IPv6 Host-Based Self-Defense Against Rogue Route Advertisement

Itarun Pitimon[1],
Sirapat Boonkrong[2],
and Nawaporn Wisitpongphan[3]
Faculty of Information Technology,
King Mongkut's University of Technology North Bangkok, Thailand
[1]itarun.p@gmail.com
[2]sirapat.b@it.kmutnb.ac.th
[3]nawaporn.w@it.kmutnb.ac.th

Abstract - **The automatic address allocation of IPv6 host is a part of Neighbor Discovery Protocol. Hosts collect necessary parameters and create routing table in order to enable communication to the external network. However, this procedure does not incorporate authentication of the gateway router, which means that any malicious host can exploit this vulnerability to manipulate parameters and provide other hosts with falsified parameters. This can cause a serious effect to the routing table and inappropriate data flow to malicious nodes. This paper proposes a concept of router spoofing prevention by incorporating data verification process at the gateway router. The process employs the Path Maximum Transmission Unit Discovery (PMUTD) method and determines the test probe randomly. The fundamental parameters as well as additional parameters derived from the verification process are then used to determine the validity of the gateway router. The proposed method employs existing diagnosing tools provided with the operating system and the verification process is performed directly to the collected data.**

Keywords - **IPv6, Rogue Gateway, Router Advertisement**

I. INTRODUCTION

Neighbor Discovery Protocol (NDP) is a part of Internet Protocol version 6 (IPv6), responsible for address reference in the Link layer and Internetworking layer. It is accounted for automatic configuration of host addresses, neighbor resolution process, duplicate address detection, router discovery and providing information services, i.e., network prefix, Domain Name System (DNS). Moreover, neighbor reachability is also maintained by NDP. NDP is an integral part of Internet Control Message Protocol version 6 (ICMPv6) [1] which incorporates neighbor resolution and management into the IPv6 protocol suite.

Addresses of routers received from NDP mechanism, namely Router Discovery function, are adopted by hosts in the network to generate their routing tables. In inter-network communication, these router addresses are used for default gateway identification. Under normal circumstance, the communication across networks is in the form of source-gateway router-destination (in another network).

The process of Router Discovery relies on NDP which consists of crucial network parameters exchange, i.e., network prefix and default gateway address. Without parameter verification, any malicious host can manipulate parameters and provide other hosts with falsified parameters [2-3]. This can cause

a serious effect to the routing table and inappropriate data flow to malicious nodes. The router spoofing, an act that the malicious router masquerades itself as a legitimate router by falsifying its address is a serious threat to this vulnerability. Solutions to counteract this threat are proposed in [4-5] by incorporating key management into play. The introduced process includes data verification via NDP such as Secure Neighbor Discovery (SeND) and only allows devices to broadcast parameter obtained via valid channel, i.e., Router Advertisement Guard (RA Guard).

Due to the problems above, a solution is proposed. This work relies on the fundamental property of networking, that is, a Link Local Address (lladdr) must be unique while IP address may not. Consequently, lladdr can be used as a reference for a unique address of a default gateway. The contribution of this work is two-fold. First, our method enables the verification of routers present in the network through existing commands provided with the operating system. Second, each router under investigation can be verified for forwarding capability to other networks, again, through existing commands provided with the operating system.

Router discovery in IPv6 is realizable through NDP which is also a part of ICMPv6, involving addressing services. This is to identify hosts and routers in the same network due to the fact that neighboring hosts and routers can directly communicate without transiting through other nodes.

In this work, the host-router discovery function plays an important role and it is useful to briefly touch on the subject. The host-router discovery function consists of Router Discovery, Prefix Discovery, Parameter Discovery, and Address Autoconfiguration. Router Discovery is essential to the network operation such that there is a need of default gateway for any network requesting for inter-network communication. This default gateway, also known as a router, is responsible for connecting and relaying information across two or more networks. Other hosts in the network need to know a router network in order to enable inter-network communication. The Router Discovery is in charge for this operation.

II. RELATED WORK

Recently, several methods have been proposed to prevent RA broadcasting from untrusted channel. In [6-7], the authors proposed a method, called Secure Neighbor Discover (SeND), to prevent invalid RA broadcasting. The proposed method involves packet encryption and only packet encrypted from trusted source can be correctly decrypted. SeND mainly relies on Certificate Authority as an agency to generate valid digital certificates for routers, called CR. Likewise, hosts in the network are required to have digital certificate, generated by Certificate Authority, called C0. These CRs and C0s play a major role in RA verification, that is, only RA encrypted with legitimate router's CR is able to be correctly decrypted by host's C0. Nevertheless, the drawback in SeND implementation is in congruent with any system involving key management and encryption-decryption complexity.

Another method called RA guard [8-9], is proposed to limit the channel of RA broadcasting at the distribution node, to only trusted channel. In other words, the distribution node, i.e., network switch, only allows incoming RA from trusted ports. This method is suitable for network where SeND is inapplicable. However, not only an in-depth understanding from network administrator is required but also RA guard compliance network switch is mandatory.

In [10], the authors proposed a method with Router Preference Option. In other words, RA packet can have different level of importance, i.e., low, medium, and high, depending on originating router's importance. This method is useful for network requiring a backup route. However, it cannot prevent rogue routers from advertising RA with high importance and renders illegitimate RA prevention useless.

It can be seen that although several methods have been proposed to reduce the risk of rouge router advertisement problem, there are still many disadvantages to them. This is why it is important that a more simple and effective approach will be proposed here.

III. THREATS OF TPV6 ROUTER DISCORY

There exists vulnerability in Router Discovery function that may lead to a serious security breach. NDP does not require authentication during route advertisement and malicious hosts, also known as rogue router [11-13], can masquerade themselves as a legitimate ones and perform malicious acts. This can cause confusion to route selection of the host and may lead to data communication failure, depending on the advertised router location.

For example, if the rogue router receives packets from other hosts but never forwards them, it is called Denial of Service (DoS) [7]. On the other hand, if the rogue router receives packets from other hosts, inspects or modifies packets and then forwards them, it is called Man in The Middle (MiMT) [8].

The flow of data, in case of DoS, originates from source node and terminates at the rogue router so it is inevitable that the source node will not be able to communicate with the intended destination. However, the flow of data, in case of MiMT, originates from source node, passing through the rogue router and the default gateway, and then finally terminates at the intended destination in other networks. In this case, the source node is able to communicate with the intended destination, but is unaware of eavesdropping.

Herein, we briefly discuss two types of Route Advertisement (RA) attacks, RA spoofing and RA flooding [14].

In RA spoofing, the attacker broadcasts illegitimate RA and hosts in the network update their routing table according to parameters received in RA. Consequently, data will be routed to the rogue router and incurs MiTM attack. Any information sent by the source node poses the risk of eavesdropping or tampering by the rogue router.

In RA flooding, the attacker broadcasts illegitimate RA with invalid parameters at a very high packet rate. The intention is to disturb the network by creating unreachable destination and incurs DoS attack.

IV. PROBING WITH DIRECT DETECTION (PDD)

Our proposed method utilizes IPv6 mechanism for rogue router identification. The information from routing table, neighbor table, address table, and route cache table, together with various mechanisms, RA input, PMTUD [15], and ICMP, are used to obtain lladdr and router address. In general, the packet destined to external network should only spend a single hop within the internal network.

In this work, we propose a method, called Probing with Direct Detection (PDD), to detect router spoofing. PDD utilizes an existing Neighbor table in IPv6, together with 5 PDD specific tables shown in Fig. 1. In Neighbor table, LLA/IP is node's address, MAC is lladdr, and Type signifies whether it is a router. In GwList table, MACs is lladdr of a source node and LT is lifetime of a node that advertises RA. Flag and cP in ProbeGw table are gateway's status (pass, fail, and unidentified) and probe counter, respectively. In topology table, nHop reveals number of hops to the corresponding address.

Next, we state assumptions used in this work. In standard practice of IPv6, every router in the network must join all router multicast address (FF02::2) and node can only obtain its gateway through router discovery process. We then discuss PDD's 6 working modules as follows:

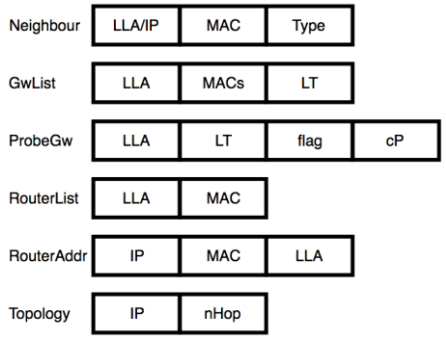

Fig. 1 Tables used in PDD

A. RA Packet Detection

Once the node receives RA packet, it obtains (MACs, LLA) pair. Then it checks if LLA is in RouterList table. If found, it proceeds to search for LLA in Neighbor table and verifies whether the corresponding MAC is similar to MACs. If not, the received RA is invalid. Otherwise, (LLA, MACs) and Lifetime are inserted into GwList table. This process distinguishes valid RAs, sent by actual routers, from malicious RAs and put actual routers in GwList.

B. New Gateway Selection

After deriving the list of routers in previous section, we check for validity of each router in GwList using lifetime. If it expires then the record is purged. Otherwise, the flag parameter is checked if it is null. If not, this router is previously trusted and has to be probed again if half of its lifetime has passed. The Flag is then set to N, designated a new gateway, and cP is set to 1 (1st probe). Finally, (LLA, LT), flag, and cP are inserted into ProbeGw table.

C. Gateway Forwarding Verification

In this section, the router is tested for its ability to forward packets. The result of this process is a list of routers in the path between source to a test target. Each router in ProbeGw table is checked if its flag is set to M, designated an unidentified router. If is it M and its cP is more than 3, then the router is removed from ProbeGw. If is it M and its cP is less than 3, then nHop is incremented by cP and proceeds to PMTUD testing below.

On the other hand, if router's flag is set to N, PMTUD is used to derive a list of routers in the path of nHop. The node address in the nth hop (IP, nHop) is inserted into Topology table. Fig. 2 shows, the process of gateway forwarding verification.

D. Router Address Identification

Another crucial step is to check for active routers in the network. This process is possible by sending Internet Control Message Protocol (ICMP) echoRequest to multicast address (FF02::2) and wait for response. For each ICMP echoReply received, its LLA is used to obtain MAC as well as type through Neighbor table. The pair (LLA, MAC) are then inserted into Router List table. The process is shown in Fig. 3.

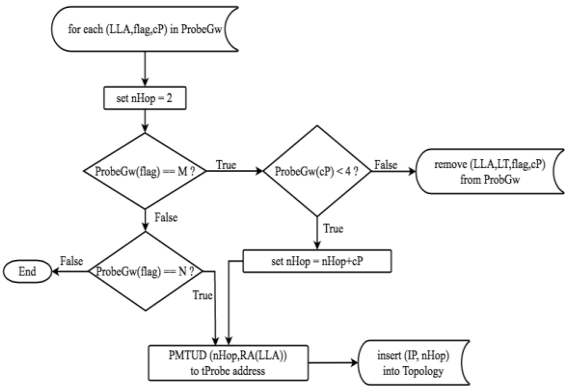

Fig. 2 Gateway Forwarding Verification

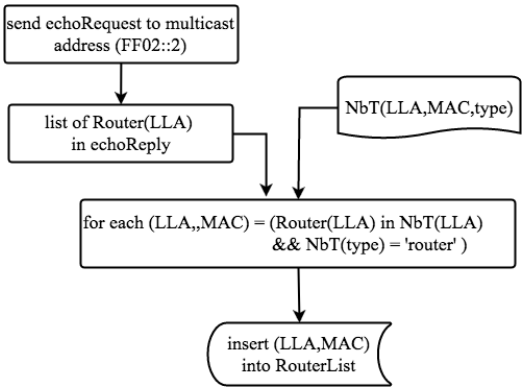

Fig. 3 Router Address Identification

E. Router Address Identification at Specific Hop

Another important process is to identify MAC of each router in Topology table. The process is similar to the above, that is, the echoRequest is sent to router's IP and wait for response. For each echoReply received, the pair (IP, MAC), LLA are then inserted into RouterAddr table. Otherwise, the ProbeGw

table is updated with flag set to M and cP incremented by 1.

F. Trusted Gateway Identification

The final process of PDD is to identify if the gateway is trusted. The key to the process is the fact that the trusted gateway can only be in the first hop from packet source and MAC information from the second hop onwards cannot be obtained. The relationship among 3 tables, GwList table, RouterAddr table, and Topology table, are used to find MAC that corresponds to IP at the nth hop and forwarded by router in GwList. If MAC is resolvable, the corresponding router is a rogue router and then removed from GwList. Otherwise, the corresponding router is a trusted router, the flag is then set to P and the GwList table is updated.

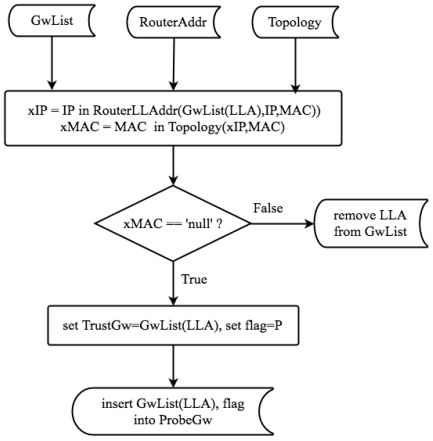

Fig. 4 Trusted Gateway Identification

V. EXPERIMENT SETUP

In this section, we thoroughly evaluate our proposed method under virtual machine (VM) environment. The benefit of using VM is not only an ability to control environment under test but also capability to independently increase number of testing nodes. The testing environment is as follows: Simulation hardware with CPU Intel core i5-2400 equipped with 16 GB memory, Windows 10 x64 operating system, and VMware Workstation virtualization software.

We classify VMs in to four categories, source nodes, gateway routers, rogue routers that perform MiTM attack, and rogue router that performs DoS attack. Fig. 5 shows, the network topology under test. Src1 and Src2 are source nodes that initiate packet transmission. Gw1 and Gw2 are legitimate gateway routers. M1 to M8 are MiTM rogue routers. Finally, D represents DoS rogue router. Src1, Src2, and D are allocated with a single core CPU with 512 MB memory, running Debian 7.0 operating system. M1 to M8 are allocated with a single core CPU with 1 GB memory, running vyOS operating system. All VMs are equipped with Gigabit Ethernet.

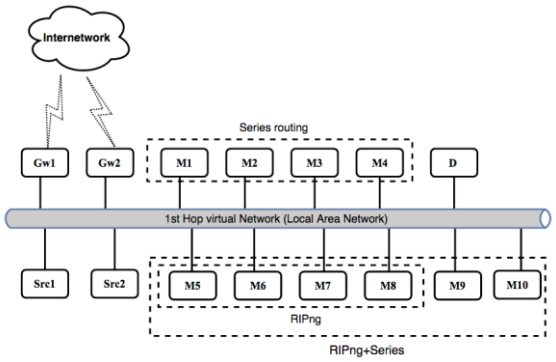

Fig. 5 Network Topology Under Test

We employ three testing tools, ping6, tracepath6, and nuttcp, for performance evaluation. Ping6 is used for Round Trip Time (RTT) [16] measurement while hop count measurement is viable through tracepath6. Lastly, nuttcp is accounted for throughput measurement.

We devise the performance evaluation into five parts. The first part aims to obtain the baseline measurement of source nodes that initiate packet transmission in both protocol stack and local network. The second part targets at deriving throughput and RTT in case of internetwork communication via either Gw1 or Gw2. We introduce the PDD mechanism into play and employ a single MiTM attack in the third part. In part four, we investigate the PDD mechanism under serial MiTM attacks, i.e., rogue routers forward packet to its rogue neighbors in series. In other words, all rogue routers are configured with static route, that is, no routing protocol is implemented. Finally, we investigate the PDD mechanism under multiple MiTM attacks when rogue routers are not limited by static route configuration.

VI. EXPERIMENTAL RESULT

We test the system performance when multiple RAs are advertised by different gateways. The test originates from Src2 to various destinations, through different gateways that incur different path and hence different hop counts. The hop counts incurred by several gateways are shown in Table I.

Here, we categorize gateways into 4 groups: The first group comprises of Gw1 and Gw2 which are legitimate gateways and capable of forwarding packets to external networks. However, their forwarding paths are different and Gw2 experiences a larger hop count than Gw1. The second group consists of rogue gateways, M1 to M4, which have no access to external networks and are only capable of forwarding packets to theirs neighbors in series, i.e., M4 can only forward packets to M3 and M3 can only forward packets to M2 and M2 can only forward packets to M1. However, M1 is the only rogue gateway that has an exception. That is, it can forward packets to Gw1 and can enable packet transmission from source node to any destination. Consequently, without disruption in packet transmission, the source node is unlikely to realize that it is under attack. The third group composes of rogue gateways, M5 to M8, which have no access to external networks but are implemented a routing protocol, RIPng, among them. Moreover, M5 is the only rogue gateway that has an exception. That is, it can forward packets to Gw1 and enable packet transmission from source node to any destination. The routing protocol, implemented among M5 to M8, is contained within their own entities and conducted to observe the impact of hop count variation on system performance. Finally, M9 and M10 constitute the fourth group, consisting of rogue gateways which have no access to external networks and have limited packet forwarding capability, that is, M10 can only forward packets to M9 and M9 can only forward packets to M5, M6, M7, and M8.

TABLE I
GATEWAY PROPERTIES

Gateway	Hop Count	Property
Gw1	4	Trusted gateway
Gw2	5	Trusted gateway
M1	5	MiTM route via Gw1
M2	6	MiTM route via M1
M3	7	MiTM route via M2
M4	8	MiTM route via M3
M5	5	MiTM route via Gw1
M[6-8]	6	MiTM RIPng with M5
M9	7	MiTM route via M[6-8]
M10	8	MiTM route via M9

The performance evaluation of PDD is conducted by comparing elapsed time upon trusted gateway identification process completion. Src1 has PDD implemented while Src2 does not have PDD mechanism in effect.

Fig. 6 shows, elapsed time required for gateway identification for both PDD and non-PDD equipped source nodes. It is clear that the PDD equipped source node is able to identify whether the gateway under test is a rogue gateway much faster, approximately 5 times on average. Moreover, the elapsed time of the PDD equipped node is marginally affected by increasing number of attacking complexity (multiple rogue routers with routing capability involved) while the elapsed time of the non-PDD equipped node is monotonically increasing with increasing number of attacking complexity. Even for trusted gateway identification, i.e., Gw1 and Gw2, the PDD equipped node outperforms non-PDD equipped node by approximately 2.5 times.

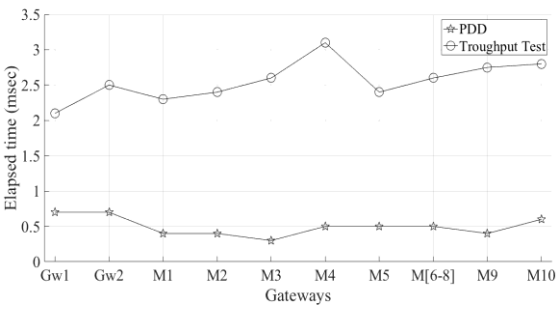

Fig. 6 Time Required to Identify Rogue Gateway

Next, we further investigate the effect of rogue gateway on TCP throughput to observe their relationship. We employ nuttcp to determine the raw TCP throughput between source node and destination node. We observe the behavior of TCP throughput in both upload and download directions with respect to test scenarios, shown in Fig. 5. The test parameters are set as follows: all gateways advertise RAs and PDD is implemented on Src1 but not on Src2. Unless specifically stated, the test duration is 180 seconds with one second sampling interval.

Fig. 7 shows, the average TCP throughput between source node (internal network) and destination node (external network) in upload direction. Data points represent the average TCP throughput of gateways and the corresponding 95% confidence interval are plotted as error bars in the figure. It is clear that the average TCP throughput of Gw1 is higher than Gw2. This is not surprising since the path through Gw1 experiences fewer hop count than Gw2. Interestingly, the average TCP throughput of M1, M5, M6, M7, and M8 are in congruent with Gw1 despite higher hop count experienced when compared to Gw2. However, it is obvious that the average TCP throughput of M3, M4, M9, and M10 significantly decrease when compared to Gw1. The effect of hop count on TCP throughput becomes obvious when the hop count is higher than 3 hops.

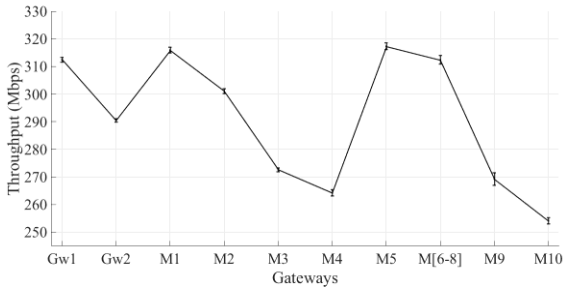

Fig. 7 Average TCP throughput in Upload Direction

The average TCP throughput between source node (external network) and destination node (internal network) in download direction is shown in Fig. 8. Again, data points represent the average TCP throughput of gateways and the corresponding 95% confidence interval are plotted as error bars in the figure. On the contrary, the average TCP throughput of Gw2 is higher than Gw1. This is possible if the routing is asymmetric and the path selection is determined by external entity, beyond the control of both Gw1 and Gw2. Likewise, the average TCP throughput of Gw1, M1, M5, M6, M7, and M8 are similar to the average TCP throughput observed in upload direction. Nevertheless, it is obvious that the average TCP throughput of M3, M4, M9, and M10 significantly decrease when compared to Gw1. The effect of hop count on TCP throughput becomes obvious when the hop count is higher than 3 hops.

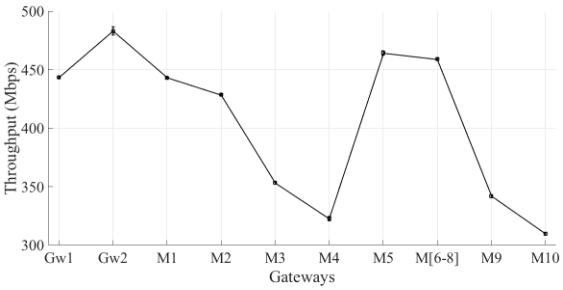

Fig. 8 Average TCP throughput in Download Direction

The summary of average TCP throughput in both upload and download directions is shown in Fig. 9 and it is clear that the average TCP throughput of Gw1, M1, M2, M5, M6, M7, and M8 are marginally different in spite of difference in hop counts. Again, the summary of average TCP throughput of M3, M4, M9, and M10 significantly decrease when compared to Gw1. Consequently, the effect of hop count becomes obvious when the hop count is higher than 3 hops.

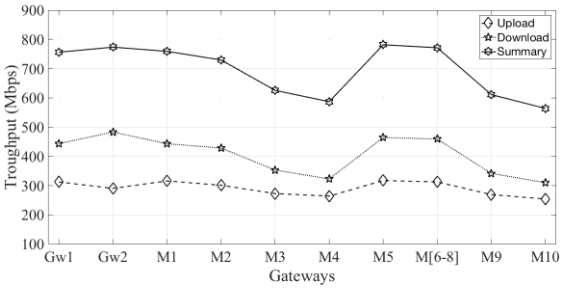

Fig. 9 Summary of Average TCP throughput

In summary, Gw1 has 7.56% higher percentage of TCP throughput than Gw2 in upload direction while Gw2 has 8.18% higher percentage of TCP throughput than Gw1 in download direction. It implies that it is more efficient to transmit packets through Gw1 and receive packets via Gw2.

VII. CONCLUSION

The use of parameters received from unverified RAs can cause a serious effect to the routing table and inappropriate data flow to malicious nodes. In this work, we propose a concept of router spoofing prevention by incorporating data verification process at the gateway router. The proposed method, called PDD, largely outperforms the classical method and very scalable. It is also shown that the hop count and TCP throughput can correctly identify rogue gateways only when the hop count is higher than 3 hops, consequently, a drastic impact on TCP throughput. On the contrary, PDD can precisely identify rogue gateways and is not limited by these circumstances.

VIII. ACKNOWLEDGMENTS

The authors would like to thank Prof. Prusayon Nintanavongsa and UniNet, Office of the Higher Education Commission for their contribution.

REFERENCES

(Arranged in the order of citation in the same fashion as the case of Footnotes.)

[1] Conta, A. and Gupta, M. (2006). "Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6) specification". <https://tools.ietf.org/html/rfc4443>. Accessed 20 August 2014.

[2] Elejla, O.E., Anbar, M., and Belaton, B. (2016). "ICMPv6-Based DoS and DDoS Attacks and Defense Mechanisms: Review". IETE Technical Review, pp. 1-18.

[3] Dawood, H. and Jassim, K.F. (2013). "Mitigating IPv6 Security Vulnerabilities". International Conference on Advanced Computer Science Applications and Technologies (ACSAT), pp. 304-309.

[4] AlSa, A., Rafiee, H., and Meinel, C. (2012). "IPv6 stateless address autoconfiguration: Balancing between security, privacy and usability". Proceedings of the 5th International Conference on Foundations and Practice of Security, pp. 149-161.

[5] Choudhary, A. and Sekelsky, A. (2010). "Securing IPv6 network infrastructure: A new security model". Proceedings of IEEE International Conference on Technologies for Homeland Security (HST), pp. 500-506.

[6] Park, J. and et al. (2007). "A Survey of the SEcure Neighbor Discovery (SEND) and Multi-Key Cryptographically Generated Addresses (MCGAs)". Proceddings of the 9th International Conference on Advanced Communication Technology, Vol. 3, pp. 2124-2127.

[7] AlSa'deh, A. and Meinel, C. (2012). "Secure Neighbor Discovery: Review, Challenges, Perspectives, and Recommendations". IEEE Security and Privacy, Vol. 10, No. 4, pp. 26-34.

[8] Gont, F. (2014). "Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)". <https://tools.ietf.org/html/rfc7113>. Accessed 20 January 2015.

[9] Levy-Abegnoli, E. and et al. (2011). "IPv6 Router Advertisement Guard". <https://tools.ietf.org/html/rfc6105>. Accessed 26 February 2015.

[10] Draves, R. and Thaler, D. (2005). "Default router preferences and more-specific routes". <https://tools.ietf.org/html/rfc4191>. Accessed 8 June 2015.

[11] Dawood, H. (2012). "IPv6 Security Vulnerabilities". International Journal of Information Security Science, Vol. 1, No. 4, pp. 100-105.

[12] Alangar, V. and Swaminathan, A. (2013). "Ipv6 security: Issue of anonymity". International Journal of

Engineering and Computer Science, Vol. 2, No. 1, pp. 2486-2493.

[13] Chown, T. and Venaas, S. (2011). "Rogue IPv6 Router Advertisement Problem Statement". <https://tools.ietf.org/html/rfc6104>. Accessed 10 December 2014.

[14] Barbhuiya, F.A., Biswas, S., and Nandi, S. (2011). "Detection of Neighbor Solicitation and Advertisement Spoofing in IPv6 Neighbor Discovery Protocol". Proceedings of the 4th International Conference on Security of Information and Networks, New York, NY, USA, pp. 111-118.

[15] Luckie, M. and Stasiewicz, B. (2010). "Measuring path MTU discovery behavior". Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement, pp. 102-108.

[16] Mudaliar, K. (2015). "Performance evaluation of defence mechanisms against ICMPv6 router advertisement flood attacks". A thesis submitted in partial fulfilment of the requirements for the degree of Master of Computing. Unitec Institute of Technology.