Volume 2, Issue 9, September 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Performance Analysis of IPSec VPN over VoIP Networks Using OPNET

Masqueen Babu
Department of Computer Science & Engineering
Dr.B.R.Ambedkar National Institute of Technology Jalandhar

***Abstract*- Security and privacy become mandatory requirements for VoIP communications that needs security services such as confidentiality, integrity, authentication, non-replay and non repudiation. The available solutions are generic and do not respect voice specificities and constraints. Thus, Quality of Service (QOS) of the voice is affected by delay, jitter, and packet loss. New security solutions must take into account the real-time constraint of voice service and their mechanisms should address possible attacks and overhead associated with it. Nowadays IPSEC VPNs (Virtual Private Networks) is considered the strongest security solutions for communications over IP networks. In this paper, analysis and experimental results for an evaluation of the (QOS) of voice traffic are presented. A certain metrics like Packet Delay Variation, MOS (Mean Opinion Score), Packet End to End Delay, Traffic Received, Traffic Sent, are obtained and analysed. These results are further observed to study the effect of IPSEC VPN on these performance metrics. Experimental results confirm that, depending on the type of the traffic, the overall security of the networks is improved, with a reasonable decrease in term of performance.**

***Keywords*— IPSec VPN, Security,VOIP, Firewall,Opnet**

1. INTRODUCTION

Multimedia communication is one of the fastest growing Internet applications today and supporting reliable real-time service is one of its major concerns for widely deployment in IP-based networks. However, on the other hand it gives us the burden of finding feasible solutions to meet its stringent time requirements. It is a well known fact that the Internet backbone, which is the transport medium for any information across the globe, is time-variant. The characteristics of the Internet backbone are not known in advance, since they depend on the behaviour of the other connections throughout the network [1]. The connectivity may be hampered for several reasons rendering networking applications ineffectual. Often the networks suffer congestion i.e. traffics exceeding the capacity of the network are routed through it. The effect of this event is that the data packets suffer from high delay and loss while passing through the network. Such delay and loss are unacceptable in case of real-time applications. Of the various real-time applications we have concentrated on Voice over IP (VoIP) since it has gained importance over the past few years owing to its low cost and ease of interfacing between data and voice traffic [2]. VoIP (Voice over IP), also known as IP telephony, is the transport of voice traffic by using the Internet Protocol, rather than the public switched telephone network (PSTN). VoIP holds great promise for lowering the cost of telecommunications and increasing the flexibility for both businesses and individuals.

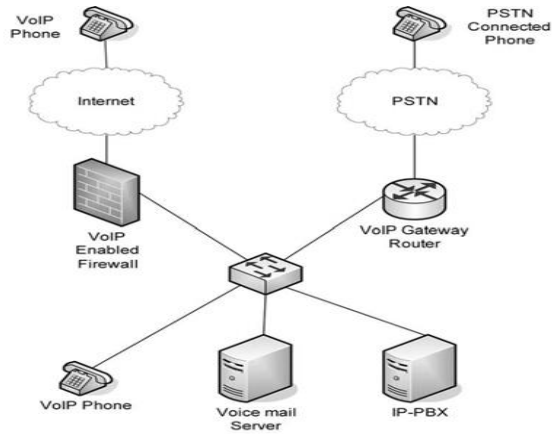

Figure 1. Typical VoIP network structure

The VoIP infrastructure consists of endpoints, control nodes, gateway nodes, and the IP-based network. The IP network can utilize various media including Ethernet, fiber, and wireless. The VoIP system interacts with both local and remote VoIP phones

using the intranet and Internet as well as interacting with phones connected to the PSTN through gateways. Figure 1 illustrates a simple VoIP network [3].

The problem of offering security to VOIP is that security does not come for free and, security and efficiency are conflicting requirements, for instance introducing security layer will affect the performance and QOS of voice traffic.

The key for securing voice traffic is to use security mechanisms like those deployed in data networks (firewalls, encryption, etc.) to emulate the security level currently enjoyed by PSTN network users without affecting the performance and the quality of voice. Various security requirements have to be met to secure multimedia transmission: Authentication, Privacy and Confidentiality, Integrity, Non repudiation, Non replay and Resource availability. Regarding IPSEC Virtual Private Network (VPN), it is considered actually as the strongest security solution for communications between users and corresponding node inside the intranet over unsecured IP network.IPSEC Virtual Private Network (VPN) is a technology that provides secure communication for data as it transits through insecure regions of information technology infrastructure [4].

This paper presents the IPSEC VPN performance for VOIP. A simulated environment is created where voice applications are in use at a time. This network model is based on OPNET14.5.The performance metrics of real time applications are measured on the basis of these simulation results. Then results are further analysed to study the effect of implementing IPSEC VPN on network performance.

This paper is organized as follows: Section 2 presents overview of IPSEC VPN. Section 3 describes the network topology studied. Section 4 analyzes results and discussion. Section 5 concludes this paper.

2. IPSEC VPN

IPSec VPN [RFC 2401] is designed to provide security between two gateways, firewalls and routers, or between a client and gateway. IPSec provides two different modes: Transport Mode, applicable only for host-to-host security, provides protection for the payload of IP packet, while Tunnel Mode provides security between two networks by protecting the entire IP packet. Both intranet and extranet VPNs are enabled through this mode (figure 2).

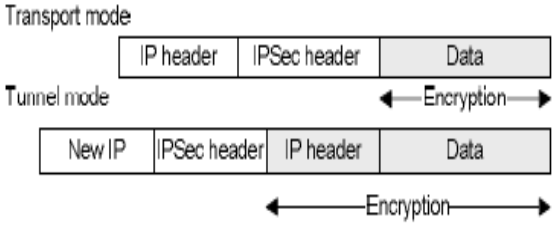

Figure 2. IPSec in transport and tunnel mode

IPSec is based on two encapsulation protocols: ESP (Encapsulation Security Payload) and AH (Authentication Header). AH provides origin authentication, data integrity and anti-packet repetition.

ESP also provides all characteristics mentioned above and additionally provides confidentiality through data encryption [5] [6]. ESP modifies the original IP packet inserting a new ESP header (after the IP header but before the data payload) and a packet trailer. The ESP header is not encrypted but a section of the trailer and the complete data payload are encrypted (Figure 3).

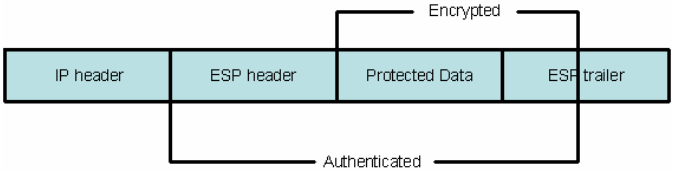

Figure 3. Encapsulated IP packet with ESP

The packet authenticated part includes: ESP header, data payload and a trailer section. Figure 3. Encapsulated IP packet with ESP When the destination node receives the IPSec packet, it receives it in clear: the Security Association (SA), the packet sequence number and the hash. This order is because of the same process of receiving that consists in three steps:

1. Sequence number verification.
2. Data integrity verification.
3. Decipher of information.

Before deciphering the information, which is a process that consumes lots of computational resources, the packets need to be checked to see if it did not delay (according with previous received packets) nor repeated. If the packet is valid, the next step is to verify the hash calculation and therefore check that the received information was not modified during transmission by a non authorized user or by a media failure. Finally the information is deciphered using the encryption shared key generated with IKE (Internet Key Exchange Protocol). At this moment the data is ready to be processed. IKE is a hybrid protocol that gives different services to IPSec such as: IPSec peer authentication, security association agreement and key generation/regeneration for cipher algorithms used by IPSec. IKE negotiates the IPSec SAs. This process requires that IPSec peers get authenticated first

with the help of digital certificates or pre-shared keys. After doing this, IKE can take further actions for the negotiation of IPSec SAs.The next section explains the basic parameters needed to quantify the QOS performance.

3. NETWORK TOPOLOGY

This section describes the network topology used for the simulations. In this network we are using three departments namely Entertainment, Research, Education and three servers namely Voice, Video and Data. All departments are connected to Router1 (Ethernet4_slip8_gtwy) via switch (Ethernet16_switch_adv).Servers are connected to Router 2.A firewall is implemented between Router 1 and Router 2 via IP Cloud. Each subnet contains wireless workstations and one access point. Entertainment Department support voice application and video applications while Research Department support video and data applications and Education Department support video, voice and data applications. Firewall is connected to the IP cloud which in turn connected to Router 2 using PPP DS1 at Data rate 1.544Mbps. Servers are connected to Router 2 using 100 base T with data rate of 100 Mbps. Subnets are connected to switch which in turn connected to Router 1 using 100baseT at data rate of 100Mbps. The network model is shown in the Figure 4.

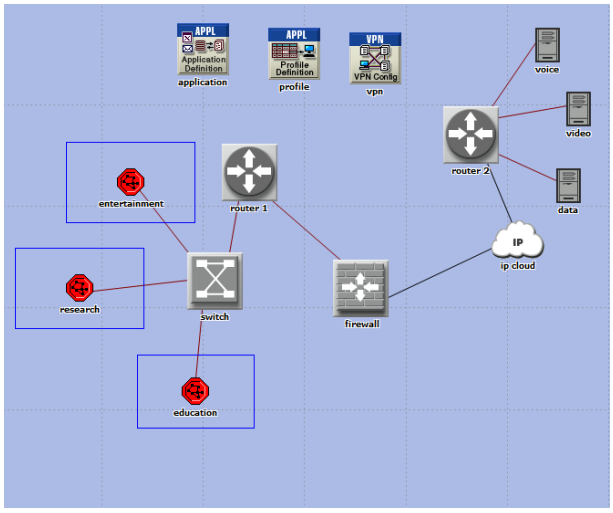

Figure 4 Network Topology Used

3.1 Parameters used in the network

Throughout the configuration of the wireless network of the type IEEE 802.11b passes at the same moment by the configuration applied to the machines which are connected to it (wireless Router and Access Point), but also by certain parameters. We are going to detail at first the configuration of the wireless local area network applied to machines as follows.
The wireless LAN group characteristics are: the limit of RTS(Request to send) is 2347 bytes, the data transfer rating is 11Mbps, the technique of spreading of spectra is DSSS (Direct Sequence Spread Spectrum), the power of emission is 1 mW, the power limit at reception is 7.33 x10-14 W, the short retry limit is 7, the long retry limit is 4, the bandwidth is 22 MHz, the channel is chosen in an unpredictable way, the size of the superior buffer is 256 Kbytes, the maximum waiting time at the reception is 500 ms, the treatment of BIG packets is destroyed [7].

3.1.1 Workstation: Throughout our simulation we used wlan_wkstn_adv node model it represents a workstation with client-server applications running over TCP/IP and UDP/IP. The workstation supports one underlying Wlan connection at 1Mbps, 2Mbps, 5.5Mbps and 11Mbps.This workstation requires a fixed amount of time to route each packet, as determined by the "IP forwarding Rate" attribute of the node. Packets are routed on a first-come-first serve basis and may encounter queuing at the lower protocol layers, depending on the transmission rates of the corresponding output interfaces.

3.1.2 Server: In our network we use Ethernet Server .This Ethernet server model represents a server node with server applications running over TCP/IP and UDP/IP. This node supports one underlying Ethernet connection at 10Mbps, 100Mbps, or 1 Gbps.

3.1.3 Switch: In our network we use ethernet16_switch.This node model support up to 16 Ethernet interfaces. The switch implements the spanning tree algorithm in order to ensure a loop free network topology. The number of interconnections is limited to 16 for this type of switch. In addition, the connections can be at 10Mbps, 100Mbps, or 1000Mbps.

3.1.4 Subnet: It is a single network object that contains other network objects (links, nodes, and other subnets). Sub-networks allow us to simplify the display of a complex network through abstraction. It also helps us in logically organize network model.

3.1.5 Firewall: The firewall, which can also be seen such as a Concentrator VPN follows the model OPNET "ethernet2_slip8_firewall". It thus contains two interfaces Ethernet, those who interest us here, but also 8 interface series, unused in our case. It is characterized by the same parameters (CPU/Workstations, ARP/Wireless Router, IP: Ethernet /Server). Since the most common WLAN usage is considered, the wireless speed was configured at 11Mbps with the random CSMA/CA DCF access mode [8].

3.1.6 IP cloud: In our network we use ip32_cloud node model.It represents an IP cloud supporting up to 32 serial line interfaces at a selectable data rate through which an IP traffic can be can be modelled. IP packets arriving on any cloud interface are routed o the appropriate output interface based on their destination IP address.

3.1.7 Access point: Throughout our simulation we use wlan_ethernet_router_adv. This is a wireless LAN based router with one Ethernet interface.

3.1.8 Router: The ethernet4_slip8_gtwy node is used as router in our network. This model represents an IP based gateway supporting four Ethernet hub interfaces, and eight serial line interfaces. IP packets arriving on any interface are routed to the appropriate output interface based on their destination IP address. This gateway requires a fixed amount of time to route each packet as determined by the "IP Routing Speed" attribute of the node.

3.2 Metrics used in the network

3.2.1 Packet Delay Variation: It represents the variance among end to end delays for voice packets and is measured from the time it is created to the time it is received.
3.2.2 Mean opinion score (MOS): MOS is used to check which factor affecting the quality of voice its value changes to 1 to 5, the lowest value show the lowest quality of voice and highest value show the best quality of voice[9].
3.2.3 Traffic Received (packets/sec): Average number of packets per second forwarded to all voice applications by the transport layer in the network.
3.2.4 Packet End To End Delay: It represents the time taken to send voice applications to a destination node application layer. This statistic records data from all the nodes in the network.
3.2.5 Traffic Sent (packets/sec): Average number of packets per second submitted to the transport layer by all voice applications.

3.3 Implementation

In our network we use three subnets namely Entertainment Department, Research Department, Education Department. The internal design of Entertainment Department is shown in Figure 5. It contains 10 wireless workstations and one access point. There are 6 clients who support voice applications and 4 clients support video applications. Research Department is shown in Figure 6. This Department contain 5 video clients and 5 clients support data applications. Education department is shown in Figure 7. This department contains 2 clients which support data applications, 3 clients support voice applications and 5 clients which support video applications. The data rate of each client in all three subnet is 5.5Mbps and for the Access point is 11Mbs.

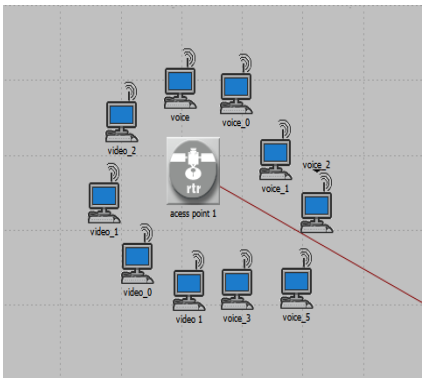

Figure 5
Entertainment Department

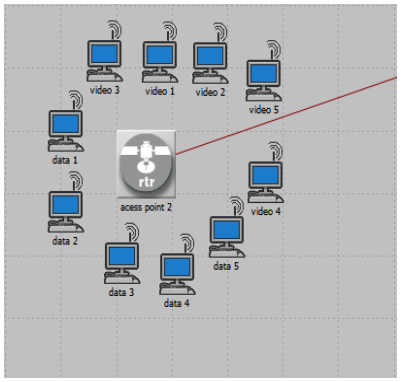

Figure 6
Research Department

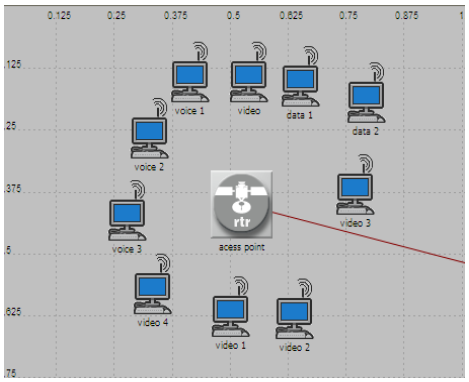

Figure 7
Education Department

In our network we are using three Scenarios namely:
1) Without Firewall: In this Scenario we allowed all the clients in the subnets to access all the traffic i.e. voice, video &data from the server.

2) With firewall: We assume that we need to protect the video applications in the server from external access, including the entertainment depts., so we used a firewall in order to do this.

3) Firewall_VPN: In the firewall Scenario, we protected the video traffic in the server from any external access using the firewall router. Suppose we want to allow the video clients in the entertainment depts. to have access to the video applications in the server .Since the firewall filters all video related traffic regardless of the source of the traffic, we need to consider the VPN solution [10, 11]. The firewall will not filter the traffic created by video clients because the IP packets in the tunnel will be encapsulated inside an IP datagram.

4. RESULT ANALYSIS AND DISCUSSION

4.1 Packet Delay Variation

The maximum packet delay variation for voice traffic in different scenario is shown in figure 7. It can be easily seen that for voice traffic these variations vary from 0.02 to 0.28 and 0.29 seconds for without firewall, with firewall and firewall_VPN respectively.This clearly indicates that packet delay variation is high in case of firewall_VPN. This can be explained as delay, the time past in the queue but also the time of treatment (encapsulation and de-encapsulation) of packages IP on the firewall (IP Processing Delay).

4.2 Mean opinion score (MOS)

The maximum observed values of MOS for voice traffic were found in the range of 3.056, 3.022 and ~3.025 for without firewall, with firewall and for firewall_VPN and presented in figure 8. From the graph it is clearly visible that MOS in case of firewall_VPN, with firewall and without firewall in between the range of 1 to 5 means users are satisfied with the voice quality.

4.3 Traffic Received

It is clearly observed from the figure 9. That for voice traffic the maximum packets received in case of without firewall is 461 while in case of with firewall is 483. The packets for firewall_VPN are found 291.This indicates that network performance is degraded in case of VPN because less number of packets is received due to delay in IP processing.

4.4 Packet end to end delay

The value for voice traffic is 0.70 sec in case of without firewall, 2.43 sec in case of firewall and 2.63 sec for firewall_VPN. The packet end to end delay is shown in figure10.

4.5 Traffic Sent

For voice traffic a maximum of 3852 packets are sent in case of without firewall, in case of firewall maximum of 3669 packets are sent and for VPN 951packets are sent across the network as shown in figure 11.

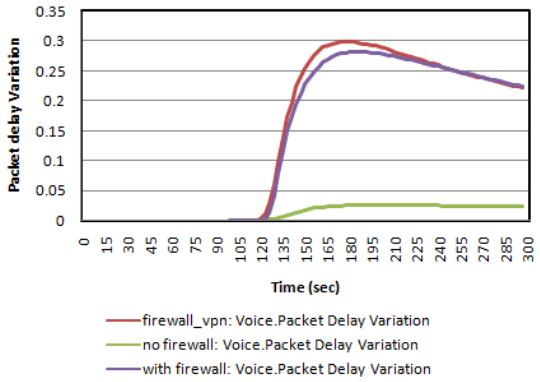

Figure 7. Packet delay variation for voice

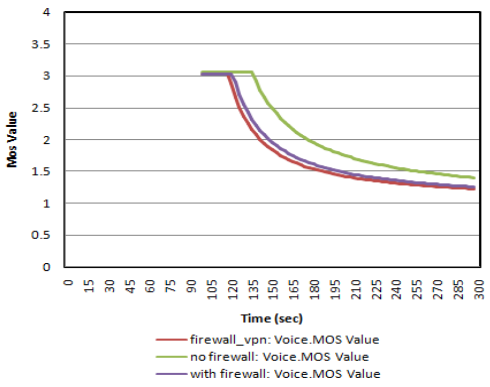

Figure 8. MOS value for voice

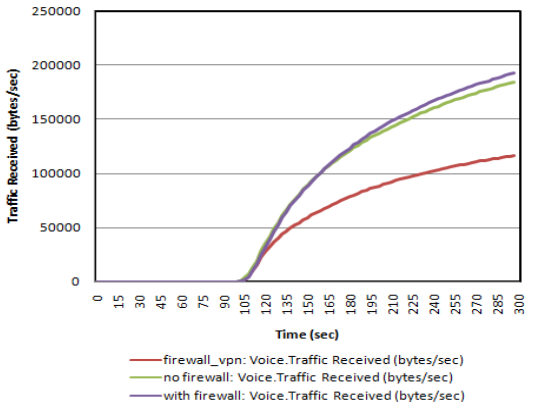

Figure 9. Voice traffic received

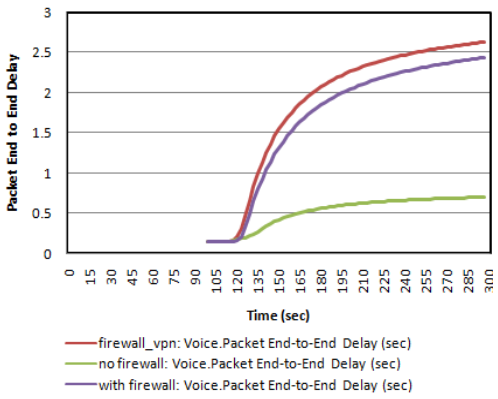

Figure 10.Packet end to end delay

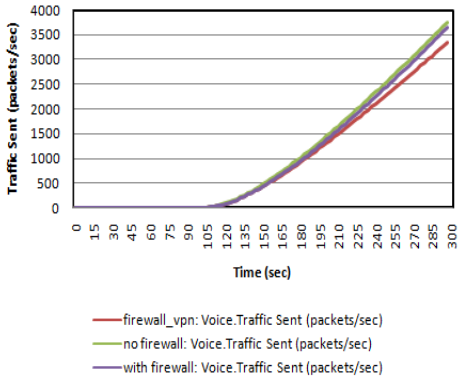

Figure 11.Traffic sent for voice Application.

5. CONCLUSIONS

This work focuses on performance analysis of IPSEC VPN for voice over IP networks. We shows the network topology used. We compare the result of three scenarios (without firewall, with firewall and Firewall_VPN) for the voice traffic; relevant statistics to validate a real implementation of this type of network were considered. It was demonstrated that Packet Delay Variation and Packet End to End Delay for voice traffic increases by using the IPSEC VPN. The main reason behind this is the additional encapsulation time needed. On the other hand MOS was not affected by the IPSEC VPN. It is observed that for IPSEC VPN less number of packets are received and sent across the network. It is concluded that using IPSEC VPN the security level increases however a reasonable decrease in the network performance was observed, which may be due to the encryption process and added authentication headers for packets. As for future work, it would be interesting to simulate more scenarios in both cases predetermined schemes and post-calculated schemes.

ACKNOWLEDGEMENT

The author is thankful to the Department of Computer Science and Engineering, Dr.B.R. Ambedkar National Institute of Technology, Jalandhar for providing the computing facilities to carry out this work. She is also thankful to her guide Dr Harsh K.Verma and her parents (Shri Chandrapal Pal Malik and Ishwari Malik) for their continuous support.

REFERENCES

[1] Bolot J. C. , Vega-Garcia A., "Control mechanisms for packet audio in the Internet," in Proc. IEEE Annual Joint Conference of the IEEE Computer Societies. Networking the Next Generation, pp.232-239, San Francisco, USA, 24-28 March 1996.

[2] Davidson J., Peters J., A Systematic Approach to undersatnding the basics of VoIP, Voice over IP Fundamentals, CISCO press, 2000.

[3] Butcher D., Xiangyang Li, Jinhua Guo. Security Challenge and Defense in VoIP Infrastructures. IEEE transactions on systems, man, and cybernetics—part c: applications and reviews, VOL.37, NO.6, NOVEMBER 2007.

[4] Narayan S., Kolahi S.S., Brooking K., Vere S.D. "Performance Evaluation of Virtual Private Network Protocols in Windows 2003 Environment"IEEE International Conference on Advanced Computer Theory and En gineering, 978-0-7695-3489-3/08 2008.

[5] Kent S. "IP Authentication Header", RFC 2402, IETF Network Working Group, 1998. http://rfc.net/rfc2402.html
[6] Kent S. "Encapsulating Security Payload", RFC 2406,IETF Network Working Group, 1998.http://rfc.net/rfc2402.html
[7] Kebreau S., Constantinescu B., Pierre S., "A NEW SECURITY APPROACH FOR WLAN", IEEE 1-4244-0038-4 2006.
[8] Gast M.S., 802.11 WIRELESS NETWORKS: THE DEFINITIVE GUIDE. Editor O'Reilly, April, 2002.
[9] Malik R., Syal R.,"Performance Analysis of IP Security VPN", International Journal of Computer Applications (0975 – 8887)Volume 8– No.4, October *2010*
[10] http://www.opnet.com/products/opnet-products.html.
[11] http://www.opnet.com/products/modeler/home-1 html.

