Research on IPv6 Neighbor Discovery Protocol (NDP) Security

Tao Zhang
College of Information Science and Engineering,
Ocean University of China,
Qingdao, China
e-mail: oucseczt@126.com

Zhilong Wang
College of Information Science and Engineering,
Ocean University of China,
Qingdao, China
e-mail: zhilongwang@foxmail.com

Abstract—**With the benefit of large address space, flexible header extension, high security and mobility, IPv6 is introduced as the next generation Internet protocol. NDP is a necessary part of IPv6 and provides nodes with a method to get the link-local addresses of nodes on the link. NDP has the functions of address resolution, router discovery and duplicate address detection. However, NDP is designed with the assumption that nodes in the network are trusted. So it is vulnerable to various attacks such as DoS, DDoS, replay and redirect. SEND is proposed to come across the threats against NDP, but it does not work well as expected. Security considerations are the main reasons for the application of IPv6. NDP security is an important part of IPv6 security. We analyze the security of NDP and SEND, and summarize the latest advances on how to protect NDP against attacks and enhance NDP security.**

Keywords-IPv6; NDP; SEND; security research

I. INTRODUCTION

The current version of Internet Protocol, Internet Protocol version 4 (IPv4), is robust, interoperable, and easy to implement [1]. With rapid development of Internet and its application, IPv4 is limited in the address space, mobility, QoS (quality of service), security and so on. According to the CERNET(China Education and Research Network), there is no IPv4 address to allocate in Asia, Europe, Latin America and Northern America.

Internet Protocol version 6 (IPv6) is introduced as the next generation Internet Protocol, which is designed by IETF(Internet Engineering Task Force) to replace IPv4[2]. Exhaustion of IPv4 address space and security considerations are the major impetuses of introduction of IPv6. Compared with IPv4, IPv6 [3] increases the IP address size from 32 bits to 128 bits, simplifies header format, improves support for extensions and options, enables the labeling of packets, and supports authentication, data integrity and mobility. IPv6 defines a new type of address called anycast address to send packets to any one of a group of nodes. IPv6 simplifies necessary header fields and introduces extensions and options to support authentication, data integrity, and other functions.

In April 2016, according to CERNET, there are 71 countries and regions who applied for 341 IPv6 addresses in total. IPv6 is formally published in 1996, however, it does not commercialize by now. Security issues is the main reason for the application of IPv6 [4]. NDP (Neighbor Discovery Protocol) is used for address resolution process in IPv6. However, NDP assumes that all nodes in the link are reliable and trusted. So there are many security risks and threats with the practical use of NDP. And NDP security is an important part of IPv6 security. We are to analyze the security of NDP and SEND, to discuss latest advances in NDP security, and to provide guidelines for better and securer application of NDP.

The organization of this paper is as follows. In section II, we introduce NDP, SEND and analyze the security threats of the two protocols. In section III, we survey on existing solutions proposed by researchers to mitigate security threats against NDP and SEND. Finally we present our conclusions in section IV.

II. NDP AND SECURITY ANALYSIS

A. NDP[5]

NDP is a necessary part of IPv6 protocol suite, provides an method for an node in the local link to discover the link-local address. With the use of NDP, nodes can discover other nodes on the link, determine their link-layer addresses to find routers, and maintain reachability information about the paths to active neighbors. NDP also has many specific functions such as Address Auto-configuration, Router Discovery (RD), Neighbor Un-reachability Detection (NUD), Address Resolution, and Duplicate Address Detection (DAD).

1) Neighbor discovery message

NDP defines five kinds of ICMPv6 messages, including Router Solicitation(RS), Router Advertisement(RA), Neighbor Solicitation(NS), Neighbor Advertisement(NA) and Redirect.

Router Solicitation. Hosts send RS to prompt routers to generate RA message.

Router Advertisement. RA is sent by routers as a response to RS. Routers may also send RS periodically.

Neighbor Solicitation. When one node wants to communicate with another node, it will send NS to request the link local address of the target node with its own link local address.

Neighbor Advertisement. Nodes will send NA to respond to NS.

Redirect. Routers will send redirect messages to hosts when finding a better path to hosts. And only routers can send redirect messages.

2) Neighbor discovery options

978-1-4673-9026-2/16/$31.00 ©2016 IEEE

Neighbor Discovery messages can have zero or more options, some options may appear more than 1 time in the same message. There are four options in neighbor discovery.

Source/Target Link-layer Address. The Source Link-Layer Address option contains the link-layer address of the sender. It is used in the NS, RS, and RA packets. The Target Link-Layer Address option contains the link-layer address of the target. It is used in NA and redirect packets.

Prefix Information. The Prefix Information option provides hosts with on-link prefixes and prefixes for Address Autoconfiguration.

Redirected Header. The Redirected Header option is used in Redirect messages and contains the information to be redirected.

MTU (Maximum Transmission Unit). The MTU option is used in RA messages to ensure that all nodes on a link use the same MTU value when the link MTU is not known.

3) Functions of NDP

Address Resolution. Nodes do address resolution when nodes want to communicate with a node when only knowing the node's link-layer address. It occurs only when nodes do not know neighbor's link-layer address.

Neighbor Un-reachability Detection (NUD). IPv6 nodes use neighbor un-reachability to track the reachability of neighbors and update routing table according to the reachability of neighbors. A neighbor is considered reachable if the node has recently received an acknowledgment of a NA message that is a response to a NS message.

Duplicate Address Detection (DAD). IPv6 nodes use manual configuration and auto-configuration to generate global IPv6 addresses. As part of stateless address configuration, DAD is part of address auto-configuration that is used to check if the addresses generated are successfully configured. DAD must be performed prior to assigning an address to an interface in order to prevent multiple nodes from using the same address simultaneously.

B. Security Analysis of NDP

Both hosts and routers use NDP and NDP assumes that all nodes in the network are trusted. So NDP suffers from various attacks in practical applications.

Hop limit is a method to protect NDP. There is a *hop limit* field in the RA/RS and NS/NA message format. The hop value is *255* in ND packets, the hop will minus *1* after passing a router. The router will discard packets if the hop value of the packet does not equal *255*, which means it is not from the local link. However, the protection from *hop limit* field is limited, because it can not prevent attacks from local link.

DoS (Denial of Service) and DDoS (Distributed Denial of Service) are major attacking modes both in IPv4 and IPv6 networks. DoS attacks based on NDP in IPv6 networks are as follows.

Fake prefix and network configuration parameters. Attackers can send RA message with forged subnet prefix; attackers can forge as a router to destroy the legal communication by changing the value of *MTU*, *hop limit*, *Router TTL(time to live).*

DoS attacks based on DAD. Attackers can monitor DAD packets and addresses of the receiver of DAD in the local link. Then send NA response message to prevent legal hosts from achieving valid IP addresses.

DoS attacks based on NUD [6]. Attackers can send forged NA response messages to prevent legal hosts from achieving valid IP addresses.

Based on the vulnerabilities of NS/NA, RS/RA messages, attackers can launch redirect attacks [7], [8].

Last hop router attack. Attackers send RA messages and forge as the last hop router, stating that *TTL* is *0*. The host being attacked will think that router is out of service and choose attacker as default router. Then a man-in-the-middle attack (MIMT) can be launched.

ARP spoofing. Attackers can send NS/NA messages with different MAC addresses, which will cause cache table errors. Because the cache table will update periodically, so ARP spoofing attack should be done as soon as possible.

Fake redirect packet. Attackers can use last hop router as source address and redirect source packets to legal hosts. Legal hosts will accept the packet after detecting the source address, which means that the legal hosts accept the malicious redirecting.

There is a override flag in NA message. Once the flag set, NA should override the cache entry and update link layer address in the cache table. Attackers can sniffer NS message and forge NA message by setting override flag using forged link layer address and send it to the host. If the host accepts the message, it will update network gateway address in the cache table and be hijacked [9].

It is recommended that we use IPsec to protect NDP messages in the NDP specifications, but there is no specific ways and related explanations [10]. We do not know how to use IPsec to properly protect NDP messages and it is hardly used in the practical way.

C. SEND and Security Analysis

NDP is vulnerable from various kinds of attacks in untrusted networks. Secure Neighbor Discovery (SEND) protocol was proposed to counter most of the threats against NDP[11]. SEND introduces four NDP options to protect NDP message, *RSA Signature* option, *Cryptographically Generated Addresses (CGA)* option, *Timestamp* and *Nonce*. SEND uses *RSA option* to protect Neighbor and Router discovery messages, uses *CGA* to prevent faking address attacks. *Timestamp* and *Nonce* are used to prevent replay attacks.

SEND can prevent NS/NA spoofing, neighbor un-reachability detection failure, RA/RS attacks, replay attacks and DoS attacks based on NS.

However, SEND is not widely deployed[8]. There is only a little SEND deployment in Windows and Linux. NDProtector and Easy-SEND are SEND applications in Linux and WinSEND is for Windows. So most of IPv6 users did not get protection from SEND.

RSA signature option is used in SEND to authenticate NA message in the DAD response process, which is vulnerable to DoS attacks[10].

D. *SEND Privacy and Security*

In the Stateless address autoconfiguration (SLAAC) process, when a new node joins the link, the link-local address will be generated automatically. Then the node will send NS message to corresponding node's multicast address. Link-local address is a key address of network interface. The 64 leftmost bits of IPv6 address(128 bit) is the subnet prefix and the 64 rightmost bits of the IPv6 address is generated by Extended Unique Identifier (EUI-64).

The privacy and security issues of Interface Identifier(IID) generation algorithm[12].

The link-local address is generated by EUI-64, IID is the rightmost 64 bit of IPv6 address and changes occasionally. In IPv6 networks, attackers can get users' link-local addresses easily, then get gateway's MAC address by link-local address. Attackers can attack users by tracking users' IID. A good way to protect users' privacy is to change nodes' IID frequently. However, the IID is generated by MAC address, users are also under privacy related attack when the IID changed frequently.

CGA, an option of SEND, provides nodes with randomly generated IID and the proof of ownership of IPv6 address. But IID generated with CGA can not be changed frequently, which makes it vulnerable to privacy related attacks.

III. Existing Solutions

The introduction of SEND (Security enhanced neighbor discovery) solves a lot of security problems of NDP. However, the trusted system of SEND is hard to establish[9]. There are also some researchers who focus on the security of NDP and propose some novel mechanisms to improve the security of NDP.

Feng[7] introduces an authentication mechanism to improve the security of NDP. The proposed framework uses multicast key management protocol as application layer key management scheme to solve multicast problems in neighbor communication. The framework introduces IPSec AH (Authentication Header) and Media Access Control (MAC) address option in NDP to realize communication packet authentication and prevent forged ND message attack. The improved NDP security strategy can provide effective defense on NDP security attacks, such as SYN flood, fake prefix address attack and ARP cheating.

IPsec is mandatory in IPv6 and makes traffic much securer. IPSec can protect IPv6 hosts from all kinds of DoS attacks pertinent to the IPv6 neighbor discovery protocols[13]. Because IPsec can recognize the spoofed source address of spoofed packets received. IPSec can also be used to protect IPv6 hosts from DDoS attacks, such as TCP-Flood, UDP-Flood, ICMP-Flood and Smurf. However, there is no related application standards and users do not prefer to implement IPsec in practical applications. What is worse, clients are not aware of these security risks in IPv6 networks[9].

Liu[9] proposed defense tools based on DNSSEC (DNS Security Extensions) to prevent Man-In-The-Middle Attack. The defense tools are composed of detection tool and filtering tool. The detection tool is to fetch the correct information, and the filtering tool is to reject the malicious messages. The defense tools use DNSSEC's trust system to authenticate NDP and RDP messages, which can help users to aware and defense existing security risks efficiently.

There are some SEND implementations in Linux, but no implementation for Windows. Rafiee proposed WinSEND[8] to promote implementation in Windows. WinSEND uses winpcap API to directly access raw sockets and bypass normal TCP/IP stack. It is the first application for windows users to protect NDP. WinSEND can have direct access to NIC (Network Interface Card) and process NDP messages efficiently. With the proposition of WinSEND, there are SEND implementations both in Linux and Windows operation systems.

The design of DAD makes nodes that do not configure successfully vulnerable to DoS (Denial of Service) attacks[14]. The introduction of SEND and SAVI(Source Address Validation Improvement) can not relieve address spoofing attack in DAD process. Enhanced DAD is used to strengthen DAD process, solves the loopback in DAD. However, the enhance DAD can not prevent DoS attacks.

Rehman [14] proposed a new mechanism known as *Node Controller Model* to prevent DoS attacks in DAD detection process. The node controller framework is based on the rule-based system. To secure NS and NA message exchange between the nodes, the framework introduces *message authentication model* to authenticate the message. The message authentication model uses a *secure tag* option appended to NDP messages to maintain integrity between the sender and receiver during DAD process. The proposed DAD mechanism allows the hosts to verify the uniqueness of self-generated IP addresses while preventing malicious hosts to disrupt the verification process. This novel mechanism can improve DoS attacks on DAD process.

Rafiee proposes *Stable privacy enhanced IID* generation algorithm and *application layer based lifetime* to ensure the security in IPv6 networks. The *Stable privacy enhanced IID* generation algorithm is used to make sure that the IID generated is unique and it is difficult to guess what the next IID will be. To provide support for the application layer lifetime, Rafiee proposes the second algorithm to ensure that IID will change only if the subnet prefix changes[12]. The two algorithms can greatly enhance the security and privacy in IPv6 networks with little CPU usage.

Shah[15] proposes a method which can generate a highly randomized address to maintain privacy and ensure the uniqueness of IPv6 address. The method uses SHA-1 hash encryption to replace CGA. The method also suggests to use SHA-256 to replace SHA-1 and ECC (Elliptic Curve Cryptography) instead of RSA, because SHA-1 is vulnerable to collisions and ECC uses shorter key size compared with RSA. The method can provide robust security against DoS attacks during DAD process and can mitigate other attacks, such as Address Spoofing and MIMT.

The key to mitigate NDP security problems in existing solutions is fragmentation. Netze[16] introduces IPv6 *fragmentation header* to simplify and improve the effectiveness of monitoring and filtering of ND messages.

Because it is difficult for attackers to hide attack using fragmentation. However, relying on fragmentation may cause attacks based on IPv6 fragmentation.

Hassan [17] proposed a mechanism using cryptography to enhance NDP security. When a node joins a local link, it will multicast public key to all attached link in the network. All nodes will have each other's public keys finally. When any nodes in the link receive messages, they will decrypt the message using the sender's public key pair. When a node receives a spoofed message, the node will detect the private key of sender inside the message and match with the public key stored before. Then the spoofed message will be dropped. The mechanism can detect NS/NA spoofing, MIMT and DoS attacks.

Barbhuiya [18] proposed a scheme as Intrusion Detection System (IDS), for detection NS/NA spoofing attacks in IPv6 networks. The scheme assumes that all nodes are configured with static IP addresses or using SLAAC mechanisms, and IDS is a trusted machine with a static IP-MAC binding. The scheme use an active verification mechanism to ensure the genuineness of IP-MAC binding. When a node sends or receive a NS/NA message, there will be an entry in the data tables. NS packets will be regarded as spoofed and be recorded in *log table* if the IP-MAC pair does not match with records in the *Authenticated bindings table*. The scheme is composed of two main modules, *NS-Handler()* and *NA-Handler()*, and three sub-modules. With novel algorithms, these modules can detect with NS and NA messages respectively. The proposed scheme does not change the format of NDP. It is a software based approach and does not need any special hardware. The scheme can detect NS spoofing, NA spoofing, MIMT and DoS attacks successfully.

IV. Conclusion

IPv6 is introduced partly to improve the security shortcomings in IPv4. However, the adoption of IPv6 also brings new security problems. Security issues are key problems to deployment of IPv6. NDP is among new features introduced in IPv6 and NDP security is an important part of IPv6 security. With design defects, NDP suffers from various attacks, such as DoS, DDoS attacks, last hop router attack, MIMT, ARP spoofing and fake redirect packet. We introduce NDP and SEND and analyze security of NDP and SEND. Then we summarize and analyze the latest advances on NDP security. Many researchers have proposed suggestions and novel mechanisms to improve NDP security and mitigate threats against NDP. However, NDP is still incomplete with practical use and there are no best practices to ensure the security of NDP. We need to learn from these latest advances in NDP security, make NDP much securer, and propose best practices for NDP application in IPv6.

Acknowledgment

Our research is supported by CERNET Innovation Project (NGII20151203).

References

[1] R. Radhakrishnan, M. Jamil, S. Mehfuz and M. Moinuddin, "Security issues in IPv6," Networking and Services, 2007. ICNS. Third International Conference on, Athens, 2007, pp. 110-110. doi: 10.1109/ICNS.2007.106

[2] Hao, LU Yin SHI Jin HUANG, and X. I. E. Li. "A Survey on Security Issues in IPv6." Computer Science 5 (2006). 001.

[3] Deering, Stephen E. "Internet protocol, version 6 (IPv6) specification." (1998).

[4] W. Hui, Y. y. Sun, J. Liu and K. n. Lu, "DDoS/DoS Attacks and Safety Analysis of IPv6 Campus Network: Security Research under IPv6 Campus Network," Internet Technology and Applications (iTAP), 2011 International Conference on, Wuhan, 2011, pp. 1-4. doi: 10.1109/ITAP.2011.6006421

[5] Narten, Thomas, et al. "Neighbor discovery for IP version 6 (IPv6)." (2007).

[6] C. E. Caicedo, J. B. D. Joshi and S. R. Tuladhar, "IPv6 Security Challenges," in Computer, vol. 42, no. 2, pp. 36-42, Feb. 2009.doi: 10.1109/MC.2009.54

[7] F. Xiaorong, L. Jun and J. Shizhun, "Security analysis for IPv6 neighbor discovery protocol," Instrumentation and Measurement, Sensor Network and Automation (IMSNA), 2013 2nd International Symposium on, Toronto, ON, 2013, pp. 303-307. doi: 10.1109/IMSNA.2013.6743275

[8] Rafiee, Hosnieh, Ahmad Alsa'deh, and Christoph Meinel. "Winsend. Windows secure neighbor discovery." Proceedings of the 4th international conference on Security of information and networks. ACM, 2011.

[9] W. Liu, P. Ren, D. Sun, Y. Zhao and K. Liu, "Study on attacking and defending techniques in IPv6 networks," 2015 IEEE International Conference on Digital Signal Processing (DSP), Singapore, 2015, pp. 48-53. doi: 10.1109/ICDSP.2015.7251328

[10] Gelogo, Yvette E., Ronnie D. Caytiles, and Byungjoo Park. "Threats and Security Analysis for Enhanced Secure Neighbor Discovery Protocol (SEND) of IPv6 NDP Security." International Journal of Control and Automation 4.4 (2011). 179-184.

[11] Arkko, Jari, et al. Secure neighbor discovery (SEND). No. RFC 3971. 2005.

[12] Rafiee, H., & Meinel, C. (2013). Privacy and security in IPv6 networks. challenges and possible solutions. In SIN '13. Proceedings of the 6th international conference on security of information and networks, November 2013.

[13] X. Yang, T. Ma and Y. Shi, "Typical DoS/DDoS Threats under IPv6," Computing in the Global Information Technology, 2007. ICCGI 2007. International Multi-Conference on, Guadeloupe City, 2007, pp. 55-55. doi: 10.1109/ICCGI.2007.61

[14] Rehman, Shafiq Ul, and S. Manickam. "Novel Mechanism to Prevent Denial of Service (DoS) Attacks in IPv6 Duplicate Address Detection Process." International Journal of Security & Its Applications Vol.10.No.4(2016).

[15] Shah, Junaid Latief, and J. Parvez. "Optimizing Security and Address Configuration in IPv6 SLAAC." Procedia Computer Science 54(2015).177-185.

[16] Netze, Heise. "Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery." Heise Zeitschriften Verlag (2013).

[17] Hassan, Rosilah, A. S. Ahmed, and N. E. Othman. "Enhancing security for IPv6 neighbor discovery protocol using cryptography." American Journal of Applied Sciences 11.9(2014).1472-1479.

[18] Barbhuiya, Ferdous A., S. Biswas, and S. Nandi. "Detection of neighbor solicitation and advertisement spoofing in IPv6 neighbor discovery protocol." International Conference on Security of Information and Networks, Sin 2011, Sydney, Nsw, Australia, November 2011.111-118.