Impact of IPSec on Real Time Applications in IPv6 and 6to4 Tunneled Migration Network

Junaid Latief Shah
Dept. of Computer Science
University of Kashmir
Srinagar, India

Javed Parvez
Dept. of Computer Science
University of Kashmir
Srinagar, India

***Abstract*—IPSec is the amalgam of protocols dispensing security in IP networks. It has been the rudimentary security component in IPv4 and IPv6 networks providing for data authentication, integrity and confidentiality. Earlier security was not embedded at the IP level however with emergence of large scale public and corporate internets, the user data became vulnerable to malicious activities like privacy attacks and thefts. To mitigate this and secure network traffic, IETF introduced IPSec for robust network communications. IPSec is a framework that provides sublime options for encryption and authentication of data packets. IPSec architecture provides a flexible and agile approach for securing network traffic. Initially IPSec was introduced as an additional component in IPv4, but in next generation internet protocol IPv6, it's an inbuilt component implemented as a part of extension header. Although IPSec is the panacea for securing IP protocol, its implementation and management is unequivocally complex in nature. The implementation involves key management and exchange through IKE, protocol negotiations and establishment of security associations which can significantly decrease performance and degrade IP communication. This fact has a significant impact on real time communication. This paper makes an empirical investigation of the parameters that are affected by implementation of IPSec in IPv6 and 6to4 Tunneled Migration Networks. The investigation is significant and evaluates about the performance decay that is encountered by incorporating security. The simulation approach is used and measurements are performed in OPNET Simulator ver. 14.5.**

***Keywords*— IPSec, IPv4, IPv6, IKE, IETF, 6to4, OPNET**

I. INTRODUCTION

The internet protocol was designed with no inherent security model [1]. Communication in a hostile environment like internet where attacks like Network Sniffing, Eaves dropping and Man-in-the-middle are recurrent; mandate the requirement for encryption and data protection to achieve data integrity, confidentiality and authenticity [3].To achieve these goals, IETF (Internet Engineering Task Force) through set of RFC's introduced Internet Protocol Security(IPSec) as a framework of protocols that can be adjoined with IP datagram's for secure transmission over unprotected public network [4].The Original IPv4 design lacked security mechanisms. IPSec was later retrofitted as an additional component to provide interim security measure while as in Next Generation Internet Protocol IPv6, it's an integral element and implementation is mandatory to ensure security among the communicating devices. IPSec is administered in IPv6 as a part of extension headers identified by Next Header protocol number 50 for ESP and 51 for AH. The main objectives achieved by IPSec between two communicating peers over an untrusted network are Data Integrity, Data Confidentiality and Data Origin Authentication and Security against Replay attacks [4], [5]. Data Integrity requires maintaining accuracy and consistency of data. The data should not be tampered while in transmission over public networks. Data Confidentiality demands encryption of data during transmission. This means even if data is accessed somehow, it cannot be interpreted. Data Origin Authentication verifies the source of data and ensures that it is sent by legitimate sender. In IPv6; IPSec is implemented using Site-to-Site network tunneling and plays a major role in ensuring that data is transmitted securely and efficiently. In fact most of the corporate VPN's (Virtual Private Networks) having branches throughout the world are secured through IPSec. Since IPSec is deployed at network layer, it ensures security of IP level packets only. Despite numerous benefits of IPSec, its implementation does have some performance issues. The issues are mainly attributed to complex key management and protocol negotiations between two communicating parties.

The remaining paper is structured as follows. Section II discusses about the layout of IPSec and its associated protocols. Section III highlights and debates about issues that are prevalent with IPSec implementation and integration with current IP networks. Section IV surveys the related work in the area. Section V explains the simulated network model and implements the simulation test. In section VI, simulation results are discussed. Finally we conclude and summarize our findings in section VII.

II. IPSEC ARCHITECTURE ANALYSIS

The design of IPSec is expounded through RFC 4301 which describes security architecture for IPv4 as well as IPv6 [3].The general framework of IPSec encompasses the following elements:

- Security requirement interpretation.
- Protocol specification for encryption (Encapsulated Security Protocol or ESP) and authentication (Authentication Header or AH).

978-1-4799-6818-3/15/$31.00 © 2015 IEEE

- Negotiations on use of cryptographic algorithms for encryption and authentication.
- Negotiations of security policies and associations.
- Internet Key Management.

The IPSec lists down two protocol headers for providing network security and confidentiality: The Encapsulating Security Protocol (ESP) Header and Authentication header (AH) [6].Both these headers are implemented as extension headers in IPv6.The main difference between AH and ESP lies in the fact that AH does not provide the confidentiality option.

A. Authentication Header

The Authentication Header (AH) as defined in RFC 4302 dispenses connectionless integrity and data source authentication (without confidentiality factor) for all end-to-end transmission of IP packets. AH provides varied authentication mechanisms and also protection against replay attacks. In IPv6; the AH having next header value of 51 in extension header succeeds Hop by Hop, Routing and Fragment extension headers. The AH is sand witched between Upper layer protocol headers (TCP, UDP) and the IP. Figure 1 below illustrates the format of AH.

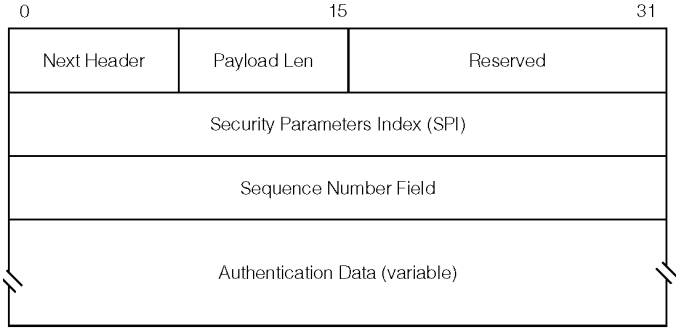

Fig 1 : Authentication Header

- *Next Header* implies the class of header that follows authentication header.
- *Payload Length* defines the length of the header in four byte units.
- *Reserved* Field is not used and is initialized to zero.
- *Security Parameter Index* helps in unique identification of security association for a particular datagram.
- *Sequence Number* makes a counter of number of packets sent from source to destination.
- *Authentication data* contains the checksum value (integrity check value) for the packet. It is of variable size.

B. Encapsulating Security Protocol

The Encapsulating Security protocol header as defined in RFC 4303 provides for connectionless integrity, data source authentication and confidentiality of IP packet data.ESP encrypts the packet payload using different encryption algorithms to provide confidentiality. The potential services rendered by ESP are negotiated when Security Associations are established. In IPv6; the next header value of 50 in extension header indicates the ESP Header which consists of following fields as shown in figure 2 below.

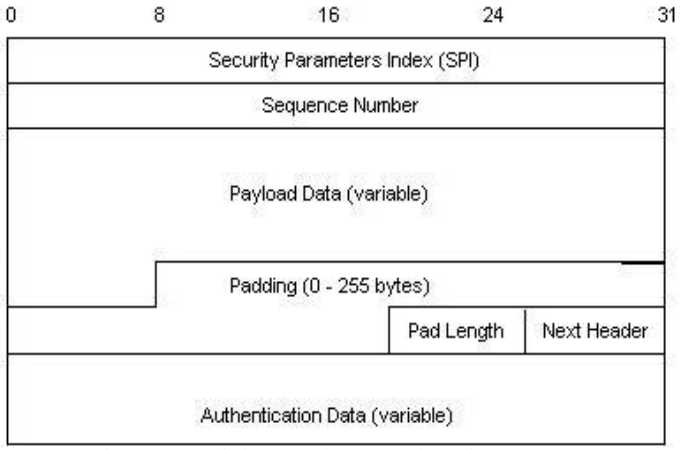

Fig 2: Encapsulating Security Protocol Header

- *Security Parameter Index* helps in unique identification of security association for a particular datagram.
- *Sequence Number* makes a counter of number of packets sent from source to destination.
- *Payload Data* contains encrypted data and initialization vector (IV) if mandated by encryption mechanism.
- *Padding* is used mainly to align packet in multiples of 4 bytes. It's also required because of encryption.
- *Pad Length* determines the length of padding used.
- *Next Header* implies the class of header following the ESP header.
- *Authentication data* contains the checksum value (integrity check value) for the packet. It is of variable size.

In both AH and ESP, message authentication and integrity are achieved by using keyed MAC (Message Authentication Code) based on symmetric encryption algorithms like MD5, SHA-1.IPSec protocol runs in one of the two modes: The Transport mode or The Tunnel Mode. The Transport mode IPSec establishes connections between two end systems directly. In this mode; the whole IP payload is protected leaving the original header intact. IPSec in the Tunnel mode creates a virtual secure tunnel between two gateway systems that lie in the path of two end systems. Tunnel Mode encrypts and encapsulates whole IP datagram and creates an outer IP header. The AH and ESP both operate in Transport as well as Tunnel Mode as shown in figure 3 and 4.The Transport mode ESP safeguards the original IP header and adds new ESP extension header with an optional trailer. These provide encryption of data payload. The Transport mode may also contain optional ESP authentication trailer which assists in HMAC authentication of original header and payload. The AH in Transport mode provides authentication of original IP header and payload by adding new extension header.

In Tunnel mode, ESP and AH create a new IP header that encapsulate the actual header and payload. In ESP, the original IP header and payload is encrypted as well as authenticated; while as compared to AH, it's only authenticated and not encrypted.

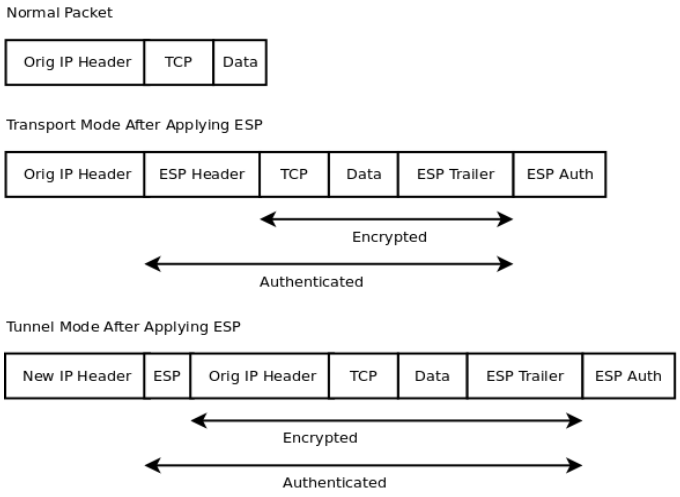

Fig 3: ESP Data Packet

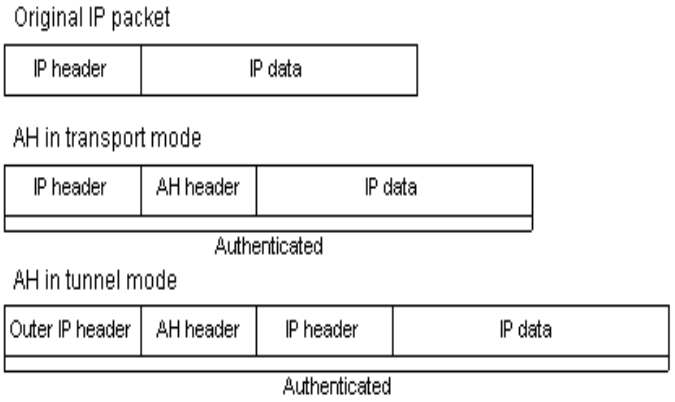

Fig 4: AH Data Packet

C. *IPSec Security Associations*

Before the communication between two different peers, there needs to be establishment of agreements known as Security Associations (SA). The framework of security association rests on the following building blocks which include [7]:

- *Time Validity* of Association
- *Mode of Operation*-whether Tunnel or Transport
- *Cryptographic Parameters* like Key, Encryption protocol and Authentication Mechanism.
- *Sequence Number and Anti Replay Window*

Security Associations operate unidirectional, which means that if two nodes want to encrypt and authenticate a two way communication session; four security associations need to be established (two for encryption and two for authentication).A device can establish SA's with several nodes. To uniquely identify SA, combination of 32-bit Security Parameter Index (SPI) and endpoint IP address is used. Each IPSec header contains value of SPI which is used by end node to identify SA. Every communicating peer maintains a database for incoming and outgoing SA's. This database is commonly referred to as SADB (Security Association Database).

D. *IPSec Key Management*

For secure communication; two peers must agree on encryption algorithms, authentication algorithms and keys that are going to be used [3].To facilitate this key exchange mechanism, IPSec uses IKE protocol. The IKEv1 as specified in RFC 2409 uses UDP on port 500 or 4500 with two phases: Phase 1 sets up secure communication channel for ensuing communications between end nodes. Phase 1 exchange which uses Diffie- Hellman key exchange conventionally executes in Main mode or Aggressive mode. The Aggressive mode is little faster but less secure. Authentication is achieved either through Pre-shared keys (RSA checksum encrypted with private key of sender) or combination of receiver's public key with its X.509 certificate. Phase 2 also called Quick mode involves negotiation on other parameters like encryption algorithms, keys/certificates which are used for actual communication. The IKEv1 phase 2 output results in SA that define security services needed to protect data traffic.

III. ISSUES WITH IPSEC

Despite IPSec's secure services which have contributed to its popularity, IPSec implementation suffers certain drawbacks [2]. These drawbacks are owing to complex key exchange mechanisms, protocol negotiations, Security Association setup. These issues are significant and have considerable amount of impact on the performance of network. For example, using IPSec Tunnels, nodes may suffer encapsulation and decapsulation delays due to additional new headers. These delays impede the performance and throughput of network. Additional headers also lead to increased packet size than permissible MTU of given node's interface [8]. As a result, some routers may not fragment and forward the data packets if they are larger than permissible MTU. This results in increased packet drop.

The IPSec implementation is incompatible with NAT. The NAT Translation device fiddles with IP header which can render Authentication data as invalid and cause IPSec integrity check at receiver to fail. The Authentication data calculation involves source and destination IP address. With AH in Transport mode, the source address gets translated after the Authentication Data computation. This causes the message integrity check at the receiver to fail. With ESP in Transport mode, checksum calculation in TCP header includes the source and destination IP addresses. Because NAT revamps the source IP which renders TCP checksum as invalid. The checksum value needs to be re-computed by NAT device if encryption is not used. However this would cause message integrity check to fail. The only feasible option is IPSec ESP in Tunnel mode which does not cause incompatibilities.

NAT also elevates problems for IKE negotiations if the parameters are modified [9], [10]. For example while using pre-shared key authentication in main mode; the address change can lead to tossing out packets.NAT can also lead to overlapping Security Association Database (SAD) entries when multiple nodes behind the NAT try to make a contact

with same host. This host may send response packets to wrong nodes because of identically occurring Security Associations. IPSec Implementation mandates for higher computational power in nodes for cryptographic hash calculations and key generations. Sufficient amount of power may not be available in Low Power Devices (6LOWPAN) and mobile phones.

IV. Related Work

Due to large scale magnification in public internet, IPSec is used as a fundamental security solution. A lot of work is getting carried with the aim to overcome the complexities and evaluate the performance. In [11] authors have evaluated the effect of IPSec on Interactive communications. The work is significant and shows that IPSec can be used to secure multimedia communications over a wireless link without noticeably degrading the perceived quality. However; the main application of IPSec is in securing VPN's. Authors in [12] discuss about the imperatives and issues of IPSec based VPN's.The issues involved and performance evaluation is also done.VPN's which are commonly used for private transmission over public networks provide a safe heaven for malicious activities unless protected by security protocols. Yasinovsky et.al [13], discusses the impact of IPSec and 6to4 on VoIP quality over IPv6.The authors have conducted the experiment in a LAN environment and measured VoIP performance in varying background traffic conditions. IPSec as we know suffers divergence towards NAT. Authors in [14], [15] address and explore the issue of incompatibility between IPSec and NAT. In fact, [14] proposes a workable solution to implement end to end IPSec in heterogeneous IPv4 and IPv6 networks. Experimental results show that the mechanism is feasible to establish a successful IPSec connection across IPv4/IPv6 translation gateway.

V. Simulation Scenario Setup

This section describes the experimental setup for evaluating the impact of IPSec on Real Time applications like VoIP and Video conferencing in IPv6 and 6to4 Tunneling Migration Network. The simulation is carried in a controlled environment using elementary internetworking devices and network elements. The network devices that we use include workstations, internet gateways devices, IP backbones and communication links like Ethernet 100baseT and PPP_DS3 cables. The experiment is carried in three different networks scenarios: IPv6 Only, IPv6 with IPSec and 6to4 Tunneling (IPv4 to IPv6 Migration Technique).In first scenario no IPSec is configured in IPv6 only network. In second scenario IPSec Tunnel is configured between Routers R1 and R2.In third Scenario we check the impact on IPv4 to IPv6 migration network (6to4).In this scenario PC-1 and Server are running IPv6 while the network in between is IPv4.6to4 Tunnel as well as IPSec Tunnel is configured on R1 and R2.The topology used for the simulation is shown below in figure 5.

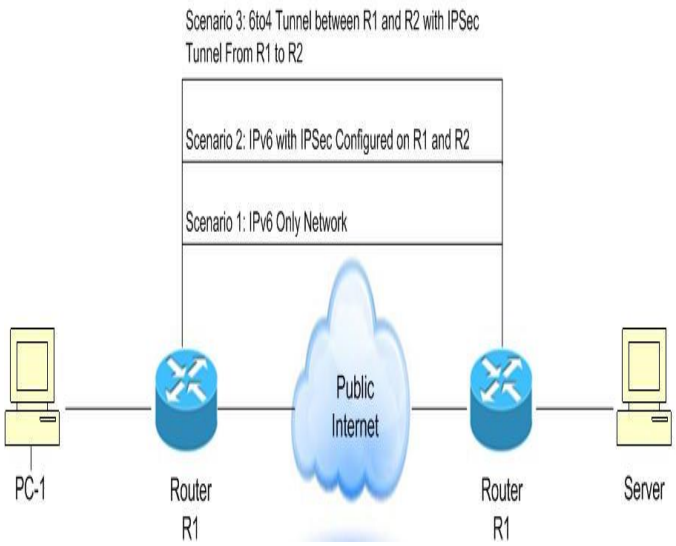

Fig 5 Network Topology

All the three scenarios are modeled in OPNET simulator ver. 14.5.The network traffic consists of VoIP and video conferencing. We chose these two Real time applications because they are sensitive to delay and require desired performance. Any delay or distortion in the network will effect these applications. We chose the network as IPv6 due to its vast and rapid adoption. Researchers have shown a notable interest on measuring IPv6 security performance metrics and behavior. As IPv4 address space has depleted and to maintain connection with the legacy protocol; we also evaluate IPSec effect on 6to4 which is one of the internet migration techniques.

The parameters that we want to measure are *IP End-to-End Delay, Throughput, Jitter, Packets Drop Rate, Tunnel Delay* (Scenario 2 and 3). *IP End-to-End Delay* may be described as time taken for the packet to reach its destination from its source measured as the difference between the time a packet arrives at its destination and the creation time of the packet. *Jitter* may be defined as delay variation in packets belonging to same flow. This is an important QoS parameter and can impact the quality of streaming in video and voice applications. If two consecutive packets with time stamps ts1 & ts2 leave the source node and are sent back at time ts3 & ts4 the destination node, then:

Jitter = (ts4 – ts3) - (ts2 - ts1)

Negative jitter implies that the time differentiation across packets at the destination node was less than that at the source node. Typically tolerance level of voice data packets is about 0.075 seconds but preferable jitter is within 0.040 seconds. *Throughput* is defined as the average data transferred across the medium per unit time. *Packet Drop Rate is the* number of IP datagram's dropped by all nodes in the network across all IP interfaces. *Tunnel Delay* is the delay experienced by a packet coming through a tunnel, i.e. the difference between the time at which the packet is sent in on the tunnel and the

time at which it is received at the opposite end, in seconds. This includes the encapsulation and decapsulation delays.

VI. RESULTS

All scenarios were run separately and performance parameters were collected. The total simulation runtime for each scenario was 15 minutes. Figure 6 to 9 shows the result of performance parameters that were collected. For simplification the average of each collected value is shown in table I.

TABLE I. AVERAGE VALUES OF SIMULATION

		Network Scenario		
		IPv6 without IPSec	IPv6 with IPSec	6to4 Tunnel with IPSec
IP Voice	Throughput (bits/sec)	48880.7	38706.3	36554.1
	Packet Dropped (packets/sec)	0.022	0.0255	0.0768
	IP End-to-End Delay (sec)	0.0711	0.0723	0.0744
	Jitter (µsec)	0.0000149	0.0000197	- 2.4
	Tunnel Delay (sec)	n/a	0.0031	0.0035
	Total Delay (sec)	0.0711149	0.0754197	0.0779024
Video	Throughput (bits/sec)	933355 .2	884961	867231.33
	Packet Dropped (packets/sec)	0.0244	0.0255	0.0835
	IP End-to-End Delay (sec)	0.0149	0.0155	0.0159
	Tunnel Delay (sec)	n/a	0.0065	0.0098
	Total Delay (sec)	0.0149	0.022	0.0257

Analyzing Table I, we notice that IPSec has a significant effect on IPv6 and 6to4 (IPv4 to IPv6) migration network. When we implement IPSec security we notice considerable decrease in throughput and increase in delay in the network. The delay is caused due to additional security headers that an IP packet has to handle. The nodes in addition to packet forwarding have to carry encryption/decryption, cryptographic hash calculations, Internet key exchange and encapsulation/decapsulation of data packets. This is a cumbersome process contributing to delay. The results also show that large packet drop rate is experienced by implementing IPSec on IPv6 and 6to4 Tunnel. In simulation we noticed that if we use IPv6 without IPSec; performance is fairly better but is less secure. Steps need to be carried in devising methods which can both be optimal as well as secure.

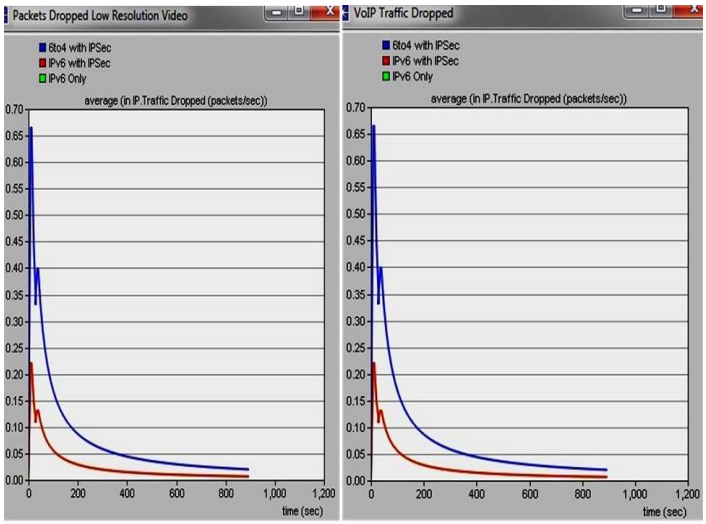

Fig 6: Packets Dropped (a) Video (b) VoIP

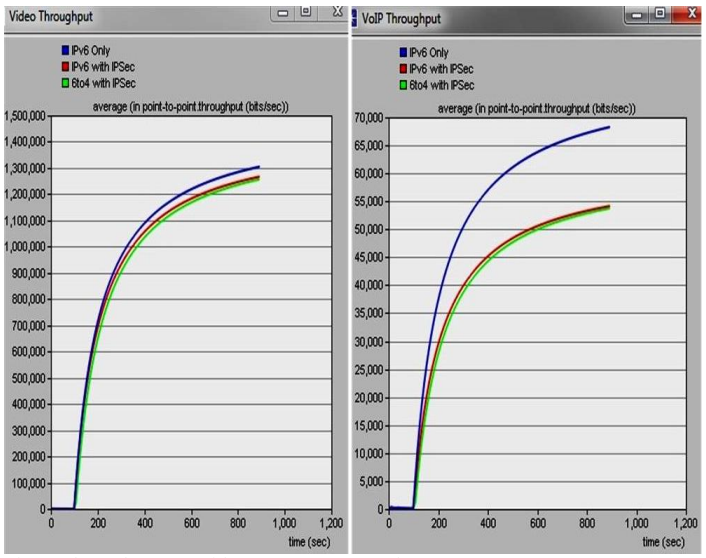

Fig 7: Throughput (a) Video (b) VoIP

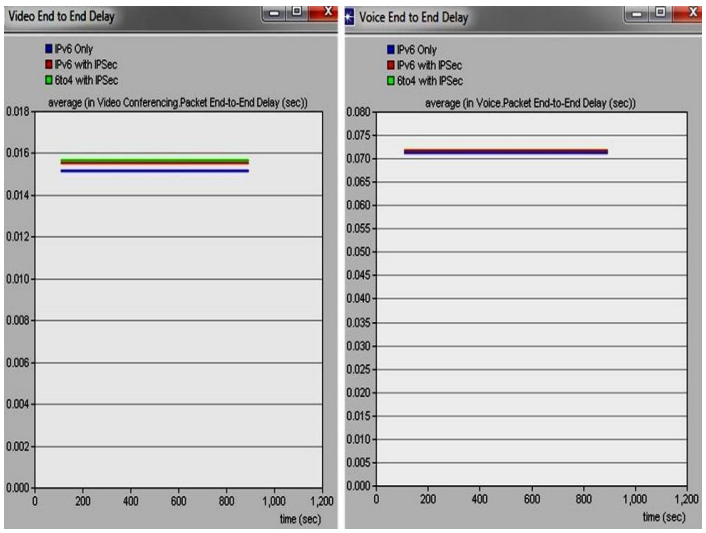

Fig 8: End-to-End Delay (a) Video (b) VoIP

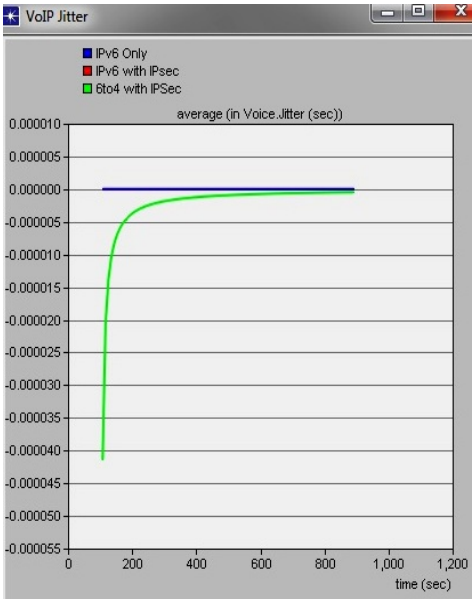

Fig 9: VoIP Jitter

VII. CONCLUSION

IPSec is a broader step towards security in IPv4 and Next Generation Internet Protocol IPv6.As stated earlier, the paper examined IPSec architecture framework and made a discussion on its associated protocols. The paper highlights IPSec issues and its incompatibility with current IP Network. The paper surveyed about recent work being carried out in this area. This paper also made an empirical investigation of the parameters that are affected by implementation of IPSec in IPv6 and 6to4 Tunneled Migration Networks and compared the results with IPv6 network without using IPSec. We notice that IPSec has notable impact on the network and performance gets decreased while incorporating security. This performance decay affects Real time application like VoIP and Video conferencing which are most sensitive to delay. So there is always a tradeoff between choosing better security or optimal performance. The performance of the network can slightly be increased if complexities in IPSec are removed. The use of caching and dynamic key generation should be preferred. If we talk of Real Time applications, QoS models and techniques should be implemented to avoid packet drop and delay. A stripped down version of IPSec should be incorporated in low power devices and mobile phones because they don't have large computational power. An approach like Header compression technique needs to be devised for accelerating IPSec enabled communication.

REFERENCES

[1] Shah, J., & Parvez, J. (2015). Security Issues in Next Generation IP and Migration Networks. IOSR Journal of Computer Engineering, 17(1), 13-18.

[2] Shah, Junaid Latief, and Javed Parvez. "An examination of next generation IP migration techniques: Constraints and evaluation." *Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on*. IEEE, 2014.

[3] Hogg, Scott, and Eric Vyncke. *IPv6 security*. Pearson Education, 2008.

[4] Kent, S., and K. Seo. "Security architecture for the internet protocol 2005." (2008).

[5] IPsec. (2015, January 20). In *Wikipedia, The Free Encyclopedia*. Retrieved 14:19, March 2, 2015,

[6] Hagen, Silvia. *IPv6 essentials*. " O'Reilly Media, Inc.", 2014.

[7] Menezes, Bernard L. *Network Security and Cryptography*. Wadsworth Publishing Company Incorporated, 2012.

[8] Issues with IPSec. Retrieved 14:19, March 2, 2015 https://www.shrew.net/static/help-1.0.x/issueswithipsec.htm

[9] Zheng, Liangbin, and Yongbin Zhang. "An enhanced IPSec security strategy."*Information Technology and Applications, 2009. IFITA'09. International Forum on*. Vol. 2. IEEE, 2009.

[10] Shah, Junaid Latief, and Javed Parvez. "Performance evaluation of applications in manual 6in4 tunneling and native IPv6/IPv4 environments."*Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on*. IEEE, 2014.

[11] Klaue, Jirka, and Andreas Hess. "On the impact of ipsec on interactive communications." *Parallel and Distributed Processing Symposium, 2005. Proceedings. 19th IEEE International*. IEEE, 2005.

[12] Miteshkumar S, Arvind D, "*Imperatives and Issues of IPSEC Based VPN"*.nternational Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-1, Issue-2, January 2013

[13] Yasinovskyy, R., A. L. Wijesinha, and R. Karne. "Impact of IPSec and 6to4 on VoIP quality over IPv6." *Telecommunications, 2009. ConTEL 2009. 10th International Conference on*. IEEE, 2009.

[14] Ahmad, Nazrul M., and Asrul H. Yaacob. "IPSec over Heterogeneous IPv4 and IPv6 Networks:Issues and Implementation " *IJCSNS* 13.7 (2013): 96.

[15] Heinlein, Alexander. "Problems of IPsec in Combination with NAT and Their Solutions." *Hauptseminar Telematik WS 2008/2009* (2009): 135.

[16] Shah, Junaid Latief. "Next Generation Internet Protocol A Survey on Current Issues and Migration." (2015).*International Journal of Computer science and Mobile Computing.*Vol 4,Issue 1,Jan 2015

[17] Zhang, Yunhe, et al. "A new approach for accelerating IPSec communication."*Multimedia Information Networking and Security, 2009. MINES'09. International Conference on*. Vol. 2. IEEE, 2009.

[18] Ahmad, Nazrul M., and Asrul H. Yaacob. "End to End Ipsec Support across Ipv4/Ipv6 Translation Gateway." *Network Applications Protocols and Services (NETAPPS), 2010 Second International Conference on*. IEEE, 2010.

[19] Volker, Lars, Marcus Scholler, and Martina Zitterbart. "Introducing QoS mechanisms into the IPsec packet processing." *Local Computer Networks, 2007. LCN 2007. 32nd IEEE Conference on*. IEEE, 2007.

[20] Shue, Craig A., Minaxi Gupta, and Steven A. Myers. "Ipsec: Performance analysis and enhancements." *Communications, 2007. ICC'07. IEEE International Conference on*. IEEE, 2007.

[21] Shah, J. L., & Parvez, J. (2014, September). Evaluation of queuing algorithms on QoS sensitive applications in IPv6 network. In Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on(pp. 106-111). IEEE.