to monitor IPv6 messages in the SLAAC process and detect attacks based on signatures. A Trust Based Security (TBS) mechanism was proposed in [5] to ensure the integrity and availability of NDP messages in IPv6 through a central management system. All the above proposals require extra and complex process to provide such security mechanisms, in addition to the high overhead requirements.

In this paper we study and compare the performance of different defence mechanisms, which are widely supported by most networks, against RA flood attacks for IPv6 networks. The defence mechanisms considered here are Access Control Lists (ACLs), Disable Router Discovery, RA Guard, Validate Source MAC and VLAN. The mechanisms are compared according to their TCP throughput, TCP round-trip time (RTT) and CPU utilisation. RA flood attacks are generated in three ways. The test environment consists of a router, an attacker machine, a victim machine with Linux Debian 7.5 operating system, and two monitoring machines. To authors' knowledge there is no such study to compare these mechanisms yet. Results show that ACL mechanisms are the most effective methods to protect against such attacks.

The paper is organized as follows, section 2 includes a detailed discussion on RA flood attacks on IPv6 neighbour discovery protocol. Section 3 discusses the working principles of the studied defence mechanisms against RA flood attacks, followed by the network setup in Section 4. An analytical comparison of the performance for the studied defence mechanisms regarding the throughput, the RTT and CPU utilisation is presented in section 5, and finally the conclusion in is presented in section 6.

## II. ROUTER ADVERTISEMENT FLOOD ATTACKS

IPv6 networks rely on multicast addresses to communicate with all-nodes in the network, using multicast address ff02::1, and to communicate with all-routers, using multicast address ff02::2. NDP process uses ICMPv6 to support its management and control functionalities within the local network. One of these functionalities is Stateless Address Auto-configuration (SLAAC) to allow hosts to generate their own link-local IPv6 addresses to communicate with other hosts within the subnet. The generated local IPv6 addresses depend on the on-link prefix information and the default router address that are included in the router advertisement message (To communicate with nodes in other subnets, the node needs to use a global IPv6 address). If a host needs a local-link IPv6 address, it sends a Router Solicitation request to the all-routers multicast address (ff02::2) and the immediate router responds by sending a RA to all-nodes multicast address (ff02::1) [9, 10].

Since there are no authentication mechanisms in place for the Router Discovery and SLAAC processes, an attacker can

launch a DoS attack known as RA flood attack by transmitting masses of malicious RA messages (ICMP packets) on the local network segment targeting these multicast addresses to overwrite the legitimate routing entries on a host's interface, causing these nodes to lose their connections to the network and overflow the entire network with these malicious packets.

In addition to flooding the network with thousands of packets, RA message can be fragmented into several unnecessary parts to confuse some default security mechanisms, as the fragments do not hold enough information for the network devices to make decision about these packets, and they do not have the ability to reassemble the original packets, which allows the fragments to bypass the security devices in the network. Those fragments can also exhaust the resources of the victim nodes during reconstruction [6], and if the attacker drops few fragments it will be impossible to reconstruct the RA message at the destination node, causing the victim node to suffer from overload fragment reassembly buffers.

Another way to deceive the network security devices is to use many extension headers for RA messages. This will push the payload that contains the upper layer protocol (ULP), i.e. the ICMP payload, away from the initial fragment. Since network devices do not have the ability to reassemble the fragments to parse the entire ICMP packet, processing each fragment individually will not help to identify that these ICMP fragments belong to an attack, as individual fragments do not contain enough information for the network device to make a decision. Thus, the RA flood attack can go through the network [11].

Many tools are available to perform RA flood attacks, such as Flood_router26 from The Hackers Choice (THC) IPv6 toolkit, ra6 from SI6 Networks' IPv6 toolkit and Scapy [12, 13, 14].

## III. Defence Mechanisms Against RA Flood Attacks

There is no single defence mechanism that is able to provide all the security and monitoring services against all types of attacks. Below is a description of the defence mechanisms, which are considered in this work:

- Access Control Lists: ACLs have proven to be effective against DoS flood attacks [15, 16]. ACLs can ensure that NDP ICMPv6 messages such as Router Advertisements are not permitted if they arrive to the network from the Internet or other networks [17]. ACLs can also be configured to drop incoming malicious Router Advertisements on Ethernet ports to which end-user computers are connected, since only router ports can transmit Router Advertisements (port-based ACLs). Other usages of ACLs that they can be configured to search for certain keywords may appear in the attacking packets that rely on fragmentation and block them. One keyword is "fragments" that appears when RA flood attack packets are fragmented. Using ACLs the security devices can assume that these fragments belong to a malicious RA message and discard them, as legitimate RA messages do not need to be fragmented. Another keyword is "undetermined-transport", which is contained in the RA flood attack fragments when the header is extended and the first fragment does not contain the ULP part. Again, these fragments will be discarded as the ULP is expected to be in the initial fragment.
- Disable Router Discovery (Manual Configuration): If IP addresses are configured manually on a host, the auto router discovery will be disabled and most operating systems ignore any RA messages a host receives and prevent many common NDP attacks [18].
- RA Guard: is a mitigating technique used in layer 2 switches meant to immediately drop incoming router advertisements on a port if the device connected to it is not a router. Thus, it can prevent malicious hosts from launching DoS attacks [11, 18].
- Validation of Source MAC Addresses: ports on layer 2 switches can be configured to bind the source MAC addresses of NDP packets with their corresponding source link-local IPv6 address of the router. NDP packets which do not provide this match will be dropped, as they will be spoofing-based attacks [19].
- VLAN Partitioning: using VLAN in a network reduces the impact of the DoS attacks, as only the partition that suffers from the attack will be affected. Nevertheless, these attacks exhaust the switch's finite hardware resources by flooding the switch with unnecessary packets.

## IV. Network Setup

Fig.1 shows the testing environment used in the evaluation of the defence mechanism. The network consists of a router,

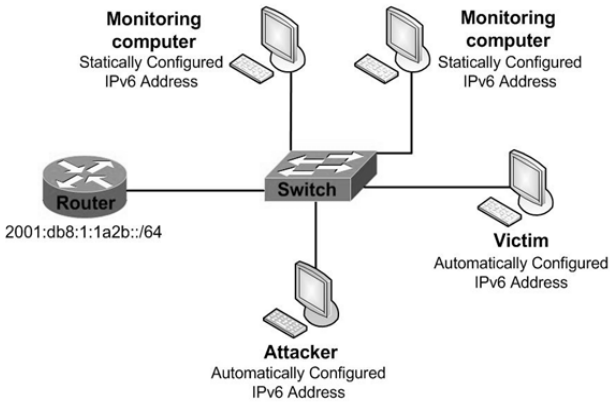


Fig. 1 The test environment to evaluate the defence mechanisms against RA flood attacks.

two monitoring computers with Windows OS, one attack computer with Kali Linux OS and one victim computer with Debian 7.5 operating system. The router is configured to automatically distribute IPv6 addresses using the SLAAC process with prefix 2001:db8:1:1a2b::/64. The automatically configured computers use this prefix to generate their local IPv6 addresses. The attacker and the victim computers are on auto IPv6 configuration, while the monitoring computers are on static IPv6 configuration. During the attack, the victim computer (and all other computers with automatic configuration for IPv6, except the attacker) loses its network connection. The monitoring computers are equipped with Iperf and TCPing to record TCP throughput and TCP RTT, respectively. To monitor the CPU utilization of the victim machine, Saidar tool is used on the victim machine. In addition, Wireshark is also installed on the monitoring computers to observe the attack traffic. Results are gathered before and during the RA flood attacks as well as after the defence mechanisms are implemented

Two types of layer 2 switch in Fig. 1 are used, Cisco 3560G switch is used for most of the defence mechanisms except for RA Guard and Validate Source MAC defences, where Cisco 300-10 switch is used, as those two mechanisms are not supported by Cisco 3560G switch. On the other hand, Cisco 300-10 switch does not support IPv6 ACLs.

The attacker is equipped with THC Flood_router26 tools to emulate RA flood attack. Flood_router26 floods the local link with around 100000 RA messages per second to all nodes multicast address (ff02::1). This prevents computers from joining the IPv6 network and causes computers that have already joined the network using automatic configuration for their IPv6 to lose their network connections [20]. The attacks are generated in three different ways:

1. Attack 1: The default RA flood attack with single packets flooding the network.
2. Attack 2: RA flood attack with packets, where each one is divided into two fragments before sending.
3. Attack 3: RA flood attack with packets, where each one is extended over a large followed by a fragment.

The configurations of the used defence mechanisms are summarized in Table 1. All defences are configured on the switch except Disable Router Discovery configured on the host.

TABLE I
A SETTING SUMMARY OF THE USED DEFENCE MECHANISMS.

| Defence mechanism | Description / Configuration |
|---|---|
| ACLs | - drop any RA message not coming from the router port.<br>- drop RA fragments with keywords "fragment" or "undetermined-transport", as they are most likely to belong to malicious RA messages. |
| Disable router discovery | - static configuration.<br>- turn off router discovery (the received RA message is not processed). |
| RA Guard | define a policy on the switch's router-port with option "Match RA Address" to match the layer 2 source address of an incoming RA message with that of the legitimate router. |
| Validate Source MAC | define a policy for the default VLAN to match the source MAC address of the NDP packets against the link-local IP address of the router. |
| VLAN | the victim, attacker and router are on the same VLAN while the monitoring computers are on a different VLAN. |

## V. RESULTS ANALYSIS

The performance of these deference mechanisms against the three types of attacks is analysed according to TCP throughput (the average number of Byte received successfully by the destination over the link at a given time), TCP round-trip time (RTT) (the time between sending the TCP segment and receiving the acknowledgment) between the monitoring computers, as the victim computer will lose its network connection once the attack is started, and CPU utilisation on the victim machine.

### A. *Attack 1: The default RA flood attack*

Fig. 2 shows the average TCP throughput percentage with and without the defence mechanisms using the two switches, Cisco 3560G and Cisco 300-10. The throughput percentages during the attack and after applying the defences are calculated in relation to the throughput before the attack (which is considered 100%). During the attack, the throughput is dropped severely to nearly no throughput (0.65% in case of Cisco 3560G switch and 0.32% in case of Cisco 300-10 switch). Disable Router Discovery does not have any effects as it does not try to fight the malicious RA messages, it only makes the victim machine to ignore the malicious messages. It could only increase the throughput to 0.70% of the original

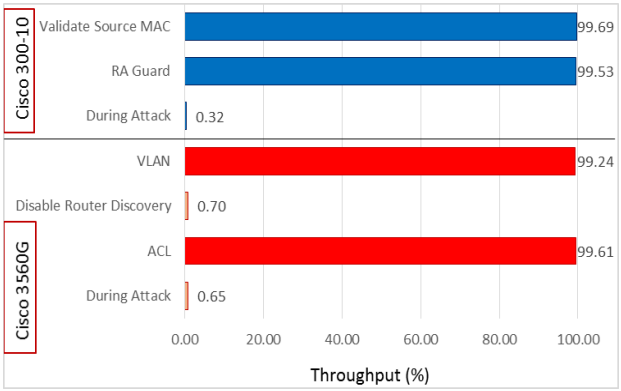


Fig. 2 Average TCP throughput percentage for RA flood attack using Cisco 3560G and Cisco 300-10 switches.

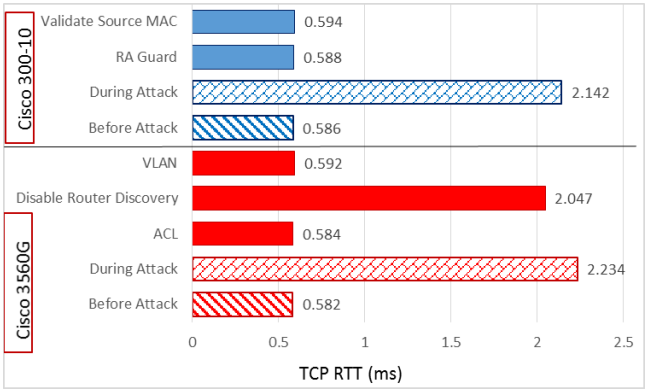


Fig. 3 The Average TCP RTT in (ms) for RA flood attack using Cisco 3560G and Cisco 300-10 switches.

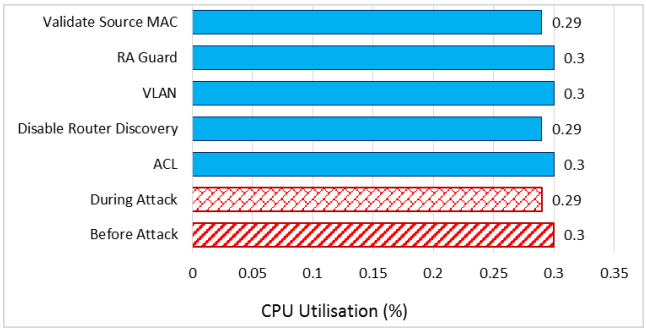


Fig. 4 Average CPU utilisation before and during the attack, and after using the defence mechanisms for RA flood attack.

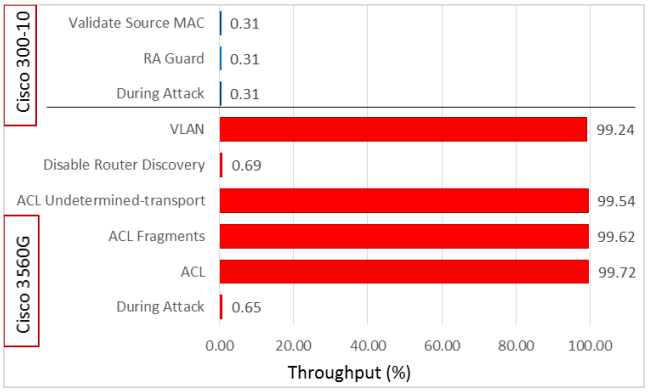


Fig. 5 Average TCP throughput percentage for RA flood attack with two-fragment packets using Cisco 3560G and Cisco 300-10 switches.

throughput. On the other hand, the other defences significantly increase the throughput to more than 99%.

Fig. 3 shows the average TCP RTT results for the defence mechanisms using the two switches. During the attack, the RTT is increased to more than 2 milliseconds (increased by more than 350% compared to the value before the attack). All the defence mechanisms, apart from Disable Router Discovery, reduce the RTT to a level equivalent to RTT before the attack. Disable Router Discovery failed to reduce the RTT to an acceptable level, for the same reason described before.

Fig. 4 shows the average CPU utilisation results for the defence mechanisms. The attack did not have any effect on victim's CPU utilisation, which continued to be extremely low, as Debian operating system on the victim machine sets a constraint on the number of route advertisement information it receives over a period of time [20]. Even after using the defence mechanisms, Debian did not process any Router Advertisements. All defences dropped the Router Advertisements at the switch except Disable Router Discovery, but for Disable Router Discovery the victim machine drops the unused Router Advertisements without having any effect on the CPU utilisation.

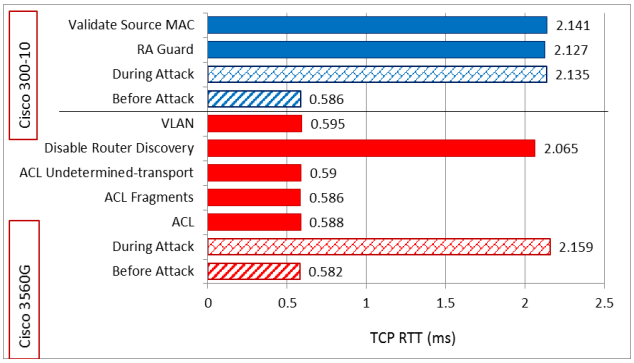


Fig. 6 Average TCP RTT for RA flood attack with two-fragment packets using Cisco 3560G and Cisco 300-10 switches.

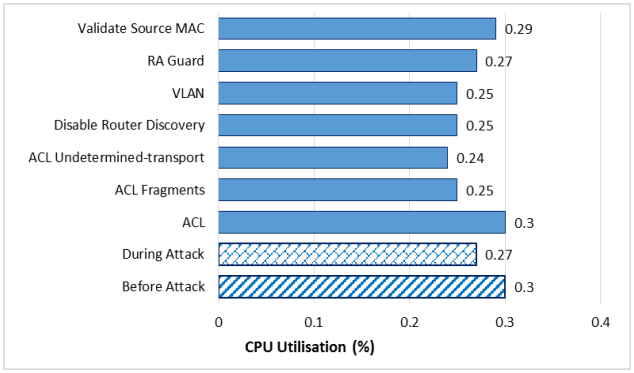


Fig. 7 Average CPU utilisation using the defence mechanisms for RA flood attack with two-fragment packets.

### *B. Attack 2: RA flood attack with two-fragment packets*

Using the second type of RA flood attacks where each packet is divided into two fragments before sending, Fig. 5 illustrates the average TCP throughput with and without the defences as a percentage of the throughput before the attack. When the attack is launched, the throughput is dropped to less that 1% of the original throughput before the attack (near 0 Mbps). After using the defence mechanisms; ACL, ACL Fragments, ACL Undetermined-transport and VLAN managed to bring the throughput back to more than 99%, with marginal differences between these mechanisms. However, Disable Router Discovery, RA Guard and Validate Source MAC are ineffective, as these defences do not have the ability to stop the fragments, and the malicious fragments managed to flood the network.

Similar behaviour is shown for the average TCP RTT in Fig. 6. The attack increases the RTT to more than 2 milliseconds. Defences ACL, ACL Fragments, ACL Undetermined-transport and VLAN managed to bring the RTT back close to its original value before the attack. Disable Router Discovery, RA Guard and Validate Source MAC failed to make any differences, as the switch has not got the ability to reconstruct the fragments and make decision to filter out the attacking packets.

Fig. 7 shows the average CPU utilisation for these defences. As in attack 1, the CPU utilisation was very low prior to the attack and no significant changes are shown after using the defence mechanisms. As explained before, this is due to that Debian OS sets a constraint on the number of RA information it receives over a period of time.

### *C. Attack 3: RA flood attack with extended-header packets*

For type 3 of the RA flood attack where each packet is divided into a large header without ULP followed by a fragment before sending. Five defence mechanisms were evaluated against RA Flood Attack 3, namely ACL, ACL Fragments, ACL Undetermined-transport, Disable Router Discovery and VLAN. With RA Guard and Validate Source MAC the attack exhausts the resources of the switch because it is not possible to send any legitimate packets to measure the TCP throughput and TCP RTT when they are used. For that there is no need to consider Cisco 300-10 switch, only Cisco 3560G switch.

Fig. 8 shows the average TCP throughput, with and without defences, as a percentage of the throughput before the attack. During the attack, the throughput has dropped to around 68.50%. Only VLAN and ACL Undetermined-transport managed to increase the throughput close to its full capacity before the attack (more than 98.5%).

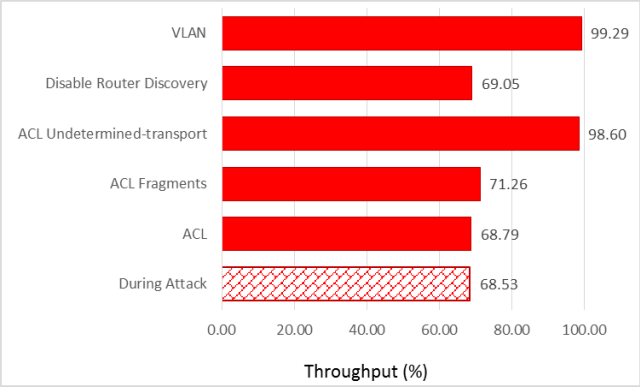


Fig. 8 Average TCP throughput percentage for RA flood attack with extended-header packets using Cisco 3560G switch.

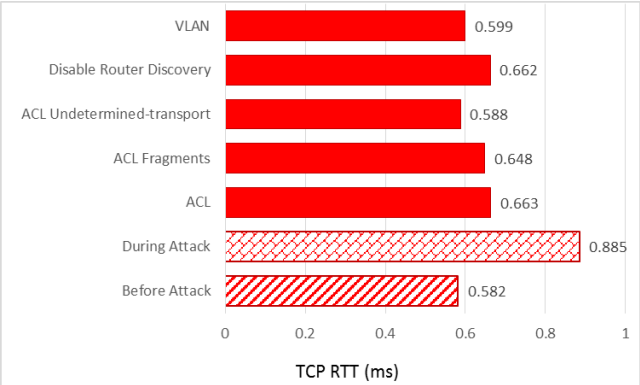


Fig. 9 Average TCP RTT for RA flood attack with extended-header packets using Cisco 3560G switch.

Fig. 9 illustrates the average TCP RTT with and without defences. The RTT increased from 0.582 milliseconds to 0.885 milliseconds during the attack. ACL Undetermined-transport managed to reduce the RTT from 0.885 to 0.588 milliseconds, very close to the value before the attack. VLAN is also effective as the RTT has dropped from 0.885 milliseconds to 0.599 milliseconds. ACL, ACL Fragments and Disable Router Discovery also reduced the RTT, however; they are not as effective as VLAN and ACL Undetermined-transport.

The average CPU utilisation in attack 3 it is similar to two previous attacks. The CPU utilisation was very low before the attack and no a significant change is observed during the attack and after the defence mechanisms are used.

## VI. CONCLUSION

This paper provides a comprehensive evaluation of performance for different defence mechanisms against route advertisement (RA) flood attacks for victim nodes with Linux Debian operating system. The performance is compared according to TCP throughput, TCP round trip time (TTR) and CPU utilisation. Three types of RA flood attacks are considered: Attack1: the default RA flood attack with thousands of single packets flooding the network. Attack2: the RA packets are fragmented into two parts to flood the network in order to bypass network security devices and complicate the reconstruction of the RA messages at the destination node. Attack 3: the RA packets use an extended header and fragments to bypass the network security devices.

Several defence mechanisms are considered here, namely ACL (with ACL Fragments and ACL Undetermined-transport), Disable Router Discovery, RA Guard, Validate Source MAC and VLAN. The network setup consists of a router to generate RA messages, an attacker machine to generate the RA flood attacks, a victim machine with Linux Debian operating system and two monitoring machines equipped with Iperf, TCPing, and Windows Resource Monitoring tools to record TCP throughput, TCP RTT and CPU utilisation, respectively. The victim machine loses its network connection once any type of the attacks is launched.

Test results show that ACL mechanisms provide the best performance and managed to restore the status of the victim machine very close to its status before the attack. On the other hand, Disable Router Discovery, RA Guard and Validate Source MAC are the least effective ones. For attack 2 ACL (fragments) and ACL (undetermined-transport) give the same performance and both outperform the original ACL. For attack 3 ACL (undetermined-transport) outperforms ACL (fragments) and gives throughput and RTT very close to the one before the attack.

## VII. REFERENCES

[1]. E. Durdagi, and A. Buldu, "IPv4/IPv6 Security and Threat Comparisons", *Procedia Social and Behavioral Sciences, Elsevier* 2(2), 5285–5291, 2010

[2]. S. S. Kolahi, A. A. Alghalbi , A. F. Alotaibi, S. Ahmed, and D. Lad, "Performance Comparison of Defense Mechanisms Against TCP SYN Flood DDoS Attack", *6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, St. Petersburg, Russia, 2014.
[3]. J. M. Stewart, Network Security, Firewalls and VPNs (2nd Ed.). *Burlington, MA: Jones & Bartlett Learning*, 2013.
[4]. M. Sande, "So you've got IPv6 address space. Can you defend it?" *master's thesis, University of Bergen*, Bergen, Norway, 2014.
[5]. Supriyanto, R. K. Murugesan, A. Osman, and S. Ramadass, "Security Mechanism for IPv6 Router Discovery Based on Distributed Trust Management", *IEEE International Conference on RFID- Technologies and Applications*, Johor Bahru, Malaysia, September 2013.
[6]. F. Gont, "Security Implications of IPv6 Fragmentation with IPv6 Neighbour Discovery", *RFC 6980*, August 2013.
[7]. R. Hassan, A. S. Ahmed, and N. E. Osman, "Enhancing Security for IPv6 Neighbor Discovery Protocol Using Cryptography", *American Journal of Applied Sciences*, 11(9), 1472-1479, 2014.
[8]. M. Schutte, T. Scheffler, and B. Schnor, "Development of a Snort IPv6 Plugin – Detection of Attacks on the Neighbor Discovery Protocol", *International Conference on Security and Cryptography*, Rome, Italy, 2012.
[9]. A. Pilihanto, A Complete Guide on IPv6 Attack and Defence, *SANS Institute*, 2012.
[10]. T. Narten, E. Nordmark, and W. Simpson, "Neighbor Discovery for IP version 6 (IPv6)", *Network Working Group, RFC 4861*, 2007.
[11]. F. Gont, "Implementation Advice for IPv6 Router Advertisement Guard (RA Guard)", *RFC 7113*, February 2014.
[12]. Kali Linux Penetration Testing Tools, http://tools.kali.org/
[13]. SI6 Networks' IPv6 Toolkit, www.si6networks.com
[14]. Scapy, http://www.secdev.org/projects/scapy/
[15]. S. S. Kolahi, K. Treseangrat, and B. Sarrafpour, "Analysis of UDP DDoS Flood Cyber Attack and Defense Mechanisms on Web Server with Linux Ubuntu 13", *International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, Sharjah, United Arab Emirates, February 2015.
[16]. K. Treseangrat, S. S. Kolahi, and B. Sarrafpour, "Analysis of UDP DDoS Cyber Flood Attack and Defense Mechanisms on Windows Sever 2012 and Linux Ubuntu 13", *International Conference on Computer, Information and Telecommunication Systems (CITS)*, Gijon, Spain, 2015
[17]. S. Frankel, R. Graveman, J. Pearce, and M. Rooks, "Guidelines for the Secure Deployment of IPv6", *National Institute of Standards and Technology, US Department of Commerce*, 2010.
[18]. T. Chown, and S. Venaas, "Rogue IPv6 Router Advertisement Problem Statement", *RFC 6104*, February 2011.
[19]. D. McPherson, F. Baker, and J. Halpern, "Source Address Validation Improvement (SAVI) Threat Scope", *Internet Engineering Task Force (IETF), Request for Comments: 6959*, May 2013.
[20]. M. Grob, and E. Hoffmann, "What is wrong with the IPv6 RA protocol? Some analysis and proposed solutions", *IPv6-Kongress*, Frankfurt, Germany, May 2012.