Risk Analysis of the Implementation of IPv6 Neighbor Discovery in Public Network

Supriyanto[1,2], Iznan Hasbullah[2], Mohammad Anbar[2], Rajakumar Murugesan[3], Azlan Osman[4]

[1]Universitas Sultan Ageng Tirtayasa, Indonesia
[2]National Advanced IPv6 Centre, Universiti Sains Malaysia, Malaysia
[3]Taylor's University, Malaysia
[4]School of Computer Sciences, Universiti Sains Malaysia

supriyanto@ft-untirta.ac.id, iznan@nav6.usm.my, anbar@nav6.usm.my, rajakumar.murugesan@taylors.edu.my, azlan@cs.usm.my

***Abstract*—Internet is ubiquitous, and in recent times its growth has been exponential. This rapid growth caused the depletion of the current Internet Protocol version 4 (IPv4) address, prompting IETF with the design of the new Internet Protocol version 6 (IPv6) in the 1990's. IPv6 is the next generation of the Internet Protocol designed with much larger address space and additional functions to ease its use for the users. One of the new functions is address auto configuration of new host's via Neighbor Discovery Protocol (NDP). However, the implementation of NDP is not without risk in terms of security. This paper analyzes the risk of NDP implementation in public network. The result shows a number of risks that appear on the implementation of NDP over a Public Network. Neighbors cannot be trusted 100%. One of them could be an attacker who may exploit the NDP message to get their own benefit. In addition the number of insiders increases time to time.**

Keywords—ipv6; neighbor discovery; IPv6 address; security; public network

I. INTRODUCTION

Today, Internet connection is available anywhere, any time and possibly in everything. People now think about Internet of Everything [1] to mean everything in the world could get IP address. The growth of Internet users had reached 566.4% in 2012 [2]. A person nowadays may use more than one device connected to the internet such as laptop, smart phone, tablet, etc. Exponential growth of the Internet and has caused the depletion of Internet addresses [2]. The current Internet Protocol, IPv4, has 32 bits of IP address space which is equivalent to about 4.3 billion Internet addresses. Although it seems like a big number, it is much smaller than the latest world population that reaches more than seven billion in 2014.

To solve the IP address depletion problem, researchers proposed a new IP protocol with larger address space which is now called Internet Protocol Version Six (IPv6). IPv6 uses 128 bits address space which can spare millions of IP addresses for every millimeter square of earth surface [3]. There are other solutions such as Network Address Translation (NAT) [4] as well as CIDR (Classless Inter-Domain Routing) [5]. However, these mechanisms are temporary measure and only suited for a limited time.

Other than offering larger address space, the new protocol also has other advantages including simpler header format, extension header for extensibility as well as address auto configuration. The address auto configuration is defined by Neighbor Discovery Protocol (NDP) [6]. There are two types of address auto configuration – stateless address auto configuration [7] and stateful address auto configuration that uses Dynamic Host Configuration Protocol (DHCP) [8]. Both addressing types rely on NDP message exchange. NDP in IPv6 borrows concepts from a number of protocols in IPv4 including Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), Router Discovery and Redirect protocol.

New technology often comes with both advantages and disadvantages. The NDP facilitates new local IPv6 hosts to obtain IPv6 address which is required before it can communicate with other nodes whether on the same link or external link. The original specification of NDP does not include any security mechanism possibly on the assumption that the neighbors on a local network are trustworthy, which not necessarily be. This would cause the local IPv6 communication to be vulnerable to malicious activities from neighbors. Attackers connected to the same link could manipulate the NDP message to do malicious activities targeting other local nodes.

Considering the important role of NDP in IPv6 link local communication, a survey on the security vulnerability was done in [9]. The paper showed a number of threats on IPv6 link local communication including Router Advertisements (RA) spoofing, RA flooding, Duplicate Address Detection (DAD) failure etc. It also discussed a number of proposed solutions to secure the NDP such as Secure Neighbor Discovery [10] and RA Guard [11]. However, the paper does not consider the real network condition that prompted attackers to do malicious activities using NDP messages. Attacking activities could be perpetrated due to the existence of opportunity or with malicious intent. This paper analyzes the current implementation of IPv6 NDP in dual stack environment on a public network that provides chances as well as attracting people to commit malicious activities.

The rest of this paper consists of overview of IPv6 neighbor discovery in Section 2 followed by analysis of methodology in

Section 3. Section 4 provides experimental results and also discussion of the implementation of NDP protocol in terms of security risk. The last section is the conclusion of the paper.

II. Overview of IPv6 Neighbor Discovery

Neighbor Discovery is a concept of neighboring nodes communication that is usually implemented in wireless environment such as in wireless sensor network [12] and wireless ad hoc network [13]. In the Internet Protocol, this approach is new and was not used in IPv4. This is why NDP is considered as as one of the IPv6 advantages. The NDP concept specified for IPv6 was standardized in RFC 2461 [14] and updated in RFC 4861 [6]. NDP is a layer 3 protocol that supports the operation of IPv6 as the main protocol for Internet communication.

NDP works on top of Internet Control Message Protocol version 6 (ICMPv6) protocol messages. It uses up to five ICMPv6 messages to solve a number of problem regarding the interaction between neighboring nodes in the same link. The interaction could be divided into two categories: host-to-router communication and host-to-host communication. The five messages are Router Solicitation (RS), Router Advertisement (RA), Neighbor Solicitation (NS), Neighbor Advertisement (NA) and Redirect message.

A. Host- to- Router Communication

In an IPv6 network, there are two types of nodes – host and router. Host is an IPv6 node that is not a router. Router in this case is an edge router connected directly to the internal host(s) and at the same time connected to the Internet cloud externally. It acts as a border gateway between local network and external network. It would forward IPv6 packets from and to the host(s) in the local network. Prior to performing this function, the access router first has to communicate with the member host in local network. The communication is done using NDP protocol. There are at least five processes on the host-to-router communication including router discovery, prefix discovery, parameter discovery, address auto configuration as well as redirect.

Router discovery process could also be combined with prefix discovery and parameter discovery. It is conducted by exchanging a pair of NDP message, Router Solicitation (RS) and Router Advertisement (RA). We provided the router discovery discussion in [15]. Prefix discovery is a process to generate IPv6 address in the host. The router sends RA message containing one or more of five NDP options including MTU information, prefix information and link layer address of the router. Upon getting the RA message, the host configures itself by generating IPv6 address based on the received prefix information, sets the packet size based on the MTU information as well as stores the link layer of router in its neighbor cache.

Router Discovery is very important in the operation of IPv6 protocol in a network. This is used by an IPv6 host not only to discover routers in the same link but also to get link parameter and network parameter. Using this mechanism, an IPv6 host could generate IPv6 address which is needed to communicate with the outside world. Failure to generate an IP address would break the communication for the host. Thus, it is clear why we cannot simply block or disable ICMPv6 message in IPv6 environment.

B. Host to Host Communication

Host is defined as an IPv6 node that is not a router but, such as PC, laptop and hand phone [16]. To get IPv6 address, a host must communicate with the router using the router discovery mechanism. However, an IPv6 host also needs to communicate with other IPv6 host in the same network to get neighbor status information. This includes address resolution, next-hop determination, neighbor unreachability detection and duplicate address detection.

Address resolution is done to know link layer address of neighboring nodes. This is because an IPv6 node cannot communicate with other nodes in the same link with knowing only its IPv6 address. A node also needs link layer address or MAC address of corresponding nodes. This can be done by using address resolution mechanism. In IPv4, this mechanism is handled by address resolution protocol (ARP) [17]. ARP uses broadcast delivery method that sends ARP messages to all hosts in a local area network including computer, printer and scanner. This would potentially have effect on non related nodes in the network. IPv6 limits the number of receiving hosts by using the concept of multicast group of node as well as solicited node multicast address. Further, only certain node will receive NDP message [18].

Next-hop determination is a mechanism to determine the status of on-link neighbor to which an IPv6 packet to be sent. This is required to map destination IP address into neighboring node IP address. If the destination is on-link nodes, it requires MAC address of the destination. Otherwise, if the destination is a node outside the network, the sender will send the packet to the border router. Neighbor unreachability detection is a mechanism to track the status of reachability of neighboring node. An unreachable node could not receive any message. By knowing a neighbor's status, a sender host can determine how and where to send its packet.

IP address should be unique. In order to ensure each generated IPv6 address is unique, duplicate address detection mechanism is introduced. After a new host received the prefix information from default router, it would generate a tentative IPv6 address. It then sends a message to multicast group of nodes to confirm whether the tentative address is unique. If there is no response, it means the address is not in used. Otherwise, it will generate a new tentative IPv6 address and repeat the duplicate address detection procedure again. All the host-to-host communication is done by exchanging a pair of NDP messages, Neighbor Solicitation (NS) and Neighbor Advertisement (NA).

III. Methodology

Current implementation of IPv6 is done in dual stack mode as most Internet infrastructure is still dependent on IPv4. Currently, all recently produced networking devices as well as operating system have already supported IPv6 protocol beside IPv4. This study was conducted in the dual stack environment both for wired and wireless in National Advanced IPv6 Centre, Universiti Sains Malaysia. We captured the network traffic in the lab in order to get sample of IPv6 traffic from and to local host in the lab.

The captured traffic is then classified as IPv4 traffic or IPv6 traffic. The latter were further classified into neighbor discovery traffic to identify the router discovery and neighbor discovery message. The NDP packet is observed in order to understand the behavior of the traffic as well as the possibility for it to be exploited.

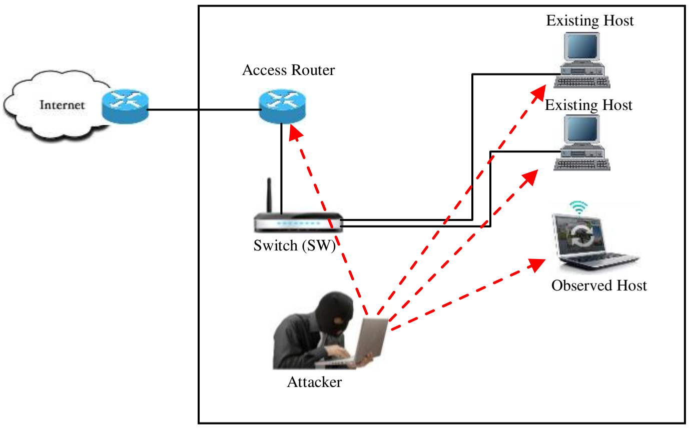


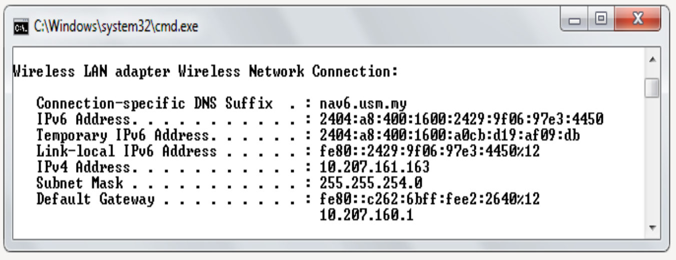
Figure 1. Topology on the Experimentation

Figure 1 is a topology of the experiment to observe the exploitation of RA message used to attack an observed host on wireless link. There are five nodes in the setup - an access router, a switch, an existing host, an observed host and an attacker. The nodes were connected directly via a layer two switch. The attacker captured all communication messages between router and existing host as well as observed host. Afterward, the attacker exploits the RA message to attack the observed host.

IV. Result and Discussion

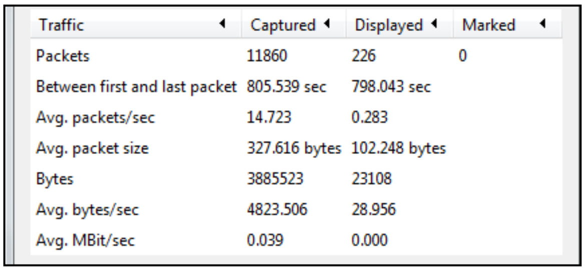
The experiments were done to get sample of Internet traffic in NAv6 computer lab. As the lab network is a dual stack IPv4 and IPv6 network, each connected nodes supporting dual stack will have at least one IPv4 address and a minimum of two IPv6 addresses. Figure 2 shows an example of IP configuration on one of the hosts. Host's IPv4 address is 10.207.161.163 and its IPv6 address is 2404:a8:400:1600:2429:9f06:97e3:4450, 2404:a8:400:1600:a0cb:d19:af09:db and fe80::2429:9f06:97e3:4450%12. The host has three IPv6 address generated by the host itself with prefix from the access router. The gateway is 10.207.160.1 for IPv4 link and for IPv6, fe80::c262:6bff:fee2:2640%12. The IPv6 address of the gateway is a link local address of the default router connected to the host. The '%' is to identify the interface used to communicate with neighboring node.

As shown in the Figure 2, the host under observation is connected using wireless adapter. The host can be relocated from one network to another. It is also usable in public area such as at airport, coffee shop as well as office BYOD. In a period of 13.5 minutes, we managed to capture 11,860 IP packets in various format and protocol as summarized in Figure 3. The displayed traffic shown in Figure 3 is the total number of IPv6 packets that were captured. Only 226 packets or 2% of the total number of packets captured were IPv6 packets. This is because almost all Internet infrastructures are still using IPv4. IPv6 packets could also be sent through the network using tunneling mode that will be categorized as IPv4 packet by packet capture applications. In addition, most of accessed website is still using IPv4.



```
Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . : nav6.usm.my
   IPv6 Address. . . . . . . . . . . : 2404:a8:400:1600:2429:9f06:97e3:4450
   Temporary IPv6 Address. . . . . . : 2404:a8:400:1600:a0cb:d19:af09:db
   Link-local IPv6 Address . . . . . : fe80::2429:9f06:97e3:4450%12
   IPv4 Address. . . . . . . . . . . : 10.207.161.163
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : fe80::c262:6bff:fee2:2640%12
                                       10.207.160.1
```

Figure 2. IP Configuration in Observed Host



Traffic	Captured	Displayed	Marked
Packets	11860	226	0
Between first and last packet	805.539 sec	798.043 sec	
Avg. packets/sec	14.723	0.283	
Avg. packet size	327.616 bytes	102.248 bytes	
Bytes	3885523	23108	
Avg. bytes/sec	4823.506	28.956	
Avg. MBit/sec	0.039	0.000	

Figure 3. Summary of Captured IP Packet

The more important aspect is the kind of IPv6 packet captured in the observation. 167 packets out of 266 IPv6 packets, which is equivalent to 74%, are ICMPv6 packets. Then, out of the 167 ICMPv6 packets, 140 or 84% of it are neighbor discovery message. This means communication between IPv6 nodes in local network are dominated by the NDP messages. This is happening behind the scene without the user's knowledge or intervention. In addition, this will be done dynamically and continuously as long as there is host connected in the IPv6 local network. This is the nature of NDP mechanism in an IPv6 network.

Even when there is no IPv6 traffic flowing from and to external network (Internet cloud), the local IPv6 traffic will still be present. Neighbor discovery message is exchanged by IPv6 nodes inside a local network itself. This would be done automatically if the host has support for IPv6 protocol. However, for majority of newer devices, the IPv6 protocol support is configured to run immediately when the devices start up.

The NDP messages captured during the experimentation could be classified into two: host-to-router communication and host-to-host communication. The first is shown by the router discovery message including RS and RA. However, due to the observed host has already gotten the IPv6 address (Figure 2), there is no RS message. RS message is sent by host requesting router information. Router will reply by sending RA message.

However, the router also sends RA message periodically. When a new host has already configured an IPv6 address and discovered on link, it will not send RS message anymore.

While the host-to-host communication consist of both NS and NA message as communication between hosts in the local network. NS is sent to request any information including link layer address, uniqueness address confirmation as well as neighbor unreachability status. The captured IPv6 packets could be classified as in Figure 4.

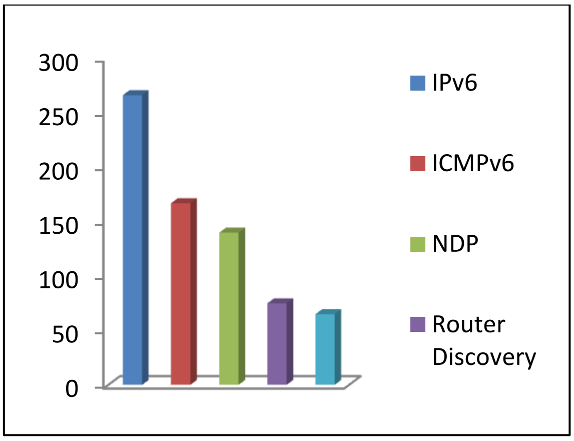
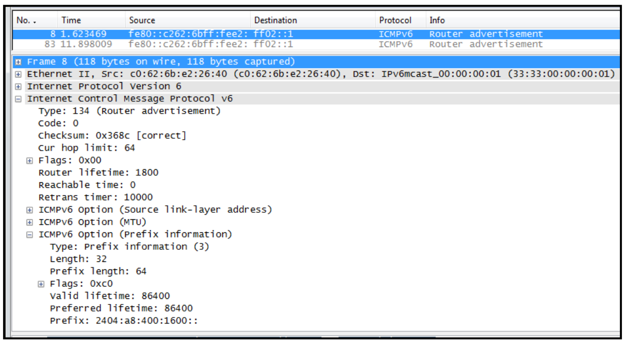


Figure 4. IPv6 Packet Classification



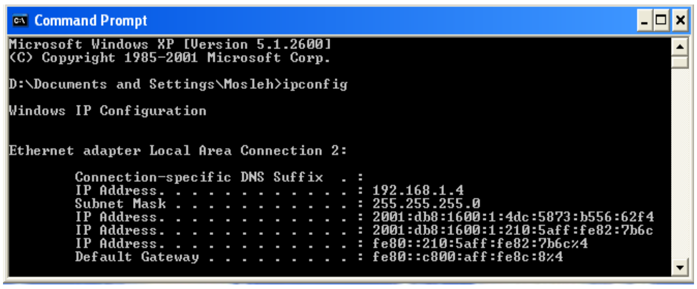
```
No. .   Time        Source                 Destination   Protocol  Info
      8 1.623469    fe80::c262:6bff:fee2:  ff02::1       ICMPv6    Router advertisement
     83 11.898009   fe80::c262:6bff:fee2:  ff02::1       ICMPv6    Router advertisement

⊞ Frame 8 (118 bytes on wire, 118 bytes captured)
⊞ Ethernet II, Src: c0:62:6b:e2:26:40 (c0:62:6b:e2:26:40), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
⊞ Internet Protocol Version 6
⊟ Internet Control Message Protocol v6
    Type: 134 (Router advertisement)
    Code: 0
    Checksum: 0x368c [correct]
    Cur hop limit: 64
  ⊞ Flags: 0x00
    Router lifetime: 1800
    Reachable time: 0
    Retrans timer: 10000
  ⊞ ICMPv6 Option (Source link-layer address)
  ⊞ ICMPv6 Option (MTU)
  ⊟ ICMPv6 Option (Prefix information)
      Type: Prefix information (3)
      Length: 32
      Prefix length: 64
    ⊞ Flags: 0xc0
      Valid lifetime: 86400
      Preferred lifetime: 86400
      Prefix: 2404:a8:400:1600::
```

Figure 5. Router Advertisement Message

The result presented in Figure 2, Figure 3 and Figure 4 clearly show NDP messages were exchanged between IPv6 nodes in the local area network. This process is hidden from the view of users. In addition, most Internet users are oblivious to the version of Internet Protocol they are connected to. Their only concern is about getting internet connectivity regardless of which Internet Protocol their network is using.

In a public network, everybody could use the available Internet connection to do anything including malicious activities. An attacker usually needs other node IP address to direct their attacking activities. They usually perform scanning on the network to obtain other node address. In IPv6 environment, there is no need for network scanning at all to discover the network. They just need to capture the NDP message transmitted from and to other nodes in the local network they are attached to. They can get all IP addresses as well as MAC addresses of other nodes in the same link.

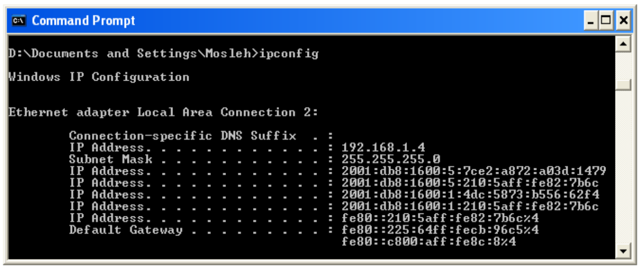
The NDP message could be exploited to do harmful activities as summarized in [19]. In this paper we just show result of experimentation on the exploitation on RA message as in Figure 5. Attacker could use the message to perform a number of malicious activities such as RA spoofing, RA flooding, kills the default router, rogue router, etc. All host in the network usually connected to a default gateway or default router. This means the host will get RA message from the router when they connect to the network. Currently most of recently manufactured network devices have built-in support for IPv6. Therefore, we cannot avoid the automatic communication between hosts in IPv6 connection even though the local network does not connect to external IPv6 network.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\Mosleh>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.4
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : 2001:db8:1600:1:4dc:5873:b556:62f4
        IP Address. . . . . . . . . . . . : 2001:db8:1600:1:210:5aff:fe82:7b6c
        IP Address. . . . . . . . . . . . : fe80::210:5aff:fe82:7b6c%4
        Default Gateway . . . . . . . . . : fe80::c800:aff:fe8c:8%4
```

Figure 6. Default Gateway before Attack

Attacker in Figure 1 captured RA message sent from the access router to observed host. After learning the RA message content, changes were made to the message prior to resending the forge message using the same source address. For example, the attacker could replace the default router information with its own information. The IPv6 address of the node before the successful attack is shown in Figure 6. The default gateway is fe80::c800:aff:fe8c:8%4. The attacker manipulates the RA message and resends to observed host. The observed host receives the message then updates its cache table including the default router information. The new default router, pointing to the attacker's machine, is put on the top of the list as shown in Figure 7. When the victim wants to send any packet through a router, the packet will be sent to the attacker instead of to the legitimate access router. Thus, the packet will not reach the destination.



```
D:\Documents and Settings\Mosleh>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.4
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : 2001:db8:1600:5:7ce2:a872:a03d:1479
        IP Address. . . . . . . . . . . . : 2001:db8:1600:5:210:5aff:fe82:7b6c
        IP Address. . . . . . . . . . . . : 2001:db8:1600:1:4dc:5873:b556:62f4
        IP Address. . . . . . . . . . . . : 2001:db8:1600:1:210:5aff:fe82:7b6c
        IP Address. . . . . . . . . . . . : fe80::210:5aff:fe82:7b6c%4
        Default Gateway . . . . . . . . . : fe80::225:64ff:fecb:96c5%4
                                            fe80::c800:aff:fe8c:8%4
```

Figure 7. Node A after Attack

In terms of fake prefix information, Figure 7 also shows that the observed host has two different global prefixes. One prefix came from a legitimate access router and the other one from the attacker. We can see that the legitimate default gateway appears at the bottom of the list. The attacker could also perform RA flooding attack by sending thousands of RA messages with different prefixes information. If so, the observed host will receive many prefixes and thus generate many different IPv6 addresses.

V. CONCLUSION

IPv6 is the successor of the current Internet Protocol that has depleted its address space. The new protocol was designed with a number of advantages including the NDP as supporting component in IPv6 operation. However, the protocol does not have any built-in security mechanism. Therefore, the implementation of NDP is vulnerable to local threats using NDP message exploitation.

This paper presented the risks on the implementation of NDP protocol on IPv6 network. Since the use of IPv6 is a necessity in internet environment, disabling or disconnecting IPv6 network is not an option. Therefore, a security mechanism must be in place to avoid compromise and exploits of the protocol in the future. Even though there has been a number of security mechanisms proposed such as SeND and RA Guard, their use is very much limited, thus NDP still remain vulnerable.

ACKNOWLEDGMENT

This research was supported by the Research University Grant No: 1001/PNAV/846064 funded by Universiti Sains Malaysia, in collaboration with Directorate General of Higher Education, Ministry of Education and Culture, the Republic of Indonesia and Taylor's University, Malaysia.

REFERENCES

[1] Ashton, K., *That 'internet of things' thing.* RFiD Journal, 2009. **22**: p. 97-114.

[2] *World Internet Statistic*. [cited 16 April 2014]; Available from: http://www.internetworldstats.com/.

[3] *IPv4 Exhaustion Counter*. [cited 2012 February 20]; Available from: www.ipv6forum.org.

[4] Davies, J., *Understanding IPv6* 2008, Washington: Microsoft Press.

[5] Audet, F. and C. Jennings, *Network address translation (NAT) behavioral requirements for unicast UDP*, 2007, BCP 127, RFC 4787.

[6] Rekhter, Y. and T. Li, *An architecture for IP address allocation with CIDR*. 1993.

[7] Narten, T., E. Nordmark, and W. Simpson, *H. Soliman," Neighbor Discovery for IP version 6 (IPv6)*, 2007, RFC 4861.

[8] Thomson, S. and T. Narten, *RFC 2462 IPv6 Stateless Address Autoconfiguration, 1998.* URL reference: http://www.ietf.org/rfc /rfc2462. txt.

[9] Droms, R., et al., *RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6).* Standards Track, http://www.ietf. org/rfc/rfc3315. txt, 2003.

[10] Supriyanto, et al., *Survey of Internet Protocol Version 6 Link Local Communication Security Vulnerability and Mitigation Methods*. IETE Technical Review, 2013. **30**(1): p. 64-71.

[11] Arkko, J., et al., *Secure neighbor discovery (SEND)*, 2005, RFC 3971.

[12] Levy-Abegnoli, E., et al., *IPv6 Router Advertisement Guard*, 2011, RFC 6105, Internet Engineering Task Force.

[13] Angelosante, D., E. Biglieri, and M. Lops. *Neighbor discovery for wireless networks*. ISIT 2007. IEEE International Symposium on Information Theory. 2007.

[14] Broch, J., et al. *A performance comparison of multi-hop wireless ad hoc network routing protocols*. in Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking. 1998. ACM.

[15] Narten, T., E. Nordmark, and W. Simpson, *RFC 2461 Neigbhour Discovery for IP Version 6 (IPv6), 1998.* URL reference: http://www. ietf. org/rfc/rfc2461. txt.

[16] Supriyanto, et al. *Security mechanism for IPv6 router discovery based on distributed trust management*. in RFID-Technologies and Applications (RFID-TA), 2013 IEEE International Conference on. 2013.

[17] Jankiewicz, E., J. Loughney, and T. Narten, *RFC 6434: IPv6 Node Requirements.* Internet Engineering Task Force, RFC, 2011.

[18] Plummer, D., *Address Resolution Protocol*, 1982, STD 37, RFC 826.

[19] Blanchet, M., *Migrating to IPv6 : A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks*. 2006, Québec, Canada: John Wiley & Sons Ltd.

[20] Nikander, P. and J. Kempf, E. Nordmark, *IPv6 Neighbor Discovery (ND) Trust Models and Threats*, 2004, rfc 3756.