Journal of Computer Science 10 (7): 1344-1354, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.1344.1354 Published Online 10 (7) 2014 (http://www.thescipub.com/jcs.toc)

ENHANCED ENCAPSULATED SECURITY PAYLOAD A NEW MECHANISM TO SECURE INTERNET PROTOCOL VERSION 6 OVER INTERNET PROTOCOL VERSION 4

Rosilah Hassan, Amjed Sid Ahmed, Nur Effendy Othman and Samer Sami

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 2013-11-24; Received 2013-11-27; Accepted 2014-03-04

ABSTRACT

A considerable amount of time will be needed before each system in the Internet can convert from Internet Protocol version 4 (IPv4) to Internet Protocol version 6 (IPv6). Three strategies have been proposed by the Internet Engineer Task Force (IETF) to help the transition from IPv4 to IPv6 which are dual stack, header translation and tunneling. Tunneling is used when two computers using IPv6 want to communicate with each other and the packet will travel through a region that uses IPv4. To pass through this region, IPv6 packet must be encapsulated in IPv4 packet to have an IPv4 address in order to make it IPv4 routing compatible. Internet Protocol security (IPsec) in transport mode carries the payload of the encapsulating packet as a plain data without any mean of protection. That is, two nodes using IPsec in transport mode to secure the tunnel can spoof the inner payload; the packet will be de-capsulated successfully and accepted. IETF mentioned this problem in many RFCs. According to RFC 3964 there is no simple way to prevent spoofing attack in IPv6 over IPv4 tunnel and longer term solutions would have to be deployed in both IPv4 and IPv6 networks to help identify the source of the attack, a total prevention is likely impossible. This study proposed a new spoofing defense mechanism based on IPsec's protocol Encapsulated Security Payload (ESP). ESP's padding area had been used to write the IPv6 source address of the encapsulated packet. Simulation is conducted based on two scenarios, one with spoofing attack and one without. The outcome proved that proposed mechanism has managed to eliminate spoofing threat in IPv6 over IPv4 tunnel.

Keywords: IPv6, IPsec, ESP

1. INTRODUCTION

Until a full deployment of IPv6 done, IPv4 and IPv6 will co-exist and interacts together under many circumstances (Bouras *et al*., 2003). IPv6 over IPv4 Tunnel is applied when IPv6 hosts inside native IPv4 network need to communicate with native IPv6 network, but there is no direct IPv6 link between them. Tunneling IPv6-in-IPv4 has become common at the early stage of IPv6 deployment. The general idea is to make the IPv6 packet as the payload of IPv4 packet, i.e., IPv6 packets are encapsulated in IPv4 packets and then are transmitted over IPv4 networks like ordinary IPv4 packets (Raicu and Zeadally, 2003).

Since commonly that IPv6 hosts/networks are separated by IPv4 network, IPv6 over IPv4 Tunnel is very important for IPv6 transition. In IPv6 over IPv4 tunnel, when a tunnel end point receives an encapsulated data packet, it de-capsulate the packet and sends it to the other local forwarding scheme. Because IPv6-in-IPv4 tunnels do not use any form of authentication, a tunnel destination will accept an encapsulated packet sent by any node as

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

long as the source IPv4 address of the packet is the IPv4 address of the tunnel source (Colitti *et al*., 2004).

The security threats in IPv6 over IPv4 tunnel are caused by the spoofed encapsulated packet sent by the attackers in IPv4 networks. The target of attacks can be either a normal IPv6 node or the tunnel end point (Bi *et al*., 2007). When IPv6 packet is encapsulated in IPv4 payload then there is no means for administrators to know about IPv6 traffic that has tunneled into their networks (Sabnis and Tech, 2013). Unfortunately tunneling introduces security threats in which intruders may spoof the address of the packet origin and potentially inject the packet at the tunnel endpoint (Taib and Budiarto, 2010). Spoofing in IPv6 over IPv4 tunnel still represents a serious problem today, one of the solutions that been proposed is to use IPsec with ingress filtering. In order to do ingress filtering, the network needs to know which IP addresses each of the networks it is connected to may send. This is not always possible. For instance, a network that has a single connection to the Internet has no way to know if a packet coming from that connection is spoofed or not.

2. BACKGROUND

2.1. Spoofing

A crucial element enabling numerous different types of Internet Protocol (IP) attacks is the ability for an adversary to modify their source IP address and the ports they are communicating on to appear as though traffic initiated from another location or another application. This so-called “spoofing” attack is prevalent despite the presence of best practices to mitigate the usefulness of the attack (Sharma, 2010). IP spoofing is one of the major network spoofing techniques. It consists of SYN flooding, Transfer Control Protocol (TCP) hijacking and Address Resolution Protocol (ARP) spoofing (Wang, 2009). IP spoofing is a technique used to gain unauthorized access to computers by which the attacker acts as a trusted computer either by using an internal IP address within the range of the network or alternatively by using an authorized external IP address. The first step that attacker must do is to determine a valid IP address of a trusted host and then modify the packet header to make it appear that it come from that trusted host (Bidgoli, 2009). Spoofing could be executed at DNS, Web and email level (Kamal and Issac, 2007).

2.2. IPv4 Verses IPv6

IPv4 is the delivery mechanism which used by TCP/IP protocols to deliver a packet from some source to another destination. **Figure 1** shows the location of IPv4 in the TCP/IP suite. IPv4 is a connectionless and a non-reliable datagram protocol which did not provide any means for error control or flow control (except for the header’s error detection). Because IPv4 assumes the unreliability of the underlying layers it does it best-effort to get a transmission through to its destination, but with no guarantees. If reliability is important, IPv4 must be paired with a reliable protocol such as TCP. The best-effort delivery service could be explained clearly through the post office example. The post office does its best to deliver the mail but sometimes it fail to deliver a particular letter. If an unregistered letter is lost, it is up to the sender or would-be receipt to discover the loss and rectify the problem. The post office itself does not keep track of every letter and cannot notify a sender of loss or damage. IPv4 is also a connection less protocol for a packet-switching network that uses the datagram approach. This means that each datagram is handled independently and each datagram travel through a different route to the destination. This implies that datagram sent by the same source to the same destination could arrive out of order. Also, some could be lost or corrupted during transmission. Again, IPv4 relies on a higher-level protocol to take care of all these problems. Because IPv4 has some deficiencies, listed below, that makes it unsuitable for fast-growing internet:

- Address limitations
- Lack of resources reservation and minimum delay strategies
- No encryption or authentication is provided by IPv4

IPv6 also known as Internetworking Protocol next generation (IPng) was proposed to solve these deficiencies. IPv6 is an evolution of IPv4 and it was designed as an upgrade version of IPv4. In IPv6, the Internet protocol was extensively modified to handle the sudden growth of the Internet. The format and the length of the IP address were changed along with the packet format. Related protocols, such as Internet Control Message Protocol (ICMP), were also modified. Other protocols in the network layer, such as ARP, Reverse Address Resolution Protocol (RARP) and Internet Group Management Protocol (IGMP), were either deleted or included in the ICMPv6 protocol. Routing protocols, such as Routing Information Protocol (RIP) and Open Shortest Path First (OSPF), were also slightly modified to accommodate these changes.

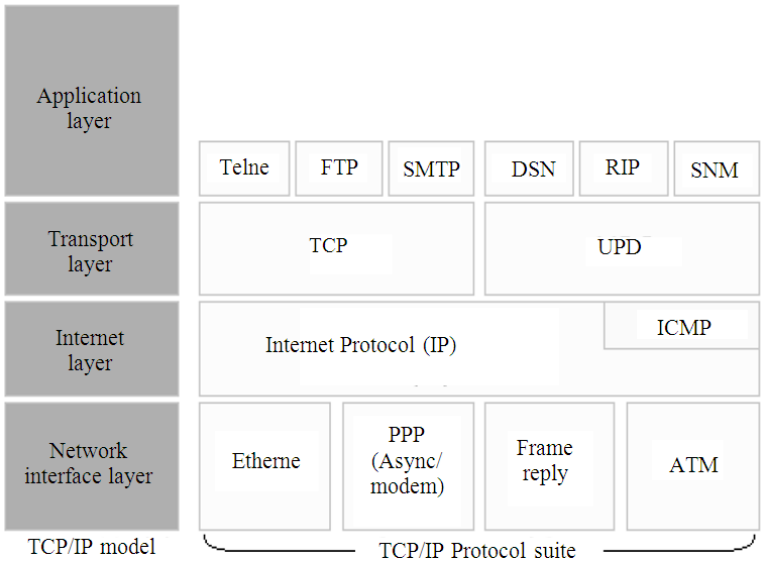

Fig. 1. Transfer control protocol/internet protocol.

Communications experts predicted that IPv6 along with its related protocols will soon replace the current IP version. The adaption of IPv6 has been slow. This is because the original motivation behind its development, limitation of IPv4 address, has been remedied by short-term strategies such as classless addressing and NAT. But sooner or later the fast-spreading use of the Internet and new services such as cloud computing (Tsai and Lin, 2011), mobile IP (Hassan and Hassan, 2011), IP telephony and IP-capable mobile telephony, will require the total replacement of IPv4 with IPv6. The next generation, or IPv6, has some advantages over IPv4 that can be summarized as follow:

- Better header format
- New options that allow additional functionalities
- Allowance for extension
- Support for resource allocation
- Support for more security

Still the main difference between IPv4 and IPv6 is in their addressing formats and inclusion of IPsec (Murugesan *et al*., 2009). IPv4 uses 32-bit (4-bytes) addresses to uniquely identify nodes within the global Inter-net. IPv6 uses 128-bit (16-bytes) addresses to uniquely identify nodes within the global Internet. With IPv6 large address space, it is clearly can resolve address depletion problem in IPv4 (Sailan *et al*., 2009), but still behave ap-proximately the same throughput as IPv4 (Ismail and Abidin, 2009).

2.3. IP Spoofing Defense Methods

Spoofing defense's solutions originally can be broken down into three categories (Ehrenkranz and Li, 2009).

2.3.1. End-Host-Based Solutions

These types of solutions are implemented on the end-hosts; the aim of these solutions is to allow the end-hosts to detect the spoofed packets. These kinds of solutions do not require any change in the network infrastructure and they are the easiest in deployment, but they are acting too late because the spoofed packets will arrived to the end-host before they are recognized.

2.3.2. Router-Based Solutions

These types of solutions are applied by routers, either at the core and edge of the Internet or at each side separately. These solutions in general face more difficulties to implemented, but they are the most effective because they stop spoofed packets from even reach end-hosts. Routers may apply some reactive mechanisms like tracing from where a malicious packet is arrived. However, routers may not be perfect for the scalable attacks (Saini *et al*., 2011).

2.3.3. Solutions Requiring the Use of Both Routers and End-Hosts

In order for these solutions to work routers and end-hosts must work together. A clear difference between host-based and router-based mechanisms refers to the end-to-end argument. Host based mechanisms obviously relate to end-to-end principles while router-based mechanisms

do not. This makes the deployment of host-based mechanisms to be much easier than router-base solutions. Host based solutions in general can be deployed even on a single host, without the need of any other host or router. **Table 1** overviews different spoofing defense mechanism.

2.4. IP Security

IPsec is mandated in the IPv6 protocol. Every implementation claiming support for IPv6 is expected to provide IPsec as part of the protocol (Radwan, 2005). IPsec is originally developed by the Internet Engineer Task Force, IETF, IPsec Working Group. IPsec was developed and design to provide several services such as access control, connectionless integrity, origin authentication, replay protection and confidentiality (Dhall *et al*., 2012). IPsec provide these services by dividing its protocol suite into two traffic security protocols, the Authentication Header (AH) and the Encapsulation Security Payload (ESP) (Shue *et al*., 2007). The AH protocol provides source authentication and data integrity but no confidentiality. The ESP protocol provides authentication, data integrity and confidentiality (Meenakshi and Raghavan, 2006). Both AH and ESP could be run in either transport mode or tunnel mode as we will explain later in this study (Kizza, 2005). In order for the IPsec to provide security it must first get as much information as possible on the security arrangement of the two communicating hosts. This information about how the security will look like between two communicating hosts is called Security Association (SA). An IPsec SA defines the following information as a part of the security association:

- Destination IP addresses
- The security protocol that will be used
- Secret keys
- Encapsulation mode
- Security Parameter Index (SPI)

IPsec keep the security association in a special data base called Security Association Database (SAD) and as sign an index for each of them, by using security association index (Black, 2000). IPsec operates in one of two different modes: The transport mode or the tunnel mode as shown in **Fig. 2**.

In the transport mode, IPsec protects what is delivered from the transport layer to the network layer. In other words, the transport mode protects the network layer pay-load, the payload to be encapsulated in the network layer. Note that the transport mode does not protect the IP header. In other words, the transport mode does not protect the whole IP packet; it protects only the packet from the transport layer (the IP layer payload). In this mode, the IPsec header and trailer are added to the information coming from the transport layer. The IP header is added later. IPsec in the transport mode does not protect the IP header; it only protects the information coming from the transport layer.

Table 1. Spoofing defense methods

Host-based solutions		Router-based solutions		
Active	Passive	basic	Distributed	Combination
Cryptographic: IPsec Probing: OS fingerprint, IP ID field probing, TCP probing Other: SYN cookies, IP puzzles		Martian address filtering, ingress/egress filtering, reverse path forwarding	Spoofing Prevention Method (SPM), Passport.	Path Identifier (Pi), StackPi

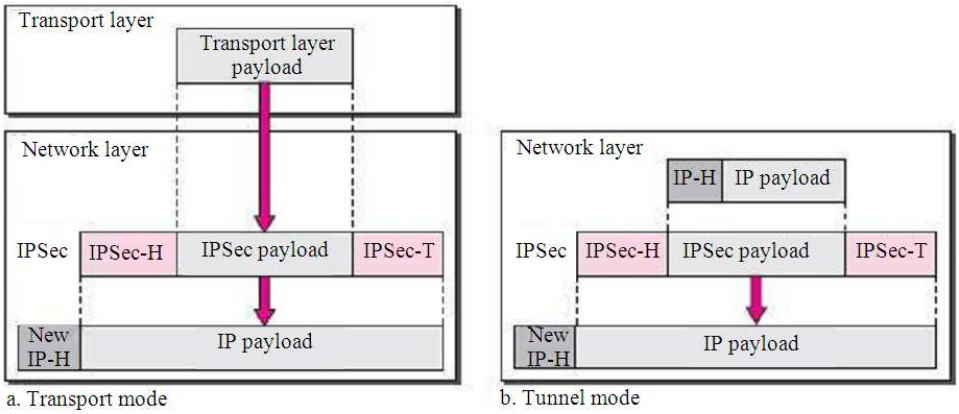

Fig. 2. IP security modes

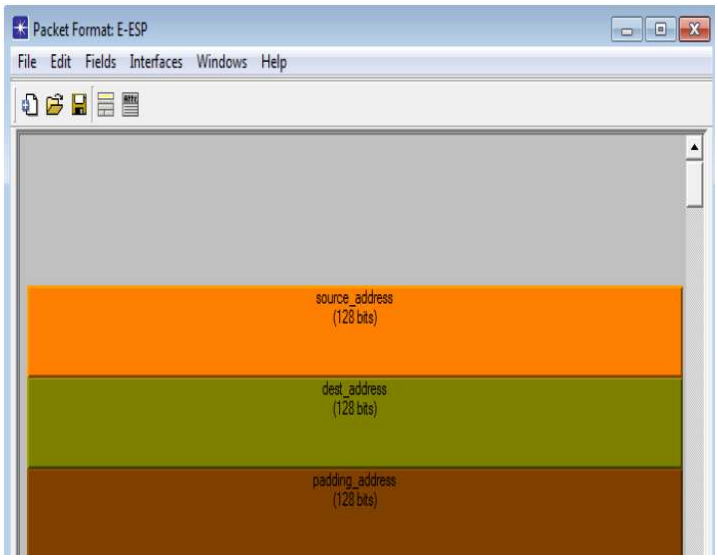

Fig. 3. E-ESP's Packet

The transport mode is normally used when we need host-to-host (end-to-end) protection of data. The sending host uses IPsec to authenticate and/or encrypt the payload delivered from the transport layer.

The receiving host uses IPsec to check the authentication and/or decrypt the IP packet and deliver it to the transport layer. In the tunnel mode, IPsec protects the entire IP packet. It takes an IP packet, including the header, applies IPsec security methods to the entire packet and then adds a new IP header. The new IP header has different information than the original IP header. The tunnel mode is normally used between two routers, between a host and a router, or between a router and a host. In other words, we use the tunnel mode when either the sender or the receiver is not a host. The entire original packet is protected from intrusion between the sender and the receiver. It's as if the whole packet goes through an imaginary tunnel. IPsec in tunnel mode protects the original IP header.

3. EXPERIMENTAL WORKS

Simulation is conducted based on two scenarios. The first scenario represents the first case implementation of our proposed defense mechanism, in which the IPv6 source address of the encapsulated packet is left intact. The second scenario represents the second case implementation of our proposed defense mechanism, in which we execute spoofing attack to change the IPv6 source address of the encapsulated packet. Both scenarios are run based on a customized packet which we call it Enhanced Encapsulated Security Payload (E-ESP) packet as in **Fig. 3**.

Set V1
Set V2
Set up the tunnel
Encapsulate IPv6 frame into IPv4 frame
Sending the encapsulating packet
Execute spoofing attack (V1 := V3)
IF V1=V2 Receive the packet
Else
Drop the packet

Fig. 4. E-ESP's Algorithm

3.1. Algorithm

For both scenarios we have two variables V1 and V2 which represents IPv6 source address of the encapsulated packet and IPv6 source address in padding area respectively. In addition we used a third variable called V3 to represent the spoofed IPv6 source address. **Figure 4** below shows the algorithm used to implement the proposed defense mechanism.

3.2. Process Flow Chart

Following is the process flow chart of the proposed defense mechanism as per **Fig. 5**.

3.3. Simulation Results

The results of the first scenario shown that packets which have IPv6 source address of the encapsulated packet match the IPv6 source address in padding area were successfully delivered as per **Fig 6**. On the other

hand, the results of the second scenario shown that packets which have mismatch between IPv6 source address of encapsulated packet and IPv6 source address in the padding area were dropped as per **Fig. 7**.

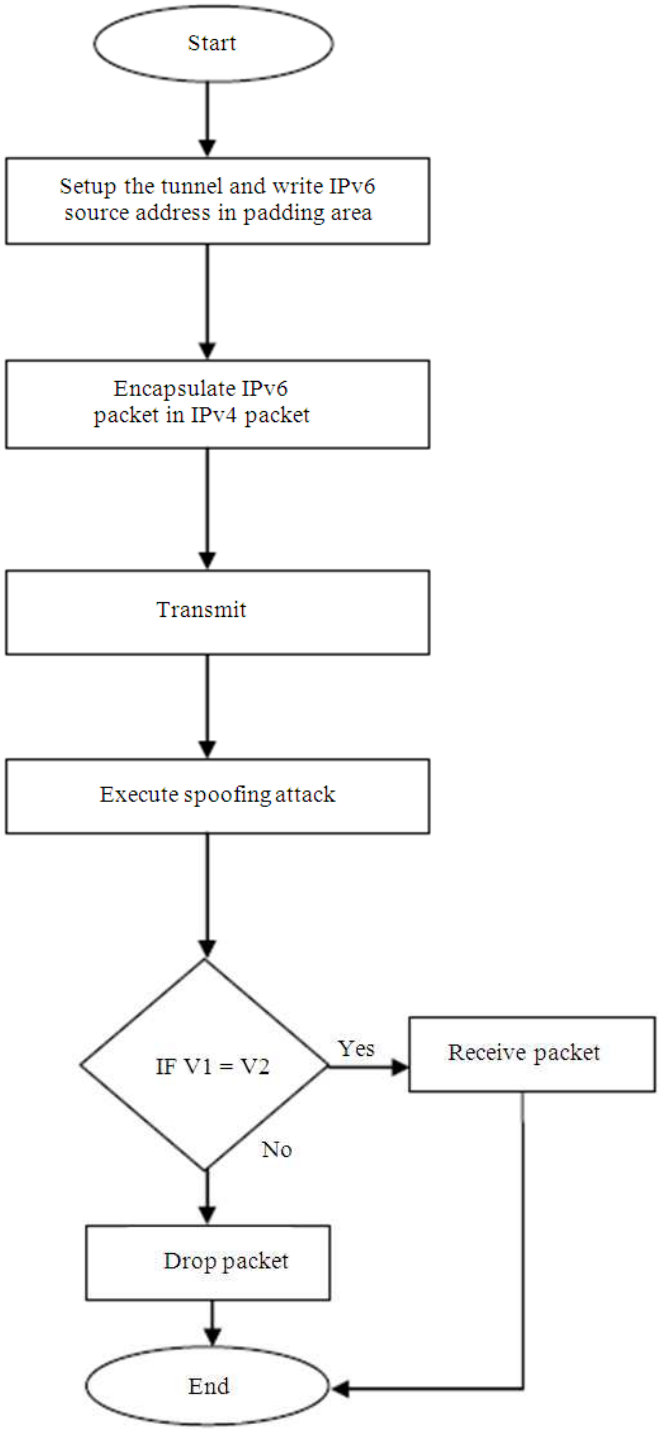

Fig. 5. Mechanism's process flow chart

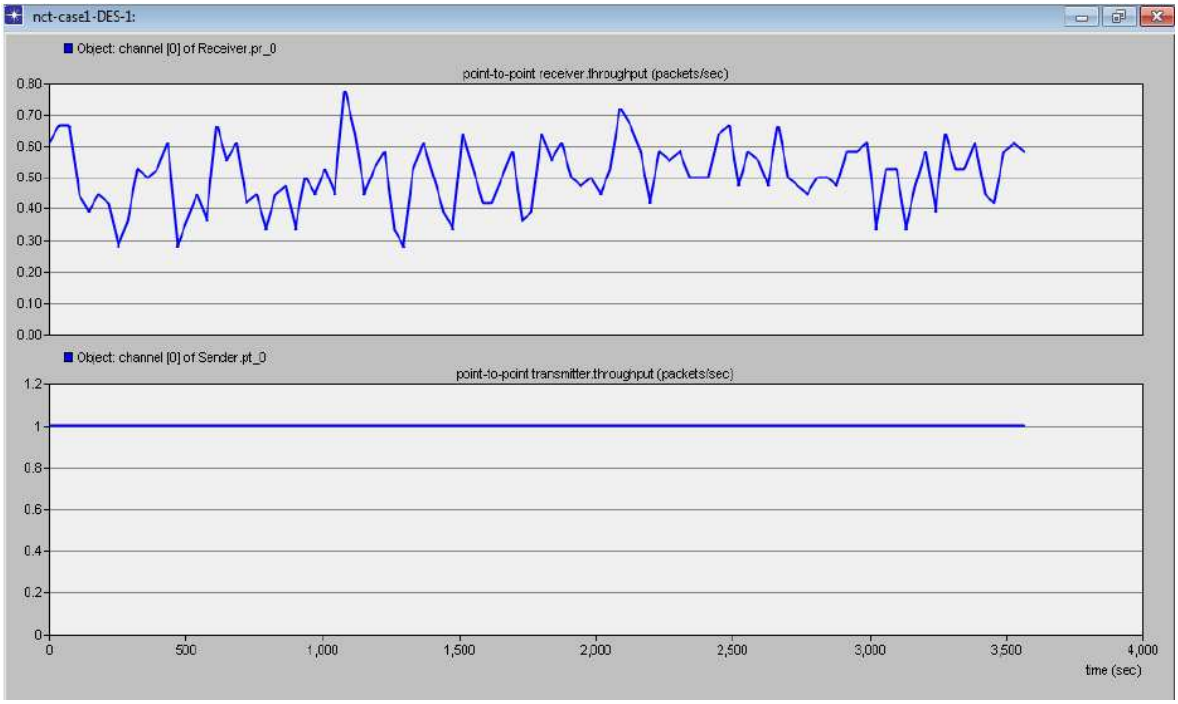

Fig. 6. First scenario's results

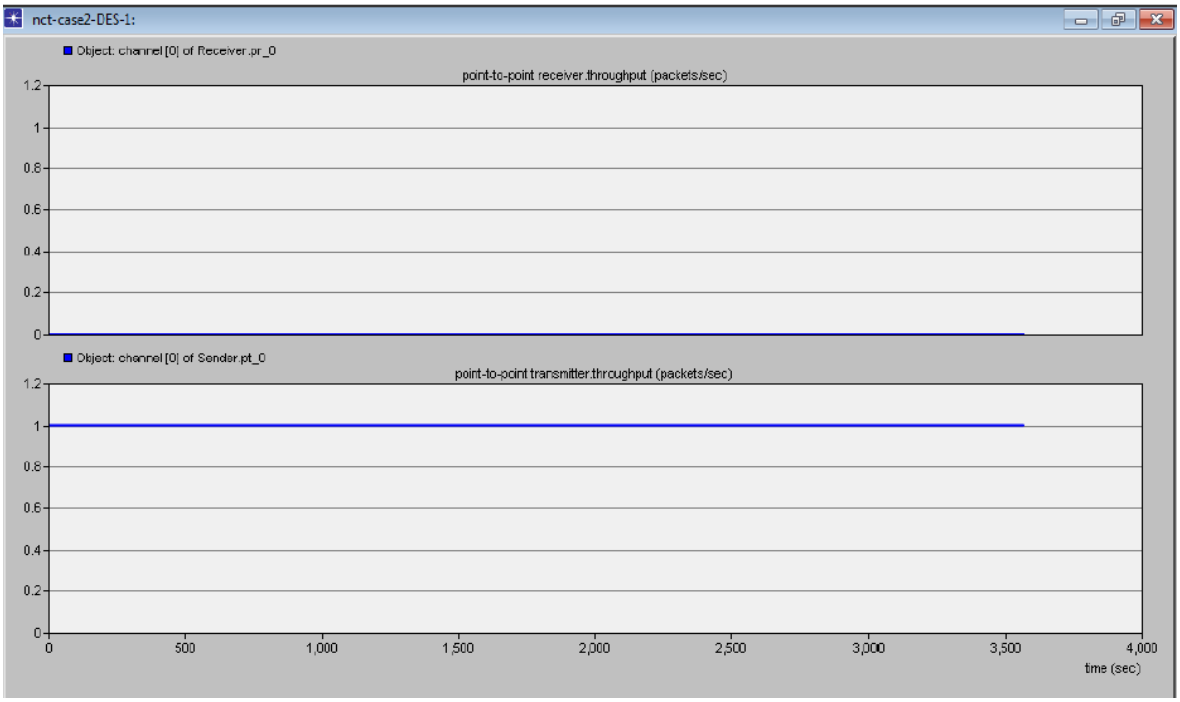

Fig. 7. Second scenario's results

4. DISCUSSION

IPsec suite could be run either in transport mode or tunnel mode to secure communication between two nodes. In case of transport mode IPsec protects the pay-load of the network layer, but did not protect the original IP header. As we mentioned earlier in this article, in order to send IPv6 packet (inner) through IPv4 region, we have to encapsulate it into IPv4 packet (outer). When using IPsec in transport mode to secure IPv6 over IPv4 tunnel IPsec carries IPv6 packet (which includes IPv6 source address) as plain data with no mean of protection. That is any two nodes share the tunnel can de-capsulate the pack-et easily and using IPv6 source address to execute spoofing attack. The mechanism proposed in this article is working based on runs IPsec's ESP and using an empty space in ESP frame (padding area) to write the IPv6 source address of the inner packet before encapsulate it into IPv4 packet to transmit it, ESP adds a header and trailer. Note that ESP's authentication data are added at the end of the packet which makes its calculation easier. **Figure 8** shows the location of ESP's header and trailer and **Fig. 9** shows the proposed area (padding).

When an IP datagram carries an ESP header and trailer, the value of the protocol field in the IP header is 50. A filed inside the ESP trailer holds the original value of the protocol field. The ESP working procedure follows these steps:

- An ESP trailer is added to the payload
- The payload and the trailer are encrypted
- The ESP header is added
- The ESP header, payload and ESP trailer are used to create the authentication data
- The authentication data is added to the end of the ESP trailer
- The IP header is added after the protocol value is changed to 50

Referring to the ESP's procedure steps and **Fig. 8**, the payload and the trailer are encrypted and by referring to the **Fig. 9** and see the location of the proposed area to write the IPv6 source address on it (padding area) we can sense the level of the security added to defend against IP spoofing in IPv6 over IPv4 tunnel. We have the IPv6 source address written in the ESP's trailer and the whole trailer is encrypted. The only one have the key to decrypt the ESP trailer is the node of the receiving end point of the tunnel. In the receiving end, the receiver will de-capsulate the IPv6 frame and before forward the packet will match the IPv6 source address in the encapsulated packet with the one written to the padding area in IPsec's ESP frame and only forward the packet if they matched. If the receiver detect a difference between IPv6 source address of the encapsulated packet with the one in ESP's padding area this will imply that an intruder spoof the IPv6 source address of the encapsulated packet and accordingly will drop the packet. Although the proposed mechanism has solved the problem still it has limitation in a circumstance of networks which have large number of mobile nodes. In such circumstance the padding area may be fully used for other network purposes. We involved a proposed solution for this limitation in the conclusion and future works section. **Figure 10** represents a logical diagram of how E-ESP works. The proposed defense mechanism shown a good performance and eliminate the spoofing threat in IPv6 over IPv4 tunnel.

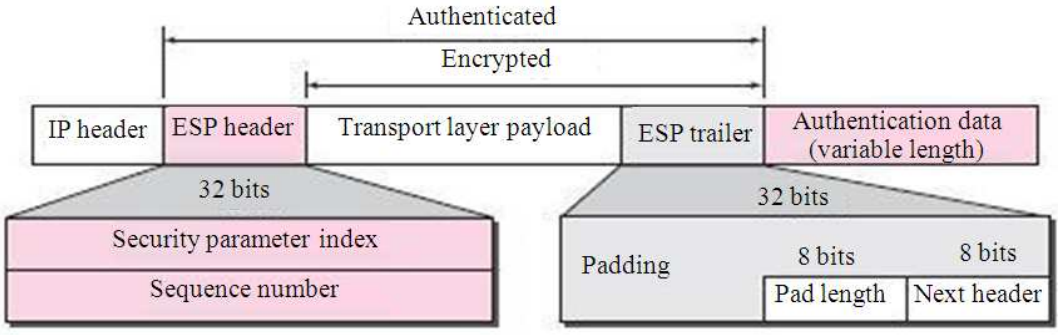

Fig. 8. Encapsulated Security Payload (ESP) protocol in transport mode

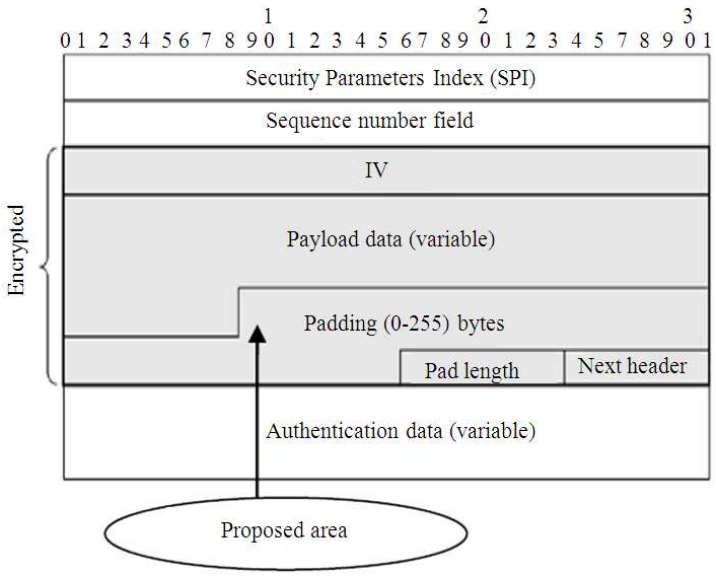

Fig. 9. Encapsulated security payload frame

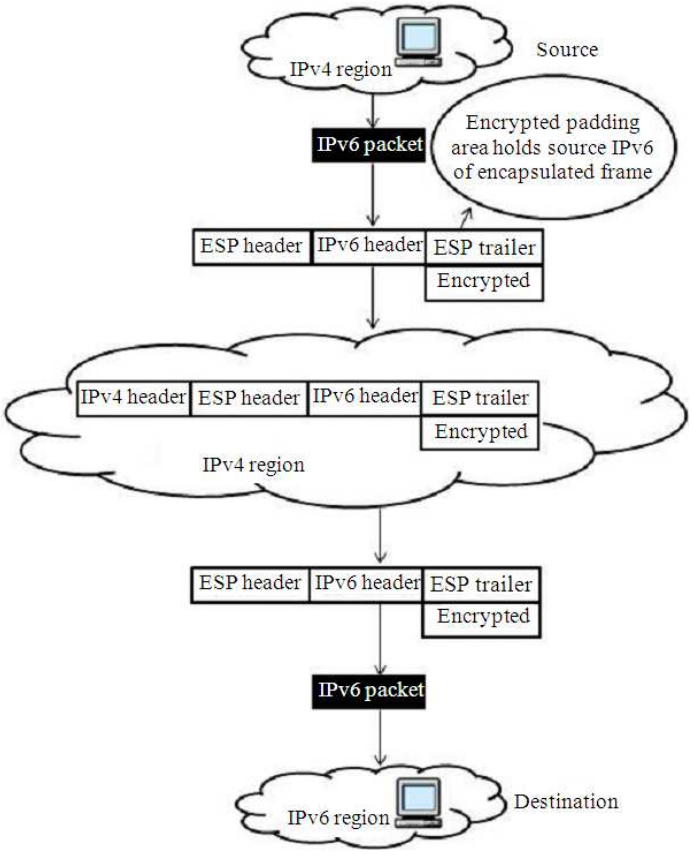

Fig. 10. Logical diagram of E-ESP

5. CONCLUSION

In this article we introduced a new spoofing defense mechanism to eliminate spoofing threat that happen when using IPsec in transport mode to secure IPv6 over IPv4 tunnel. The new mechanism work based on IPsec protocol ESP, it uses the padding area of ESP to write the IPv6 source address of the packet that will travel across IPv4 region. Simulation is done based on two scenarios. The outcome of the collected results shown that the proposed defense mechanism works with a good performance rate. Because the verification and authentication are done per packet the proposed defense mechanism can detect spoofed packets whatever the number of hops does it cross in the IPv4 region. We introduced the proposed mechanism in (Ahmed *et al*., 2012) as a theoretical concept. After which we go for algorithms formulation in (Hassan and Ahmed, 2013) and finally shift to the implementation and experimental works to evaluate the results. There are many potential directions for future research that can be done based on this article. As future works we should give a good concern about networks which have large number of mobile nodes, under such circumstance the padding area sometimes is almost fully utilized. A study about queuing mechanism to manage the padding area in case of fully used should be carried out. Also we should consider the possibility of adding new field in the original ESP frame to carry the IPv6 source address of the encapsulated packet instead of using the padding area. By restructuring the ESP frame padding area could be saved for other network usage purposes. A research about enhancing the encryption algorithm that used to encrypt ESP payload and trailer should be carried out for better security and faster process.

6. REFERENCES

Ahmed, A.S., R. Hassan and Z.M. Ali, 2012. Eliminate spoofing threat in IPv6 tunnel. Proceeding of the 8th International Conference of Information Science and Digital Contents Technology, Jun. 26-28, IEEE Xpolre Press, Jeju, pp: 218-222.

Bi, J., J. Wu, X. Leng, 2007. IPv4/IPv6 transition technologies and univer6 architecture. Int. J. Comput. Sci. Network Security, 7: 232-242.

Bidgoli, H., 2006. Handbook of Information Security, 1st Edn., Wiley, USA, Wiley, ISBN-10: 0471648337, pp: 3366.

Black, U.D., 2000. Internet Security Protocols: Protecting IP Traffic. 1st Edn., Prentice Hall PTR, USA, ISBN-10: 0130142492, pp: 304.

Bouras, C., A. Karaliotas and P. Ganos, 2003. The deployment of IPv6 in an IPv4 world and transition strategies. Internet Res., 13: 86-93. DOI: 10.1108/10662240310469033

Colitti, L., D.G. Battista and M. Patrignani, 2004. IPv6-in-IPv4 tunnel discovery: Methods and experimental results. IEEE Trans. Network Service Manage., 1: 30-38. DOI: 10.1109/TNSM.2004.4623692

Dhall, H., D. Dhall, S. Batra and P. Rani, 2012. Implementation of IPSec protocol. Proceedings of the 2nd International Conference on Advanced Computing and Communication Technologies, Jan. 7-8, IEEE Xpolre Press, Rohtak, Haryana, pp: 176-181. DOI: 10.1109/ACCT.2012.64

Ehrenkranz, T. and J. Li, 2009. On the state of IP spoofing defense. ACM Trans. Internet Technol., University of Oregon. DOI: 10.1145/1516539.1516541

Hassan, R. and A.S. Ahmed, 2013. Avoiding spoofing threat in IPv6 tunnel by enhancing IPSec. Int. J. Adv. Comput. Technol., 5: 1241-1250. DOI: 10.4156/ijact.vol5.issue5.148

Hassan, S.S. and R. Hassan, 2011. IPv6 network mobility route optimization survey. Am. J. Applied Sci., 8: 579. DOI: 10.3844/ajassp.2011.579.583

Ismail, M.N. and Z.Z. Abidin, 2009. Implementing of IPv6 protocol environment at university of kuala lumpur: Measurement of IPv6 and IPv4 performance. Proceedings of the International Conference on Future Computer and Communication, Apr. 3-5, IEEE Xplore Press, Kuala Lumpar, pp: 443-449. DOI: 10.1109/ICFCC.2009.145

Kamal, S. and B. Issac, 2007. Analysis of network communication attacks. Proceeding of the 5th Student Conference on Research and Development, Dec. 12-11, IEEE Xplore Press, Selangor, Malaysia, pp: 1-6. DOI: 10.1109/SCORED.2007.4451370

Kizza, J.M., 2005. Computer Network Security. USA, Springer.

Meenakshi, S.P. and S.V. Raghavan, 2006. Impact of IPSec overhead on web application servers. Proceedings of the International Conference on Advanced Computing and Communications, Dec. 20-23, IEEE Xplore Press, Surathkal, pp: 652-657. DOI: 10.1109/ADCOM.2006.4289981

Murugesan, R.K., S. Ramadass and R. Budiarto, 2009. Improving the performance of IPv6 packet transmission over LAN. Industrial Electron. Applic., 1: 182-187. DOI: 10.1109/ISIEA.2009.5356462

Radwan, A.M., 2005. Using IPSec in IPv6 Security. Proceedings of the 4th International Multi Conference on Computer Science and Information Technology, (SIT' 05), pp: 471-474.

Raicu, I. and S. Zeadally, 2003. Evaluating IPv4 to IPv6 transition mechanisms. Proceedings of the IEEE 10th International Conference on Telecommunications, Feb. 23-Mar. 1, IEEE Xplore Press, pp: 1091-1098. DOI: 10.1109/ICTEL.2003.1191589

Sabnis, P. and M. Tech, 2013. To filter malicious ipv6 packet encapsulated in ipv4 using outbound filtering. Department of Computer Engineering.

Sailan, M.K., R. Hassan and A. Patel, 2009. A comparative review of IPv4 and IPv6 for research test bed. Proceedings of the International Conference on Electrical Engineering and Informatics, Aug. 5-7, IEEE Xplore Press, Selangor, pp: 427-433. DOI: 10.1109/ICEEI.2009.5254698

Saini, D.K., S.A. Maskari and H. Saini, 2011. Malicious objects trafficking in the network. Proceedings of the 7th International Conference on Digital Content Multimedia Technology and its Application, Aug. 16-18, IEEE Xplore Press, Busan, pp: 4-69.

Sharma, V., 2010. IPv6 and IPv4 security challenge analysis and best-practice scenario. Int. J. Adv. Network. Applic. 1: 258-269.

Shue, C.A., M. Gupta and S.A. Myers, 2007. Ipsec: Performance analysis and enhancements. Proceedings of the IEEE International Conference on Communications, Jun. 24-28, IEEE Xplore Press, Selangor, Glasgow, pp: 1527-1532. DOI: 10.1109/ICC.2007.256

Taib, A.M. and R. Budiarto, 2010. Securing tunnel endpoints for IPv6 transition in enterprise networks. Proceedings of the International Conference on Science and Social Research, Dec. 5-7, IEEE Xplore Press, Kuala Lumpur, Malaysia, pp: 1114-1119. DOI: 10.1109/CSSR.2010.5773699

Tsai, C.L. and U.C. Lin, 2011. Information security of cloud computing for enterprises. Adv. Inform. Sci. Service Sci., 3: 132142.

Wang, J., 2009. Computer Network Security: Theory and Practice. 1st Edn., Springer, Berlin, ISBN-10: 3540796975, pp: 400.