ISSN (e): 2250 – 3005 || Volume, 06 || Issue, 02 ||February – 2016 ||
International Journal of Computational Engineering Research (IJCER)

A Comparative Analysis of Additional Overhead Imposed by Internet Protocol Security (IPsec) on IPv4 and IPv6 Enabled Communication

[1]Muhammed NuraYusuf, [2]Badamasi Imam Ya'u
[1,2]*Faculty of Science AbubakarTafawa Balewa University, P.M.B 0248 TafawaBalewa Way, Bauchi State, Nigeria.*

Abstract
IPSec, an Internet layer three (3)-security protocol suite is often characterising with introducing an additional space and processing overhead when implemented on a network for secured communication using either internet protocol version 4 or 6; IPv4 or IPv6. The use of Internet protocol security (IPSec) on IPv4 is an alternative that offers solutions and addresses the security vulnerabilities in network layer of the open system interconnect (OSI) and transmission control protocol/internet protocol (TCP/IP) protocol stack. In IPv6, IPSec is one among many other features added to the earlier Internet protocol to enhance efficiency and security. This paper, set as its objective to reports on the impact of processing and space overhead introduced by IPSec on both IPv4 and IPv6 in relation to packet end-to-end delay based on different IPSec transformations with different authentication and encryption algorithms deployed in different scenarios simulated using NS2. The experiment result reveals that the cost of IPSec added overhead is relatively small when smaller packet sizes are involved for both protocols in comparison with large packet sizes that were IPSec protected with the same configuration as the smaller packet, unless in the cases whereby the packet was very large which has to be fragmented. This paper can therefore, serve as a guide for network administrators to trade up between processing cost and larger address space specifically for transmission involving larger IP packets.
Keywords: *end-to-end delay, Internet Protocols,IP Security, Overhead, Packets, Processing, Space,*

I. Introduction

It is a well-known fact that internet protocol version 4 (IPv4) the most widely adopted internet protocol as of today for packet transmission is vulnerable to a number of attacks at the network layer of the open system interconnect (OSI) and transmission control protocol/internet protocol (TCP/IP) protocol stack[1]. The optional provision of Internet Protocol Security (IPSec)protocol on IPv4 deployment in technologies such as virtual private network (VPN) has been in the rescue for the vulnerable operation of plain IPv4, the technology provides immunity and protection against network layer attacks by ensuring secured end-to-end transmission channel. In the other hand, IPv6 is yet another Internet protocol that is set to replace the use of IPv4completely in the near future in the computer networking industry [2]. It has been around the corner for many years now, in fact it services is already being exploited in some parts of the world. IPv6 can simply be seen as an upgrade version of IPv4 [2]; it introduces so many features to address the defect of the existing IPv4. Among the new features introduced is the compulsory implementation of IPSec protocol. This implies that by default IPv6 is protected against any possible network layer attack.

Both Internet protocol version (IPv4) with Internet protocol security (IPSec) enabled and (IPv6) introduced additional overheads to the actual IP datagram, which may be significant to performance parameters such as end-2-end delay, throughput, round trip time etc. Hence, the need for a study/analysis to investigate the overheads introduced by the protocols for their proper deployment and suitable selection of configuration options among them, considering scarce resources such as bandwidth and processing speed etc.

The general objectives of the study was to provide a practical working, network administration guidance for making a right selection of configurations under a pre-defined and strict networking condition, IPSec protocols suite had to offer to suit a particular network environment while bearing in mind the cost/penalty of overheads involvement on performance. While the basic objectives of this study include were to investigate the impact of IPSec overheads on Ipv6 network compared to Ipv4 network, to evaluate the processing and space overheads

imposed by different cryptographic algorithms on IPv4 and IPv6 networks currently supported by IPSec. This is because, [4] put forward that over time, the future of Internet communication is certain to be occupied by IPv6. This is in spite of the fact that IPv4 is still in use for Internet communication, a scenario that could probably be so for many more years ahead, the reasons for that is obtained from the post made by Nicolas Boillot 1st Jun 2006 on IEEE Spectrum website "But migration to the Internet IPv6 is proving to be painfully slow. Originally, that was because it took a long time for computer scientists and engineers to hammer out the details. During that initial delay, a stopgap, called Network Address Translation (NAT), did such a good job of relieving the need for more IP addresses that it has become a permanent part of the IPv4 landscape. And it lets the administrators of the world's biggest networks continue to put off the dreary task of changing over to IPv6." So will the Internet and your home or work computer ever move to IPv6? Certainly that's the future. Most of the Internet routers that your data travels through can now accommodate IPv6. For some years, leading manufacturers such as Alcatel, Avici, Cisco, Juniper, Lucent, and Nortel have been adding the necessary software to their wares. All the leading operating systems—such as Windows, Mac OS X, and Linux—support IPv6, and the U.S. Department of Defence has mandated IPv6 for its own networks by 2008.Yet a June 2005 survey by Juniper Networks, Sunnyvale, Calif., found that "few organizations are in the process of migrating from the current standard of IPv4 to the improved IPv6." For one thing, IPv6 is not backward compatible with IPv4. This means companies will have to support two protocols simultaneously.

IPv4 and IPv6 may have to coexist for some time. IPv4 can finally be jettisoned only when all carriers, ISPs, routers, switches, firewalls, and servers accommodate packets that use IPv6. Asia will probably lead the way. Demand for IPv6 is highest there, says Tony Downes, principal technologist at Data Connection Ltd., a London-based maker of networking and communications products. Another option is running the both protocols as dual stack, but running that depends on your network. But in most cases for an infrastructure network providing IP transit, it's fairly easy. For a lot of content providers it won't be too complicated, but there are some things that they're going to need to keep in mind, depending on the way their particular site is implemented. Where it's going to be hardest is going to be the enterprise networks, because they've become so ingrained with the technology known as network address translation and, you know, certain ways of doing things that just don't scale to an IPv6 world[5]. An ISP "Hurricane Electric is fully deployed in dual stack and completely ready to serve everybody's"

II. Materials and Method (The Experiment Design Approach).

Network Simulator 2 (NS2) a discrete event computer network simulator was used to design and simulate the experiment. The experiment was performed on a network consisting of clients, a gateway and a server as illustrated on the physical topology in figure 1. Clients' access severs through a gateway via a duplex link channel set up at 2mbs and 10ms. The queue limit size is setup at 10;transmission control protocol (TCP) agents are attached to the clients' nodes with the following parameters:

fid_ 1, window size-_ 50, maxburst _ 50,maxcwnd_ 50, while tcpbase_hdr_size was set at 64, and aggressive maxburst was kept at 50. For the tcp packet size, it was set according to the IPSec configuration setting being used.

Different sizes of the protected packet were calculated. File transfer protocol (FTP) traffic was attached to the transmission control protocol (TCP)agent while a TCP sink is attached to receivers and connects to the traffic agents as shown in figure 1.

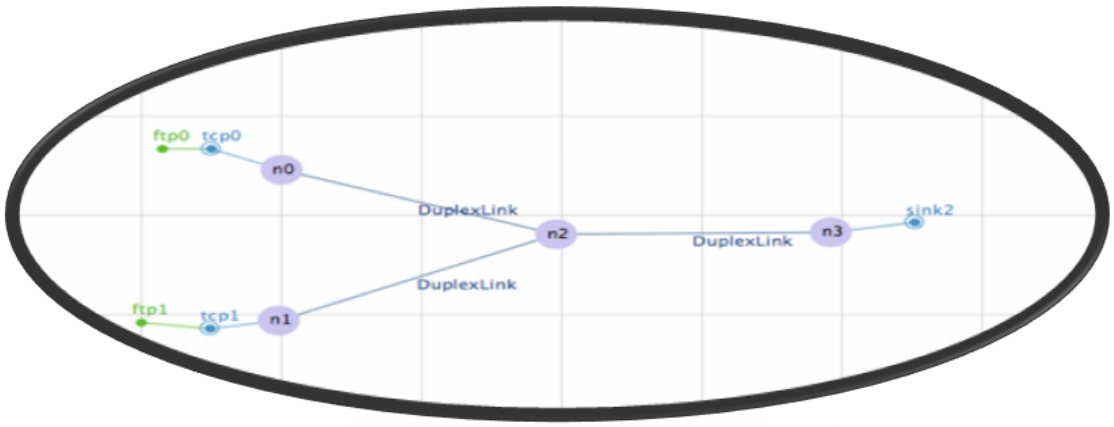

Figure (1)The Experiment Network Design Diagram

III. The Simulation Experiments Scenarios.

The simulation experiments were conducted using NS2 by employing different scenarios. The scenarios involved the two different IPSec modes (tunnel mode and transport mode of operations). Authentication and encryption algorithm are deployed in a different scenario as outline below. The investigation is carried out on end-to-end delay performance parameter; by examining FTP traffic in different IPSecenabled network scenarios of IPv4 and IPv6. The scenarios include:

Test Case 1: IPv4 only, under the following scenarios.

a. Plain IPv4 Packet with no IPSec: in this scenario the packet is encapsulated plainly and transmitted with out any IP security with IPv4 protocol
b. IPv4 with Authentication Header (AH): Here the send packet is transmitted using IPv4 transmission protocol and encapsulated in IPSec header enforcing and ensuring authentication only.
c. IPv4 with Encapsulation Security Payload (ESP): while in this scenario the send packet is transmitted using IPv4 transmission protocol and encapsulated in IPSec header enforcing and ensuring confidentiality of the datagram only.
d. IPv4 with both AH & ESP: while in this scenario the send packet is transmitted using IPv4 transmission protocol and encapsulated in IPSec header enforcing and ensuring both authentication and confidentiality of the datagram.

Test case 2: IPv6 only, under the following scenarios.

a. Plain Unmodified IPv6: Plain IPv6, in this scenario the packet is encapsulated plainly and transmitted with out any modified IP security with IPv6 protocol
b. IPv6 with AH *(e.g.MD5, SHA-1):* Here the send packet is transmitted using IPv6 transmission protocol and encapsulated in IPSec header enforcing and ensuring authentication only.
c. IPv6 with ESP: while in this scenario the send packet is transmitted using IPv6 transmission protocol and encapsulated in IPSec header enforcing and ensuring confidentiality of the datagram only.
d. IPv6 with Both AH and ESP: while in this scenario the send packet is transmitted using IPv6 transmission protocol and encapsulated in IPSec header enforcing and ensuring both authentication and confidentiality of the datagram.

Test case 3: IPv4 vs. IPv6 under the following scenarios (For Authentication Check).

a. Plain IPv4 with no IPSec: in this scenario the packet is encapsulated plainly and transmitted with out any IP security with IPv4 protocol
b. Unmodified IPv6: Plain IPv6, in this scenario the packet is encapsulated plainly and transmitted with out any modified IP security with IPv6 protocol
c. IPv4 with AH: Here the send packet is transmitted using IPv4 transmission protocol and encapsulated in IPSec header enforcing and ensuring authentication only.
d. IPv6 with AH: Here the send packet is transmitted using IPv6 transmission protocol and encapsulated in IPSec header enforcing and ensuring authentication only.

Test case 4: IPv4 vs. IPv6 under the following scenarios (for confidentiality Check).

a. Plain IPv4: in this scenario the packet is encapsulated plainly and transmitted with out any IP security with IPv4 protocol
b. Unmodified IPv6: Plain IPv6, in this scenario the packet is encapsulated plainly and transmitted with out any modified IP security with IPv6 protocol
c. IPv4 with ESP: while in this scenario the send packet is transmitted using IPv4 transmission protocol and encapsulated in IPSec header enforcing and ensuring confidentiality of the datagram only.
d. IPv6 with ESP: while in this scenario the send packet is transmitted using IPv6 transmission protocol and encapsulated in IPSec header enforcing and ensuring confidentiality of the datagram only.

Test case 5: IPv4 vs. IPv6 under the following scenarios (For Combine Authentication And Confidentiality Check)

a. Plain IPv4 Packet with no IPSec:in this scenario the packet is encapsulated plainly and transmitted with out any IP security with IPv4 protocol

b. Unmodified IPv6: Plain IPv6, in this scenario the packet is encapsulated plainly and transmitted with out any modified IP security with IPv6 protocol

c. IPv4 with AH plus ESP *(3DES + MD5, AES + MD5):* in this scenario the send packet is transmitted using IPv4 transmission protocol and encapsulated in IPSec header enforcing both authentication and ensuring confidentiality of the datagram.

d. IPv6 with AH plus ESP *(3DES + MD5, AES + MD5)* while in this scenario the send packet is transmitted using IPv6 transmission protocol and encapsulated in IPSec header enforcing both authentication and ensuring confidentiality of the datagram.

IV. Results and Discussion.

To accomplish the objectives setup by the paper as outlined. Different experiment scenarios involving distinct combination of IPSec mode of operation, authentication and encryption algorithms as shown were configured, Regardless of the fact that IPSec ensures effective and efficient information protection of network connectivity between two endpoints, yet there exists is a worrisome cost of overheads associated with it in terms of latency, router processing and memory, in addition to processing support for other networking functions [6]. However, the scenarios were deployed to investigate their discrepancies and similarities with respect to Internet protocol versions 4 and 6. Similarly, the performance metric investigated is: end-to-end delay.

AWK scripting language, an interpreted programming language was used to extract, process and manipulate the NS2 trace file output, it was used to measure and calculates the end-to-end delay experienced during the transmission of the FTP traffic of different file sizes under the different IPSecconfiguration deployed. The file sizes used are 1byte, 10bytes 100bytes, 1024bytes 10240bytes, 102400bytes, 1048576bytes, 1024460bytes, and 104857600bytes plus the IPSec header of the IPSec transform employed. The data is then exported, and analysedto illustrate the behaviour of the IP protocols with respect to different IPSec transform.

Earlier studies have shown that the overheads introduced by IPSec on networks vary with respect to the adopted IPSec security scenario; the algorithms used for its deployments, the transmitting medium and the file size. For instance, algorithms like HMAC-SHA1 introduced an additional 9% increase in packet transfer time than HMAC-MD5. Hence network load involved due to AH authentication and ESP encryption on small files had a greater ratio of increase when relate to authentication and encryption by ESP alone. This indicates that the choice of ESP for authentication purpose ahead of traditional AH when both encryption and authentication are needed for small files is better; especially when the number of encryption and authentication occurrences is significant and the bandwidth is limited. Moreover, wireless transmission medium significantly suffer more from IPSec overheads with respect to transfer time. This is because more time is needed to affect the transfer compared to the wired medium [7]

[1]in similar study indicated that IPSec overheads affects overall performance with respect to packet transfer time and increase in the network load, they also stated that these overheads are relative to different protocol, file size, algorithm, network traffic and services employed on the network. The research gap here is that the study has not go further to carry out specific investigation on how different file sizes/user datagram secured using different authentication (AH) and encapsulation Security pay load (ESP) algorithm transmitted using different either of the following protocols; (IPv4 or IPv6) can affect end to end delay; although [8] investigated the effects of some these parameters but with respect to bandwidth and processing time, ignoring the end-to-end delay which our study considered. Other performance matrix such as throughput were earlier confirmed to suffer depreciation due encryption and decryption process of datagram for authentication and confidentiality check of packets, because both the ciphering and IPSec encapsulation enlarges the eventual packet that will be transmitted thus building up space overheads. [9]

The result presented in Figure (2) shows the end-to-end delay experience while using IPv6, it could be noticed that based on the result displayed on the graph there was insignificant/small difference in the average end-to-end delay between, when AH only is used or when ESP only is used or when both AH plus ESP put together or when no IPSec was used at all. This happened when the packet size was between 1byte to 102400byte. Noticeable/significant difference in the end-to-end delay among the different IPSec configuration employed with respect to the Internet protocol in play began to emerge and show clearly when the file size was large. The packet transmission experience higher delay, when AH & ESP put together; followed by a situation when ESP header was used.

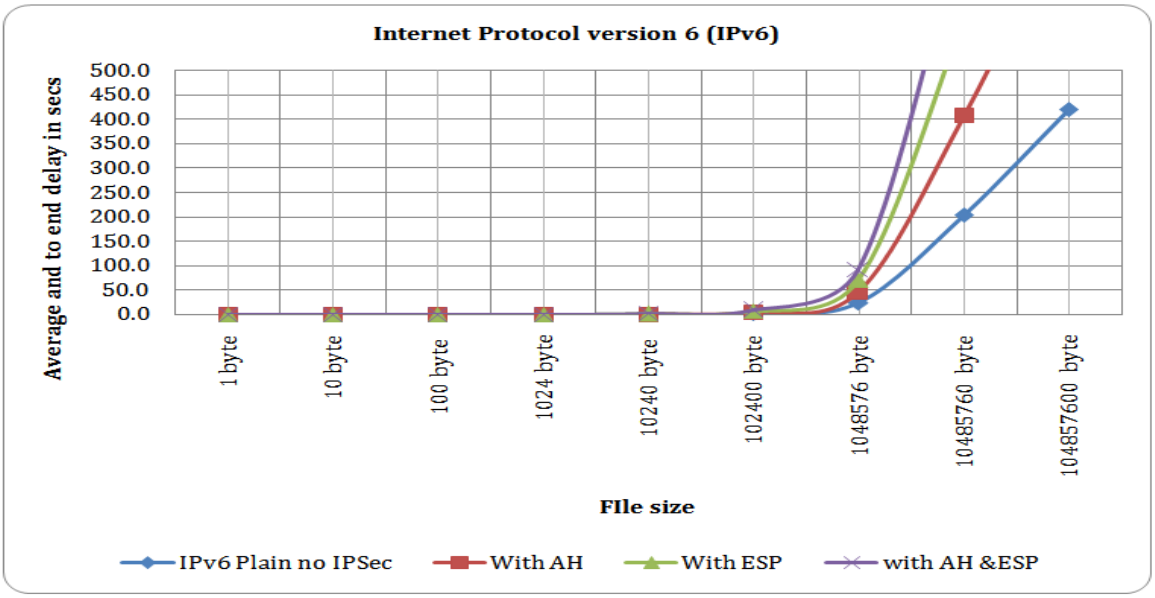

Figure (2) Test case 2 Result (IPv6 Only)

The same trend in the average delay is noticed when IPv4 was used as Figure (3) indicated. The results from figure (3) and figure (2) suggested that both IPv4 and IPv6 behave alike with regard to addition of IPSec header on the packet. They both experience low end–to-end delay when the file size was small, small between 1byte and 102400byte and the delay was significant/small when the packet size increased to 102400byte upward. In both cases the end-to-end delay was higher when AH plus ESP was used to provide the IP security. Similarly, AH when used alone bring on lower delay compared to when ESP is used alone.

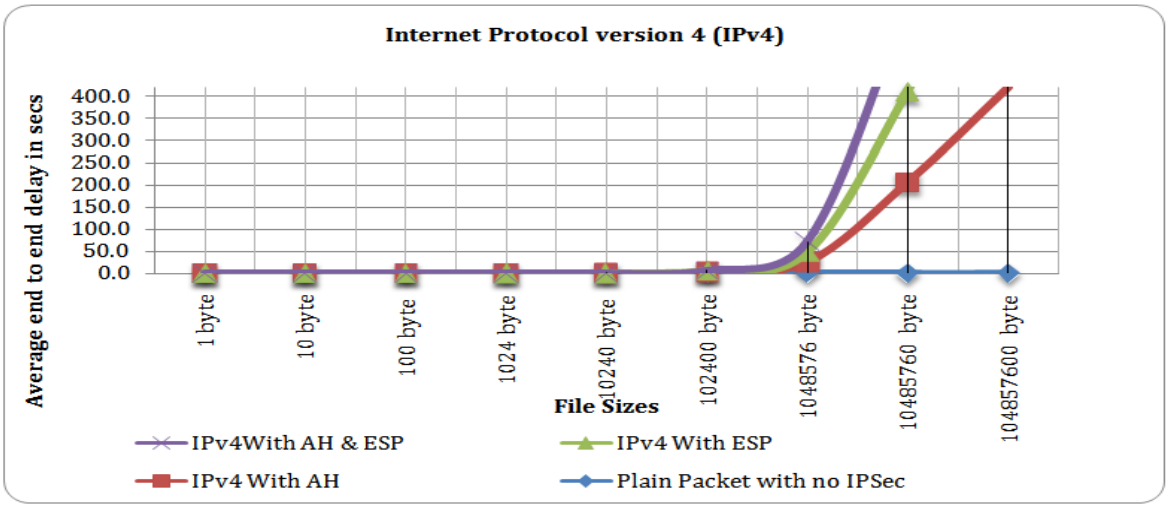

Figure (3): Test case 1 Result (IPv4)

However, the result displayed in Figure (4) compares the difference in the average end-to-end delay between IPv4 and IPv6 when AH header was added to the packet. The result indicated that IPv6 with AH caused higher end-to-end delay than IPv4. Figure (5) and Figure (6) show the difference in the situation when ESP and when AH plus ESP were used respectively. In both cases IPv6 end-to-end delay was higher than the end-to-end delay incurred with IPv4. This of course, could be attributed to the space and processing overhead cost as a result of authentication and encryption of packet during transmission was higher in IPv6 than in IPv4 in all cases, even though, IPSec header added the same number of bytes on both IPv4 and IPv6. The reason in this case was that the packet is very large that it has to be fragmented, as such IPv6 experienced higher overhead than IPv4. This happened due to the fact that the manner at which IPv6 handles fragmented packet when IPSec is involved was completely different with the way IPv4 tackles it. IPv6 applied IPSec header to all fragmented portion of the packet while IPv4 applied it to the very initial fragment only.

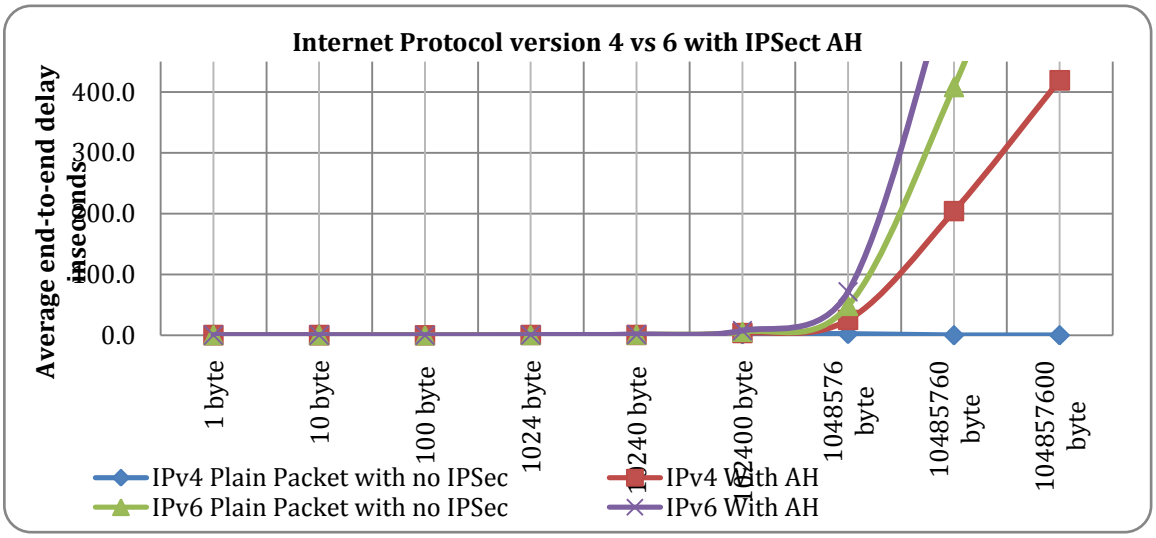

Figure (4) Test Case 3 Result (IPv4 vs. IPv6 with AH only)

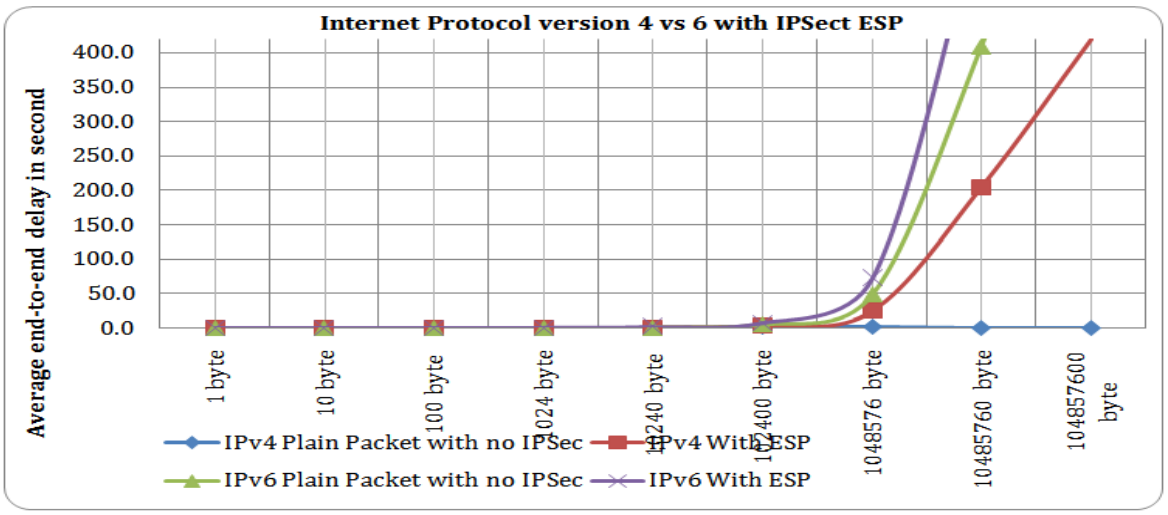

Figure (5) Test case 4 Result (IPv4 vs. IPv6 with ESP only)

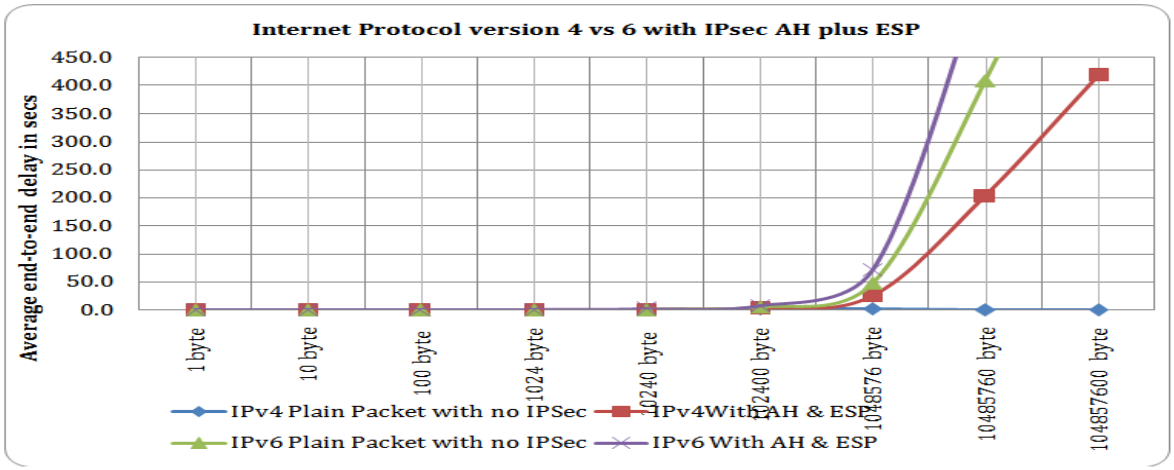

Figure (6) Test Case 5Result (IPv4 vs. IPv6 with AH plus ESP)

V. Conclusion

This paper as initially stated and set as its objective to reports on the impact of processing and space overhead introduced by internet protocol security (IPSec) on both internet protocol version 4 and 6, (IPv4 and IPv6) in relation to packet end-to-end delay based on different IPSec transformations under different authentication and encryption algorithms deployed in different scenarios simulated using NS2, had demonstrated how the said IPSec headers under different protocol configurations setup introduced the additional processing and space overhead with respect to different file size on the two different Internet protocols I.e. version 4 and 6; (IPv4 and IPv6). The idea is to investigate the impact of IPSec overheads on Ipv6 network compared to Ipv4 network, to evaluate the processing and space overheads imposed by different cryptographic algorithms on IPv4 and IPv6 networks currently supported by IPSec.

The study indicated that the cost of IPSec added overhead was smaller when smaller packet sizes were involved for both protocols compare to larger packet sizes that are IPSec protected with the same configuration as the smaller packet. The only exception wasin the cases whereby the packet is very large that it has to be fragmented. In such case IPv6 experienced higher overhead than IPv4. This happened due to the fact that the manner at which IPv6 handles fragmented packet when IPSec is involved was completely different with the way IPv4 tackles it. IPv6 applied IPSec header to all fragmented portion of the packet while IPv4 applied it to the very initial fragment only.Therefore,the general objectives of the study was to provide a practical working, network administration guidance for making a right selection of configurations under a pre-defined and strict networking condition, IPSec protocols suite had to offer to suit a particular network environment while bearing in mind the cost/penalty of overheads involvement on performance.

References

[1] A.A. Muhammad, M. Zaka-Ul, T. Usman, S.M. Ahsan, A.N. Muhammad, R. Imran, and A. Muhammad. Overhead Analysis of Security Implementation Using IPSec. (PP 1-7)(2009)

[2] K.S.Mohd, H. Rosilah, and P. Ahmed P. A Comparative Review of IPv4 and IPv6 for Research Test Bed. 2009 International Conference on Electrical Engineering and Informatics 5-7 Selangor, Malaysia, Institute of Electrical Electronics Engineers (IEEE Xplore Digital Library), pp. 1-7, August 2009.

[3] L. Lambros.andK. Peter. Integrating Voice over IP services in IPv4 and IPv6 networks. Proceedings of the International Multi-Conference on Computing in the Global Information Technology (ICCGI'07) Institute of Electrical Electronics Engineers (IEEE Xplore Digital Library), pp.1-6, 2007

[4] R. Radhakrishnan.,M. Jamil., S. Mehfuz., and Moinuddin; Security issues in IPv6, Third International Conference on Networking and Services (ICNS), 2007, pp.110, 19-25, 2007,

[5] E. Gregory. Iterative Block Ciphers' Effects on Quality of Experience for VoIPUnicast Transmissions under Different Coding Schemes. A thesis submitted to the University of Bedfordshire in partial fulfillment of the requirements for the degree of Doctor of Philosophy November 2010.

[6] S. Iftikhar.andP. Atul. Cost Overhead Analysis Associated with IPSec in the Next Generation Satellite Network.IEEEAC paper #1647, Version 2, Updated December 16, 2007 Institute of Electrical Electronics Engineers (IEEE Xplore Digital Library), pp. 1-6, 2007.

[7] C.H. George.,J. Nathaniel., I.V. Davis, F. Scott. andF. Midkif. IPSec Overhead in Wireline and Wireless Networks for Web and Email Applications, IEEE Institute of Electrical Electronics Engineers (IEEE Xplore Digital Library), pp. 1-5, 2003.

[8] S.P.Meenakshi and S.V. Raghavan. Impact of IPSec Overhead on Web Application Servers, Institute of Electrical Electronics Engineers (IEEE Xplore Digital Library), pp 1-6, 2006.

[9] X. Christos.,L. Nikolaos., M. Lazaros, and S. Ioannis. A generic characteristic of the overheads imposed by IPSec and associated cryptographic algorithms, ScienceDirect computer networks 50(2006):3225-3241, 2006.