Indian Journal of Science and Technology, *Vol 8(30), DOI: 10.17485/ijst/2015/v8i30/85940, November 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Significance of Duplicate Address Detection Mechanism in Ipv6 and its Security Issues: A Survey

Shafiq Ul Rehman* and Selvakumar Manickam

National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM), Penang, Malaysia; shafiq@nav6.usm.my

Abstract

IPv6 deployment is currently under way at a rapid pace. IPv6 introduced new features and capabilities lacking in IPv4 but as with any new technology, there are always security risks and challenges that need to be addressed. Duplicate Address Detection (DAD) is part of IPv6's Network Discovery Protocol that is vulnerable to security threats such as: Spoofing, Denial of Service (DoS). This survey paper, aims to present various techniques that were introduced to mitigate such security threats and highlight the limitations of techniques. Herein, we will discuss a) the concepts of Neighbor Discovery Protocol in IPv6 b) Duplicate Address Detection process c) security issues in Duplicate Address Detection d) proposed mitigation techniques and their limitations to encounter security threats and finally, conclusion and future work.

Keywords: DoS, Duplicate Address Detection, IPv6, Neighbor Discovery Protocol, Security, Source Address Validation

1. Introduction

The advancement of Internet technologies has raised various security issues including the limitation of IP address space, due to drawbacks in the IPv4 protocol as stated in[1]. To overcome these challenges, IETF defined a new version of the IP protocol IPv6 as described in[2,3], bringing with it advanced builtin services such as very large address space, simpler header format, autoconfiguration, builtin security feature as well as extensibility of IPv6 extension header as defined in[4].

One of the main objectives of IPv6 was to ease the addressing issues among the hosts, the discovery of network components. For such purpose, Neighbor Discovery Protocol (NDP) as described in[5]. It does not only replaces the traditional Address Resolution Protocol (ARP) but also provides several functionality such as Router Discovery, Nodes discovery on the same link, determines link-layer addresses, Duplicate Address Detection, and maintains the reachability information about paths to an active neighbor[6].

This survey paper will focus on Duplicate Address Detection (DAD)[7] and its security issues. Duplicate Address Detection (DAD) mechanism is part of NDP process and it is used to check the uniqueness of a self-generated address when IPv6 Stateless Address Autoconfiguration (SLAAC)[8,9] is enabled, which gives the host the ability to configure an interface automatically. However, stateful mechanism (DHCPv6) is out of the scope as this paper will focus only IPv6 Stateless Address Autoconfiguration (SLAAC) mechanism. Currently, Duplicate Address Detection (DAD) is vulnerable to security threats such as spoofing attacks, Denial of Service attacks (DoS)[10] etc.

2. Background

2.1 Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP)[5], one of the main protocols in the IPv6 suite, comprises Neighbor Discovery for IPv6 Request for Comments (RFC)

**Author for correspondence*

4861[5] and IPv6 Stateless Address Auto-configuration (SLAAC)[8].

The ND protocol uses five types of ICMPv6 (Internet Control Message Protocol version 6) messages[11]. These messages are: Router Solicitation (RS) type 133, Router Advertisement (RA) type 134, Neighbor Solicitation (NS) type 135, Neighbor Advertisement (NA) type 136, and Redirect type 137.

RS is sent by IPv6 hosts to discover neighboring routers on an attached link.

- RA is sent by IPv6 routers periodically or in response to a RS message.
- NS is sent by IPv6 nodes to resolve a neighbor's IPv6 address to its link-layer address (MAC address) or to verify if an IPv6 node is still reachable.
- NA is sent by IPv6 nodes in response to a NS message or to propagate a link-layer address change.
- Redirect messages are sent by IPv6 routers to inform hosts of a better first-hop for a destination.

ND messages comprise of an ND message header, ICMPv6 header, some ND message-specific data, and with zero or more ND options. Figure1 shows the format of a Neighbor Discovery message[12].

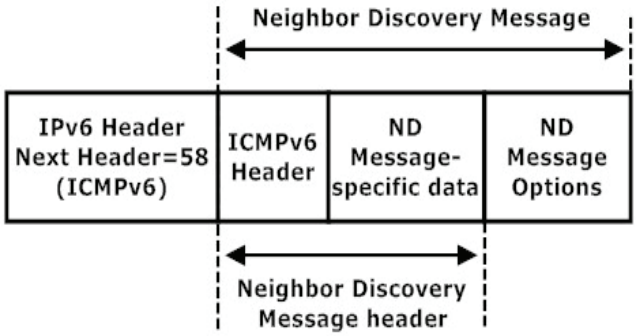

Figure 1. Format of a neighbor discovery message.

2.2 Neighbor Discovery

The aim of an IPv6 Neighbor Discovery (ND) is to allow IPv6 nodes to discover the presence and link-layer addresses of the other nodes on the same link. Also, it provides methods for router discovery on the local link, for detecting when a local node becomes unreachable, for resolving Duplicate Addresses Detection, and for routers to inform nodes when another router is more appropriate (redirect)[6]. To learn the link-layer address of another node that is assumed to be directly attached to the local link, the node that needs the address sends a Neighbor Solicitation (NS) message to a multicast address specified by the target address. If the target node is indeed present, it should be listening to the multicast address. Upon receiving the solicitation, it replies with a Neighbor Advertisement (NA) message. Figure 2 depicts basic neighbor discovery proces[6].

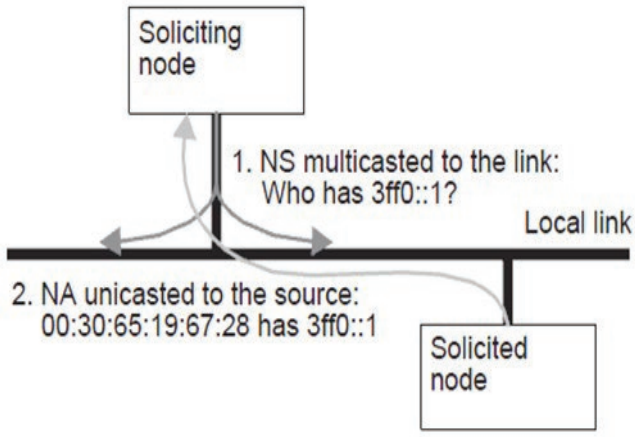

Figure 2. Basic neighbor discovery process.

2.3 IPv6 Stateless Address Autoconfiguration (SLAAC)

IPv6 stateless address auto-configuration (SLAAC)[8] was defined in RFC 4862 is a mechanism that enables IPv6 hosts to obtain IPv6 addresses from the local link automatically without any human intervention. A host performs several steps to autoconfigure its interfaces in IPv6. Initially, a new host sends a Router Solicitation (RS) message to router requesting for prefix information. In reply router sends a Router Advertisement (RA) message carrying router prefix information. Once a host receives router prefix can generate Interface Identifier (IID). In the absence of routers, a host can generate only link-local address which is enough for hosts to communicate within a same link[13,14]. Finally, an autoconfiguration process verifies its uniqueness on a link by performing a DAD process[9]. Figure 3 describes address autoconfiguration process.

2.4 Duplicate Address Detection (DAD)

Duplicate Address Detection ensures that all configured addresses are likely to be unique on a particular link,

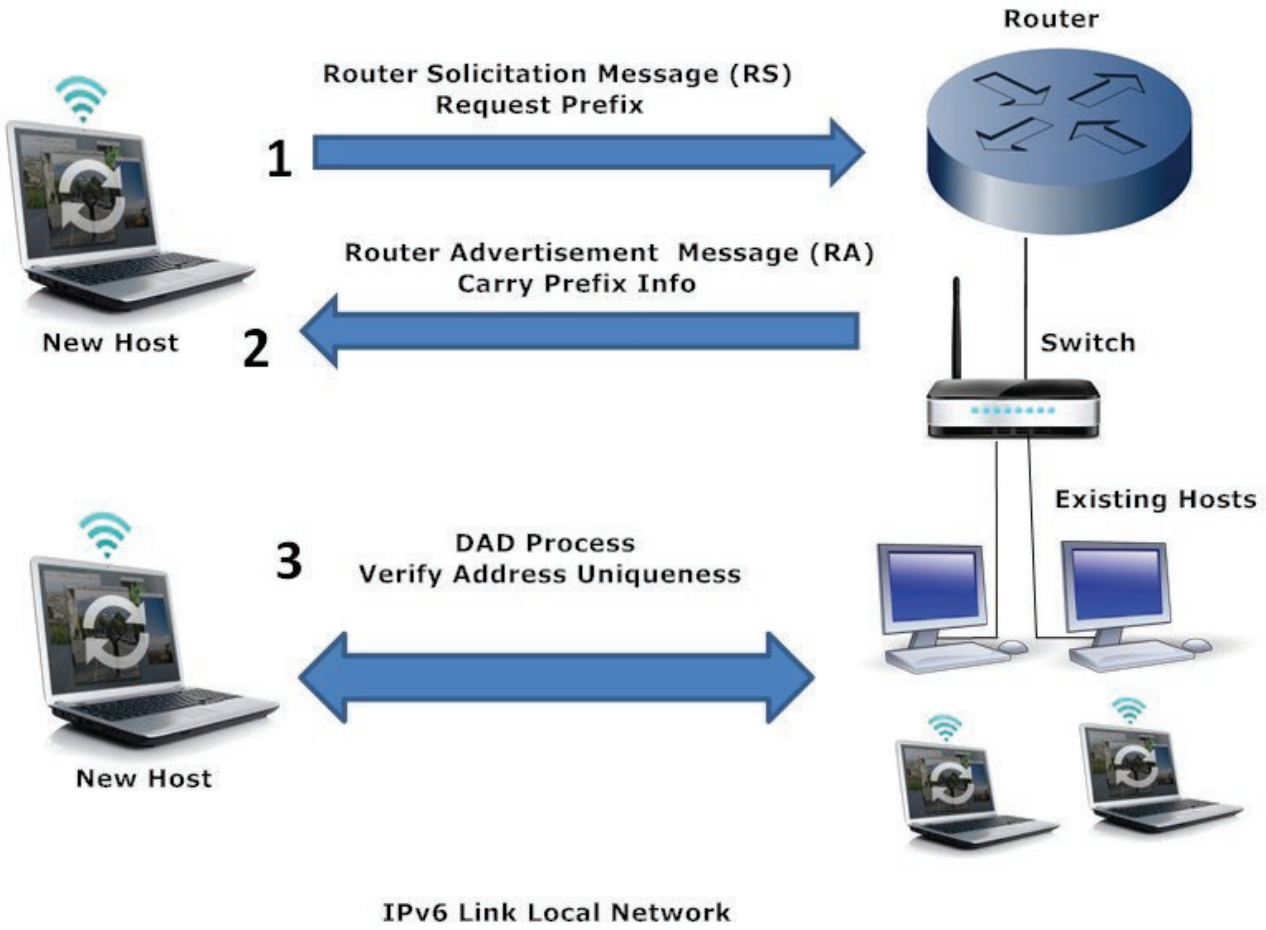

Figure 3. Address auto-configuration process.

every nodes has to perform DAD process before assigning the addresses to an interface[7,15]. When a new node joins the local link network or an existing node on the same link plans to take a new address for its own use. At first, it must make sure that no other node on the same link uses that address already. This is done by sending a series of Neighbor Solicitation (NS) messages to the local link. These messages contain the tentative IP address that the host would like to use. If the tentative address is already in use by some other host, the node already using the address will send a Neighbor Advertisement (NA) in response, and the first host must select a new tentative address. If the first host receives no replies to its solicitations, it is free to use the address[7,8]. Figure 4 illustrated Duplicate Address Detection process[6].

As illustrated in Figure 4, the new node firstly checks whether the IPv6 address it wants is already used by existing node(s), this is achieved by periodically multicasting Neighbor Solicitation (NS) messages with an unspecified source address targeting on the address which need to be checked. If the address being checked is already used by another node, a Neighbor Advertisement (NA) will be sent by this node as response. Otherwise, if there isn't corresponding Neighbor Advertisement (NA) received, the processing node may consider the address being checked is available.

3. Security Issues in Duplicate Address Detection

During unique address verification process, Duplicate Address Detection (DAD) assumes that all the nodes on local link are trusty to each other. However, if the Neighbor Solicitation (NS) message is replied by a malicious node continuously, it will stop link local nodes to generate unique addresses thus will prevent them from address

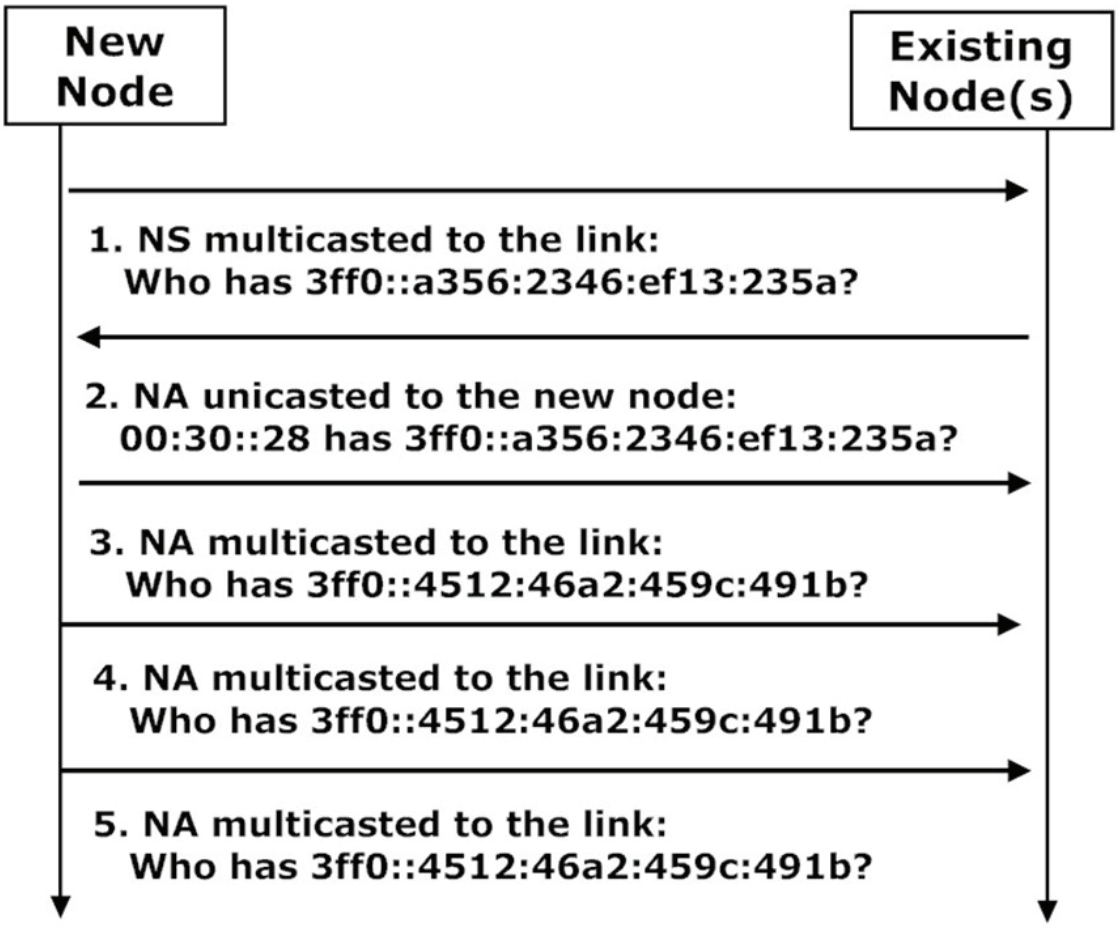

Figure 4. Duplicate address detection process.

configuration. Also, the chances are NS message could get lost on a local link or the reply NA messages could get lost; in that case a node may configure an address which is already used by an existing node thus can cause conflict in an address configuration[7,16].

Therefore, from the studies[13,17,18] it has been found that the original Duplicate Address Detection (DAD) process is vulnerable to security threats like Spoofing attacks, Denial of Service attacks (DoS).

3.1 Spoofing Attack

In Neighbor Discovery an attacker can run spoofing attack during Duplicate Address Detection (DAD) process. When a host sends Neighbor Solicitation (NS) message to verify the uniqueness of address on a particular link an attacker can spoof the IP address and later reply back to the host with Neighbor Advertisement (NA) message to claim that IP address as shown in Figure 5[10]. Figure 5 presents spoofing attack.

3.2 Denial of Service Attack

In Denial of Service (DoS) attack an attacking node can respond to every Duplicate Address Detection attempts. In case an attacker claims addresses, the other nodes in a local link will never be able to obtain an address as stated in[19].

Normally, in DoS attacks a victim node's can be denied from the services by wasting victim node's resources and disrupt the victim node's communication with other nodes on a local link.

During the DAD process an attacker can disguise the victim node while attempting to obtain an IPv6 address by using the specific address and respond to the detection message, thus makes victim node unable to get an IPv6

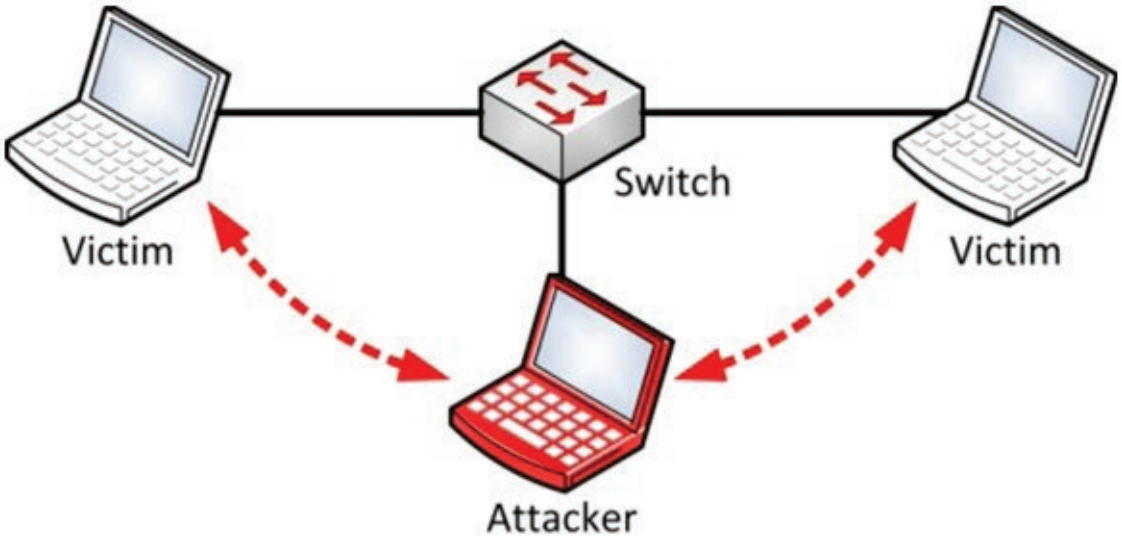

Figure 5. Spoofing attack.

address. Figure 6 depicts the Duplicate Address Detection attack[17].

4. Current Mitigation Techniques in Duplicate Address Detection and Their Limitations

Considering the importance of security, IPv6 protocol was developed with builtin security feature known as Internet Protocol Security (IPSec)[20] in order to make secure communication possible over the networks. IPSec is IP based Security mechanism which is supposed to provide end-to-end security. But, the drawback with IPSec implementation is that it raises bootstrapping issues while using Internet Key Exchange (IKE)[21]. Thus, IPSec option is not suitable for link local communication as mentioned in[22]. To counter this issue, the Internet Engineering Task Force (IETF) introduced Secure Neighbor Discovery (SeND)[23] which is actually the extension to NDP protocol.

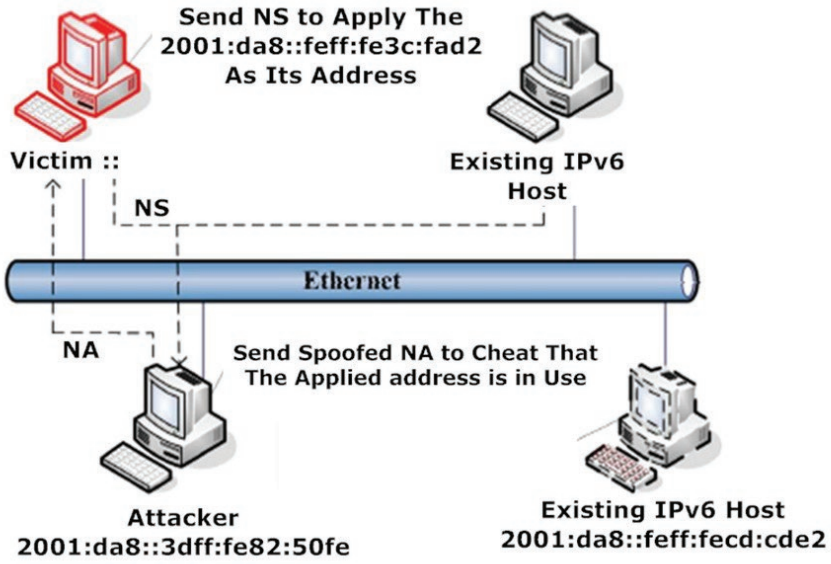

Figure 6. Duplicate address detection attack.

4.1 Secure Neighbor Discovery (SeND)

Secure Neighbor Discovery (SeND) has been proposed and standardized in[24,25]; SeND provides functionality to protect NDP messages against both link layer and network layer threat. Thus, improves the overall security of Neighbor Discovery Protocol (NDP), including the security in DAD process. SeND is an extension of NDP protocol with advanced security features such as Cryptographically Generated Addresses (CGA)[23,26] parameters, RSA signature nonce, and timestamp. It also uses two new ICMPv6[11] messages: Certificate Path Solicitation (CPS) and Certificate Path Advertisement (CPA). Although SeND addresses almost all threat and vulnerability issues with neighbor discovery. However, it does not cover NDP communication confidentiality and link layer security including the DAD process.

As per the study[18], it has been found that SeND has a few limitations that restrict the NDP extension being widely implemented. Such as, the CGA option cannot ascertain the identity of real node and it is also not enough to determine the CGA address that belongs to appropriate node. Hence, attacker could catch NDP message and modify the CGA parameters. Other limitation is the implementations of SeND which results in more processing time that consume CPU as well as bandwidth of nodes. Thus, if implemented, its process (authorization and certificate validation function) can add delay and increase complexity during DAD process as highlighted in[13].

4.2 Source Address Validation

In security point of view, during the DAD process verification of the source address is crucial in order to make sure that packet comes from the valid source. Normally, an attacker can victimize the source address for spoofing purpose. Based on reviews Source Address Validation Architecture (SAVA) in[27] has been proposed to validate the source address. SAVA can be implemented on link local communication as it can prevent from spoofing from other nodes within the same link (IPv6 Prefix), by creating a binding between link local address, IP address, and/or with switch ports[28].

Later, IETF proposed an improvement of SAVA called Source Address Validation Improvement (SAVI) in[27]. In order to secure the link local communication from source address spoofing. SAVI mechanism works by snoop the interaction processes of IPv6 packets. This process will fetch some valuable information. Later, SAVI creates a binding between link local address, source IPv6 address, and with switch port. Based on such gathered information, SAVI does the packet filtering by forwarding only the matched packets while discarding others.

First Come First Serve (FCFS) SAVI[29] was proposed in order to make a secure neighbor discovery includes Duplicate Address Detection (DAD) process and to validate source address of IPv6 packets. The proposed mechanism is aimed to enhance the ingress filtering techniques to support detection and prevention of source address spoofing. Hence, during link local communication, SAVI is not concerned about other security issues on the network. Also if the binding anchor is spoofable, it could open the gates for new security threats particularly DOS attacks as stated in[27].

4.3 SSAS: Simple Secure Addressing Scheme

Simple Secure Addressing Scheme (SSAS) in[13], was proposed to address the security issues in Cryptographically Generated Addresses (CGA) in RFC 3972[26] and Privacy Extension in RFC 4941[14] in IPv6 auto-configuration addressing scheme[13]. The proposed mechanism uses new algorithm to generate the Interface Identifier (IID). Thus, reduces the computational cost while prevents from security threats such as IP spoofing. Although, Simple Secure Addressing Scheme (SSAS) offers some security enhancement to the existing autoconfiguration addressing system yet it does not prevent DoS attacks on Duplicate Address Detection process which is still the main security concern in address autoconfiguration. Hence, as per study[13] a secure Duplicate Address Detection mechanism in IPv6 is yet to be proposed.

4.4 A Pull Model

Comparing with Secure Neighbor Discovery Protocol (SeND), a newly Duplicate Address Detection mechanism was proposed known as Pull Model[7,30] in order to reduce the overhead and enhance flexibility in address generation. Unlike normal Duplicate Address Detection (DAD) procedure, rather sending Neighbor Solicitation (NS) message to check the uniqueness of the address, Pull Model performs hash computation to check the generated tentative address with all the existing addresses on a same link. If no match found it can configure the

Table 1. Highlights a summary of the current mitigation techniques on link local communication in IPv6 security identifying their strength and weaknesses

Techniques	Security Properties	Security Issues
IPSec	Provides Security features like; Authentication, Confidentiality and Integrity	Issues of Internet Key Exchange (IKE) management in IPv6 host initialization
SeND	Counters major NDP vulnerabilities such as; address spoofing, replay attacks etc.	Confidentiality issues, more complex and lacks source address validation
SAVA	Validates source address, counters the spoofing attacks	Vulnerable to DoS attacks
SAVI	Secures host-host communication from source address spoofing	If binding anchor is spoofable. Susceptible to new vector attacks
SSAS	Reduces computational cost and prevents from IP spoofing	Unable to prevent Dos Attacks during DAD process
PULL Model	Reduces overhead in address generation	Vulnerable to brute force attacks and inverting attacks

address else it generates another address and repeats the same process.

However, the drawback with Pull Model is that if the hash function is too short it is vulnerable to brute force attack[31]. And, if the hash value is too long will opens the door for possible inverting attack. Thus, from the studies[7,31] it is found that Pull Model is also not applicable for Duplicate Address Detection process. Although, it claims to reduce overhead and enhance address flexibility but it is susceptible to possible security threats.

5. Conclusion and Future Work

Considering the future of Internet communication, IPv6 protocol was introduced not only to resolve the addressing issues but also with many features as it is also known as next generation Internet protocol. Among such features security was the major one in order to make the communication secure and reliable. IPv6 has builtin security feature known as IPSec, it is widely used for secure communication. But, it is not suitable for the link local communication due to the issues of IKE management. Thus, IETF proposed Secure Neighbor Discovery (SeND) to secure link local communication. SeND proved to counter major NDP security vulnerability. However, Secure Neighbor Discovery (SeND) does not provide confidentiality and its implementation adds more complexity in the address autoconfiguration and Duplicate Address Detection (DAD) process. Based on the study, source address is considered the crucial information to attackers. In order to counter that other security mitigation techniques were proposed such as; Source Address Validation Address (SAVA), Source Address Validation Improvement (SAVI), Pull Model and recently Simple Secure Addressing Scheme (SSAS).

However, all security mechanisms possess some limitations like SAVA is vulnerable to DoS attacks and SAVI technique if binding anchor is spoofable; might be vulnerable to other security threats. Pull Model is vulnerable to brute force and inverting attacks. Simple Secure Addressing Scheme (SSAS) is enhanced mechanism yet unable to prevent DoS attack.

Hence, from the survey it was found that there is no such security mechanism yet being proposed to secure DAD process in link local communication. Therefore, our future study would be to propose a security mechanism which ensures a secure DAD process during address autoconfiguration in IPv6 link local communication by preventing it from security vulnerabilities like Denial of Service (DoS) attacks while maintaining its less overhead process.

6. Acknowledgment

This research was supported by the Ministry of Higher Education of Malaysia, in collaboration with National Advanced IPv6 Centre (NAV6), Universiti Sains Malaysia.

7. References

1. Durdagi E, Buldu A. IPV4/IPV6 security and threat comparisons. Procedia-Social and Behavioral Sciences. 2010;2(2):5285–91.
2. Davies J. Understanding IPv6: Your Essential Guide to IPv6 on Windows Networks: "O'Reilly Media, Inc."; 2012.
3. Hagen S. IPv6 essentials: "O'Reilly Media, Inc."; 2006.

4. Deering SE. Internet protocol, version 6 (IPv6) specification; 1998.
5. Narten T, Simpson WA, Nordmark E, Soliman H. Neighbor discovery for IP version 6 (IPv6); 2007.
6. Arkko J, Aura T, Kempf J, Mäntylä V-M, Nikander P, Roe M, editors. Securing IPv6 neighbor and router discovery. Proceedings of the 1st ACM workshop on Wireless security; 2002.
7. Yao G, Bi J, Wang S, Zhang Y, Li Y, [eds]. A pull model IPv6 Duplicate Address Detection. Local Computer Networks (LCN), IEEE 35th Conference; Denver; Colorado; U.S.A; IEEE: 2010.
8. Thomson S. IPv6 stateless address autoconfiguration; 1998.
9. AlSa'deh A, Rafiee H, Meinel C. IPv6 stateless address autoconfiguration: Balancing between security, privacy and usability. Foundations and Practice of Security: Springer; 2013. p.149–61.
10. Alangar V, Swaminathan A. Ipv6 Security: Issue of Anonymity; 2013.
11. Conta A, Gupta M. Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6) specification. 2006.
12. Chiu S, Gamess E, [eds]. Easy-SEND: A Didactic Implementation of the Secure Neighbor Discovery Protocol for IPv6. Proceedings of the World Congress on Engineering and Computer Science; 2009.
13. Rafiee H, Meinel C, [eds]. SSAS: A simple secure addressing scheme for IPv6 autoconfiguration. Privacy, Security and Trust (PST), Eleventh Annual International Conference; Tarragona, Catalonia: 2013.
14. Narten T, Draves R, Krishnan S. Privacy extensions for stateless address autoconfiguration in IPv6; 2007.
15. Moore N. Optimistic Duplicate Address Detection (DAD) for IPv6; 2006.
16. Caicedo CE, Joshi JB, Tuladhar SR. IPv6 Security Challenges. IEEE Computer. 2009;42(2):36–42.
17. Yang X, Ma T, Shi Y, editors. Typical dos/ddos threats under ipv6. Computing in the Global Information Technology, ICCGI International Multi-Conference; Guadeloupe; French Caribbean: 2007.
18. AlSa'deh A, Meinel C. Secure neighbor discovery: Review, challenges, perspectives, and recommendations. Security and Privacy. IEEE. 2012; 10(4):26–34.
19. Lee Y, Shin S, Choi S, Son H-g, [eds]. IPv6 Anomaly Traffic Monitoring with IPFIX. Internet Monitoring and Protection. ICIMP Second International Conference; Silicon Valley; USA: 2007.
20. Kim T, Kim I, Zhen Z, Kim JH, Gyeong G, Eom YI, editors. A cooperative authentication of ipsec and send mechanisms in ipv6 environments. Advanced Language Processing and Web Information Technology. ALPIT'08 International Conference; 2008.
21. Arkko J, Nikander P, [eds]. Limitations of IPsec policy mechanisms. Security Protocols: Springer. 2005.
22. Khoussainov R, Patel A. LAN security: Problems and solutions for Ethernet networks. Computer Standards and Interfaces. 2000; 22(3):191–202.
23. Kukec A, Bagnulo M, Mikuc M, [eds]. SEND-based source address validation for IPv6. Telecommunications, 2009 ConTEL 2009 10th International Conference; Zagreb; Croatia: 2009.
24. Arkko J, Kempf J, Zill B, Nikander P. Secure Neighbor Discovery (SEND). RFC 3971; March 2005.
25. Cheneau T, Laurent M, [eds]. Using SEND Signature Algorithm Agility and Multiple-Key CGA to Secure Proxy Neighbor Discovery and Anycast Addressing. Network and Information Systems Security (SAR-SSI), Conference; 2011.
26. Aura T. Cryptographically Generated Addresses (CGA); 2005.
27. Hasbullah IH, Murugesan RK, Ramadass S. Survey of Internet Protocol Version 6 Link Local Communication Security Vulnerability and Mitigation Methods. IETE Technical Review (Medknow Publications and Media Pvt Ltd). 2013; 30(1).
28. Wu J, Ren G, Li X, [eds]. Source address validation: Architecture and protocol design. Network Protocols. 2007 ICNP IEEE International Conference; Beijing; China: 2007.
29. Nordmark E, Bagnulo M, Levy-Abegnoli E. FCFS SAVI: First-Come, first-served source address validation improvement for locally assigned IPv6 addresses. Request for Comments. 2012; 6620.
30. Duan Z, Gopalan K, Dong Y, [eds]. Push vs. pull: Implications of protocol design on controlling unwanted traffic. Proc USENIX Steps to Reducing Unwanted Traffic on the Internet Workshop (SRUTI 2005); 2005.
31. Apostol K. Brute-force Attack; 2012.