Performance Analysis of IP Security VPN

Ritu Malik
M.E. 2nd Year
PEC University of Technology
(Formerly Punjab Engineering College)
Chandigarh

Rupali Syal
Information Technology Department
PEC University of Technology
(Formerly Punjab Engineering College)
Chandigarh

ABSTRACT
Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. . IPSec architecture requires the host to provide confidentiality using Encapsulating Security Payload and data integrity using either Authentication Header or Encapsulating Security Payload and anti-replay protection. IPSec has become the most common network layer security control and, a widely deployed mechanism for implementing Virtual Private Networks (VPNs). This paper presents analysis of IPSec VPN for videoconference in real time traffic over a secure communication links by implementing an IPSec-based VPN technology.

General Terms
Security, Algorithms, Network.

Keywords
Authentication Header (AH), Encapsulating Security Payload (ESP), IP Security (IPSec), Tunnel, Transport, Virtual Private Networks (VPN), Quality of Service (QoS).

1. INTRODUCTION
IP networks play an increasingly important role in daily life by enabling new approaches to doing business. Transactions that previously were carried out face to face can now be done remotely through the Internet. However, new services such as e-commerce and teleconference services will not be widely used unless they have well designed security protections. The internet is in general an adversarial environment where attacks can be easy, inexpensive and may be hard to prevent or trace. In general, it is difficult to ensure the main security goals which are confidentiality, integrity and authentication. Each packet contains data that is small, easily handled and maintained. The routing of these packets through the Internet as well as other large networks makes them open to security risks such as [1]:

- **Spoofing:** a machine on the network acts as another
- **Sniffing:** another person is listening in on another's activity
- **Session Hijacking:** an attacker completely takes over another user activity.

For securing the Internet traffic, Internet Protocol Security (IPSec) standard was developed by the Internet Engineering Task Force. The IPSec standard extends the IP protocol by securing the IP traffic at the IP level using cryptographic methods. IPSec can be implemented on routers, gateways, hosts, and any electronic appliances where a secure IP connection is required. An IPSec-enabled device, in addition to access control, also provides confidentiality, integrity, authentication, and replay protection. Since IPSec is actually a collection of techniques and protocols, it is not defined in a single Internet standard. Instead, a collection of RFCs defines the architecture, services, and specific protocols used in IPSec. This paper focuses on performance analysis of IPSec VPN for real time traffic. In this the comparison is made between the four environments (without IPSec, IPSec having only AH, IPSec ESP and IPSec providing AH and ESP both) by taking some of the Quality of Service parameters like packet loss, jitter, MOS and R-Factor.

Section II gives the general overview of IP Security then Section III describes some of the protocols used for security like Encapsulating Security payload, Authentication Header and Internet Key Exchange. Then Section IV describes about the Quality of Service (QoS) and its parameters based upon which results are made. Section V describes about the Network Model and Methodology used. Section VI shows some results of the performance analysis of IPSec VPN for real time traffic based upon the some of the Quality of Service parameters like packet loss, jitter, R-Factor and Mean Opinion Score.

2. IPSEC OVERVIEW
Communications through the use of the Internet has become a normal day-to-day operation. The data sent over the internet and private networks includes passwords, credit card numbers, social security numbers and other private and personal information. When sending this sensitive data, one wants to ensure that no third party manipulates or accesses this data. With the advancement and vast growth of networks whether they are a part of the large scale internet or of a small local network; security issues will always arise. In order to ensure the integrity and security of the data, a set of standard security Internet Protocols known as IP Security (IPSec) were developed. Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPSec can be used to protect data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host. IPSec architecture requires the host to provide confidentiality using Encapsulating Security Payload, and data integrity using either Authentication Header or Encapsulating Security Payload and anti-replay protection. IPSec protects IP packets, supports a strong encryption and data integrity mechanisms and is a network layer VPN technology, meaning it operates independent of the application(s) that may use it. IPSec is a framework that provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services [2]. The security services provided by IPSec are connectionless integrity, data origin authentication, protection against replays, and

confidentiality. Optional in IPv4, IPSec is mandatory for any implementation of IPv6. Once IPv6 is widely spread, it will be possible for any user wishing to use security functions to use IPSec. RFC2401 [3] defines the basic structure of IPSec (Figure 1 [4, 5]), all specific implementation methods are built on the basis. It provided the definition of the IPSec security services, how to use them and where to use, how to build and process datagram, and how to coordinate the same policies and so on. IPSec working group of the IETF has been defined many RFC, these RFC defined IPSec on all aspects: the system, privacy key management, the basic protocol and mandatory conversion code which in order to achieve the basic protocol. The set of security services that IPSec can provide includes access control, connectionless integrity, and data origin authentication, rejection of replayed packages, confidentiality, and limited traffic flow confidentiality. Because these services are provided at the IP layer, they can be used by any higher layer protocol, e.g., TCP, UDP, ICMP, BGP, etc [3].

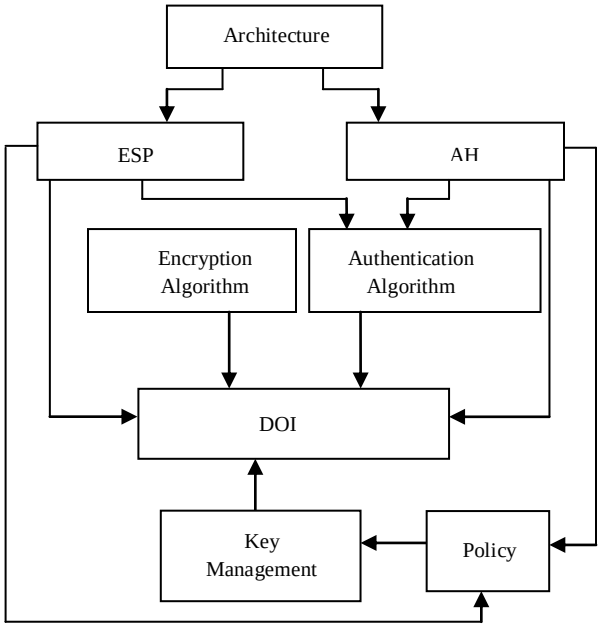

Figure 1.Basic structure of IPSec

3. IPSEC PROTOCOLS

IP Security (IPSec) is composed of a number of different pieces that together provide a set of security services. Those services include: access control, connectionless integrity, data origin authentication, protection against replays, confidentiality (encryption), and a limited traffic flow confidentiality. These services are provided by two traffic security protocols-the Authentication Header (AH) and the Encapsulating Security Payload (ESP)-plus the use of cryptographic key management procedures and protocols. There are two security mechanism of IPSec.

Authentication Header (AH)
AH is protocol 51 and is the authentication mechanism used to ensure that the endpoint one thinks they are communicating with is truly correct. AH is algorithm independent, which means that AH will operate with the algorithm of choice, depending on the level of security required. Currently the algorithm options are HMAC (Hashed Message Authentication Code) MD5 (Message Digest 5) or HMAC. Optionally AH will, if selected, provide protection against replays (man-in-the-middle attacks) as long as the receiver checks the sequence numbers. AH authenticates the entire packet including the upper protocol data, with the exception of the destination address. AH can be used alone, when only authentication is required, or in combination with ESP when a higher level of security is required.

Encapsulating security payload (ESP)
ESP is protocol 50 and normally is used to provide encryption and limited traffic flow confidentiality. ESP is also designed to be algorithm independent and the options are: Digital Encryption Standard (DES) (64 bit, commonly called 56bit), 3DES, RC5, Blowfish, Idea, Cast, and others are being added. DES, its common name, in ESP actually is DES-CBC (data encryption standard-cipher block chaining) with explicit IV (initialization vector) of 64 bits preceding the encrypted payload. Including the IV in each datagram ensures that decryption of each received datagram can be performed, even if some are dropped or reordered.

In order to understand, implement and use IPSec, it is necessary to understand the relationship among these components. The IPSec roadmap defines how various components of IPSec interact with each other. The ESP and the AH documents defines the protocol, the payload header format, and the services they provide. In addition these documents define the packet processing rule. IKE generates keys for the IPSec protocols. IKE is also used to negotiate keys for other protocols that need keys. The parameters that are negotiated are documented in a separate document called the IPSec Domain of Interpretation [6]. Authentication Header (AH) and encapsulating security payload (ESP) are two components of IPSec that are added to the plain internet protocol to meet the security requirements. Both mechanisms add a new header to the IP datagram. Important fundamental concept in the IPSec architecture is the security association (SA). It is a one-way relationship between the sender and a receiver which contains all the necessary information for secured communication, such as negotiated encryption algorithms being used, and encryption keys. For a two-way relationship, two SA are needed. This is also the case when both AH and ESP are needed for communication. An SA is uniquely identified by three parameters: SPI (security parameters index), Destination IP address and security protocol (AH or ESP). SAs are kept in an SA database (SAD) and when a datagram is sent, its destination address is looked for in the SAD and security policy database (SPD) is used to decide whether the datagram is discarded or accepted [7].

A. Setting up an IPSec Tunnel
Two databases are required to ensure proper operation of an IPSec client or gateway in the handling of both inbound and outbound IP traffic: a security policy database (SPD), and a security association database (SAD).

Security Policy Database: The SPD is constructed with the policies that specify what services are to be offered, i.e. what addresses have IPSec applied at what standard of security, and what addresses are passed through without IPSec.

Security Association Database: The SAD contains parameters associated with each security association (SA) that has been determined with the SPD. A security association is a 'connection' that affords security services to the traffic it carries. Three things found in the Ethernet packet comprise the SA: a security parameter index (SPI), a destination IP address, and a security protocol identifier.

Prior to the issuing of the first IPSec communication, all this SPD and SAD information is entered into the IPSec endpoint (client or gateway). Currently all this information must be entered into both ends of the IPSec VPN. However, as the implementation of IPSec evolves, the desire is to enter the SPD only.

B. Modes of IPSec

IPSec can be used in two modes, namely, transport mode and tunnel modes.

Transport mode provides protection primarily for upper layer protocols. It is used for end-to-end communication between two hosts. ESP encrypts and optionally authenticates the IP payload but not the IP header. AH authenticates the IP payload and non-mutable portions of the header. AH and ESP header are inserted after the original IP header and before the IP payload. The ESP trailer is inserted after the IP datagram and after at the optional ESP authentication data field can be placed.

Tunnel mode protects the entire IP datagram. It creates a "tunnel" from one IP network to another, for example, between two routers or between two hosts or between a host and a router. In tunnel mode a new IP datagram is created which includes a new IP header. The old IP header and payload are placed inside the new IP datagram. IPSec implementation can be a Host or Router implementation, the host implementation provides security end-to-end, ability to implement all modes of IPSec security, provides security on a per flow basis, and ability to maintain user context for authentication in establishing IPSec.

4. QUALITY OF SERVICE (QOS)

Quality of service (QoS) refers to resource reservation control mechanisms rather than the achieved service quality. Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. For example, a required bit rate, delay, jitter, packet dropping probability and/or bit error rate may be guaranteed. Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as voice over IP, online games and IP-TV, since these often require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource, for example in cellular data communication.There are some parameters which are necessary in order to quantify the performance. The usual ones are: Latency, Packet Loss, Jitter, Mean Opinion Score (MOS), R-Factor.

C. Packet Loss

This term refers to the loss or de-sequencing of data packets in a real-time audio/video data stream. A packet loss rate of 1% produces roughly a loss of one fast video update per second for a video stream producing jerky video. Lost audio packets produce choppy, broken audio.

D. Jitter

This refers to the variability of latencies for packets within a given data stream and should not exceed 20 - 50 milliseconds. . If a single packet encountered a jitter of 145 milliseconds or more (relative to a prior packet), an underun condition may occur at the receiving endpoint, potentially causing either blocky, jerky video or undesirable audio.

E. Mean Opinion Score (MOS)

MOS is used to check which factor affecting the quality of voice. The MOS is an overall value which represents the quality of voice. Its values are 1 to 5, the lowest value shows lowest quality of voice and highest value shows best quality of voice.

F. R-Factor

R-Factor is an alternative method of assessing call quality. Scaling from 0 to 120 as opposed to the limited scale of 1 to 5 makes R-Factor a somewhat more precise tool for measuring voice quality. R-Factor is calculated by evaluating user perceptions as well as the objective factors that affect the overall quality of a VoIP system.

When the above all parameters recommended limits are exceeded, it does not necessarily mean that the communication will be lost: it means that the quality of voice and video will be degraded in proportion to the exceeded recommended limit.

5. NETWORK MODEL AND METHODOLOGY

The model was designed according to a small size network that includes 2 hosts and includes some of the intermediate routers to transfer the data from source to destination. This model was created to measure the performance seen in the network topology. In this configuration the network was an ideal scenario where no congestion occurred. This network model was implemented in order to appreciate the behavior of the real time traffic using an IPSec VPN. The scenario was consisted of two nodes Node A and Node B for the videoconference (Figure 2). In this the IPSec VPN was implemented within two hosts (A and B) creating one IPSec tunnel to protect exclusively the voice and video packets. Two nodes (Node A and Node B) held a videoconference with VIGO VCON proprietary consoles, cameras and microphones. The protocols for multimedia traffic were G.722 (for voice) and H.263 (for video). The IPSec cipher specification was DES as the encryption algorithm, HMAC-SHA as the integrity mechanism, ESP and AH security protocols for encapsulation and authentication, IKE as the key interchange protocol and the IPSec authentication was made with pre-shared keys.

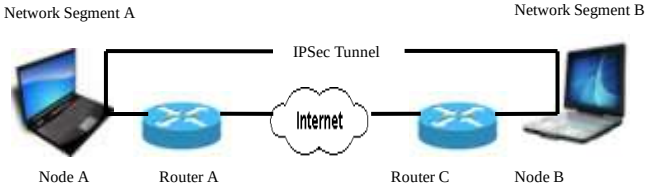

Figure 2.Test Scenario

Testing consisted on capturing the UDP voice and video packets that traveled from Node A to Node B with the use of TamoSoft Sniffer i.e. CommView. Both the nodes have installed the sniffer on it so that both can capture the incoming and outgoing traffic. The results only considered the UDP packets coming from the videoconference. The remaining traffic (FTP, HTTP and ICMP) was discarded since it was just injected for increasing the traffic. In order to perform the QoS evaluation, we established 4 real time videoconferences. Every videoconference lasted 5 minutes, during that time all multimedia packets were captured making a total of 20 minutes of videoconference packets captured and for every videoconference 5 samples have been taken and according to that the average performance is shown in the result. In test scenario, five minute videoconference for every sample was implemented firstly without the IPSec VPN, all others using the IPSec VPN with different security protocols like providing firstly only authentication (AH), then providing the confidentiality (ESP) and providing both authentication plus confidentiality (AH + ESP).

6. RESULT ANALYSIS

G. Packet Loss

The important parameter considered in quality of service was the packet loss. As shown in Table 1 and Figure 3 the average packets loss of five samples was almost null or 0.9% for video traffic in the test scenario in case of without providing the IPSec VPN and a 3.5% loss in case of providing the IPSec VPN. The percentage was obtained based on the total amount of packets transmitted by the origin node towards the destination.

$$\text{Packet Loss} = \frac{\text{Number of lost packet}}{\text{Number of lost packet+Number of packets received successfully}}$$

Table 1 Average Packet Loss

Average Packet Loss (5 samples)	Voice	Video
Without IPSec	0.7%	0.9%
With IPSec AH	1.3%	1.8%
With IPSec ESP	2.0%	2.5%
With IPSec (AH + ESP)	2.3%	3.1%

The result shows that after providing the IPSec in every case the voice and video packet loss is higher than the average result of without providing the IPSec this is because the IPSec introduces the overhead while transit because with data it also includes the AH and ESP header.

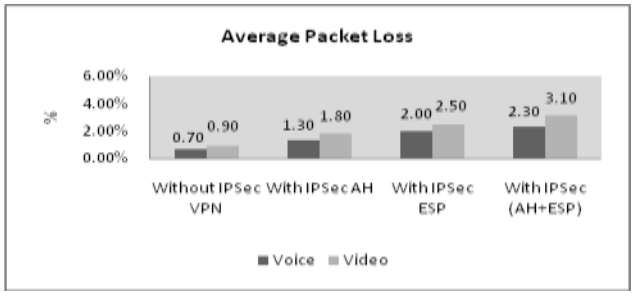

Figure 3.Average Packet Loss

H. Packet Jitter

The jitter for voice packets with VPN was higher (almost 10ms) than the recommended 50ms. For the video packets, the jitter was remained around 35ms and 60ms for both the environments (with and without VPN see Table 2 and Figure 4). It can be seen that the encryption process did not influence in the jitter parameter for G.722 and H.263 traffic.

Table 2.Average Packet Jitter

Average Packet Jitter (5 Samples)	Voice	Video
Without IPSec	34.6	35.44
With IPSec AH	45.5	39.26
With IPSec ESP	58.7	50.4
With IPSec (AH + ESP)	63.2	56.5

Despite of the 60ms video jitter average, the end user did not notice a bad voice quality for two main reasons: first, 60ms are not too far away from 50ms and second, the end user listen the voice with hardware dedicated consoles. These consoles have memory for buffering that could compensate the changes in the arrival time. Having buffers for jitter control, the asynchronous arrival time became synchronous, therefore improving the voice and video quality.

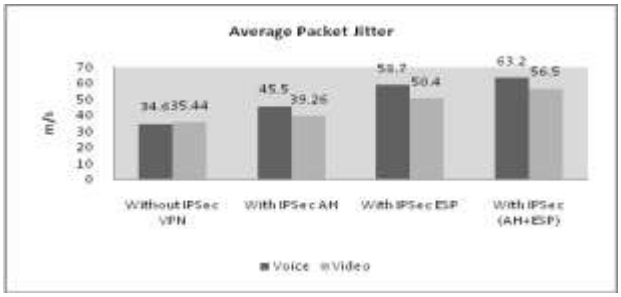

Figure 4.Average Packet Jitter

I. R-Factor

R-Factor is a method of assessing call quality. Its values start from 1 and end with 120 (See Table 3 and Figure 5).
The R-Factor can be obtained by the following expression:

$$R = R0 - Is - Id - Ie + A$$

Where, $R0$ represents the basic signal-to-noise ratio; Is represents the combination of all impairments which occur more or less simultaneously with voice signal; Id represents the impairments caused by delay; Ie represents impairments caused by low bit rate codecs and A is the advantage factors.

Table 3.Average R-Factor

Average Packet R-Factor	Voice
Without IPSec	81.2
With IPSec AH	81.2
With IPSec ESP	80.2
With IPSec (AH + ESP)	76.4

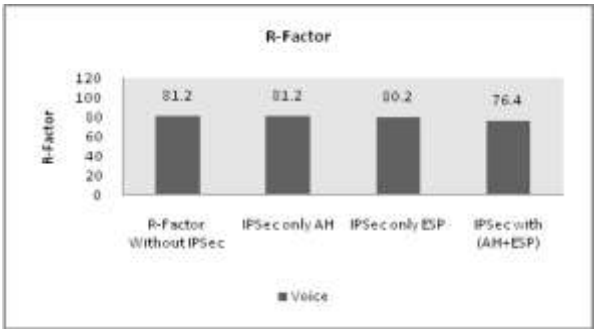

Figure 5.Average R-Factor

J. MOS

MOS is used to check which factors are affecting the voice quality. The MOS indicates the perceived voice quality of a VoIP conversation, ranking the call quality as a number in the range 1 to 5. The R-Factor can be converted to MOS rating in ranges from 1 (worst case) to 5 (excellent case).
After the calculation of R-Factor the conversion is done by relation between R-Factor and MOS rating:

For $R < 6.5: MOS = 1$

For

$$6.5 \leq R \leq 100: MOS = 1 + (0.035) * R + (0.000007) * R * (R - 60) * (100 - R)$$

For $R > 100: MOS = 4.5$

Table 4.Average MOS

Average Packet MOS	Voice
Without IPSec	4.1
With IPSec AH	4.1
With IPSec ESP	4
With IPSec (AH + ESP)	3.9

As shown in Table 4 and Figure 6 without IPSec VPN and with IPSec VPN provides the same MOS i.e. in between the range of 3.9 to 4.1 means users are satisfied with the voice quality.

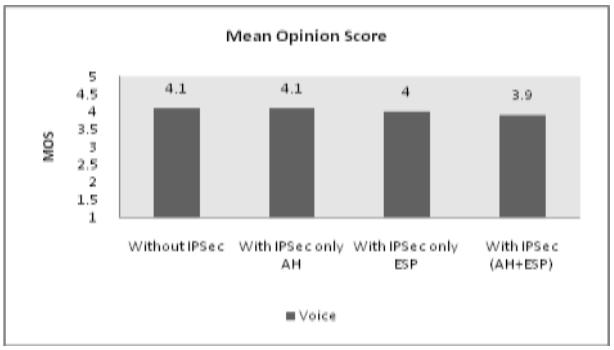

Figure 6.Average MOS

7. CONCLUSION

This work focuses on performance analysis of IPSec VPN for real time traffic. In this the comparison is made between the four environments (without IPSec, IPSec having only AH, IPSec ESP and IPSec providing AH and ESP both) by taking some of the Quality of Service parameters like packet loss, jitter, MOS and R-Factor. The results show that the QoS in a videoconference using IP infrastructure is most affected by the packet loss parameter when using IPSec tunnels. The main reason behind this is the traffic load. When IPSec is used to protect the data between two hosts, or between two gateways, or between a host and a gateway then with the data AH and ESP headers are also included so it increases the overhead and that's why the traffic load also increases. And if traffic load increases then there may be the case of congestion in the network that leads to result in packet loss. On the other hand, jitter is not much affected by the IPSec VPN. Even though the average result remained a little over the ideal limit with and without VPN, it did not affect the videoconference quality in a visible or audible way. Other parameters like R-Factor and MOS was also not affected by the IPSec VPN because in all the environments the user is satisfied by the voice quality. From above reasons, it can be deduced that it is feasible to implement IPSec VPNs for the small size network where there is no congestion in the network. And if IPSec VPN is applied in highly saturated networks with higher traffic loads it is necessary to use techniques that are able to protect and prioritize the information in order to make the traffic transmission secure without affecting the QoS parameters. Also in order to support both QoS and security with IPSec, a future work will consider adding some QoS parameters into the IPSec Security Association.

8. REFERENCES

[1] http://nislab.bu.edu/sc546/sc441Spring2003/ip_sec/Why%20it%20is%20important.htm.

[2] Roland, J.F., and Newcomb, M.J., 2003, CSVPN Certification Guide, CISCO Press

[3] Kent S, Atkinson R. Security architecture for the Internet protocol, RFC 2401 , 1998.

[4] L.A. Sanchez, H. Orman. A Roadmap for IPSec Policy Management draft- ietf- ipsp- roadmap- 01.txt, November 16, 2000.

[5] http://technet.microsoft.com/en-us/library/ bb726946.aspx

[6] Doraswamy, N., and Harkins, D., 2003, 'The New Standard for the Internet, Intranets, and Virtual Private Networks: Prentice-Hall' ISBN: 013046189-X

[7] Niemi, A., "End-to-end web security – protocol overview", Department of Computer Science University of Helsinki, Finland, December 2003.