International Journal of Current Engineering and Technology
ISSN 2277 - 4106

Available at http://inpressco.com/category/ijcet

Research Article

Effect of some Security Mechanisms on the Qos VoIP Application using OPNET

Hussein A. Mohammed[A] and Adnan Hussein Ali[B *]

[A]Iraqi Commission for Computers and Informatics/Informatics Institute for Postgraduate Studies.
[B]Electrical & Electronics Engineering Techniques College - Baghdad

Accepted 01 November 2013, Available online 01 December 2013, **Vol.3, No.5 (December 2013)**

Abstract

Voice over Internet Protocol (VoIP) is an application from the internet services that allows us to communicate with each other. VoIP requires Quality of Service (QoS) because it is very sensitive to loss and delay of the information. Therefore, QoS of VoIP is needed to ensure that voice packets are not delayed or lost during the transmission over the network. The objective of this research is to study the effect some of the Security Mechanisms on the VoIP Qos. In this work, simulation tool OPNET Modeler version 14.0 is used to implement the proposed network (VoIP Network). The proposed network is a private network for a company with two locations located at different countries around the world in order to simulate the communications within the same location locally and the communications between two locations as a long distance and analyze VoIP QoS based on measuring the major factors that influence the QoS for VoIP according to international telecommunication union (ITU) standards including: delay, jitter and packet loss. In this research, a comparison was executed between some security mechanisms like Packet Filter Firewall and Virtual Private Network (VPN) and it was found that VPN gives the better QoS from the traditional firewall for VoIP networks.

Keywords: *OPNET, FIFO Queue, Priority Queue, Weighted-Fair Queue, QoS, ToS.*

Introduction

Voice over Internet Protocol (VoIP) is a rapidly growing technology that enables transport of voice over data networks such as Ethernet local area networks (LANs) or internet. This growth is due to the integration of voice and data traffic over the existing networking infrastructure, low cost, and improved network management offered by the technology (Di Wu, 2002). But consolidating voice and data traffic can add to the common infrastructure of the entire network some risks where the voice networks are now subject to viruses, worms, Denial of Service (DoS) attacks, and other well-known threats. The key to securing VoIP is to use the security mechanisms like those deployed in data networks like firewalls, encryption and Virtual Private Network (VPN) (White Paper, USA, April, 2006).

There are most security solutions usually add delay such as using some encryption complex algorithms. In general, balance must be made between the desired security and the desired quality during implement the security solution with a minimum of delay, jitter and packet loss to ensure that QoS (Greg S. Tucker, 2004).

VoIP Quality of Service (QoS)

QoS measures a degree of user satisfactions and network performance. QoS has become a critical issue, because some applications as FTP, HTTP and e-mail are not sensitive to delay of transmitted information, while other applications such as voice and video are more sensitive to loss, delay and jitter of the information. Therefore, QoS of VoIP is an import concern to ensure that voice packets are not delayed or lost during the transmission over the network (Haniyeh Kazemitabar *et al*, 2010).

VoIP QoS is measured according to ITU recommendations based on different parameters like (delay, jitter, and packet loss). VoIP QoS is improved by controlling the values of these parameters to be within the acceptable range. Factors affecting QoS are briefly described in the following sections (Haniyeh Kazemitabar *et al*, 2010):

1. Latency: As a delay sensitive application, voice cannot sustain too much delay. Latency is the average time it takes for a packet to travel from its source to its destination. The source is the person speaking into the phone and the destination is the listener at the other end as shown in one-way latency (Greg S. Tucker, 2004). Ideally, must keeping on the delay as low as possible but if there is too much traffic on the line (congestion), or if a voice packet gets attached behind a bunch of data packets (such as an email attachment), the voice packet will be too delayed until that the quality of the call is compromised (Gouda I. Salama *et al*, 2009). The Maximum amount of latency that a voice call can tolerate one way is 150 Milliseconds (0.15 sec) but is preferred to be 100

*Corresponding author: **Dr. Adnan Hussein Ali**

Milliseconds (0.10 sec) (Qinxia *et al*, 2007). Equation (1.1) shows how to calculate the delay where **Average delay (D)** is expressed as the sum of all delays (*di*), to the total number of all measurements (*N*) (Furat Nidhal Tawfeeq *et al*, 2009).

$$D = \sum_{i=1}^{N} di / N \quad (1.1)$$

2. Jitter (Variation of Delay): voice packets must arrive at regular Intervals in order to be intelligible. Jitter measures the degree of variability in packet arrivals, which can be caused by bursts of data traffic or just too much traffic on the line (Gouda I. Salama *et al*, 2009). Voice packets can tolerate only about 75 Milliseconds (0.075 sec) but is preferred be 40 Milliseconds (0.040 sec) of jitter delay (Qinxia *et al*, 2007).

Equation (1.2) shows the calculation of jitter (j). Both average delay and jitter are measured in seconds. Obviously, if all (*di)* delay values are equal, then *D = di* and *J = 0* (i.e., there is no jitter) (Furat Nidhal Tawfeeq *et al*, 2009).

$$J = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(di - D)^2} \quad (1.2)$$

3. Packet loss: is the term caused by the ignoring of data packets in a network , the packets that do not arrive at the purposed destination that happened when a device (router, switch, and link) is overloaded and cannot accept any incoming data at a given moment (Jishu Das Gupta, 2005). Packets will be dropped during periods of network congestion. Voice traffic can sustain less than a 3% loss of packets (1% is optimum) before callers feel at gaps in conversation (Qinxia *et al*, 2007).

Packet loss ratio can be defined as a ratio of the number of lost packets to the total number of transmitted packets as shown in eq. (1.3), Where N describes the total number of packets transmitted during a specific time period, and N_L equals the number of packets lost at the same time period (Furat Nidhal Tawfeeq *et al*, 2009).

Loss packets ratio = (N_L / N) × 100% (1.3)

VoIP Security Mechanisms

The voice networks are now subject to viruses, worms, Denial of Service (DoS) attacks, Eavesdropping, Spam over Internet telephony (SPIT) and other well-known threats. There are a number of best security mechanisms that enable from minimize the risk of attacks on VoIP systems. These mechanisms include: Passwords, encryption algorithms, firewall, authentication and VPN (White Paper, USA, April, 2006). In this research, will be talking only about Firewall and VPN.

Firewalls

Firewalls are a prime of security in today's IP networks. Whether protecting a LAN, WAN, or to protecting a single computer, a firewall is usually the first line of defense against would be attackers. Firewalls Install between private network and public network as internet to protect private networks from the Internet. Firewalls work by blocking traffic malicious from flowing through them. Traffic not meeting the requirements of the firewall is dropped. Processing of traffic is determined by a set of rules programmed into the firewall by the network administrator such as Block all FTP traffic (port 21) or Allow all HTTP traffic (port 80). Much more complex rule sets are available in almost all firewalls. A firewall is provides a central location for security policies. It is the ultimate bottleneck for network traffic because when properly designed, no traffic can enter or exit the LAN without passing through the firewall (Richard Kuhn *et al*, 2005). There are many kinds to firewall such as: Packet Filter Firewall, Proxy Firewall and Stateful Event Monitor (SEM) (Timothy Kelly, 2005). In this research, will be talking only about Packet filter firewall.

Network Level Firewall (Packet Filter Firewall): is a router device which comes preprogrammed with level of firewall security and used in some small companies. It forwards packets from one network to another, but it also filters the packets that flow through it, and after that will decide the decision of either denying or accepting the traffic as shown in (figure 1) (Timothy Kelly, 2005). Packet Filter Firewall describes a method for the analysis and tracking of sessions to distinguish between the beginning of the session and the end of the session depend on examine packet headers such as: source IP address, destination IP address, source ports , destination ports and protocol type (Andrew Williams , 2006).

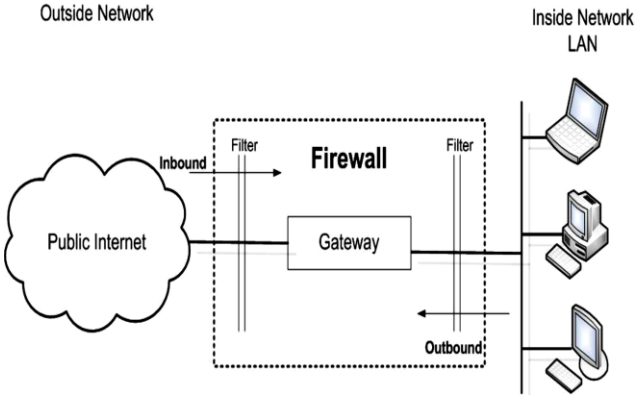


Figure 1: Packet Filter Firewall (Gulfam Asghar , 2010).

Virtual Private Networks (VPN)

VPN allows creating a secure link to private network with two or more from the locations across public network such as the internet. This secure link called Tunnel which creates using a combination of the hardware and software. In each location connected to the private network over public internet require Gateway, firewall and VPN software install on the gateway. Gateway allows to connected each location in private network to the internet, routing all traffic over the Internet to each of the other locations in the private network and gateway include VPN

software that performs some tasks such as encrypting and decrypting data transferred through the gateway and Authentication to verify identify users and devices for authorized to access network. In addition to encapsulation the traffic transferred through the gateway which could be used to provide secure communication (Timothy Kelly, 2005). Firewall is used to support VPN which can be set up in each location to prevent unauthorized packets from entry into the protected locations of the private network. But because the high cost of securing each VPN location's network, VPN designs are proving to work well when the network has no more than five to eight locations (Timothy Kelly, 2005).

A VPN is:

- ***Virtual***, because there is no real direct connection between private network with two or more from sites over public internet, but only a virtual connection provided by VPN software .
- ***Private***, because only the members of the private network connected by the VPN software are allowed to read the data transferred (Samara Isam Saeed Banno , 2008).

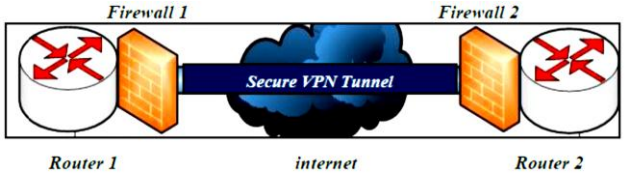


Figure 2: The VPN Tunnel between two locations to private network over the public network (internet) (Gulfam Asghar , 2010).

OPNET Simulator

OPNET is a simulation tool for making network modeling and QoS analysis of simulation of network communication, network devices and protocols. OPNET Modeler has a vast number of models for network elements and protocols. These make real-life network environment simulations in OPNET very close to reality. OPN*Et al*so includes features such as comprehensive library of network protocols and models, user friendly GUI (Graphical User Interface), Web report is feature allows to organize and distribute the results of simulations in form graphical results and statistics (Di Wu, 2002). The user doesn't need to have any programming knowledge in order to use OPNET (KeerthiPramukh Jannu , 2010). Automatic simulation generation OPNET models can be compiled into executable code (Furat Nidhal Tawfeeq *et al*, 2009).

Implementing the Proposed Network with OPNET

The network model for simulation consists from two companies that are located in two different countries around the world. The local area network (LAN) structure for both companies is the same (as shown in Figure 3).

In each LAN (three floors and in each floor are 15 Ethernet workstations, three Ethernet switch , one main switch called (Bay Networks Centilion100 Switch) and one router called (Cisco C4000 Router) connecting to IP cloud by bi-directional PPP_DS1 link. The workstations are connected to the switches by bi-directional 10Base_T links. The proposed network carries applications FTP, Video simultaneously along with VoIP.

There are some important objects in OPNET that are used to simplify and facilitate the work with it. In this research, some of these objects that are used are Application Configuration and Profile Configuration as show in fig.3:

1. Application Configuration Object: is an object used to define and configure all Applications in the network according to the user requirements. OPNET has most common applications like: HTTP, E-mail, video, File transfer, Voice, database. In this research, there is one application in the network model is a Voice.

2. Profile Configuration Object: is an object that can be used to create users profiles, profile can contains one or more applications and each application can be configured by the starting time and ending time. In this research, there is only one profile to all users called VoIP_ profile.

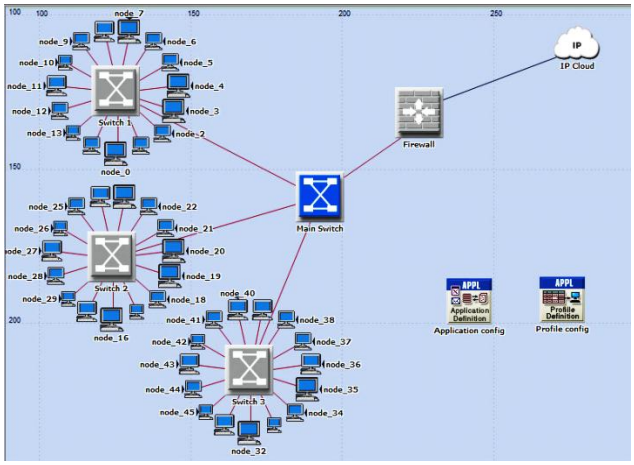


Figure 3: The Simulation Network Model.

Network Simulation Results and Discussions

In this research, a Comparison between the effect of some Security Mechanisms like Packet Filter Firewall and VPN on the VoIP Qos. To measure the QoS of the VoIP application during collected major factors that affect the VoIP QoS such as: Voice delay (sec), Voice jitter (sec), Voice traffic sends (packet/sec) and Voice traffic received (packet/sec). The duration of simulation is 8 minutes and the results are obtained as shown in figure4.

Figure 4: Comparison between Firewall and VPN in VoIP Network.

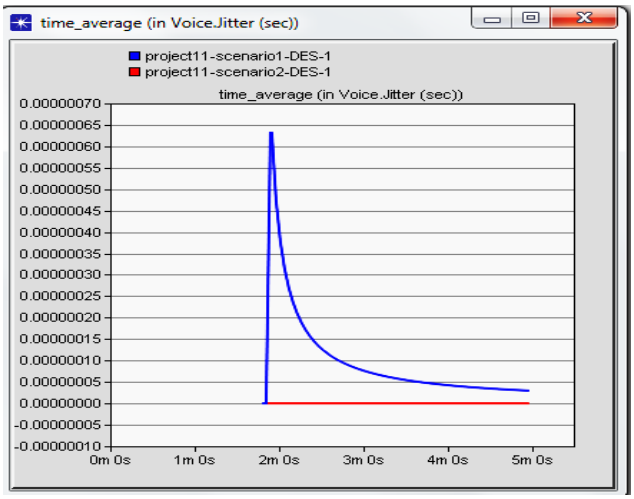
The blue line represent using Firewall; whereas the red line represent using VPN.

Figure (a) shows the Jitter using Firewall and VPN did not exceed the time constraint (0.075 sec).

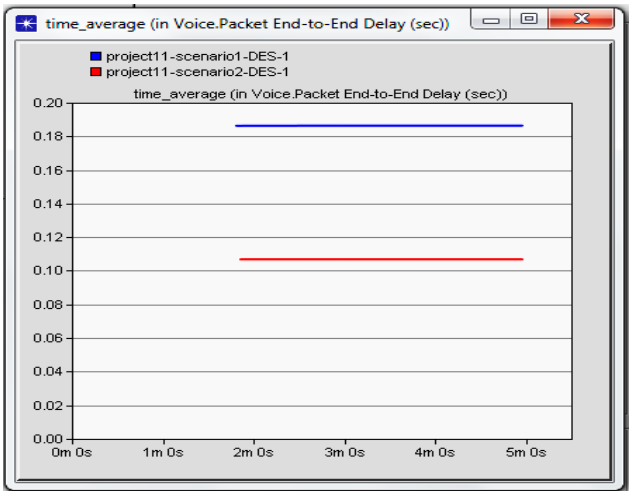
Figure (b) shows the end to end delay using Firewall did exceed the time constraint (0.15 sec) but using VPN did not exceed the time constraint (0.15 sec).
Figure (c) shows the voice traffic received using Firewall = 200 Packets/sec) and the voice traffic received using VPN = 200 (Packets/sec).
Figure (d) shows the voice traffic sent using Firewall = 200 Packets/sec and the voice traffic sent using VPN = 200 (Packets/sec).

Figure (4) shows using the packet filter firewall degrade QoS where introduce end to end delay exceed the time constraint (0.15 sec) because the firewall will inspect each packet that passes through it. But using the VPN is end to end delay does not exceed the time constraint (0.15 sec) because the firewall will not filter the traffic because the IP packets in the tunnel will be encapsulated inside an IP datagram. In both cases (firewall and VPN) no packet loss and jitter has acceptable ratios. VPN introduces better QoS from the traditional firewall; therefore NPN is more suitable to VoIP network.

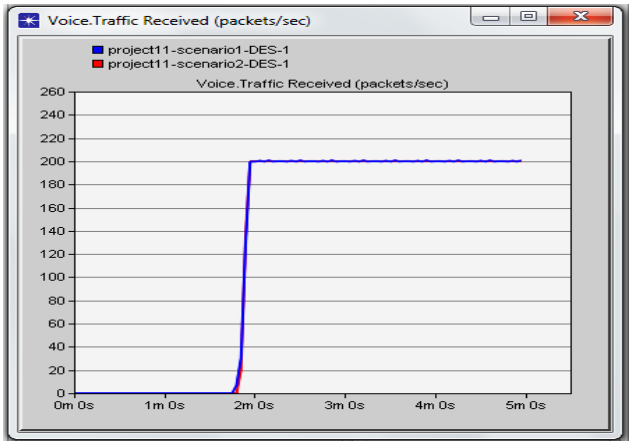
Different parameters captured to security mechanisms (traditional firewall and VPN) are summarized in Table 1.



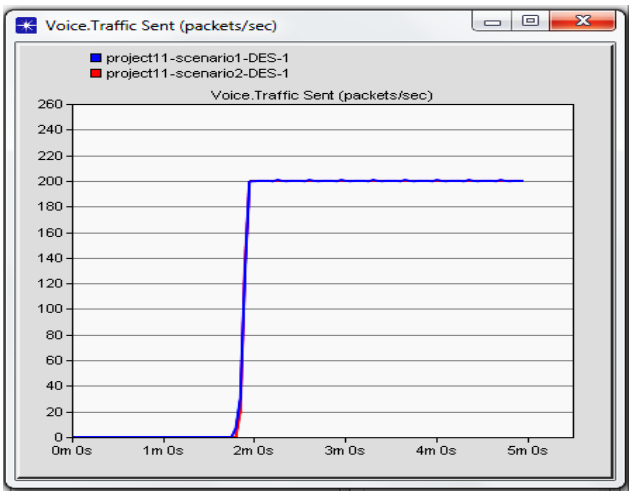
(a) Voice Jitter



b) Voice Packet end to end delay



(c) Voice Traffic Received (packet/sec)



(d) Voice Traffic Send (packet/sec**)**

Table 1: Comparison between Effect Firewall and VPN on VoIP QoS.

Parameters	**Firewall**	**VPN**
Voice Jitter (sec)	0.00000060	0.0
Voice Packet End-to-End Delay (sec)	0.186	0.106
Voice Traffic Received (packets/sec)	200	200
Voice Traffic Sent (packets/sec)	200	200
Packet loss	0.0	0.0

From the result summarized in Table 1, Traditional Firewall will cause degrade QoS by introduce delay with unacceptable ratio. While the VPN best QoS from Firewall in VoIP networks where introduce delay with acceptable ratio not exceed constraint (0.15 sec). Consequently, running VoIP over a VPN can ensure security and high QoS.

Conclusions

The presented research of the affects some of the Security Mechanisms such as Packet Filter Firewall and Virtual Private Network (VPN) on the Qos VoIP application using

OPNET and analyzed simulations of the results allow to be made conclusions as follows: VPN gives best QoS from Firewall because the values of the parameters that effect on QoS such as: delay, jitter, packet loss to be within the acceptable range.

References

Di Wu (2008), Performance Studies of VoIP over Ethernet LAN, Thesis Msc, Department of Computer and Information Sciences, *Auckland University of Technology,* India .

Enterprise VoIP Security (2006), White Paper, USA, April, 2006, Available in the site: http://www.juniper.net .

Greg S. Tucker (Oct 2004), Voice Over Internet Protocol (VoIP) and Security, Paper in *SANS Institute*.

Haniyeh Kazemitabar, Sameha Ahmed, Kashif Nisar, Abas B Said, Halabi B Hasbullah (2010) , A Survey on Voice over IP over Wireless LAN , Paper in World Academy of Science, *Department of Computer and Information Sciences, University Technology,* Malaysia.

Gouda I. Salama, M. Elemam Shehab, A. A. Hafez, M. Zaki (May 2009),Performance Analysis of Transmitting Voice over Communication Links Implementing IPSec , Paper in *13th International Conference on Aerospace Sciences and Aviation Technology (ASAT),* Military Technical College, Cairo, Egypt.

Qinxia (Alice) He (July 2007), Analyzing the Characteristics of VoIP Traffic, Thesis Msc, Department of Computer Science, *University of Saskatchewan, Canada*.

Furat Nidhal Tawfeeq (March 2009),Network Congestion and Quality of Service Analysis Using OPNET, Thesis, *Department of Information Engineering, Al-Nahrain University.*

Jishu Das Gupta (2005), Performance Issues for VoIP in Access Networks, Thesis Msc, *Department of Mathematics and Computing Faculty of Sciences, University of Southern Queensland.*

Richard Kuhn, Thomas J. Walsh, Steffen Fries (Jan 2005), Security Considerations for Voice over IP Systems, Paper in *National Institute of Standards and Technology (NIST)*.

Timothy Kelly (2005), VoIP for Dummies , Book, Canada.

Andrew Williams (2006) , Practical VOIP Security , Book.

Samara Isam Saeed Banno (Sept 2008), Simulation of a VPN Intranet for University Campus, Thesis, Department of Information Engineering, *Al-Nahrain University.*

Gulfam Asghar (June 2010), Security Issues of SIP, Thesis, *Department of Communication, Blekinge Institute of Technology*.

KeerthiPramukh Jannu , Radhakrishna Deekonda (June 2010) , OPNET Simulation of Voice over MPLS with Considering Traffic Engineering Thesis , Department Electrical Engineering , *Blekinge Institute of Technology, Sweden*