American Journal of Applied Sciences 11 (9): 1472-1479, 2014
ISSN: 1546-9239

doi:10.3844/ajassp.2014.1472.1479 Published Online 11 (9) 2014 (http://www.thescipub.com/ajas.toc)

ENHANCING SECURITY FOR IPV6 NEIGHBOR DISCOVERY PROTOCOL USING CRYPTOGRAPHY

Rosilah Hassan, Amjed Sid Ahmed and Nur Effendy Osman

Research Center for Software Technology and Management, Network and Communication Technology Lab,
Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia,
43600 UKM Bangi, Selangor, Malaysia

Received 2014-04-08; Revised 2014-04-21; Accepted 2014-07-03

ABSTRACT

Internet Protocol version 4 (IPv4) would gradually be replaced by Internet Protocol version 6 (IPv6) as the next generation of Internet protocol. The Neighbor Discovery Protocol (NDP), one of the main protocols in the IPv6 suite, comprises Neighbor Discovery for IPv6. NDP is used by both hosts and routers. Its functions include Neighbor Discovery (ND), Router Discovery (RD), Address Auto configuration, Address Resolution, Neighbor Unreachability Detection (NUD), Duplicate Address Detection (DAD) and Redirection. If not secured, NDP is vulnerable to various attacks: Neighbor Solicitation (NS) spoofing and Neighbor Advertisement (NS) spoofing, redirection, stealing addresses, denial of service are examples of these attacks. Since its early stages of designing and development NDP assumes connections between nodes will be safe but deployment stage prove this assumption is incorrect and highlight the security holes. This fact leads Internet Engineer Task Force (IETF) to request solutions in order to overcoming these drawbacks. SEcure Neighbor Discovery or SEND is then proposed, SEND solve a part of the threats associated with NDP and request for more researches to find a better solution that manage to forbid all these threats and ignore its limitations. This study presents a new mechanism to avoid security threats for IPv6 NDP based on digital signature procedures. The proposed solution is manage to eliminate the threats because it do mapping and binding between IP address, MAC address and public keys of the nodes in the node's neighbors cache, intruders will not be able to spoof other nodes' IP addresses.

Keywords: IPv6, NDP, NS, NA, Digital Signature

1. INTRODUCTION

There is increasing in number of hosts in internet expert expectations that IPv4 along with its associated protocols will soon be replaced in its entirety by IPv6 (Rosilah and Ahmed, 2013). One such protocol from Internet Protocol Suite 6 is the Neighbor Discovery Protocol (NDP) (Gelogo *et al*., 2011). Neighbor Discovery (ND) perform a number of tasks including an examination of the local link for the link-layer addresses of the other nodes, the discovery of routers, the detection of unreachable local nodes, resolving duplicate addresses and redirection to more appropriate routers (redirect). In addition, it constitutes a employs nodes in an IPv6 network as a learning mechanism of the local network to identify the IP and MAC addresses and the prefixes of the routers in addition to mapping the local nodes address mappings [RFC 3756]. This is a crucial step in the last hop network access for IPv6 nodes. Hosts and routers employ Neighbor Discovery Protocol to keep a record of all reachable neighbors while detecting all changes in link-layer addresses. This allows rapid purging of invalid cache values while also enabling packet forwarding by detecting willing neighboring routers. This function is important in the event of router failure, whereby functioning alternates

Corresponding Author: Rosilah Hassan, Research Center for Software Technology and Management, Network and Communication Technology Lab, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia

are actively searched for. Neighbor Discovery security is necessary, especially for open network environments wherein joining a local link requires minimal or no link-layer authentication (Arkko *et al*., 2002). Protecting ND is important as it is frequently subjected to attacks (Liu and Qing, 2013). Known to cause disruption in the flow of IP packets. IP spoofing which is defined as a technique used to gain unauthorized access to computers (Hassan *et al*., 2014; Ahmed *et al*., 2012) and Denial of Service (DoS) are examples of the outcome of such attacks. When this protocol is disrupted, IP traffic is threatened. NDP is a particularly vulnerable protocol given that it can be accessed or manipulated via hosts and routers thereby raising several serious security threats.

2. NEIGHBOR DISCOVERY PROTOCOL

Consisting of a set of processes and messages as defined by [RFC 4861], IPv6 Neighbor Discovery (ND) is essentially a mechanism that determines how neighboring nodes relate to each other. ND was constituted as a replacement for the limited functionality of IPv4. It works along with IPv6 and replaces Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP) router discovery and the ICMP Redirect message used in IPv4.

Nodes employ ND as a tool to perform a range of tasks. These tasks include non-router or host specific tasks, as well as router specific tasks. Among its general tasks are resolving problems associated with the neighboring node in regards to the link-layer address to which the IPv6 packet is being forwarded. In addition, it determines the reachability of a neighboring node along with its link-layer address. As for host specific tasks, ND is a tool to discover neighboring routers in addition to performing an automatic configuration of addresses, routes and prefixes among others parameters. As far as routers are concerned, ND seeks for router alternatives for improved next-hop performance to forward packets, in addition advertising router presence, configurations, routes and on-link prefixes.

2.1. Neighbor Discovery Message Format

There are five different types of ND messages, namely Router Solicitation (ICMPv6 type 133), Router Advertisement (ICMPv6 type 134), Neighbor Solicitation (ICMPv6 type 135), Neighbor Advertisement (ICMPv6 type 136) and Redirect (ICMPv6 type 137). All ND messages are formatted in a very specific way to operate within an ICMPv6 message structure. Messaging in ND consists of a message header, composed of an ICMPv6 header and ND message-specific data and zero or more ND options. **Figure 1** shows the format of an ND message (Davies, 2012). ND messages consist of several options that perform specific functions. These functions provide additional information, such as indicating MAC and IP addresses, on-link network prefixes, on-link MTU information, redirection data, mobility information and specific routes. As Identified in (Barbhuiya *et al*., 2013) all the messages that performs various functions pertaining to IPv6 ND:

- Router Solicitation
- Router Advertisement
- Neighbor Solicitation
- Neighbor Advertisement
- Redirect

2.1.1. Router Solicitation

As a means to discover presence of IPv6 routers on the link, IPv6 hosts are used to send a multicast Router Solicitation message prompting an instant response from IPv6 routers as opposed to waiting for an unsolicited Router Advertisement message.

2.1.2. Router Advertisement

When multiple routers are advertised on a link, this can cause synchronization problems. To remedy this, unsolicited advertisements are sent at random intervals, which prompt a solicited response in the form of Router Advertisement messages, which contains various information demanded by hosts.

2.1.3. Neighbor Solicitation

IPv6 nodes send the Neighbor Solicitation message to discover the link-layer address of an onlinkIPv6 node or to confirm a previously determined link-layer address. It typically includes the link-layer address of the sender. Typical Neighbor Solicitation messages are multicast for address resolution and unicast when the reachability of a neighboring node is being verified.

2.1.4. Neighbor Advertisement

In the event that a Neighbor Solicitation message is received, a Neighbor Advertisement message containing that information deemed necessary for nodes to determine the type of Neighbor Advertisement message and the senders details is sent in return via the IPv6 node.

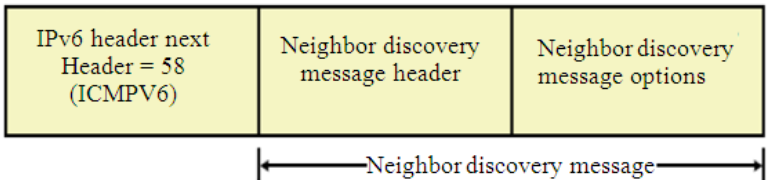

Fig. 1. ND message format

At times, the same IPv6 node can send unsolicited Neighbor Advertisements as a means to track and inform neighboring nodes of changes in the role played by the nodes, i.e., in what pertains to link-layer addresses.

2.1.5. Redirect

The Redirect message is sent through an IPv6 router to acquire the details for an alternative (often better) first-hop address for a specific destination. Only routers can send this information, which is then relayed to the original host.

2.2. Neighbor Discovery Options

2.2.1. Source and Target Link-Layer Address Options

The Source Link-Layer Address option employs the Neighbor Solicitation, Router Solicitation and Router Advertisement messages to indicate the link-layer address of the ND message sender. However, it fails to work in the event of an unspecified address (::). As for the Target Link-Layer Address option, it employs the Neighbor Advertisement and Redirect messages to indicate the neighboring node through which the link-layer address is used to send IPv6 packets.

2.2.2. Prefix Information Option

Information about address auto configuration and the prefix addresses is acquired through Router Advertisement messages. This is achieved through the Prefix Information option. Multiple address prefixes is indicated by multiple Prefix Information options.

2.2.3. Redirected Header Option

The Redirected Header option seeks to identify the specific IPv6 packet responsible for causing the router to send a Redirect message. This is achieved by sending Redirect messages.

2.2.4. MTU Option

Translational or mixed-media bridging configuration requires the IPv6 MTU for all links to be known. The MTU option overrides cases reported by the interface hardware of the IPv6MTU by sending Router Advertisement messages. In cases of multiple MTUs, such as in a bridged environment, the MTU option indicates the highest IPv6 MTU supported by all link-layer technologies on the link.

2.2.5. Route Information Option

This options seeks to add to the local routing table by enhancing hosting by means of specifying individual routes. This is achieved by sending Router Advertisement messages as articulated in [RFC 4191].

2.2.6. Neighbor Discovery Processes

There are several purposes behind message exchange within an ND protocol. These purposes include:

- Address resolution
- Duplicate Address Detection
- Neighbor unreachability detection
- Router discovery
- Redirect Function

2.2.7. Address Resolution

Resolving the problem of link-layer address of the on-link next-hop address for a given destination, requires the exchange between Neighbor Solicitation and Neighbor Advertisement messages. A multicast Neighbor Solicitation message is sent by the host which includes the link-layer address of the sending host in the Source Link-Layer Address option. Upon the target host receiving the message, the neighbor cache updates based on the source address and the link-layer address in the Source Link-Layer Address option. A Neighbor Advertisement consisting of the Target Link-Layer Address option is then sent by the target node to the Neighbor Solicitation sender. When the target nodes receives this, the neighbor cache of the sending host updates with an entry for the target after which it is possible to send unicast IPv6 traffic between the host and target.

2.2.8. Duplicate Address Detection

Duplicate address detection occurred when duplicate addresses on a local link is detected via means of Neighbor Solicitation messages, in which the Target Address field is set to the IPv6 address for which duplication is being detected, as described in [RFC 4862].

2.2.9. Neighbor Unreachability Detection

The issue of neighbor Unreachability is when failure occurs in the receipt and process of IPv6 packets sent to the neighboring node. However, it is not an absolute determination that the sent packets did not arrive the designated destination, as a neighboring node can function as both host and router. This implies that the neighboring node may not have been the targeted destination. This process seeks only to determine if the first hop to the destination is reachable. This can be determined via a unicast Neighbor Solicitation message and the receipt of a solicited Neighbor Advertisement message. The Neighbor Advertisement message must be solicited to prove reach ability. This form of verification only works from Neighbor Solicitation to Neighbor Advertisement messages and not vice versa. Among the methods of ascertaining reach ability is determining the forward progress of communication via the next-hop address. This is determined when acknowledgement segments for sent data are received. In the case of TCP, first hop reach ability to the destination is communicated to the IPv6 in the form of TCP acknowledgments. In those protocols wherein forward progress of communication cannot be determined, reach ability is determined through the exchange of Neighbor Solicitation and Neighbor Advertisement messages.

2.2.10. Router Discovery

When nodes seek to determine the set of routers on the local link, this is called router discovery. In the IPv6 protocol, this process is similar to ICMP router discovery for IPv4, as described in [RFC 1256]. The major difference between both methods of discovery is the mechanism employed by both processes to select a new default router when the previous default router is no longer available. In the IPv6 process, the time span for a default router is included in the Router Lifetime field contained with the Router Advertisement message. When the current default router is no longer available, neighbor Unreachability detection is used instead of the Router Lifetime field to immediately select a new router from the list of possible default routers. It should be noted that the IPv6 router discovery mechanism performs a number of configuration.

2.2.11. Redirect Function

We redirect routers for improved first-hop traffic processing. In normal usage, there are two common occasions wherein the redirect function is employed. Firstly, when there are multiple routers on a local link, the IP address closest to the targeted destination is identified and traffic is redirected through it. Secondly, when the prefix of the destination is not included in the prefix list of the host, this is necessary to match the prefix on the list. The IPv6 redirect process consists of several steps. It begins by sending a unicast packet to its default router, which then processes the packet on the basis that the originating host is a neighbor and that the host and next-hop address share the same link. A redirect message is the sent to the originating host. In this message is the Target Address field, which serves as the next-hop address where the packet and all subsequent packets should be sent. When the Redirect message is received, the cache of the originating host updates the destination address with the address in the Target Address field.

3. EXISTING MECHANISMS

Only a few and limited techniques have been introduced to eliminate threats within NDP. This limitation because IPv6 itself is new and still many researches about IPv6 are undergoing. Following we will highlights these techniques each of them independently, trying to shows limitations of every one.

As we knew IP Security or for short IPSec is mandatory for IPv6, so it is logic consequence to use IPSec as a solution for the threats within NDP. IPSec Authentication Header (AH) could be implemented with NDP Neighbor Solicitation and Neighbor Advertisement messages to secure the communication between the nodes. Because of the bootstrap problem arise when using Internet Key Exchange (IKE) to create the Security Association (SA) of the IPSec; SA could only be configured manually which is impractical and tedious task when the networks have large number of nodes (Ferdous *et al*., 2011).

IETF introduce industry standard solution through SEcure Neighbor Discovery Protocol or SEND for short (RFC 3971). The main idea behind SEND is using Cryptographically Generated Addresses (CGA) to communicate between nodes. CGA for small machines with limited specifications is quite expensive (Castelluccia, 2004) and do increase the cost of address generation (Arkko *et al*. 2005). However SEND is not yet widely implemented and the protocol itself facing DoS attacks. In addition SEND required overhead works and modification of the original NDP architecture.

(An and Kim 2008) suggest a mechanism for solving only a part from NDP threats, particularly DoS attack, but the mechanism is relatively weak when using a genuine working IP addresses.

A monitoring mechanism, NDPMon, to record NDP behavior was proposed in (Beck *et al*. 2007) based on Address Resolution Protocol (ARP) ArpWatch tool.

4. CRYPTOGRAPHY

4.1 Encryption

Encryption is when data is transformed into a cipher text to exclude unauthorized access to the data. Encrypted data requires decryption to return it to its original readable form. There are many layers of security to prevent unauthorized decryption, one of which is having the correct decryption key. The decryption key is an algorithm that decrypts the encrypted message. The more advanced the encryption algorithm, the more difficult it is to access the data. Where several encryption algorithms are used on a single system, this is called a cryptosystem. There are several forms of cryptosystems, one of which is private key encryption or conventional encryption where encryption and decryption are performed by using the same key. Another form is asymmetric encryption or public key encryption where a public and private key are used for encryption and decryption. Such methods secure the data and prevent unauthorized access.

4.2 Digital Signature

According to (William, 2014) Digital Signature defined as "Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery". A Digital Signature is a virtual authentication mechanism in which a code unique to the sender is attached to verify the integrity of the source of the sender (Kaur *et al*., 2012). It serves as a form of encryption in which the message carries the sender's unique key, which the recipient then unpacks, see **Fig. 2** Above. This authentication method is an NIST standard employing the secure hash algorithm. This mechanism is often used for two purposes, signing and encryption and decryption and verification.

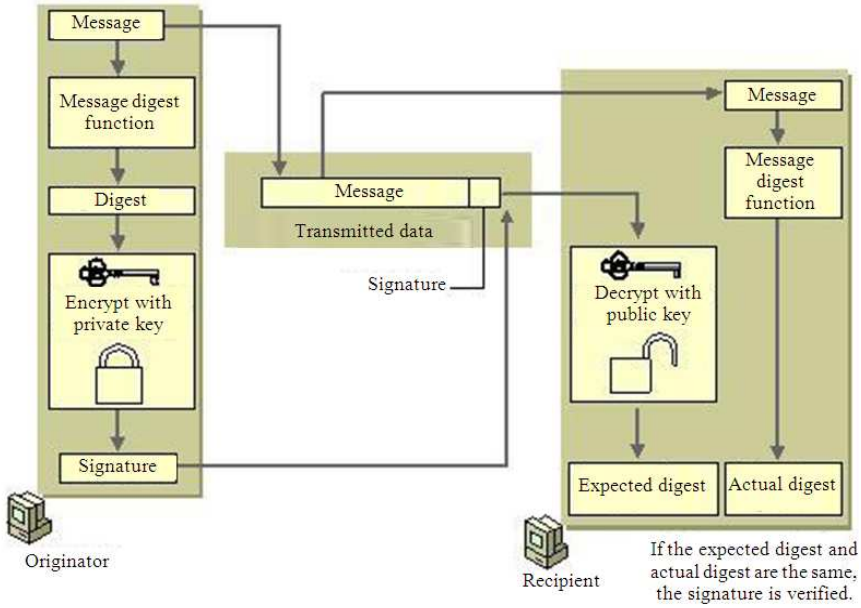

Fig. 2. Digital Signature Procedures

5. SECURITY THREATS AND PROPOSED MECHANISM

In IPv6 Neighbor discovery protocol an attacking node can cause packets for legitimate nodes, both hosts and routers, to be sent to some other link-layer address. This can be done by either sending a Neighbor Solicitation (NS) with a spoofed source link-layer address, or sending a Neighbor Advertisement (NA) with a spoofed target link-layer address (Beck *et al*., 2012). If the spoofed link-layer address is a valid one, packets will continue to be redirected, this is also lead to Man-in-The-Middle attack. The other part of the attack is Neighbor Discovery DoS attack (Kumar *et al*., 2013; AlSa'deh and Meinel, 2012) in this attack; the attacking node fabricates addresses with the subnet prefix of the target network and continuously sends packets to them. The last hop router is obligated to resolve the addresses with the Neighbor Discovery protocol. A legitimate host attempting to enter the network may be unable to obtain Neighbor Discovery service from the last hop router as the router is already busy with resolving the bogus addresses (Barbhuiya *et al*., 2013). The proposed mechanism is a cryptographic based solution. It is working according to the digital signature procedure. The nodes (Router/Hosts) will advertise their public keys once they are joined a local link to all other attached link in the network in a form of multicast message. Nodes will update their cash values with the new entries, now the nodes have each other public keys. In future any nodes receiving a message from another node will decrypt it with the sender public key they already have. If the message is spoofed one the nodes will detect this because the accompanied private key of the sender inside the message will mismatch with the sender public key that the receiver already have, the receiver will drop the message. **Algorithm 1** shows the steps for the proposed mechanism and **Fig. 3** representing the logical diagram of the proposed mechanism.

Algorithm 1

A, B network nodes;
A: Join a local link;
A: Multicast its public key;
B: Join a local link;
A: Multicast its public key;
A, B Update their cache with public keys new entries;
A, B Exchange messages according to their private keys and new entries;
IF
A send B and the keys are not matched;
THEN
Drop the packets;
Else
IF
B send A and the keys are not matched;
Then
Drop the packets;
Else
Receive the packets;

6. EXPERIMENTAL AND RESULTS

Simulation will be conducted based on Local Area Network (LAN) topology consisting of many nodes as per **Fig. 4.** All nodes are running Windows platforms and SendIP tool will be used to generate IPv6 traffic.

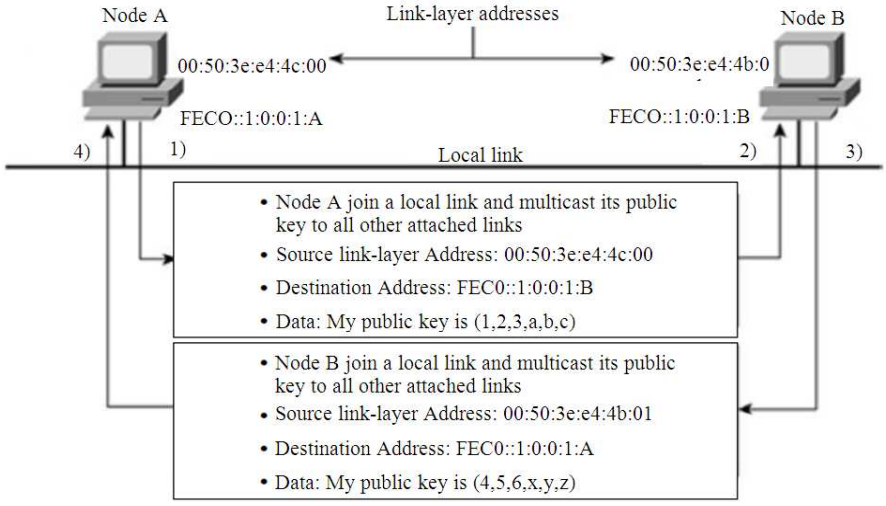

Fig.3. Mechanism's Logical Diagram

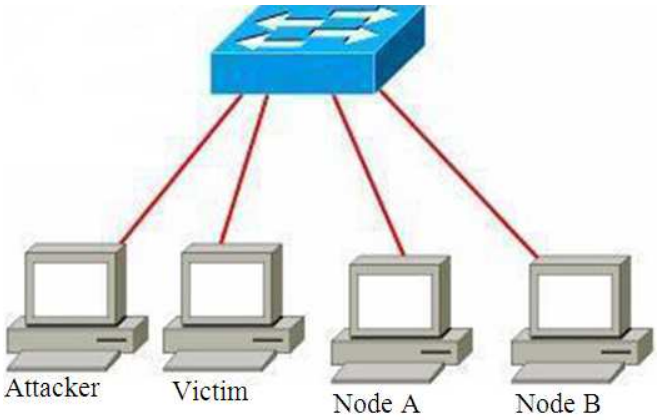

Fig. 4. Simulation LAN

One node, attacker node, will execute network attacks using THC-IPv6 tool. Two scenarios will run base on this topology, the first one representing the current NDP and second one representing NDP with the proposed mechanism. Spoofing, DoS and man-in-the-middle attacks will be executed for both scenarios and the network traffic will be captured for analysis in both receiving ends. The proposed mechanism is manage to eliminate the threats because of the binding between IP address, Public Key and MAC address of the node will not allow an attacker to use another node's address. Nodes will check their cache before replay to NDP messages to ensure the existence of the sender's IP-Public Key pair. Results for both scenarios with each kind of attacks will be analyzing and compared to evaluate the efficiency of the proposed mechanism. Currently the research is conducted at Network and Communication Technology (NCT) Lab in Faculty of Information Science and Technology (FTSM) at University Kebangsaan Malaysia (UKM). Evaluation of the results and comparisons will be published in future articles.

7. CONCLUSION

Neighbor Discovery Protocol is important in IPv6 networks for address resolution process. Because the design of IPv6 NDP, have a default assumption that communication link is safe and reliable, which is not correct in reality, the protocol facing high security threats risk. Neighbor solicitations spoofing and neighbor advertisements spoofing is one of the possible security attacks that threaten NDP. The attacks could be used to execute subsequent attacks suck as Man-In-The-Middle attack, Denial of Service attack (DoS).

Internet Engineer Task Force (IETF) request a proposals for solutions in many Request For Comments (RFC) drafts. Many proposals have been introduced by researchers using different security mechanisms. Some are using IP Security and others are using cryptographic solutions and some are using Intrusion Detection Systems (IDS). In this research we proposed the use of digital signature to secure IPv6 neighbor discovery protocol. The mechanism was introduced as a theoretical hypothesis and conceptual frame work. The proposed mechanism is able to detect NS/NA spoofing, Man in The Middle (MiTM) and DoS attacks, But still NDP have many other security threats. Router redirection, Duplicate Address Detection (DAD) and Neighbor Unreachability Detection (NUD) are some examples of these threats. Future research are requested in order to overcome the limitation of the proposed mechanism and to find a complete model to secure NDP.

8. REFERENCES

Ahmed, A.S., R. Hassan and Z.M. Ali, 2012. Eliminate spoofing threat in IPv6 tunnel. Proceedings of the8th International Conference on Information Science and Digital Content Technology, Jun. 26-28, IEEE Xplore Press, Jeju, pp: 218-222.

Alsa'deh, A. and C. Meinel. 2012. Secure neighbor discovery: Review, challenges, perspectives and recommendations. IEEE Sec. Privacy, 10: 26-34. DOI: 10.1109/MSP.2012.27

An, G. and K. Kim, 2008. Real-Time IP Checking and Packet Marking for Preventing ND-DoS Attack Employing Fake Source IP in IPv6 LAN. In: Autonomic and Trusted Computing, Chunming R., M.G. Jaatun, F.E. Sandnes, L.T. Yang and J. Ma (Eds.)., Springer Berlin Heidelberg, ISBN-10: 978-3-540-69294-2, pp: 36-46.

Arkko, J., A. Tuomas, K. James, V.M. Mäntylä and P. Nikander *et al*., 2002. Securing IPv6 neighbor and router discovery. Proceedings of the 1st ACM Workshop on Wireless Security, Sep. 28-28, ACM New York, USA, pp: 77-86. DOI: 10.1145/570681.570690

Arkko, J., J. Kempf, B. Zill and P. Nikander, 2005. Secure Neighbor Discovery (SEND), RFC 3971.

Arkko, J., T. Aura, J. Kempf, V.M. Mantyla and P. Nikander *et al*., 2002. Securing IPv6 neighbor and router discovery. Proceedings of the 1st ACM Workshop on Wireless Security, Sep. 28-28, ACM New York, USA, pp: 77-86. DOI: 10.1145/570681.570690

Barbhuiya, F.A., G. Bansal, N. Kumar, S. Biswas and S. Nandi, 2013. Detection of neighbor discovery protocol based attacks in IPv6 network. Netw. Sci., 2: 91-113. DOI: 10.1007/s13119-013-0018-2

Beck, F., Beck, F., T. Cholez, O. Festor and I. Chrisment, 2007. Monitoring the Neighbor Discovery Protocol. Proceedings of the International Multi-Conference on Computing in the Global Information Technology, Mar. 4-9, IEEE Xplore Press, Guadeloupe City, pp: 57- 57. 10.1109/ICCGI.2007.39

Beck, F., T. Cholez, O. Festor and I. Chrisment, 2007. Monitoring the neighbor discovery protocol. Proceedings of the International Multi-Conference on Computing in the Global Information Technology, Mar. 4-9, IEEE Xplore Press, Guadeloupe City, pp: 57- 57. DOI: 10.1109/ICCGI.2007.39

Castelluccia, C., 2004. Cryptographically generated addresses for constrained devices. Wireless Personal Communic. Int. J., 29: 221-232. DOI: 10.1023/B:WIRE.0000047065.81535.84

Davies, J., 2012. Understanding IPv6. 3rd Edn., Microsoft Press, ISBN-10: 0735659141, pp: 716.

Ferdous, A.B., S. Biswas and S. Nandi. 2011. Detection of neighbor solicitation and advertisement spoofing in IPv6 neighbor discovery protocol. Proceedings of the 4th international conference on Security of information and networks, Nov. 14-19, Sydney, NSW, Australia, ACM New York, USA, pp: 111-118. DOI: 10.1145/2070425.2070444

Gelogo, Y., E. Caytiles, D. Ronnie and B. Park, 2011. Threats and Security Analysis for Enhanced Secure Neighbor Discovery protocol (SEND) of IPv6 NDP Security. Int. J. Control Automat., 4: 179-184.

Hassan, R., A.S. Ahmed, N.E. Othman and S. Sami, 2014. Enhanced encapsulated security payload a new mechanism to secure internet protocol version 6 over internet protocol version 4. J. Comput. Sci., 10: 1344-1354.

Kumar, N., G. Bansal, S. Biswas and S. Nandi, 2013. Host based IDS for NDP related attacks: NS and NA Spoofing. Proceedings of the IEEE Annual India Conference, Dec. 13-15, IEEE Xplore Press, Mumbai, pp: 1-6. 10.1109/INDCON.2013.6726054

Liu, H.C. and G.D. Qing, 2013. Design of Security Neighbor Discovery Protocol. Proceedings of the International Conference on Communication Systems and Network Technologies, Apr. 6-8, IEEE Xplore Press, Gwalior, pp: 538-541. DOI: 10.1109/CSNT.2013.195

Ravneet, K. and A. Kaur, 2012. Digital signature. Proceeding of the International Conference on Computing Sciences, (ICCS' 12), IEEE.

Rosilah, H. and A.S. Ahmed, 2013. Avoiding spoofing threat in IPv6 tunnel by enhancing IPSec. Int. J. Adv. Comput. Technol., 5: 1241-1250.

William, S., 2014. Cryptography and Network Security: Principles and Practice. 5th Edn., Prentice Hall; ISBN-10: 0136097049, pp: 744.