Journal of Applied Sciences 11 (1): 118-124, 2011
ISSN 1812-5654 / DOI: 10.3923/jas.2011.118.124

Implementation of IPv6 Network Testbed: Intrusion Detection System on Transition Mechanism

[1]Nazrulazhar Bahaman, [1]Anton Satria Prabuwono and [2]Mohd Zaki Mas'ud
[1]Faculty of Information Science and Technology,
Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor D.E., Malaysia
[2]Faculty of Information and Communication Technology,
Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia

Abstract: The potential of internet protocol version 6 (IPv6) cannot be denied as compared to the current network protocol (IPv4). The IPv6 ability which is offering huge amount of IP addresses has makes it being awaited by the Internet user. To make the IPv6 implementation successfully, a transition mechanism is needed to simplify the migration process between IPv4 to IPv6. The transition mechanism is created to support the joint operation between these protocols. However, after several years of implementation, it is believed that this mechanism has become an alternative route for intruders and attackers to penetrate the existing network. The problem kept remains without even being detected by any detection tools. Based on this problem, this study proposed an IPv6 network testbed for dealing with designation and implementation of Intrusion Detection System (IDS) on transition mechanism environment. All the equipments, tools and network are configured based on real process of transmitting IPv6 packets over IPv4 network. With fully functional operation for handling basic transition between IPv6 clients over IPv4 networks and equipped with intrusion detection tools, the testbed is used for investigating the intrusion activities behavior on the transition mechanism in the real environment. The result obtained from the testing phase shows the efficiency and the functionality of all hardware and software used. Moreover, the implementation of the testbed is expected to contribute to the realization of IPv6.

Key words: IDS, Protocol-41, transition mechanism, IPv6, tunneling

INTRODUCTION

The rapid development of information technology is not a new phenomenon. Almost every daily activity nowadays is depending on information technology. From sharing file or picture among friends to buying and selling market share are done online. This phenomenon has made network and communication become an important part of everyday life of society today. However, the issues of threat to computer systems and networks are also becoming the headline to the internet user. What make it worse is that the tools to launch such activities is also rapidly developed and freely downloaded over the internet.

Realizing to the problem at hands, the network security field has become the attention by most of the researchers. According to Shu-Qiang *et al.* (2009) as a result of attacks by the existing attack a new types of attack emerged, this has make the traditional defense mechanisms are unable to meet the needs of the environment in the new network. Thus, more researches are pursuing to solve the problem on the ability of ever-changing threat over time. Hence, Intrusion Detection System (IDS) is proposed (Zhang *et al.*, 2005) to strengthen the traditional safety mechanisms.

IDS is a system that constantly monitors the dynamic behavior of a computer system to warn against actions that endanger the integrity, security and availability of resources in the system. Even though IPv6 is still in the research stage (Zagar *et al.*, 2007), several approaches have been proposed to IDS in handling the Ipv4 and IPv6 transition phase. Although IPv6 has implemented IPSec in its package still it has several security issues such as Scanning, Head of susceptibility Routing, Multicast attack and Denial-of-Service (DoS) attack which is capable of making the networking system down.

This condition will be worse when the existence of the transitional mechanism become a threat to the current environment. This mechanism is considered temporary

Corresponding Author: Anton Satria Prabuwono, Faculty of Information Science and Technology,
Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor D.E., Malaysia

and merely a catalyst to change the internet protocol but it has been extended over the expected range. According to Zagar and Grgic (2006) security threats on the transition mechanism should be considered seriously, because the transition from IPv4 to IPv6 has been carried out over ten years. Therefore, they expected that both protocols will be operating together in a longer period of time. There are still no reports or analysis done by any references to prove the effectiveness of the IDS to monitor intrusion activity on the transition mechanism. Therefore, this study proposed the initial step of investigating the effectiveness of IDS in monitoring intrusion in transition mechanism by implementing an IPv6 testbed that is equipped with IDS.

BACKGROUND

Intrusion detection system: Intrusion Detection System (IDS) can be classified into three, namely, host-based intrusion detection, network-based intrusion detection and hybrid intrusion detection (Balaz and Vokorokos, 2009). IDS is a system to detect intrusion or attacks and classify any anomalies activities as an unwanted login authority, regardless of their success (Allen *et al*., 2000). This system is responsible for identifying interference, which is defined as the illegal use, misuse or abuse of computer systems by unauthorized user. In addition, IDS is also used to help computer systems handled various types of attacks such as scanning, worm and virus attacks. One of the objectives to achieve early detection of invasion is to collect information from various systems and networks and analyze the sources of group information, looking for symptoms that lead to safety problems (Hunt and Verwoerd, 2003). By analyzing these successful of this information, it will help to detect the invasion activity in the network.

Transition mechanism: Since, the last decades, researchers have been working on IPv6 deployment to replace the current IPv4 protocol. One of the biggest challenges in this work is how to migrate IPv4-based infrastructure to support IPv6. It is impractical and costly to change the entire IPv4-based network infrastructure to fully support IPv6. Aware of these constraints, transition mechanism has been created to ensure a smooth and successful integration of IPv6 into an existing network. Basically the transition mechanisms encapsulate IPv6 packets into IPv4 packets and sent them through the IPv4 network infrastructure. The encapsulation of an IPv6 datagram in IPv4 is shown in Fig. 1.

The transition mechanisms (Narayan and Tauch, 2010) are considered as a toolset to enable the smooth

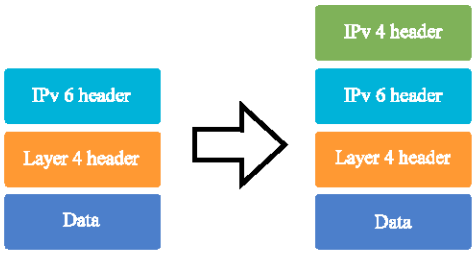

Fig. 1: Encapsulating IPv6 in IPv4

transition to the new version of the IP protocol. These mechanisms are divided into three main categories depending on their operation and the way of their implementation: dual stack mechanisms (Alain, 2001; Hirorai and Yoshifuji, 2006), tunneling mechanisms (Waddington and Fangzhe, 2002; Vazao *et al*., 2004) and translation mechanisms (Grosse and Lakshman, 2003; Kawarasaki *et al*., 2003). This study focuses on tunneling mechanism that is widely implemented nowadays.

The tunneling mechanisms may be used for the IPv6 communication over the existing IPv4 infrastructure and vice-versa. They are based on the encapsulation of IPv6 packets into IPv4 packets and the transmission over the IPv4 network. The two endpoints of the tunnel need to be dual stack routers or hosts. The tunneling strategies are presented into three categories: IPv6 over IPv4, IPv6 to IPv4 automatic tunneling and Tunnel Broker (Punithavathani and Sankaranarayanan, 2009; Narayan and Tauch, 2010).

According to Karpilovsky *et al.* (2009), from the result of analyzing the IP address structure shows that 80% of addresses fell to native IPv6 (native IPv6 tended to communicate with other native IPv6). The 6 to 4 addresses were also significant, representing 18% of addresses seen. Teredo addresses constituted approximately 2% and the remaining technologies were almost negligible.

Even if the tunneling mechanism properly implemented, it also contributes security threats. Some of the threat such as denial-of-service attack, reflection denial-of-service attacks and the service theft that a malicious node may make unauthorized use of service (Serudin, 2008). These threats can impose problem such as relay router not being able to identify whether relays are legitimate, impartially implemented relay router and administrative abuse.

ICMPv6 message: Internet Control Message Protocol version Six (ICMPv6) is used only in IPv6 (Conta and Deering, 1998; Liu *et al*., 2009). Its existence is an integral part of IPv6 and must be fully implemented by every Ipv6

Table 1: Typical ICMPv6 messages

Type	Meaning
ICMPv6 error messages	
1	Destination unreachable
2	Packet too big
3	Time exceeded
4	Parameter problem
100	Private experimentation
101	Private experimentation
127	Reserved for expansion of ICMPv6 error messages
ICMPv6 informational messages	
128	Echo request
129	Echo reply
133	Router solicitation
134	Router advertisement
135	Neighbor solicitation
136	Neighbor advertisement
200	Private experimentation
201	Private experimentation
255	Reserved for expansion of ICMPv6 informational messages

node. Additionally, each error is encountered during processing package by IPv6 node will be reported by the ICMPv6 and it also performs a diagnostics process known as ping 6.

ICMPv6 messages are grouped into two classes: Error Messages and Informational Messages. ICMPv6 Error Messages are known as such by having a zero in the high-order bit of their message Type field values. Thus, error messages have message Types from 0 to 127; informational messages have message Types from 128 to 255. Some of typical ICMPv6 messages are shown in Table 1.

IMPLEMENTATION

The main objective is to implement a suitable testbed for future use to do some experiments in order to reveal the activities done by intruders and attackers on this mechanism.

Hardware and software requirements: All processes were supported by Operating System (OS) that possible to support multiple platforms as well as several selected software and hardware. The selection of the inventory for the analysis and observation are shown in Table 2.

Snort is chosen for the purpose of monitoring the anomalies activity in the testbed. It is a full-fledge, open-source, Network Based Intrusion Detection System (NIDS) (Bin *et al*., 2006) that has the capabilities such as packet sniffing and packet logging. Faizal (2009) has mentioned that Snort as the standard factor to the network intrusion detection system. This widely used IDS is a combination of signature-based IDS and anomaly based IDS. Based on these capabilities Snort has been selected as IDS inside this implementation.

Table 2: Inventory test

System	OS	IPv6 capable
Cisco Router 2811	IOS 12.xx and above	Y
MS Windows	XP, SP2 and above	Y
	Vista	Y
	Windows 7	Y
Linux	Fedora9	Y
	RedHat Enterprise Linux5	Y
	CentOS 4	Y

By taking the inventory of the current infrastructure, it gives an outline of which software and hardware is part of the research. It is important that every part of the current situation is being described in detail. A detailed description of the infrastructure gives a good insight in which hardware and software is to be IPv6 enabled. For this experiment the following Hardware and software are used in the experiment setup:

- **Operating system:** Windows7, Windows XP SP3, Linux Fedora9, Linux CentOS 4
- **Networking tools:** Snort 2.8.3, Kiwi Syslog Server 9.0.3, WinPcap 4.1.1, Oinkmaster 2.0, WireShark 1.2.6.
- **Router:** Cisco 2811 with IOS 12.2(2) T
- **Switch:** Cisco catalyst 2960-24TT 24-Port ethernet switch

Scenario-based setup: This section describes the methods of installation and configuration of the environment required. This implementation was conducted under a controlled environment in accordance with a basic IPv6 network using IPv6 tunneling mechanism as a route to other IPv6 networks. Meanwhile, the attack scenarios were based on several IPv6 related attack (Tseng *et al*., 2004) such as port scan and selected DDoS attack.

Basically, the testbed is developed with several different networks, named IPv4/6 Network A, IPv4/6 Network B, IPv4 Network and IPv6 network. Router A, E and F act as communication equipments for the tunnel between IPv4/6 B network to IPv6 network and IPv4/6 A. Next, the IDS and Packet analyzer tool are placed at the tunnel between Router A and B. All transitions of the network traffic on this tunnel are observed by this protocol analyzer. A workstation on the IPv4/6 Network A named as Attacker is used as the attacker. At the same time, several workstations on IPv4/6 Network A and IPv6 Network are used as slaves and run multiple attacks in parallel at the same time with the attacker. A workstation in IPv4/6 Network B is assigned as the victim. This scenario is shown in Fig. 2.

Threat selection: The threat on this implementation was related to IDS functionality testing. Selection of threat

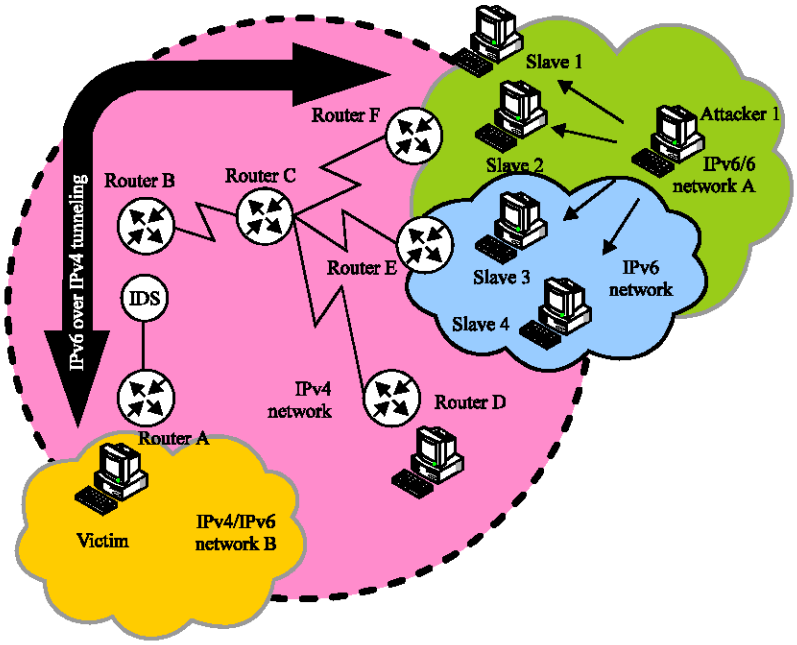

Fig. 2: Testbed architecture

Table 3: Types of attacks with IPSec protection without spoofed address status

Attacks	Status of protection
Duplicate address detection attack	Yes
Neighbour unreachability detection failure	Yes
Neighbour solicitation/advertisement spoofing	Yes
Router discovery attack	Yes
TCP-flood attack	No
UDP-flood attack	No
ICMP-flood attack	No
Smurf attack	Yes

was based on their popularity and effectiveness to networking and undetectable by IPSec. A threat on the Internet is now dominated by a DoS attack and occurred in IPv6 environment. According to Xinyu *et al.* (2007) almost all types of DoS/DDos attacks on the IPv6 environment can be controlled using IPSec but there are also weaknesses due to unprotected some of attacking conditions. This can be summarized in Table 3. Therefore attacks number 5, 6 and 7 can be implemented in IPv6 environment without being detected by IPSec. For this test, ICMPv6 flood attack without spoofed address was used as a sample of attack because it is most basic and popular within those three attacks (Udhayan and Anitha, 2009). This attack also known as ping flood attack that can be done by using ping command.

The port scan tool used in this implementation is Nmap in which it is already partially supported IPv6. It used to discover hosts and services on a computer network, thus creating a map of the network. Even though larger address spaces provided by IPv6 network seem impossible to exercise a port scan activity but in the real life it still becomes one of the most popular techniques that attackers used to discover services that they can exploit. Port scan helps the attacker find which port is always listening to request and when it is responding to a request it will give an indication regarding the services it is offering in which the information gathered can be used for further probing in order to find the vulnerabilities.

TESTING

Testing phase was to ensure that all items involved in this testbed operating at a satisfactory level. To meet the objectives of this implementation several tests were selected based on previous references. Among these are connectivity (Udhayan and Anitha, 2009), hop count, round trip time (Cho *et al.*, 2004), throughput (Raicu and Zeadally, 2003; Law *et al.*, 2008), threat and intruder detector and packet flow (Xinyu *et al.*, 2007).

Connectivity: In this test, ping and ping 6 were used to investigate the connectivity of transition mechanism, as compared to IPv4. To ensure that it operates in multi-platform operating systems, testing is done on all nodes involved. The results of these are summarized in Table 4.

Table 4: Connectivity testing result

Source	Destination	Packet	Results
Attacker 1	Slave 1	ICMPv6	Ok
	Slave 2	ICMPv6	Ok
	Slave 3	ICMPv6	Ok
	Slave 4	ICMPv6	Ok
Slave 1	Victim	ICMPv6	Ok
Slave 2		ICMPv6	Ok
Slave 3		ICMPv6	Ok
Slave 4		ICMPv6	Ok
Router 1	Router 4	ICMP	Ok
	Router 5	ICMP	Ok
	Router 6	ICMP	Ok
	Attacker 2	ICMP	Ok
Attacker 2	Victim	ICMP	Ok

Table 5: Hop count testing result

Sender gateway	Receiver gateway	Packet	Hops
IPv4/6 network A	IPv4/6 Network B	ICMPv6	1
IPv4/6 network A		ICMP	3
IPv6 network		ICMPv6	1
IPv4 network		ICMP	3

Hop count: Using traceroute and traceroute 6, determined the number of hops between the source node and the destination node. It is also an alternative way to ensure that the route of the packet from source to destination is on the right path. On this test, gateway of each network is used as a source and destination nodes as shown in Table 5.

Round Trip Time (RTT): The response times provide an indication of the quality-of-service experienced by nodes in the IPv6 and IPv4 networks. All nodes on different networks are involved by sending and receiving the ICMP and ICMPv6 to each other.

Throughput: In this test, basic transfer file protocol, ftp was used to download files across the networks. In order to have an unbiased result, the files are downloaded from servers using different operating systems. The throughput is calculated from the formula:

$$T = P/L$$

where, T represents the throughput, P represents the transferred data size and L represents the time cost in transfer. Figure 3 plots the throughput associated with IPv6 over IPv4 tunneling for packet sizes that range from 128 bytes to 1024 bytes. The results show that nodes are not influenced by the type of OS.

Threat and intruder detector: ICMP flood attack and ICMPv6 flood attack were used to produce a threat situation on early ICMP flood attacks. The packets were produced by the ICMP echo command, more popularly known as ping. This ping flood attack was used to flood large amounts of data packets to the victim's workstation in an attempt to overload the victim. Figure 4 shows the IDS warning on syslog during the attack situations. This notification proved that IDS has been activated and functional.

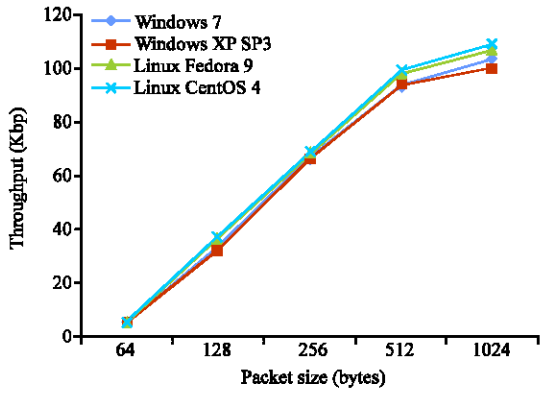

Fig. 3: Throughput to nodes with different OS

```
07-09-2010   17:28:55:Auth.Alert   127.0.0.1
Mar 09   17:28:55 NazrulAB sonrt: [1:408:5] ICMP
Echo Reply [Classification: Misc activity]
[Priority: 3]: {ICMP} 192.168.8.253 -> 192.168.2.1

07-09-2010  17:28:55 Auth.Alert  127.0.0.1  Mar 09
17:28:55 NazrulAB snort: [1:382:7] ISMP PING
Windows [Classification: Misc activity] [Priority:
3]: {ICMP} 192.168.2.1 -> 192.168.8.253
```

Fig. 4: Among IDS warning appeared on syslog

```
27  9.791703  2001:470:18:174::1
2000:480:20:184:5:5:5:254   ICMPv6 Echo request
--------------------------------------------------
Arrival Time: July  9, 2010 02:37:13.256495000
Protocols in frame: eth:ip:ipv6:impv6:data
Data (65500 bytes)

28  9.792558  2000:480:20:184:5:5:5:254
2001:470:18:174::1  ICMPv6  echo reply
--------------------------------------------------
Arrival Time: July 9, 2010 02:37:13.257350000
Protocols in frame: eth:ipv6:impv6:data
Data (65500 bytes)
```

Fig. 5: Sample ICMPv6 packet through tunneling captured

Packet flow: Network Protocol analyzer was used to analyze the packet flow in detail. Here, the network protocol analyzer was used to ensure that all packets go through the tunnel as well as passing through the IDS. The analyzer indicated that the packets travel through the tunnel and IDS as expected. This packet flow activities gathered is shown in Fig. 5.

CONCLUSIONS

This study proposed the design and implementation of intrusion detection system on the IPv6 transition mechanism. It has reflected as an IPv6 testbed network with IDS, which was developed as part of a joint research project to investigate the discovery of new resources and content distribution protocol in transition mechanisms environment. One of the key components of the testbed is a tunneling mechanism. In order to develop this mechanism with IDS is enabled a number of allotments have to be done. The result obtained from the testing phase for shows the efficiency and the functionality of all hardware and software used. Moreover, the implementation of the testbed is expected to contribute to the realization of IPv6.

In the near future, the same testbed will be used to analyze the ability of conventional IDS to detect DDoS flood attack without spoofed address under transition mechanism.

ACKNOWLEDGMENTS

The authors would like to thanks Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia for providing facilities and financial support under Research University Operation Project No. UKM-OUP-ICT-36-186/2010 and Arus Perdana Project No. UKM-AP-ICT-17-2009.

REFERENCES

Alain, D., 2001. Deploying IPv6, Internet Computing. IEEE Educational Activities Department Piscataway, 2001, NJ, USA., pp: 79-81.

Allen, J., A. Christie, W. Fithen, J. Mc Hugh J. Pickel and E. Stoner, 2000. State of the Practice on Intrusion Detection Technologies: Networked Systems Survivability Program. University of Carnegie Mellon, Pittsburgh, USA.

Balaz, A. and L. Vokorokos, 2009. Intrusion detection system based on partially ordered events and patterns. Proceedings of the International Conference on Intelligent Engineering Systems, April 16-18, Barbados, pp: 233-238.

Bin, L., L. Zhitang and L. Zhanchun, 2006. A scalable intrusion detection system for Ipv6. Wuhan Univ. J. Nat. Sci., 11: 1723-1726.

Cho, K., M. Luckie and B. Huffaker, 2004. Identifying IPv6 network problems in the dual-stack world. Proeedings of the ACM SIGCOMM Workshops, September 22, Portland, Oregon, USA., pp: 283-288.

Conta, A. and S. Deering, 1998. Internet control message protocol (ICMPv6) for the internet protocol version 6 (IPv6) specification. R. F. C.: 2463, Internet Engineering Task Force.

Faizal, A., 2009. Enhanced fast attack detection technique for network intrusion detection system. Ph.D. Thesis, Universiti Teknikal Malaysia Melaka, Durian Tunggal, Malaysia.

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

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

Hunt, R. and T. Verwoerd, 2003. Reactive firewalls-a new technique. Comput. Commun., 26: 1302-1317.

Karpilovsky, E., A. Gerber, D. Pei, J. Rexford and A. Shaikh, 2009. Quantifying the extent of IPv6 deployment. Passive Active Network Measurement, 5448: 13-22.

Kawarasaki, Y., T. Shibata and T. Takahashi, 2003. IPv4/IPv6 SIP interworking methods in dual-stack network. Proc. 9th Asia-Pacific Conf. Commun., 3: 1124-1128.

Law, Y.N., M.C. Lai, W.L. Tan and W.C. Lau, 2008. Empirical performance of IPv6 vs. Ipv4 under a dual-stack environment. Proceedings of the IEEE International Conference Communications, May 19-23, Beijing, pp: 5924-5929.

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, 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, Qinhuangdao, China, pp: V5-435-V5-440.

Punithavathani, D.S. and K. Sankaranarayanan, 2009. IPv4/IPv6 transition mechanisms. Eur. J. Scientific Res., 34: 110-124.

Raicu, I. and S. Zeadally, 2003. Evaluating IPv4 to IPv6 transition mechanisms. Proc. 10th Int. Conf. Telecommun., 2: 1091-1098.

Serudin, N.A., 2008. IPv6-to-IPv4 Transition and Security Issues. Block K, Information Technology and State Store Building, Brunei Darussalam.

Shu-Qiang, H., Z. Huan-Ming and Y. Guo-Xiang, 2009. Research of NIDS in IPV6 based on protocol analysis and pattern matching. Proceedings of the 2nd International Workshop on Knowledge Discovery and Data Mining, Jan. 23-25, Moscow, pp: 542-545.

Tseng, B., C.Y. Chen and C.S. Laih, 2004. Design and implementation of an IPv6-enabled intrusion detection system (6IDS). Proceedings of International Computer Symposium, Dec. 15-17, Taipei, Taiwan, pp: 684-689.

Udhayan, J. and R. Anitha, 2009. Demystifying and rate limiting ICMP hosted DoS/DDoS flooding attacks with attack productivity analysis. Proceedings of the IEEE International Advance Computing Conference, March 6-7, Patiala, pp: 558-564.

Vazao, T., L. Raposo and J. Santos, 2004. Migration to the new Internet Supporting Interoperability between IPv4 and IPv6 Networks. In: Lecture Notes in Computer Science, De Souza, J.N. *et al.* (Eds.). Springer-Verlag, Berlin, Heidelberg, pp: 678-687.

Waddington, D.G. and C. Fangzhe, 2002. Realizing the transition to Ipv6. IEEE Commun. Magazine, 40: 138-147.

Xinyu, Y., M. Ting and S. Yi, 2007. Typical DoS/DDoS threats under IPv6. Proceedings of the International Multi-Conference on Computing in the Global Information Technology, March 4-9, Gosier, Guadaloupe, pp: 55-55.

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

Zagar, D., K. Grgic and S. Rimac-Drlje, 2007. Security aspects in IPv6 networks-implementation and testing. Comput. Electr. Eng., 33: 425-437.

Zhang, B., W. Li, X. Shi and W. Wang, 2005. Study on intrusion detection and prevention based on IPv6 Internet. Xibei Gongye Daxue Xuebao/J. Northwestern Polytechnical. Univ., 23: 79-83.