Performance Analysis of Virtual Private Network for Securing Voice and Video Traffic

Aruna Malik
Department of Computer Science and Engineering
Dr. B. R. Ambedkar National Institute of Technology
Jalandhar, Punjab, 144011, India

Harsh K Verma
Department of Computer Science and Engineering
Dr. B. R. Ambedkar National Institute of Technology
Jalandhar, Punjab, 144011, India

ABSTRACT
Security and privacy become mandatory requirements for voice and video communications that needs security services such as confidentiality, integrity, authentication, non-replay and non repudiation. Stringent quality of service (QOS) maintenance for voice & video communication is a major challenge. New security solutions must take into account the real-time constraint of voice & video and their mechanisms should address possible attacks and overhead associated with it. Nowadays, Virtual Private Networks (VPNs) is considered the strongest security solutions for multimedia communications over IP networks. In this paper, analysis and experimental results for an evaluation of the QOS of voice and video traffic are presented. A comprehensive set of measurements like packet delay variation, Mean Opinion Score (MOS), packet end to end delay, traffic received, traffic sent are obtained . These results are further analysed to study the effect of VPN on these parameters. 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.

General Terms
Security, IPSEC, Performance Evaluation, QOS.

Keywords
Virtul Private Network, Security,Voice,Video, Firewall,Opnet.

1. INTRODUCTION
Today Multimedia communication is one of the fastest growing Internet applications. It support reliable real-time communications and this is one of its major concerns for widely deployment in IP-based networks. Providing security to voice and video traffics is one of the major problem because 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 and video traffic.

By employing security mechanisms like firewall and encryptions we can secure voice and video traffic like those deployed in data networks to emulate the security level currently enjoyed by Public Switch Telephone Network (PSTN) users without affecting the performance and the quality of voice. Various security techniques are used in order to secure multimedia transmission: Authentication, Privacy and Confidentiality, Integrity, Non repudiation, Non replay and Resource availability. Regarding 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 [1].

VPN provides a low-cost alternative to leasing a line to establish communication between sites and can work with common software and hardware vendor products. There are so many VPN products are widely available, all with different capabilities and features [2]. They all enable businesses to implement VPN tunnels (Fig.1) to create organization wide secure networks between multiple sites. To create these tunnels, there are several protocols– three commonly used are: IPSec, PPTP, and SSL.

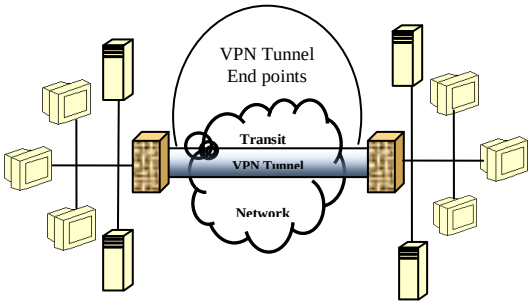

Fig. 1 VPN Tunneling

A VPN is combination of two main components: Security services and a tunnel for carrying private traffic. VPNs use encryption algorithms in order to prevent from interception and provide datagram analysis while they are in the public network. There are three different types of VPN usage: Remote-Access VPN, Site-to-Site Intranet VPN and Site-to-Site Extranet VPN. Remote-access, also called a virtual private dial-up network (VPDN), is a user-to-LAN connection used by a company that has employees who need to connect to the private network from various remote locations. In Site-to-Site Intranet VPN if a company have one or more remote locations and they wish to join in a single private network, they can create an intranet VPN to connect LAN to LAN. Extranet VPN connects companies with their business partners. A VPN technology is usually designed to be implemented with various compatible encryption and integrity algorithms. Common encryption protocols used include Triple Data Encryption Standard (3DES) and Blowfish (BF). And common data integrity protocols used includes Message-Digest 5 (MD5) and Secure Hash Algorithm (SHA1). PPTP was designed to only use a certain type of encryption, Microsoft Point to Point Encryption (MPPE) [3]. This paper presents the VPN performance for voice and video traffic. A

simulated environment is creating where voice and video applications are in use at a time and their mutual effects thereof. This network model is based on OPNET14.5.The performance metrics of real time applications are measured on the basis of these simulation results. Results are further analysed to study the effect of implementing VPN on network performance. This paper is organized as follows: Section 2 presents related work. Section 3 describes the network topology studied. Section 4 analyzes results and discussion. Section 5 concludes this paper.

2. RELATED WORK

It is necessary to include QOS mechanisms over the link for protecting the information especially when data is transmitted over internet or a shared WAN. This is required because internet is a public network and is susceptible to many attacks. The IP protocol does not protect the data itself over a public network: packets can be seen within the route towards the destination node, the IP address might be changed and also many other attacks can be mentioned [4]. In order to prevent and mitigate some attacks, the IPSec protocol suite was developed. Without any distinction, Internet protocol security (IPSec) integrates security elements to the IP protocol such as: origin authentication, data integrity, and confidentiality, no repudiation and anti packet repetition [5]. Many studies have been done to evaluate the VPN performance but the observed results do not apply to our purposes since our network infrastructure includes routers which create the IPSec tunnels. Also, the data (in our scenario) to transmit is voice and video simultaneously over the same IPSec tunnel; the data is in real time and not buffered, generated by one videoconference using wired media. The results in [6] only focus in voice traffic and not in video traffic. In [7] the test scenario consists of a wireless network and the IPSec tunnel creation is based on desktop nodes. The same happens in [8] where no network layer equipment is included and also the test did not include voice or video traffic. The scenario in [9, 10] includes wireless equipment and no multimedia traffic considered for the results. In [11] the results include streaming voice and video, but this kind of traffic is not real time like the videoconference's traffic since the data is stored in a file before it is sent. In [12] the analysis is done with a different perspective because the evaluation is based on MIPS (Millions of Instructions per Second) as the metric and not in terms of QOS parameters.

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 Fig 2.

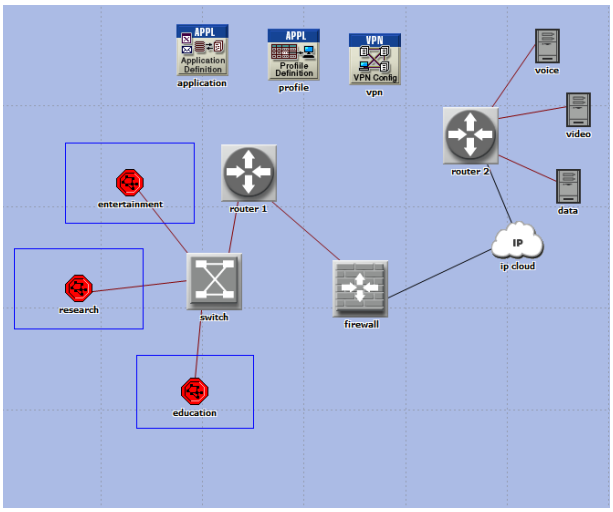

Fig. 2 Network Topology Used

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 Request to send (RTS) is 2347 bytes, the data transfer rating is 11Mbps, the technique of spreading of spectra is Direct Sequence Spread Spectrum(DSSS), 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 [13].

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 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 [14].

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 to 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 or video packets 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 & highest value show the best quality of voice[15].

3.2.3 Traffic Received (packets/sec)

Average number of packets per second forwarded to all voice or video conferencing applications by the transport layer in the network.

3.2.4 Packet End To End Delay

It represents the time taken to send a voice or video 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 or video 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 Fig 3.

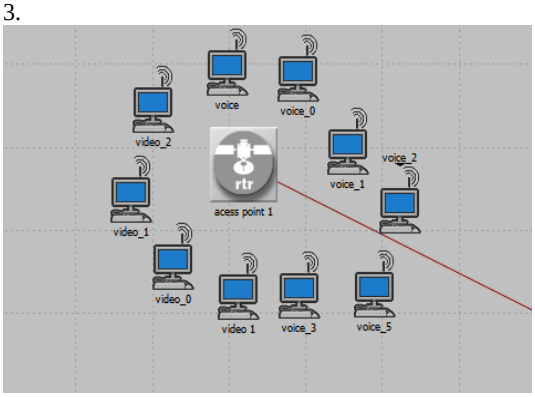

Fig. 3 Entertainment Department

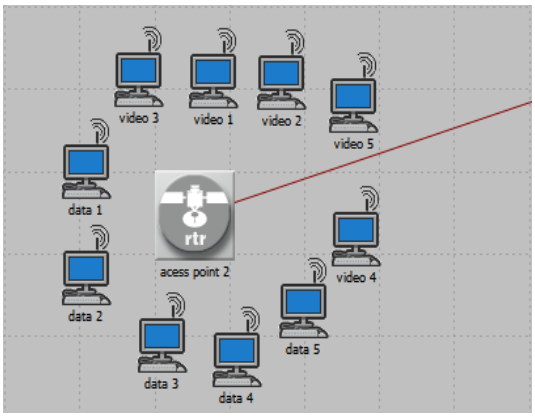

Fig. 4 Research Department

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 Fig.4, this department contain 5 video clients and 5 clients support data applications. Education department is shown in Fig.5, this department contains 2 clients who support data applications, and 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 11Mbps.In our network we are using three Scenarios namely:

3.3.1 Without Firewall

In this scenario we allowed all the clients in the subnets to access all the traffic i.e. voice, video and data from the servers.

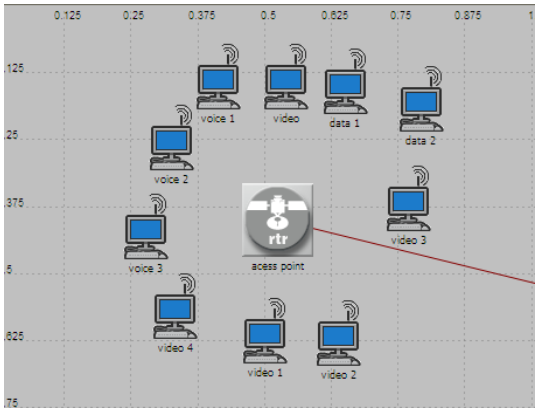

Fig. 5 Education Department

3.3.2 With firewall

We assume that we need to protect the video applications in the data server from external access, including the entertainment department, so we used a firewall in order to do this.

3.3.3 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 department 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. 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. RESULTS AND DISCUSSION

4.1 Packet Delay Variation

The maximum packet delay variation for voice and video traffic in different scenario is shown in fig. 6and fig. 7. It can be seen from fig. 6 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. Fig. 7 shows that the maximum packet delay variation of video is found 4.36 and 9.20secs for without firewall and firewall_VPN. 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 fig. 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

The next parameter is traffic received for voice and video traffic shown in fig.9. 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. When compared with video traffic 1234 packets are received in case of no firewall and no packets in case of firewall.

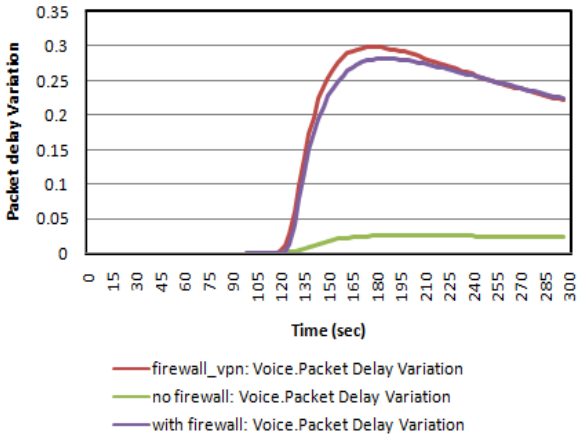

Fig.6 Packet delay variation for voice

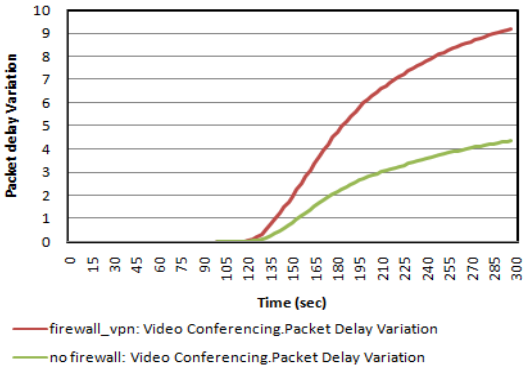

Fig.7 Packet delay variation for video

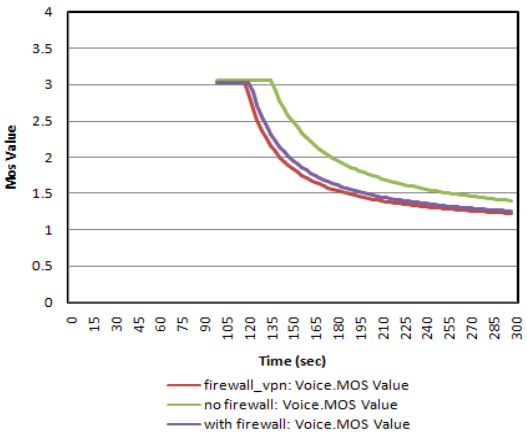

Fig. 8 MOS value for voice traffic

There are about 264 packets are received in case of firewall_VPN. 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 next parameter considered is packet end to end delay for voice as well as for video traffic. 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. For video these value were found 0.79 and 4.29 secs for without firewall and firewall_VPN. The packet end to end delay is shown in fig. 10. It represents that packets end to end delay for video traffic is high as compared to voice traffic because video packets are larger than voice packets voice packets occupied 538 bytes, while video packets average size is 1300 bytes.

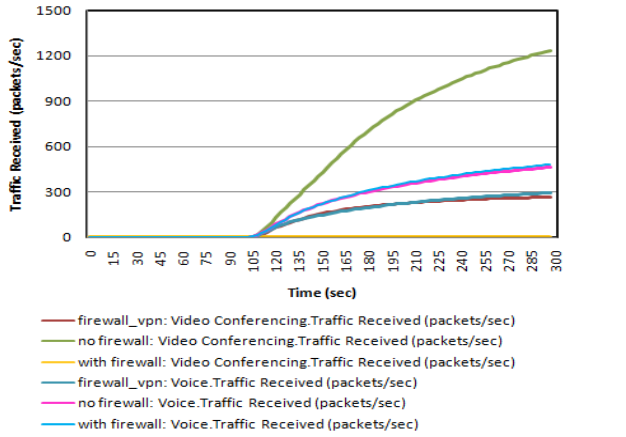

Fig.9 Traffic received in case of voice and video traffic

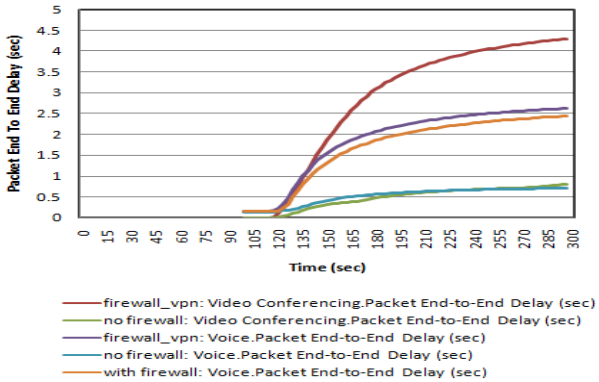

Fig. 10 Packet end to end delay for voice and video traffic

4.5 Traffic Sent

Results are shown in the Fig 11. 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. For video traffic, in case of without firewall maximum of 3769 packets are sent and 1307 packets in case of firewall_VPN are sent across the network.

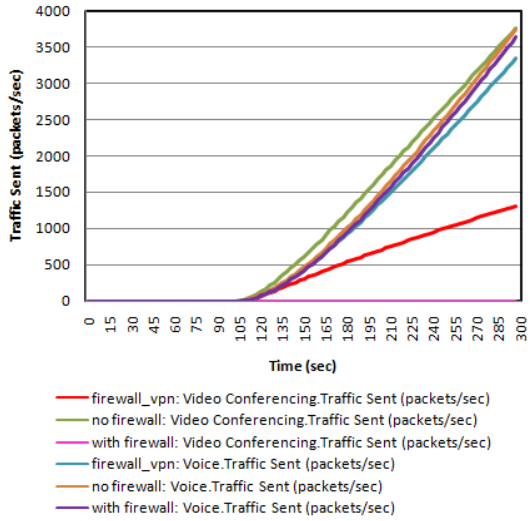

Fig. 11 Traffic sent for voice and video traffic

5. CONCLUSIONS

This work focuses on performance analysis of VPN for voice and video traffic. We shows the network topology used. We compare the result of three scenarios (without firewall, with firewall and Firewall_VPN) for the voice and video 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 and video traffic increases by using the VPN. The main reason behind this is the additional encapsulation time needed. On the other hand MOS was not affected by the VPN. It is observed that for VPN less number of packets are received and sent across the network. It is concluded that using 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.

6. REFERENCES

[1] S. Narayan , S. S. Kolahi, K. Brooking, and S.D. Veres, "Performance evaluation of virtual private network protocols in windows 2003 environment",International Conference on Advanced Computer Theory and Engineering 978-0-7695-3489-3/08 2008.

[2] S. Khanvilkar and A. Khokhar "Virtual Private Networks: An Overview with Performance Evaluation", Communications Magazine 2004, pp 146 – 154.

[3] A. Nadeem and M.Y. Javed, "A Performance Comparison of Data Encryption Algorithms," Information and Communication Technologies, *ICICT* 2005, pp.84 - 89.

[4] J. A. Pérez, V. Zárate, Á. Monte and C.García, "Quality of Service Analysis of IPSec VPNs for Voice and Video Traffic",in IEEE Proceedings of the advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services (AICT/ICIW 2006)0-7695-2522-9/06 2006.

[5] N. Doraswamy and H. Dan, "IPSec the New Security Standard for the Internet, Intranets, and Virtual Private Networks", Prentice Hall PTR Internet Infrastructure Series, 1999, ISBN 013011898.

[6] R. Barbieri, D. Bruschi and E. Rosti , "Voice over IPsec*:* analysis and solutions", Proceedings of the IEEE Computer Security Application Conference, 9-13 Dec. 2002, pp.261 – 270

[7] W. Qu and S. Srinivas , "IPSec-based secure wireless virtual private network", IEEE MILCOM 2002 proceedings , Vol. 2 ,7-10 Oct. 2002, pp.1107 – 1112.

[8] S. Khanvilkar and A. Khokhar, "Virtual private networks: an overview with performance evaluation", IEEE Communications Magazine, Vol. 42, Issue: 10, Oct. 2004, pp: 146 – 154.

[9] D. Khatavkar, E.R Hixon, R. Pendse, "Quantizing the throughput reduction of IPSec with mobile IP", Circuits and Systems, MWSCAS-2002, Vol. 3, 4-7Aug. 2002, pp: III-505 -III-508.

[10] G. C. Hadjichristofi, N. J. Davis and S. F. Midkiff, "IPSec overhead in wire line and wireless networks for Web and email applications", Conference Proceedings of the IEEE International Performance, Computing, and Communications, 9-11April 2003, pp. 543 – 547.

[11] S.Hyatt., S.A.Shaikh, B.Akhgar and J.Siddiqi ,"Performance of multimedia applications with IPSec

tunneling", IEEE Proceedings of International Conference on Coding and Computing, 8-10 April 2002, pp.134 – 138.

[12] O. Elkeelany, M. M. Matalgah, K. P. Sheikh, M. Thaker, G. Chaudhry, D. Medhi and J. Qaddouri, "Performance analysis of IPSec protocol: encryption and authentication", IEEE International Conference on Communications, ICC,Vol.2, 28April-2May 2002, pp.1164 – 1168.

[13] S. Kebreau, B. Constantinescu and S. Pierre, "A New Security Approach for WLAN", IEEE 1-4244-0038-4 2006.

[14] M.S.Gast, "802.11 Wireless Networks: The Definitive Guide", Editor O'Reilly, April, 2002.

[15] R. Malik and R.Syal, "Performance Analysis of IP Security VPN", International Journal of Computer Applications (0975 – 8887) Volume 8– No.4, October 2010.