Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 6 (3): 198-206, 2014
ISSN 1815-7432 / DOI: 10.3923/rjit.2014.198.206

Neighbor Discovery Message as Threats on 6to4 Tunneling

[1]Nazrulazhar Bahaman, [2,3]Anton Satria Prabuwono and [1]Nurul Azma Zakaria
[1]Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, 76100, Durian Tunggal, Malaysia
[2]Faculty of Information Science and Technology, University Kebangsaan Malaysia, 43600 Bangi, Malaysia
[3]King Abdulaziz University, Rabigh 21911, Saudi Arabia

Corresponding Author: Nazrulazhar Bahaman, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, 76100, Durian Tunggal, Malaysia Tel: +606 3316652 Fax: +606 3316500

ABSTRACT

The 6to4 tunneling is a type of automatic tunneling that developed among other numerous of transition mechanisms. It was introduced to ensure smooth implementation of IPv6 on existing network. However, it is believed that the implementation has been manipulated to execute several types of attacks. As a concern, this study thoroughly describes on potential of Neighbor Discovery based attack passed through 6to4 Tunneling. The preference development tools and networking mechanism suite are setup to conduct proposed attack method under testbed environment. The results carried out proved that the attacking method is feasible to attempt, while 6-4 tunnel showed the influence on the achievement of this attack in current internet.

Key words: Protocol-41, IPv6, IPv4, 6to4, tunneling and flooding attack

INTRODUCTION

Internet Engineering Task Force (IETF) was entrusted to develop and replace the existing Internet Protocol (IP) (Raicu and Zeadally, 2003). As a result they have successfully introduced the new IP structure more efficient and proficient to accommodate the current weaknesses. This new IP known as Internet Protocol version 6 (IPv6) was first introduced to the public in December 1998 (Deering and Hinden, 1998). To date, most of deployments by previous researches were to identify constraints that may occur in IPv6. Since it takes prolonged period to full implementation (Waddington and Chang, 2002), Transition Mechanism (TM) has been inspired in order to catalyze a successful integration of IPv6 into an existing network (Al-Jaafreh *et al*., 2008; Narayan and Tauch, 2010). As referred to Waddington and Chang (2002), TMs are identified into three main categories based on their operation and the way of their implementation: Dual stack mechanisms (Durand, 2001; Hirorai and Yoshifuji, 2006), tunneling mechanisms (Waddington and Chang, 2002; Vazao *et al*., 2004) and translation mechanisms (Grosse and Lakshman, 2003; Kawarasaki *et al*., 2003). Among of these mechanisms, tunneling is preferred implemented nowadays.

The IPv6 mandates the inclusion of IP Security (IPsec) (Kent and Atkinson, 1998; Zagar and Grgic, 2006) makes it is more secure than IPv4. Thus, most of threats that dominate the IPv4 network are no longer effective on IPv6 networks (Yang *et al*., 2007). Therefore, the current security related issues can be mitigated in the future implementation. However, after a few years of IPv6 services, some of IPv4 threats have been discovered by researchers at the IPv6 environment (Liu *et al*., 2009). In addition, Bahaman *et al*. (2011) stated that automatic tunneling as among the spreader threats without being detected by intrusion detection tools. Even though, it has been

acknowledged by Deering and Hinden (1998), Savola and Patel (2004) about this issue but they are provide only theoretical approach on their proposed steps.

This study proposes the possible methods of NDP based attack through the medium of 6to4 tunneling. The method focuses on flooding attack that use Router Advertisement message and 6to4 tunneling as manipulated elements. In order to implement this threat, the possible method of the attack is firstly review and identified. Next, this method is presented in equation form to understand clearly. Here, the testbed was developed in order to acquire the desired environment. Then, the packet analyzer was appointed as monitoring and validating function. Finally, the proposed attacks were constructed and triggered through the testbed. The mentioned attacks were carried out using a Python platform tool, Scapy (Burns *et al.*, 2007; Hogg and Vyncke, 2009).

IPv6 TO IPv4 TUNNELING

During transition period, by ignoring automatic tunneling when defining network security policy, will cause any possible unauthorized traffic pass through the network security devices through tunnels. Similarly, the issue wills also occurred with file sharing applications using TCP port 80 globally with IPv4. Savola and Patel (2004); Hanumanthappa and Manjaiah (2009), noted automatic tunneling mechanisms are susceptible to packet forgery that refer to DoS attacks. More terrible, these threats are the same as in IPv4 but larger on the number of paths of exploitation. In addition, relay technologies were also introduced in automatic tunneling with application of DoS vectors. These risks have no difference as IPv4 but emerged new avenues for exploitation (Savola and Patel, 2004).

In this study, the investigation is covered specifically on an automatic 6to4 tunneling as TM due to security issues. Here, 6to4 which is one of tunnel technology is preferred to grant unicast IPv6 connectivity between IPv6 sites and hosts across the IPv4 Internet. It encapsulate IPv6 packet as IPv4 payload and used protocol number neither 6 (TCP) nor 17 (UDP) but 41 (Protocol-41) in protocol field of the IPv4 header. The 6to4 assume that entire IPv4 Internet as a link. The simplest implementation of 6to4 is applied between multiple networks. The task is done by connecting each of them with IPv4 Internet connection which may be a corporate network or the global Internet.

Major requirement is to send protocol-41 packet to another via any type of networks. At the end of 6to4 tunnel consists of a 6to4 Host/Router, 6to4 Router, or 6to4 Relay Router. Once configuration of 6to4 tunnels done at any interface of the router it will be called 6to4 router. If the configuration is added and then be able to communicate with the IPv6 Internet, it is called 6to4 relay router. Figure 1 shows the tunneling components and their placement on the Ipv4 and IPv6 Internets.

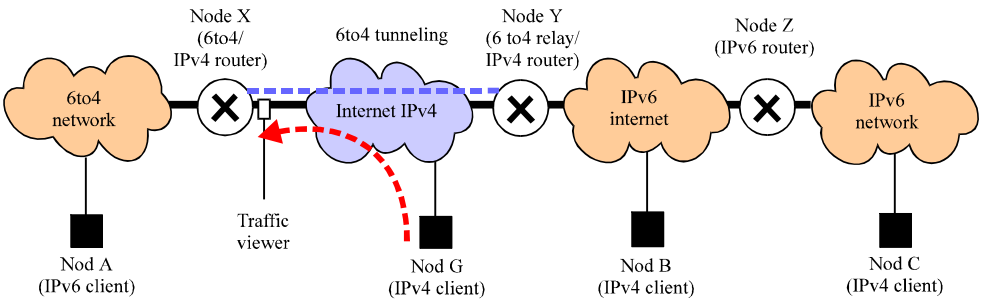

Fig. 1: Scenario of 6to4 tunneling

NEIGHBOR DISCOVERY PROTOCOL

The Neighbor Discovery Protocol (NDP) is a protocol in the Internet Protocol Suite operates in the Link Layer of the Internet model. It is used with IPv6 to perform a number of operations such as responsible for address auto configuration of nodes, discovery of other nodes on the link, determining the Link Layer addresses of other nodes, duplicate address detection, finding available routers and Domain Name System (DNS) servers, address prefix discovery and maintaining reach ability information about the paths to other active neighbor nodes.

Here, NDP is manipulated and used as a DoS attack element. According to Nikander *et al.* (2004), this NDP based DoS attack could be Router Advertisement (RA), Router Solicitation (RS), Neighbor Advertisement (NA) or Neighbor Solicitation (NS) massage. While the DoS attack types can be Flooding, Amplification and Exploitation Protocol or Spoofing attack, according to circumstances of the victim network. For the implementation techniques, it is closely related with the features that are available on the manipulated elements. Techniques that are commonly used are Direct, Spoofing Traffic, Reflection and Broadcast.

REPRESENTATIVE OF PACKET FLOW

The definitions of node and link are taken similarly from previous researchers. Generally, a node is an interface of device that receives or transmits traffic while a link is a medium of communication between nodes which the traffic may transmit through it. Then, they will be named to certain items. Colitti *et al.* (2004) and Taib and Budiarto (2007), According to basically a transmission process from sender node (Node_A) to destination node (Node_B) in IPv4 network, we may write:

$$AB \Rightarrow A:[AuB_4\ payload_4] \gg [payload_4]:B \tag{1}$$

where, A is source node, B is destination node, B_4 is destination IPv4 address, A_4 is source IPv4 address and $payload_4$ is a IPv4 payload.

While, transmission an IPv6 packet from Node_Y to Node_X is write as:

$$YX \Rightarrow Y:[Y_6X_6\ payload_6] \gg [payload_6]:X \tag{2}$$

Since IPv6 in IPv4 tunnel is established between Node_A and Node_B, we may name it as Tunnel (A, B) and packet sent through this tunnel can be write as:

$$Tunnel\ (A, B) = AB \Rightarrow A:[A_4B_4\ payload_4] \gg [payload_4]:B \tag{3}$$

An IPv6 packet encapsulated in an IPv4 payload with source and destination IPv6 address Y_6 and X_6 is written as:

$$payload_4 = Y_6X_6\ payload_6 \tag{4}$$

Then, if Eq. 2 communicate through Tunnel (A,B), we may write as:

$$Tunnel\ (A, B) \Rightarrow A:[A_4B_4\ [Y_6X_6\ payload_6] \gg][Y_6X_6\ payload_6]:B \tag{5}$$

Thus, this study is using the above interpretation on a real live tunneled network to observe its structure in general.

METHODOLOGY

Development of NDP based attack's model to address security issues of the 6to4 tunnel are discussed here. At 6to4 tunneling environment, a router will assume that all other routers and relay is "on-link". This condition is lends itself to an attack on any router with ND messages from any node in the IPv4 network. In order to more focused, targeted attacks are 6to4 pseudo interface. As long as an IP address is not used in the source or destination address, tunneling will allow the packet through it. Address of local link is seen to have the potential to realize this attack. By assuming all 6to4 routers and 6to4 relay routers are "on-link" and the entire IPv4 internet is a link, it is possible the proposed attack can be done on any node in the IPv4 network. While the victim node may either 6to4 router or 6to4 relay router.

The flooding attack with manipulating NA message technique was conducted and tested on testbed environment. Even though the flooding to cause disturbances, this study did not expect this attack to paralyze the network operation but just to ensure that the designs packet reached the destination with the proposed technique. Tunneling traffic monitoring developed and implemented to prove the result in the right order. This threat and the monitoring have been developed using free downloaded tool, Scapy because of the ability to permit building, sending, receiving and analyzing packets (Burns *et al.*, 2007). Then, a sequence of schematic flow has been designed as initiate the attack as in Fig. 2.

Design: Refer to Fig. 1, this kind of attack is operate by manipulating tunneling system and crafting multiple protocol 41 traffics between node X and node Y. Attacker is initiated from node G communicated with 6to4 router on 6to4 network. If each of the traffic flow is interpreted into the aforementioned equation, the structure of the traffics through 6to4 tunnels can be presented as follows:

- If node G as a trigger attacks from IPv4 networks and targeted to node X (6to4 Router) on 6to4 networks. In general packet flow is translated into the following equation:

$$GX \Rightarrow G:[G_4X_4\ [payload_4]\text{»}[payload_4]:X \tag{6}$$

Then Eq. 6 modified by manipulating design neighbor discovery packet as follows:

$$Tunnel(Y, X) \Rightarrow G:[Y_4X_4\ [B_6A_6\ ICMP\text{-}88]]\text{»}[B_6A_6\ ICMP\text{-}88]:X \tag{7}$$

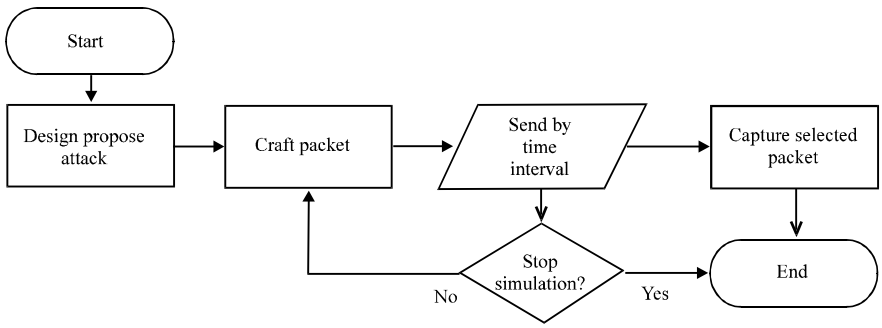

Fig. 2: Process of initiating the flood attack

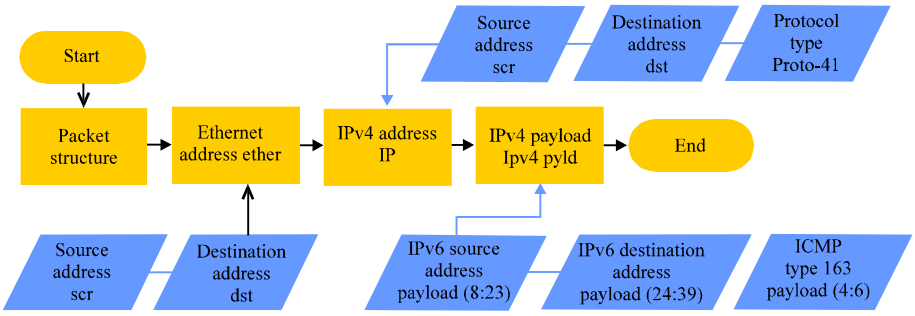

Fig. 3: Process flow diagram of packet crafting

Table 1: Instructions for each of elements in the crafted packet

Elements involved	Program commands
Source and destination Ethernet addresses	>>> ether=(Ether (src='00:00:00:00:00:0e', dst='00:00:00:00:00:0f', proto='41'))
Source and destination IPv4 addresses	>>> ipv4=IP(src='10.0.3.1' , dst='10.0.1.1')
Source and destination IPv6 addressees in IPv4 payload	>>> ipv4pyld=IP(payload(8:24) = 'fe80::1', payload(24:40)= 'fe80::2')
Neighbor advertisement in IPv4 payload	>>> ipv4pyld=IP(payload(4:6)='88')
Send the crafted traffic at regular interval onto tunnel	>>> send(ether/ipv4/ipv4pyld, iface='' loop='1' inter= 2)

Traffic GX is modified to Tunnel (Y, X) or traffic-41 protocol, payload4 is modified to packet NA, ICMPv6 type 136. When Eq. 7 entered the IP address, then:

$$\text{Tunnel (G, R1)}\Rightarrow\text{G:[10.0.3.1 10.0.1.1 [FE80::2 FE80::1 ICMP-88] [FE80::2 FE80::1 ICMP-88]:X} \quad (8)$$

Craft: Once overview of the attack technique is derived, the process started by building the attack packets as shown in Fig. 3. The development steps started with the design of packet structure. After that, IPv4 packet type 41 is build. Then, Ethernet source and destination addresses are declared and followed with their source and destination IPv4 addresses. Finally, at IPv4 payload must contained of ICMPv6 packet, source and destination IPv6 addresses and IPv6 payload containing NDP message. Table 1 shows an example of instructions for each of elements in the crafted packet.

Capture: Overall, the approach is to select specifically packet types 41 which the payload with IPv6 data and keep the preferred information into a log file. The process involved several steps as shown in Fig. 4. Briefly, the first step is filtering all traffic on tunneling. Secondly, the first byte of the payload identified as '6' in hexadecimal (IPv6 packet). Third process is to record the IP protocol value and the outer source and destination IPv4 address. The next step is chosen the inner source and destination IPv6 address is taken. Lastly, the traffic flow is kept in a log file. Table 2 shows the programming performed in accordance with the prescribed steps.

Experimental design: The 6to4 tunneling experimental (Bahaman *et al*., 2011) provides a useful testbed for this study. As an effort to reduce disturbances that may affect the accurate results, this experiment was conducted under a controlled environment. The scenario testbed as shown in Fig. 1, is developed with several different networks, named the 6to4 Network, the IPv4 Internet,

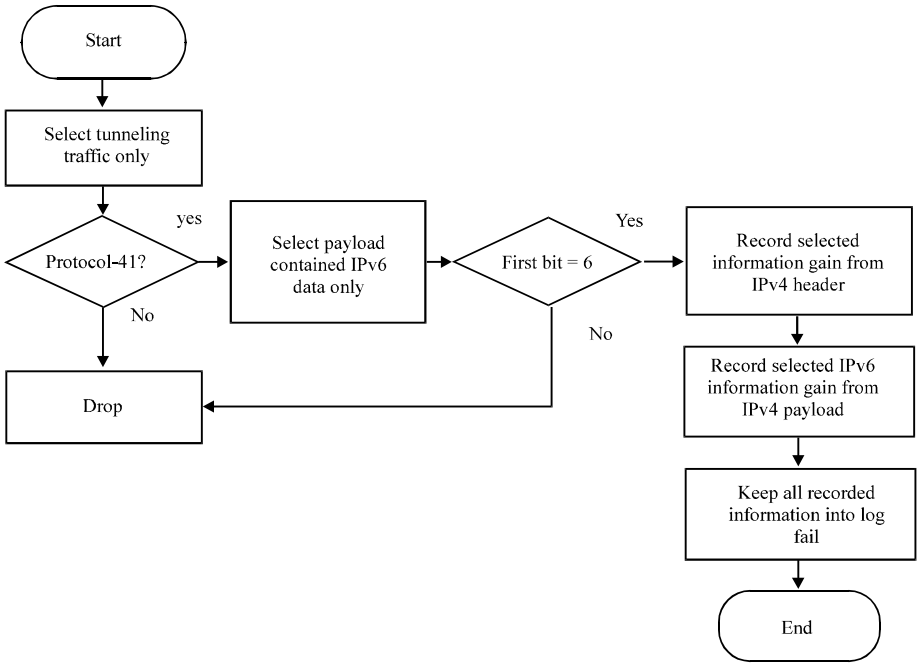

Fig. 4: Process flow diagram of the packet capturing process

Table 2: Part of the programming according to the steps implemented

Steps	Program commands
Filtering IPv4 proto-41	if pkt[IP] and pkt[IP].proto and pkt[IP].proto==41:
Identify IPv4 payload containing IPv6 data	if pkt[IP].payload and hexlist(pkt[IP].payload)[0][0] == "6":
Record the ip protocol value and the outer source and destination	v4src = str(pkt[IP].src)
IPv4 address	v4dst = str(pkt[IP].dst)
	v4p = str(pkt[IP].proto)
Record inner source and destination IPv6 address inner source and	v6src = v6tostr(hexlist(pkt[IP].payload)[8:24])
destination IPv6 address	v6dst = v6tostr(hexlist(pkt[IP].payload)[24:40])
Save the traffic flow in log file	logstate(v4src, v4dst, v4p, v6src, v6dst)

Table 3: Hardware and software

Hardware/ Software	Type	Description
Traffic builder	Scapy (Python platform)	As a tool to explore the traffic or packet by peeled some of elements
Router	Cisco 2811 with IOS 12.2(2) T	As a 6to4 and relay router to be both ends of the tunnel
Host	Linux Backtrack 5	As initiator and victim nodes

IPv6 Internet and the IPv6 Network. Here, node X and Y act as communication devices for the tunnel between the 6to4 networks to the rest of IPv6 networks. The confirmation mapped that node G as selected workstations on presented networks used as attackers.

All processes were supported by a Linux based platform OS with few selected software and hardware. The selection for essential tools for software and hardware are preferred from previous studies. The Table 3 records all chosen software and hardware for this experiment.

At the end of experiment, the proven of availability modeling attack conducted by looking into 6to4 tunneling traffic or specifically on IPv4 protocol type 41 traffic. The major goal is to identify

that the crafted packets injected pass through the tunnel were arrived at targeted destination. The process involved capturing and peeling the network traffic that could obtain the useful information so that easy to commit the further attacks. The important information in this implementation is getting the source and destination of IPv4 addresses.

RESULTS AND DISCUSSION

As mentioned earlier, this study aims on the capabilities of manipulated NDP based attack on the automatic 6to4 tunneling. For that reason, the assessment is conducted in a controlled environment on the testbed that is configured based on a real process of transmitting IPv6 packets over the IPv4 network. Initially, the simulation involved on generating tunneling traffics between nodes on different networks. Then, the threat implementation is applied on traffic builder with phyton platform. While the evaluation and understanding through analysis is obtained from revision on log file generated.

As an expected, this threat is not exhausted any resources. In other hand, it can be validated by initiator crafted packet arrived at victim's node. In Fig. 5 there is a part of the output gain from the log file which contained information of the crafted packet. From the result, the records proved that this attack is effective and can be executed under automatic tunneling network.

The findings told that the NDP based attack could use obtain information from existing IP protocol to launch on IPv6 network, respectively conventional. At the same time the attack may produce implications of other protocols. This issues has been agreed by Savola and Patel (2004) that the intruder could initiate the subsequent attack from the IPv4, IPv6 or dual stack network. As a result, the possibility of threats that could be implemented is the Network Discovery attack, Spoofing Traffic, Reflection and Local IPv4 broadcast attack. The issue will become worst as acknowledged in the study of Bahaman *et al.* (2012), most of the threats are complicated to detect by conventional security mechanisms neither IDS or firewall. Colitti *et al.* (2004) and Bahaman *et al.* (2012), the authors highlighted that these mechanisms only inspecting the exterior of the packet without investigate the payload content.

Even though among literatures propose the blocking protocol-41 on the firewall or IDS but this solution will terminate the tunnel link. On opposite approach, if the mechanisms setting is too loose it will expose the network infrastructure to invisible attacks that hide under the tunnel encapsulated packet. As sequences, the more effective solution established to mitigate this threat is to ensure that only the legal nodes are connected to the network. This implementation can be realized by using Layer 2 802.1x authentication, as has been pointed out by authors in (Carp *et al.*, 2010).

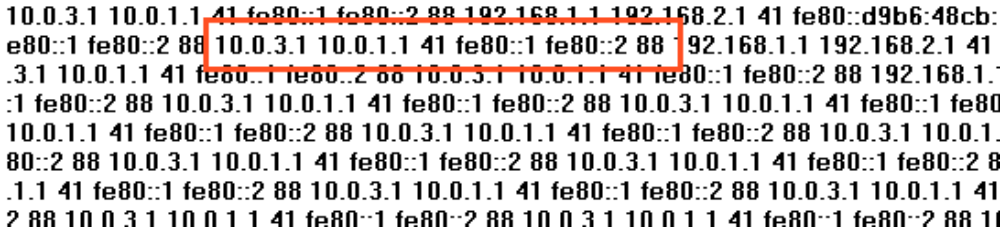

Fig. 5: Log file saved by traffic builder

CONCLUSION

As throughout the experiment found that the automatic 6to4 tunneling as IPv6 transition mechanism may abused by intruder to initiate kind of threats to IPv4, IPv6 or 6to4 network during the transition periods. Today's threat like NDP based attack which intercept various protocols of IPv4 or IPv6 traffics has shown it successful capabilities on tunnel traffic protocol-41. A propose solution by previous researcher is not a reason to ignore this matter but keep it as a motivation. Therefore, a serious action in developing the suitable techniques must be done to improve the previous work for more effective result. In the near future, the discovery is on finding another appropriate method to their corresponding threats via IPv6 transition mechanism, specifically on 6to4 tunneling. The comprehensive work is on the element of protocol-41 traffics.

REFERENCES

Al-Jaafreh, R., J. Mellor and I. Awan, 2008. Evaluating BDMS and DSTM transition mechanisms. Proceedings of the 2nd UKSIM European Symposium on Computer Modeling and Simulation, September 8-10, 2008, England, UK., pp: 8-10.

Bahaman, N., A.S. Prabuwono and M.Z. Masud, 2011. Implementation of IPv6 network testbed: Intrusion detection system on transition mechanism. J. Applied Sci., 11: 118-124.

Bahaman, N., A.S. Prabuwono, M.Z. Mas'ud and M.F. Abdollah, 2012. Effectiveness of security tools to anomalies on tunneled traffic. Inform. Technol. J., 11: 191-199.

Burns, B., J.S. Granick, S. Manzuik, P. Guersch, D. Killion and N. Beauchesne, 2007. Security Power Tools. 1st Edn., O'Reilly Media Inc., Sebastopol, ISBN 13: 9780596009632, Pages: 858.

Carp, A., A. Soare and R. Rughinis, 2010. Practical analysis of IPv6 security auditing methods. Proceedings of the 9th Roedunet International Conference, June 24-26, 2010, Sibiu, Romania, pp: 36-41.

Colitti, L., G. Di Battista and M. Patrignani, 2004. IPv6-in-IPv4 tunnel discovery: Methods and experimental results. IEEE Trans. Network Service Manage., 111: 30-38.

Deering, S. and R. Hinden, 1998. Internet protocol: version 6 (IPv6) specification. IETF, Request for Comments No. 2460, Internet Engineering Task Force. https://tools.ietf.org/html/rfc2460.

Durand, A., 2001. Deploying IPv6. IEEE Internet Comput., 5: 79-81.

Grosse, E. and Y.N. Lakshman, 2003. Network processors applied to IPv4/IPv6 transition. IEEE Network, 17: 35-39.

Hanumanthappa, J. and D.H. Manjaiah, 2009. IPv6 an IPv4 threat reviews with automatic tunneling and configuration tunneling considerations transitional model: A case study for university of mysore network. Int. J. Comput. Sci. Inform. Sec., 3: 1-12.

Hirorai, R. and H. Yoshifuji, 2006. Problems on IPv4-IPv6 network transition. Proceedings of the International Symposium on Applications and the Internet Workshops, January 23-27, 2006, Phoenix, AZ., pp: 38-42.

Hogg, S. and E. Vyncke, 2009. IPv6 Security. Cisco Press, Indianapolis, Pages: 540.

Kawarasaki, Y., T. Shibata and T. Takahashi, 2003. IPv4/IPv6 SIP interworking methods in dual-stack network. Proceedings of the 9th Asia-Pacific Conference on Communications, Volume 3, September 21-24, 2003, Malaysia, pp: 1124-1128.

Kent, S. and R. Atkinson, 1998. IP encapsulating security payload. RFC 2406, (Proposed Standard), November 1998. http://tools.ietf.org/html/rfc2406.

Liu, W., H.X. Duan, T. Lin, X. Li and J.P. Wu, 2009. H6Proxy: ICMPv6 weakness analysis and implementation of Ipv6 attacking test proxy. Proceedings of the Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing, July 7-9, 2009, Brisbane, Australia, pp: 519-524.

Narayan, S. and S. Tauch, 2010. Network performance evaluation of IPv4-v6 configured tunnel and 6to4 transition mechanisms on windows server operating systems. Proceedings of the International Conference on Computer Design and Applications, June 25-27, 2010, Qinhuangdao, China, pp: V5-435-V5-440.

Nikander, P., J. Kempf and E. Nordmark, 2004. IPv6 Neighbor Discovery (ND) trust models and threats. Internet Engineering Task Force, RFC 3756, Editor 2004.. http://www.hjp.at/doc/rfc/rfc3756.html.

Raicu, I. and S. Zeadally, 2003. Evaluating IPv4 to IPv6 transition mechanisms. Proceedings of the 10th International Conference on Telecommunications, Volume 2, February 23-March 1, 2003, Tahiti, pp: 1091-1098.

Savola, P. and C. Patel, 2004. Security considerations for 6to4. RFC 3964, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc3964.txt.

Taib, A.H.M. and R. Budiarto, 2007. Security mechanisms for the IPv4 to IPv6 transition. Proceedings of the 5th Student Conference on Research and Development, December 12-11, 2007, Selangor, Malaysia, pp: 1-6.

Vazao, T., L. Raposo and J. Santos, 2004. Migration to the New Internet-Supporting Inter Operability Between Ipv4 and Ipv6 Networks. In: Telecommunications and Networking, De Souza, J.N., P. Dini and P. Lorenz (Eds.). Springer-Verlag, Berlin, Heidelberg, ISBN: 978-3-540-22571-3, pp: 678-687.

Waddington, D.G. and F. Chang, 2002. Realizing the transition to IPv6. IEEE Commun. Magazine, 40: 138-147.

Yang, X., T. Ma and Y. Shi, 2007. Typical DoS/DDoS threats under IPv6. Proceedings of the International Multi-Conference on Computing in the Global Information Technology, March 4-9, 2007, Gosier, Guadaloupe, pp: 55.

Zagar, D. and K. Grgic, 2006. IPv6 security threats and possible solutions. Proceedings of the World Automation Congress, July 24-26, 2006, Budapes, pp: 1-7.