Improvement of Address Resolution Security in IPv6 Local Network using Trust-ND

Supriyanto*[1,2], Iznan H. Hasbullah[2], Mohamed Anbar[2], Raja Kumar Murugesan[3], Azlan Osman[4]
[1]Universitas Sultan Ageng Tirtayasa, Indonesia
[2]National Advanced IPv6 Centre, Universiti Sains Malaysia
[3]Taylor's University, Malaysia
[4]School of Computer Sciences, Universiti Sains Malaysia
*Corresponding author, e-mail: supriyanto@ft-untirta.ac.id

Abstract

The principle of a computer network is transferring information in terms of packets from one node to another. To do this the communicating nodes has to be assigned an Internet Protocol (IP) address. However, in a local area network, the availability of IP address alone is not enough to do communication. It also needs neighboring nodes Medium Access Control (MAC) address. The current Internet infrastructure IPv4 uses Address Resolution Protocol to resolve the neighbors MAC address if not known. IPv6 is the next generation communication protocol used today to overcome the exhaustion of IPv4 addresses. IPv6 uses Neighbor Discovery Protocol (NDP) to do the address resolution and not ARP. NDP lacks security and hence the address resolution mechanism is vulnerable to various attacks that include man-in-the-middle and Denial of Service. Secure Neighbor Discovery (SeND) mechanism that was introduced to solve this problem is highly complex and the message size is large. This paper introduces Trust-ND mechanism to secure the address resolution in IPv6 local network. Experiments were done and analysis on the experimental result shows the Trust-ND could decrease the complexity of SeND. The processing time of NDP message could be reduced from 1076 times for SeND mechanism to only 1.9 times for Trust-ND.

Keywords*: address resolution, neighbor discovery, IPv6, security, Trust-ND*

1. Introduction

Address resolution is a process on discovering neighboring node's link layer address by mapping IP address onto physical address. The current Internet infrastructure IPv4, uses Address Resolution Protocol (ARP) to do address resolution [1]. Since address resolution is very important in the IP packet transmission, the role of ARP becomes important. However, this link layer protocol reportedly has much vulnerability including ARP cache poisoning, Man in the Middle and DoS attacks. A number of researchers studied on the vulnerability and proposed a solution such as MITM-Resistant [2], ES-ARP [3], S-ARP [4] and TARP [5]. The ARP broadcasts ARP message to obtain the corresponding nodes physical address. This broadcast is an overhead to nodes that do not correspond to the IP address as they need to still process the ARP message. In order to overcome this overhead, IPv6 introduced NDP [6] to do the address resolution instead of ARP [7]. The NDP uses multicast [8] mechanism instead of broadcast.

The NDP does the address resolution by sending neighbor solicitation (NS) message to neighboring node that grouped in solicited node multicast address (SNMA). Using this multicasting mechanism the receiving node could be limited. This saves the other node in the network from processing address resolution unnecessarily as in ARP. However, the vulnerability in ARP exists in the NDP such as destination cache table poisoning, man in the middle attack and also DoS attack [9]. NDP may have other vulnerabilities as it is a new protocol that uses more than one NDP messages. Threats and vulnerability of NDP including the address resolution protocol was studied in [10], [11], and [12]. Research [13] has justified the existence of the threats in the IPv6 neighbor discovery implementation especially in public network such as in airport, coffee shop and bus station.

Received September 6, 2014; Revised October 30, 2014; Accepted November 22, 2014

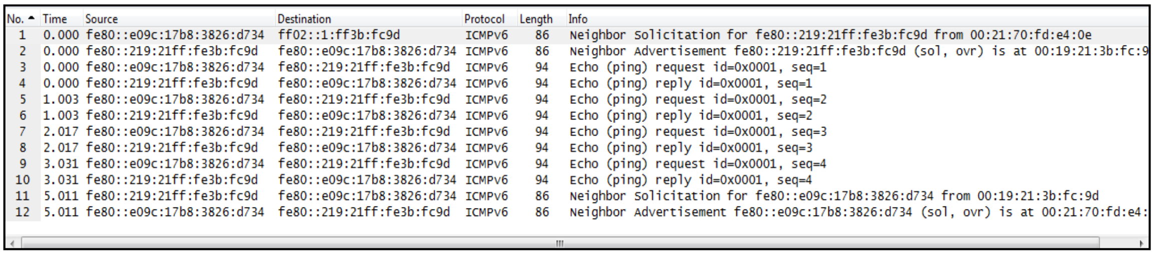
A number of proposals were made to address the security problem in the address resolution and for NDP in general. Secure Neighbor Discovery (SeND) [14] is the most complete solution on securing NDP processes especially the address resolution mechanism. SeND introduced four ICMPv6 options to make the NDP messages secure. The options include Cryptographically Generated Addresses (CGA), Nonce, Timestamp and RSA signature option. Based on the study conducted [15] and [16], these four options introduced other vulnerabilities in the NDP processes. The new vulnerability on SeND includes the complexity of option generation as well as the large size of the entire option. This makes the implementation of SeND non-trivial. The complexity of SeND also vulnerable to DoS attacks in the form of SeND messages flooding. Attacker could bombard the victim by sending more SeND message to force the victim to process the messages. Due to the complexity problem, nodes that implement SeND could crash faster than the normal non-SeND nodes.

This paper proposes to use Trust Neighbor Discovery (Trust-ND) as an integration of hard security and soft security on securing the neighbor discovery processes with the focus on address resolution function. It implements decentralized trust management between neighboring nodes within IPv6 local networks. The next section of this paper provides an overview of the address resolution mechanism, and Section 3 discusses the threats as well as vulnerability of the mechanism. Section 4 presents the related works in securing address resolution and Section 5 discusses the experimental results. Section 6 concludes the paper.

2. Overview of Address Resolution in IPv6

IP packet is transferred in Network layer using IP address as node identity [17]. The packet should know a particular destination IP address to reach the intended recipient. However, in a local network all nodes are connected directly via layer 2 switch that needs the link layer address for establishing communication between the connected nodes. Address resolution mechanism could be used to map the IP address into a link layer address and thus the neighboring node can communicate with each other. The address resolution is also required in the link local IPv6 operation. IPv6 uses neighbor discovery protocol to do address resolution.

Sending an IPv6 packet cannot be done without knowing link layer address of neighboring node that acts as the next hop unless the sender has neighbor's link layer address in its neighbor cache. However, normally even if the neighboring node are connected directly; it would not know the neighbor's link layer address without any previous interaction. Hence, before the sender could send the IPv6 packet, it should do the address resolution process. Figure 1 shows the address resolution between two computers that wish to communicate using echo request – echo reply by running ping command. It could be seen from this figure that there are two pairs of NS-NA messages before and after the echo messages. The address resolution is done by the first NS message. Destination address for the NS message is ff02::1:ff**3b:fc9d** that is based on the echo request destination which is fe80::219:21ff:fe**3b:fc9d** as the target address.



```
No. ▲ Time  Source                     Destination                Protocol Length Info
  1   0.000 fe80::e09c:17b8:3826:d734  ff02::1:ff3b:fc9d          ICMPv6   86     Neighbor Solicitation for fe80::219:21ff:fe3b:fc9d from 00:21:70:fd:e4:0e
  2   0.000 fe80::219:21ff:fe3b:fc9d   fe80::e09c:17b8:3826:d734  ICMPv6   86     Neighbor Advertisement fe80::219:21ff:fe3b:fc9d (sol, ovr) is at 00:19:21:3b:fc:9
  3   0.000 fe80::e09c:17b8:3826:d734  fe80::219:21ff:fe3b:fc9d   ICMPv6   94     Echo (ping) request id=0x0001, seq=1
  4   0.000 fe80::219:21ff:fe3b:fc9d   fe80::e09c:17b8:3826:d734  ICMPv6   94     Echo (ping) reply id=0x0001, seq=1
  5   1.003 fe80::e09c:17b8:3826:d734  fe80::219:21ff:fe3b:fc9d   ICMPv6   94     Echo (ping) request id=0x0001, seq=2
  6   1.003 fe80::219:21ff:fe3b:fc9d   fe80::e09c:17b8:3826:d734  ICMPv6   94     Echo (ping) reply id=0x0001, seq=2
  7   2.017 fe80::e09c:17b8:3826:d734  fe80::219:21ff:fe3b:fc9d   ICMPv6   94     Echo (ping) request id=0x0001, seq=3
  8   2.017 fe80::219:21ff:fe3b:fc9d   fe80::e09c:17b8:3826:d734  ICMPv6   94     Echo (ping) reply id=0x0001, seq=3
  9   3.031 fe80::e09c:17b8:3826:d734  fe80::219:21ff:fe3b:fc9d   ICMPv6   94     Echo (ping) request id=0x0001, seq=4
 10   3.031 fe80::219:21ff:fe3b:fc9d   fe80::e09c:17b8:3826:d734  ICMPv6   94     Echo (ping) reply id=0x0001, seq=4
 11   5.011 fe80::219:21ff:fe3b:fc9d   fe80::e09c:17b8:3826:d734  ICMPv6   86     Neighbor Solicitation for fe80::e09c:17b8:3826:d734 from 00:19:21:3b:fc:9d
 12   5.011 fe80::e09c:17b8:3826:d734  fe80::219:21ff:fe3b:fc9d   ICMPv6   86     Neighbor Advertisement fe80::e09c:17b8:3826:d734 (sol, ovr) is at 00:21:70:fd:e4:
```

Figure 1. Address Resolution

The NDP was developed with at least two improvements over ARP. First, the destination address of the link layer frame is multicast (33:33:ff:**3b:fc:9d**) type instead of broadcast (ff:ff:ff:ff:ff:ff). This can limit the recipient of the Ethernet frame containing the NS message [18]. The lowest byte of the destination is obtained from the last six characters of destination IPv6 address. Second, the NDP messages are actually IPv6 packet that has IP header that is very different with ARP message that uses a specific protocol. This is efficient on the protocol usage as the NDP is working on top of ICMPv6 message. The destination IPv6 address in the address resolution mechanism is started by **ff02::1:ff** that is solicited node multicast group and ended by **f3b:fc9d** taken from the intended destination IPv6 address.

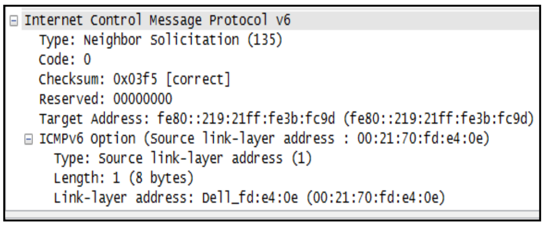
As only those nodes that have the same address will receive the NS message, the number of recepient is very limited. This is an improvement of the original address resolution that uses broadcast mechanism. A correspondent node that has the same last 24 bits would send NA message as respond to the sending NS message. Once the sender receives the NA message, the echo request can be sent to the destination. Failing to do the address resolution causes the echo request not to reach the intended destination. Further, the communication cannot be conducted between the two nodes. In order to store the identity of neighboring nodes, NDP uses neighbor cache that has the same function as ARP cache.

3. Threats on IPv6 Address Resolution

Address resolution in IPv6 is done by the neighbor security protocol using NS and NA message exchange. At the time of IPv6 development and deployment, NDP did not include a security mechanism with a possible assumption that neighboring nodes are trusted. This is vulnerable to various attacks as listed in [10] and studied in [19], [15], [12] and [13]. Since the address resolution process is under the NDP, it is also prone to the attacks. However, the address resolution itself is vulnerable to other kinds of attacks. The following are some of the threats in IPv6 address resolution.

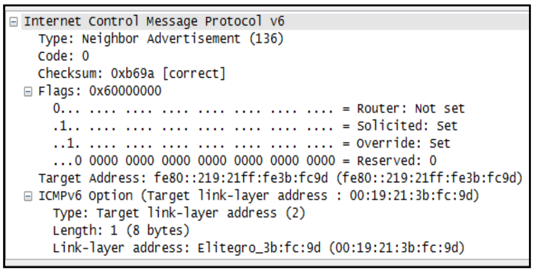
3.1. NS/NA spoofing

Since the address resolution uses the NS and NA message on its operation, an attacker could exploit one or more fields within the messages. NS and NA message is depicted in Figure 2 and Figure 3 respectively. There is a source link layer address in the NS message, and a target link layer address in the NA message. Normally, receiver machine could be host and the router will update its neighbor cache based on the information carried by the messages. It then creates a new entry or updates an old entry with the received link layer address. Attacker can spoof the link layer address within NS or NA message with nonexistent link layer address. Hence, a wrong binding of IPv6 address and link layer address would be created. Later, when the machine wants to send any IPv6 packet, the packet will go to a wrong destination. It will reach the wrong link layer machine even though the user types a valid IPv6 address. Populating neighbor cache entry with a wrong IP – link layer binding is called neighbor cache poisoning. In addition, this kind of threat can lead to other threats including MiTM attack, and DoS attack.



```
⊟ Internet Control Message Protocol v6
    Type: Neighbor Solicitation (135)
    Code: 0
    Checksum: 0x03f5 [correct]
    Reserved: 00000000
    Target Address: fe80::219:21ff:fe3b:fc9d (fe80::219:21ff:fe3b:fc9d)
  ⊟ ICMPv6 Option (Source link-layer address : 00:21:70:fd:e4:0e)
      Type: Source link-layer address (1)
      Length: 1 (8 bytes)
      Link-layer address: Dell_fd:e4:0e (00:21:70:fd:e4:0e)
```

Figure 2. Format of NS Message with Source Link Layer Address Option



```
⊟ Internet Control Message Protocol v6
    Type: Neighbor Advertisement (136)
    Code: 0
    Checksum: 0xb69a [correct]
  ⊟ Flags: 0x60000000
      0... .... .... .... .... .... .... .... = Router: Not set
      .1.. .... .... .... .... .... .... .... = Solicited: Set
      ..1. .... .... .... .... .... .... .... = Override: Set
      ...0 0000 0000 0000 0000 0000 0000 0000 = Reserved: 0
    Target Address: fe80::219:21ff:fe3b:fc9d (fe80::219:21ff:fe3b:fc9d)
  ⊟ ICMPv6 Option (Target link-layer address : 00:19:21:3b:fc:9d)
      Type: Target link-layer address (2)
      Length: 1 (8 bytes)
      Link-layer address: Elitegro_3b:fc:9d (00:19:21:3b:fc:9d)
```

Figure 3. The Format of NA Message with Target Link Layer Address Option

3.2. Man-in-the-Middle Attack

Attacker may send NS or NA message to a targeted victim with valid IPv6 address belonging to two legitimate neighbors (Alice and Bob) bound with attacker's link layer address. Once the neighbor cache of host Alice and Bob poisoned, the man-in-the-middle attack is successfull. Host Alice will send packet to host Bob but reach the host C (Attacker) and vice versa. Further, the attacker could change the transmitted IPv6 packet that may cause miscommunication between host Alice and Bob as in Figure 4.

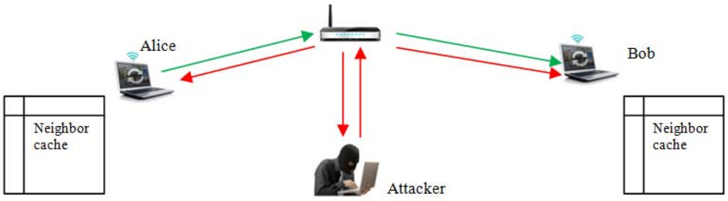


Figure 4. Man-in-the-Middle Attacks

3.3. DoS Attack

MiTM happens if the attacker forwards the transmitted packet to other corresponding nodes. If the attacker discards or not forwards the packet to the destination, it is called DoS attack. The intended destination would not receive any IPv6 packet from the sender. This DoS attack may continue even after the sender machine is restarted. The neighbor cache entry for the attacker may still exist.

4. Related Works on Securing Address Resolution in IPv6

A number of proposals have been made by researchers to address the security problem in the IPv6 address resolution. Some of them use cryptography while, some others use improved mechanism without any cryptography. Intrusion detection mechanism was proposed by [20] and [21]. It maintains the IPv6 network traffic information including NS and NA message into at least six data tables: NS table, NA table, Problem table, Authenticated Table, Log Table and Unsolicited table. However, more tables could introduce other problems on the address resolution including more memory space as well as Dos attack or flooding attack that may make all the tables full. Mutaf, P., & Castelluccia proposed Compact Neighbor Discovery that replaces the 128 bit target IPv6 address in NS message into *m* bit Bloom filter [11]. The NS message also contains the optimal number of hash functions to minimize the false positive probability. The minimum false positive possibility would reduce the number of unnecessary neighbor advertisement. This mechanism could minimize the bandwidth consumption in IPv6 local network. However, the security problem on the address resolution is still not resolved.

Arkko proposed Secure Neighbor Discovery (SeND) [19] and has been accepted by the IETF as RFC 3971 [14] to secure the neighbor discovery protocol in IPv6 including router discovery and neighbor discovery. It introduced four NDP options which are CGA address to prevent IPv6 address stealing, nonce and timestamp option to protect NDP from replay attack and RSA signature option to do authentication. Each of the NDP messages must carry all the options in every NDP processes. NDP messages without the options are treated as unsecured and the receiver should discard the messages. This security mechanism could protect the NDP processes from various attacks including DoS attack, man-in-the-middle attack, replay attack and remote attack. However, the availability of the four options also introduced other problems. The main problem on SeND is the complexity on the address generation, CGA option generation as well as the signing of the RSA signature option [16], [22] and [15]. The complexity problem also appears on the receiver on verifying the options. In addition, it is also vulnerable to DoS attack that could exploit the SeND messages. Attacker may send more packets with the four NDP options to force the victim to process it. The experimentation here on flooding attack targeting a SeND machine showed that the SeND machine could only process up to 442 NS messages within 1.43 second. This causes a lack of proper security mechanism implementation for address resolution in IPv6 environment.

Source Address Validation Improvement (SAVI) [23] was proposed by researchers in Tsinghua University, China. SAVI is intended to prevent source address spoofing in the same subnet as there are many NDP message exchange. The SAVI principle is to construct anchor information containing trusted information such as port and MAC address on an IPv6 host. It then creates a binding between the anchor information and the source IP address. It also applies a filtering policy [24] to forward packets matching filter rules and otherwise discard them. SAVI is generally configured in access switch of the IPv6 local network as ingress filtering. However, SAVI is also vulnerable to various attacks. In the RFC 6959 [24] some possible threats as well as the challenges in SAVI implementation are described. Applying SAVI on the access network would create problem on dynamic address configuration such as SLAAC and DHCPv6. This is because the difficulty to create the binding of anchor information due to the changing of IP address. The other challenge of SAVI binding creation is when it is a LAN and devices with multiple IPv6 address such as routers, multi LAN hosts and Firewalls are connected. Paper [25] added other limitation of SAVI on the lack of protocol in connecting SAVI devices. As a consequence, each SAVI device should work separately from other devices that are vulnerable to traffic spoofing.

5. Securing Address Resolution Using Trust-ND

Considering the weaknesses of the related work in the previous section, an attempt has been made here to find a new solution to secure neighbor discovery including the address resolution. The main problem in the existing security mechanism is the lack of integrity verification as well as providing availability of services. Even though there is checksum field in the ICMPv6 header [26] to do the integrity check, it is not enough to resist pre-image as well as collision attacks. It is very easy for an attacker to change the message content with the same checksum code. Another shortcoming in the existing methods is the complexity of the message generation as well as more resources requirement. Trust-ND is proposed here as an integration of hard security and soft security. Hard security includes cryptography to provide data integrity checking, while soft security is based on social interaction that uses trust management concept [27].

The hard security is in the form of hash function algorithm to assure the data integrity. However, the hash function used is the one that satisfies the three hash requirement including pre-image resistant, second pre-image resistant and collision resistant. SHA-1 [28] is the hash function algorithm used in the proposed Trust-ND that is also used in network security mechanisms such as IPsec and SeND. In order to prevent replay attack, nonce field is used instead of nonce option as in SeND mechanism. Further, the generation time is used that shows when the message is generated at the sender to prevent DoS attack. As a result, the new NDP option is proposed that is then called Trust Option as depicted in Figure 5. The format of Trust Option follows the standard of ICMPv6 option that begins with Type and Length field with the minimum value of 32 bits. The length should be multiples of 8 bytes. The total length of Trust Option is 32 bytes or 4 times 8 bytes. The hash function output is represented as the 20 bytes Message Authentication Data or MAD field that is the main field of Trust Option.

<table>
<tr><td>Type</td><td>Length</td><td>Reserved</td></tr>
<tr><td colspan="3">Ts (message generation time) – 4 bytes</td></tr>
<tr><td colspan="3">Nonce – 4 bytes</td></tr>
<tr><td colspan="3">Message Authentication Data – 20 bytes</td></tr>
</table>

Figure 5. The Format of Trust Option

The soft security is in the form of decentralized trust management system. The trust management begins with the calculation of trust value of sender of Trust-ND message on each receiver node instead of in one central node. In the case of address resolution, the trust management is illustrated in Figure 6. The sender with the role as a trustee generates Trust-NS message sent to multicast group of solicited node (SNMA). Trustor is the receiving node that has to verify the Trust-NS message. The trust calculation is based on two components which are direct trust and knowledge trust. The direct trust represents the message verification result, while the knowledge trust represents the sender history stored in its neighbor cache. The trust calculation results in three possibilities: trusted if the trust value is higher than 0.5, distrusted if the trust value is lower than 0.5, and uncertainty if the trust value is 0.5. Whatever the result, the trustor has to store or update the trust value in its neighbor cache table.

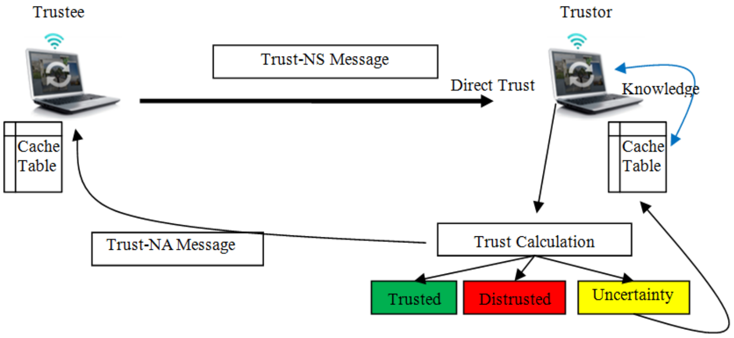


Figure 6. Trust Management on Trust-ND

6. Result and Discussion

Experiment has been done in measuring the performance of Trust-ND on securing IPv6 address resolution. The experiments included the address resolution process of the original NDP, SeND mechanism and the proposed Trust-ND. All the implementation where on the same machine with Intel (R) Core (TM) 2 Duo CPU and Windows 7 Operating System. The experimental results involved processing time in both sender and receiver, bandwidth utilization and some attacking scenarios. The processing time of NDP messages could be seen in Table 1. The processing time contains both processing time in sender and receiver for the three NDP mechanisms. The original NDP as the baseline shows the lowest processing time. The Trust-ND has a higher processing time of about 1.9 times for NS message and 1.8 times for NA message from the baseline. In opposite, the SeND mechanism introduces the highest processing time that reaches 1076 times for NS message and 1376 times for NA message.

Table 1. Processing Time of Address Resolution Messages

Address Resolution Message	Processing Time (millisecond)								
	Original NDP			Trust-ND			SeND Mechanism		
	Sender	Receiver	Total	Sender	Receiver	Total	Sender	Receiver	Total
NS	0.053	0.019	0.072	0.066	0.071	0.137	54.563	22.784	77.347
NA	0.054	0.020	0.073	0.068	0.067	0.135	76.441	24.425	100.866

The Table 1 demonstrates that the Trust-ND could decrease the complexity of SeND mechanism by reducing the NDP messages processing time. In terms of address resolution, the process of getting neighboring node link layer address could be done faster than SeND mechanism. The addition of Trust Option in NS and NA message does not add significant overhead but it could decrease the overhead significantly when compared to SeND. As the address resolution may be conducted in every IPv6 packet transmission, the network overhead could degrade the network as well as machine performance. Hence, the reduced overhead in Trust-ND as a security mechanism is very useful.

Bandwidth utilization is another parameter of the IPv6 local network performance. As observed in [13], the frequency of NDP messages in an IPv6 local network is very high. 84% of the total numbers of ICMPv6 message captured are NDP messages that generally are in the form of NS and NA messages. Further, the NDP messages exchange could affect the available bandwidth in the local network. The address resolution process involves two NDP messages which are NS and NA messages. The number of NS messages sent by the sender machine is the number of SNMA node. This is because the NS message is sent as multicast to SNMA addresses that is usually a single message. The NA message is sent as unicast to the sender of NS message, so the number of reply message is also one.

Table 2. Bandwidth Utilization

NDP Message Type	The Size of Message (bytes)			Bandwidth Utilization (Kbps)		
	NDP	Trust-ND	SeND	NDP	Trust-ND	SeND
NS	86	118	454	3.44	4.72	18.16
NA	86	118	454			

Typically, the NS message carries source link layer address option and the NA message carries target link layer address. Hence the size of NS and NA message is the same for address resolution. Since the bandwidth utilization is calculated by comparing the size of message and delay time, the bandwidth consumption is comparable with the message size. The calculation results are listed in Table 2. Trust-ND consumed higher bandwidth than the original NDP, about 37% more. In contrast, the SeND mechanism introduced 18.16 Kbps or 428% higher than the original NDP. It means the Trust-ND could save bandwidth when compared to SeND mechanism that is up to 13.44 Kbps or 285% more bandwidth efficient.

The function of a security mechanism is how to provide security services as required in the security object. This paper focuses on securing the address resolution in IPv6 local network using the Trust-ND mechanism. As aforementioned in Section 3, the main threat on the address resolution is NS/NA spoofing that leads to man-in-the-middle attack and DoS attack. In order to evaluate the performance of Trust-ND on preventing spoofing attack, this proposal has experimented by attacking the Trust-ND machine using *parasite6* tool that could generate NS and NA spoofing attacks. There are two scenarios on the attacking activity. First, it uses the existing *parasite6* tool that generates typical NS and NA spoofing. The spoofed message on this scenario is without Trust Option. Hence all the spoofed messages are detected by the receiver and discarded. Second, spoofed Trust-NS and Trust-NA message were generated using Scapy since there is possibility that an attacker could generate Trust-ND messages. The availability of Trust Option in the spoofed Trust-ND messages could make the receiver fail on detecting the spoofed message. However, since the message carries the message authentication data (MAD) as output of SHA-1 operation; any changes in the NDP messages will be detected.

6. Conclusion

Address resolution is one of the NDP functions in IPv6 local network. It is used to discover link layer address of neighboring node. Without link layer address of the next hop node or destination node, an IPv6 node cannot send any IPv6 packet. Hence, address resolution is important on local area networks. Since, the address resolution in IPv6 does not implement any security verification; this mechanism is vulnerable to various attacks or threats. Even though, there are a number of works on securing address resolution in IPv6, the implementation is still non trivial. We propose Trust-ND to solve the security problem on address resolution in an IPv6 local network. The Trust-ND introduces Trust Option to be carried by all NDP messages especially NS message and NA message that are used in the address resolution. Since the length of Trust Option is only 32 bytes, it does not add significant bandwidth consumption in the local network. In addition, Trust-ND message processing is faster compared to the SeND mechanism. The Trust-ND mechanism could save 13.44 Kbps of bandwidth on IPv6 local network and could save hundreds of millisecond in terms of time on NDP message processing. Experiments on the attacking scenario on address resolution are also shown to demonstrate that the Trust-ND could satisfy the security requirement.

Acknowledgements

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] Plummer DC. *An Ethernet Address Resolution Protocol*. Request for Comments 826, Internet Engineering Task Force. 1982.

[2] Seung Yeob N, K Dongwon, K Jeongeun. Enhanced ARP: preventing ARP poisoning-based man-in-the-middle attacks*. Communications Letters*. IEEE. 2010; 14(2): 187-189.

[3] Ataullah M, N Chauhan. *ES-ARP: An efficient and secure Address Resolution Protocol*. IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS). 2012.

[4] Bruschi D, A Ornaghi, E Rosti. *S-ARP: a secure address resolution protocol*. Proceedings. 19th Annual Computer Security Applications Conference. 2003*.*

[5] Lootah W, W Enck, P McDaniel, TARP: Ticket-based address resolution protocol*. Computer Networks.* 2007; 51(15): 4322-4337.

[6] Narten T, et al. *Neighbor Discovery for IP version 6 (IPv6)*. Request for Comments 4861. Internet Engineering Task Force. 2007.

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

[8] Wayawo A. The Transmission Multicast and The Control of QoS for IPV6 Using The Insfrastructure MPLS*. International Journal of Information and Network Security (IJINS)*. 2012; 1(1): 9-27.

[9] Convery S, D Miller. *IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation* Available from www.seanconvery.com/v6-v4-threats.pdf. 2004; 1.0

[10] P Nikander E, J Kempf, E Nordmark, *IPv6 Neighbor Discovery (ND) Trust Models and Threats*, in Request for Comments 3756, 2004, Internet Engineering Task Force.

[11] Mutaf P, C Castelluccia. *Compact neighbor discovery: a bandwidth defense through bandwidth optimization*. Proceedings of 24th Annual Joint Conference of the IEEE Computer and Communications Societies*.* 2005.

[12] 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.

[13] Supriyanto, et al. *Risk Analysis of the Implementation of IPv6 Neighbor Discovery in Public Network*. in International Conference on Electrical Engineering, Computer Science and Informatics (EECSI) Yogyakarta, Indonesia. 2014.

[14] Arkko J, et al., *Secure neighbor discovery (SEND)*. Request for Comments 3971, 2005. Internet Engineering Task Force.

[15] AlSa'deh A, C Meinel. Secure neighbor discovery: Review, challenges, perspectives, and recommendations. *Security & Privacy*. IEEE. 2012; 10(4): 26-34.

[16] Gaeil A, et al. *Analysis of SEND Protocol through Implementation and Simulation*. in International Conference on. Convergence Information Technology. 2007.

[17] Zhang J, et al., Fractals on IPv6 Network Topology*. TELKOMNIKA Indonesian Journal of Electrical Engineering*, 2013; 11(2): 577-582.

[18] Crawford. *Transmission of IPv6 Packets over Ethernet Networks*. Request for Comments 2464, 1998, Internet Engineerig Task Force.

[19] Arkko J, et al. *Securing IPv6 neighbor and router discovery*. in Proceedings of the 1st ACM workshop on Wireless security. Atlanta, GA, USA: ACM. 2002.

[20] Barbhuiya FA, S Biswas, S Nandi. *Detection of neighbor solicitation and advertisement spoofing in IPv6 neighbor discovery protocol*. Proceedings of the 4th international conference on Security of information and networks, ACM: Sydney, Australia. 2011; 111-118.

[21] Bansal G, et al. *Detection of NDP based attacks using MLD*. in Proceedings of the Fifth International Conference on Security of Information and Networks. 2012. ACM.

[22] Gelogo YE, RD Caytiles, B Park. Threats and Security Analysis for Enhanced Secure Neighbor Discovery Protocol (SEND) of IPv6 NDP Security. *International Journal of Control and Automation*, 2011; 4(4): 179 - 184.

[23] Bi J, et al. *Source Address Validation Improvement (SAVI) Framework.* Internet Draft. Internet Engineering Task Force. 2013.

[24] McPherson D, J Halpern, F Baker. *Source Address Validation Improvement (SAVI) Threat Scope.* Request for Comments 6959. Internet Engineering Task Force. 2013.

[25] Guang Y, B Jun, X Peiyao. *Source address validation solution with OpenFlow/NOX architecture*. in 19th IEEE International Conference on Network Protocols (ICNP). 2011.

[26] Conta A, S Deering, M Gupta. *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*. Request for Comments 4443. Internet Engineering Task Force. 2006.

[27] Sarwar A, et al. A Review of Trust Aspects in Cloud Computing Security. *International Journal of Cloud Computing and Services Science (IJ-CLOSER)*. 2013; 2(2): 116-122.

[28] Polk T, L Chen, S Turner, *P Hoffman. Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms*, in Request for Comments 6194. 2011.