Performance Analysis of VOIP over GRE Tunnel

Article *in* International Journal of Computer Network and Information Security · November 2015

DOI: 10.5815/ijcnis.2015.12.01

3 authors, including:

Bahareh Zarei
Chemnitz University of Technology
9 PUBLICATIONS **33** CITATIONS

SEE PROFILE

I. J. Computer Network and Information Security, **2015, 12, 1-9**
Published Online November 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2015.12.01

Performance Analysis of VOIP over GRE Tunnel

Aria. Asadi Eskandar
Minnesota State University/Department of Computer Information Science, Mankato, MN, U.S.A
Email: aria.asadi-eskandar@mnsu.edu

Mahbubur. R. Syed
Minnesota State University/Department of Computer Information Science, Mankato, MN, U.S.A
Email: {mahbubur.syed@mnsu.edu}

Bahareh. Zarei.M
Technische universität chemnitz/Faculty of Computer Science, Chemnitz Germany
Email: {bahareh.zarei-mohammadzadeh@s2014.tu-chemnitz.de}

***Abstract*—**Voice over IP (VoIP) is commonly known as phone service over the Internet. Any service using public IP network requires certain extent of security. Demand for security in VOIP technology is increasing. VPN is one of the commonly used methods to secure VOIP traffic. In this paper we simulated behavior of a VOIP communication while running over a GRE VPN Tunnel using OPNET Modeler 17.5. During the simulation, such performance parameters as: choice of voice signaling protocol, voice Codec, parameters arising from network QoS (in this study, homogenous vs. heterogeneous network environment) and type of VPN tunneling protocol, were examined. We evaluated performance of VOIP communications in homogenous and heterogeneous network environments, configured based on two different signaling protocols, namely H.323 and SIP. Also, G.711 and G.723 were configured and tested as the choice for voice Codecs. GRE was implemented as the tunneling protocol. Result analysis of this study indicated that GRE Tunnel didn't show a significant increase in such call quality of service (QoS) performance factors as: end-to-end delay, call setup time, or a decrease in call MOS value. Even though in a non-ideal (heterogeneous) network environment, call quality of service (QoS) performance factors shoed poor results; however, there was no significant evidence to suggest that GRE Tunnel is the root cause for such poor results.

***Index Terms*—**Voice over IP, Signaling Protocol, Session Initiation Protocol, H.323 Protocol, Generic Routing Encapsulation Protocol, performance analysis, simulation.

I. Introduction

During recent years we experienced explosive growth of Voice over IP (VOIP) technology. The driving motivation for using VOIP is cost saving, mostly for large companies with pre-existing network infrastructure. Another advantage of carrying voice traffic over IP networks is ability to integrate voice and data in one application [3]. However, transmitting voice over a public IP-based network such as internet has raised many security issues. In the case of VOIP, security concerns can be mutual authentication of called and caller for voice protection, session privacy and encryption (to avoid eavesdropping, sniffing, and man in middle attack), session integrity (to avoid altering VOIP packets), and protection of related data to a VOIP connection such as packets pertaining to billing system. Also, Denials of Service (DoS) attacks in VOIP applications try to bring down the system by over flooding or making it busy by sending large number of call requests [4]. Another security issue is VOIP spam which is similar to Email spam. In this case spammers will overflow voice mail inboxes with unwanted message.

Some techniques have been proposed to handle security issues in IP based communication, but among them employing Virtual Private Network (VPN) is more widely used [7]. However, VPN is expected to have an impact (a negative or positive) on VOIP performance. Other important factors that can affect VOIP service quality are various signaling protocols such as H323, and SIP; audio codecs used such as G.711, G.729, G.728, G.726, etc., and related encoding algorithms such as PCM (Pulse Code Modulation), Adaptive Differential PCM, etc. VPN protocols that can be employed are PPTP, L2TP, IPsec and GRE. Clearly, depending on the choice of VPN tunneling protocols, type of services provided to VOIP packets- by VPN- will differ and therefore each VPN protocol is supposed to have a different impact on VOIP performance. Some prior research papers have investigated impact of signaling protocol and/or choice of audio CODECs on quality of VOIP service. In this paper we examined role of VPN protocols as one of QoS parameters in VOIP a communication. We used OPNET to simulate the behavior of a VOIP system while running over IP VPN tunnel.

II. Literature Review

A. Related Works

Telecommunication standardization bodies such as International Telecommunications Union (ITU-T) and several researchers have outlined a number of contributing factors in Quality of Service (QoS) for a voice connection. These factors include ITU-U codecs and algorithms, end-to-end delay, jitter (also known as delay variation), packet loss, and network design [2, 11-12]. According to ITU-U guidelines, a voice call facing a delay greater than 150 ms (note: some authors refer to 200 ms) and/or a jitter of greater than 20 ms is not considered to be of a good quality, and accordingly any voice call facing delay of greater than 300 ms and/or a jitter of greater than 50 ms is considered to be of a poor quality [13].

Table below outlines the accepted voice quality measures.

Table 1. ITU-T VoIP Quality Measurement [13]

Network parameter	Good	Acceptable	Poor
Delay (ms)	0-150	150-300	> 300
Jitter (ms)	0-20	20-50	> 50

There are a numbers of related studies in the field which investigated performance of VOIP calls in different network environments along with different signaling protocols, voice codecs, QoS parameters and security protocols. Muhamad Amin [11] conducted a study with regards to three aspects of VOIP communications, namely call signaling protocols (H323 and SIP), VPN protocols, and network environment (Ethernet and WLAN). From the security prospective authors used VPN with two distinct tunneling protocols namely IPsec and PPTP. According to the results congestion was found to negatively impact voice quality parameters such as delay and jitter. VPN reported to have a similar effect on voice traffic. In a non-ideal network environment, the voice quality parameters even showed worse results compared with an ideal network environment.

Another interesting study in the field is presented by Ibrahim S. I. Alsukayti and Timothy J. Dennis [7]. They compared performance of VOIP while running over BGP/MPLS VPN network with that of VOIP while running MPLS network. BGP/MPLS VPN is a VPN technology which integrates Multiprotocol Label Switching (MPLS) features with security aspects of VPN. Results of the paper suggested that not only a VPN over BGP/MPLS has a positive impact on VOIP quality but also positively improves performance of VOIP as compared with its performance over an MPLS network. Regarding different VOIP codecs, a comparison has was done between G.711, G.723.1 and G.729A, over the BGP/MPLS VPN network model and the comparison result showed that G.729A (bit rate = 8 kb/s) is the best choice of voice codec for such a scenario (i.e. BGP/MPLS VPN) due to bringing a balance between end-to end delay and bandwidth efficiency.

Gouda I. Salama et al., [2] examined "impact of IPsec on the quality of transmitting voice over communication links using OPNET simulator". Result of their research showed the IPsec results in an increase in packet loss, end to end delay, call setup time, and jitter.

Barbieri et al., [10] proposed to reduce size of IPsec encapsulated packets (actual IP packet inside IPsec header) by almost 4 bytes using compression. This will address Quality of Service for IPsec transmitted packets over IP network. This approach, whoever, is criticized by Gouda I.Salama et al., [10] for neglecting actual compression time, which in turn will lead to a processing delay that might be even larger than encryption delay.

Shankar R. R [1] performed a comparison among three commonly used VOIP codecs used in peer to peer VOIP networks and found that G.729 is a better choice for VOIP applications, because it requires lower bandwidth as compared to G.711 and G.723. In another study by Henning and Jonathan Rosenberg [14], a comparative examination of the services, complexity, extensibility and scalability of the two protocols: SIP and H.323 was performed. Findings of the study suggested that SIP and H.323 provides similar services, but SIP showed less complexity, and better extensibility and scalability [14].

Last but not least, in a study performed by A. Asadi Eskandar, Mahbubur. R. Syed , and M.B. Zarei [15], impact of parameters arising from network in performance of SIP over IP VPN was examined. According to the study, VPN doesn't necessary brings the VOIP performance. For example VPN showed no negative impact in call setup time if SIP proxy servers are located in the same network segment as end-point (caller and callee) SIP phones are located. Also, findings of the study suggested that use of VPN in combination with a proper design (in the case of the above mentioned experiment, proper placement of SIP Proxy Servers) can actually improve the VOIP performance [15].

B. Voice Codec

CODEC (Coder/Decoder) is one of the essential components of VOIP. At the sender side, CODECs converts analogue voice signals to digital signals, compresses and encodes to predetermined format. ITU-T introduced and standardized various CODECs. Most commonly used ones are G.711, G.722, G.723.1 and G.729A each working with different bit rate and vary in performance [4], as detailed below:

- G.711: Minimum bandwidth needed is 128 kbps and its speech transmission is precise.
- G.722: Different compression is possible
- G.723.1: Voice quality is high but consumes high processor power
- G.726: Version of G.723 and G.721
- G729: Has efficient utilization of bandwidth. License required.

Table 2, contains a list of some VOIP's CODESs and their related bandwidth [1]:

Table 2. VOIP CODECs and Relevant Bandwidth

CODEC	Bandwidth (kbps)
G.711	64
G.722	64
G.723.1	6.3
G.726	32
G.728	16
G.729	8

Mean Opinion Score (MOS) was introduced by ITU-T and represents multimedia quality form user's prospective, ranged 1 (poor) to 5 (excellent) [4].

Each Codec and its relevent MOS is listed in table 3.

Table 3. MOS Related to each Codec

CODEC	Bit Rate (kbps)	MOS
G.711	64	4.4
G.723.1	6.3	3.9
G.726	32	3.85
G.728	16	3.61
G.729	8	3.92

As is shown in table, speech quality degrades in a non-liner manner with the decrease of data rate [1].

Another component of a VOIP connection is packetization in which encoded voice is encapsulated in packets. Each packet contains different headers at different layers, such as real-time Transport Protocol (RTP), User Datagram Protocol (UDP), and Internet Protocol (IP). Fig. 1 illustrates end to end voice transmission in a VOIP system. After encoding and packetization the packets are send out over IP based network and the process repeats reversely in the destination:

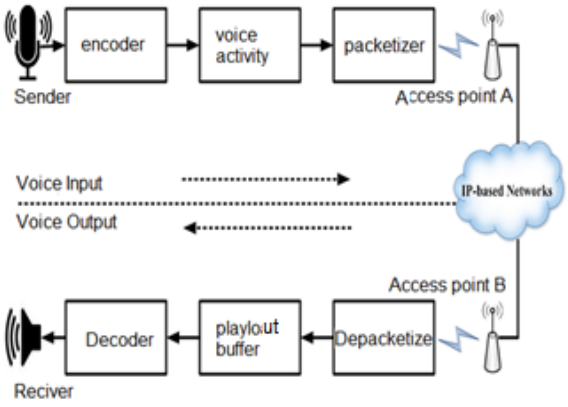

Fig. 1. End-to-End Voice Transmission 1

Playout buffer at the receiver end is used to smooth playout by mitigating the incurred jitter during transmission.

C. H.323 Signaling Protocol

One of the main key areas of a VOIP system is signaling protocol which makes different network elements to communicate with each other, establish and terminate calls [5]. Two commonly used signaling protocols are H.323 protocol suite introduced by ITU-T and SIP by ITEF. H.323 is more common standard and operates over packet switched networks such as IP network [3].

The H.323 protocol suit consists of three main control areas:

- Registration, Admission, and Status (RAS) signaling protocol, also called H.225 Signaling, is a transaction oriented protocol which operates between a H323 terminal or endpoint and a gateway. An endpoint, with the help of RAS protocol can access to a gatekeeper which has address translations. Endpoint can register or unregister with a gatekeeper [5].
- Call control/Call setup: H.225 signaling protocol for call control is used to establish connection between H.323 endpoints.
- H.245 media control and transport: H.245 protocol provides logical channel audio, data and video transmission as well as control channel information [6].

D. SIP Signaling Protocol

SIP (Session Initiation Protocol) is one of the VOIP standard peer to peer protocols which is defined in RFC 2543 and standardized by the IETF MMUSIC Working Group. This protocol contains initiation, termination and also modification standards for user sessions which consist of video or audio elements, online games, instant messaging, virtual reality or generally multimedia elements [1].

SIP configuration includes user agent and proxy server. User agent client creates and terminates requests while user agent server, generates responses after receiving SIP requests. The response can be accept, reject or redirect. Proxy servers can also act as client and generate requests on behalf of other clients. Mainly proxy servers act as routers. Fig. 2, shows SIP components and protocols.

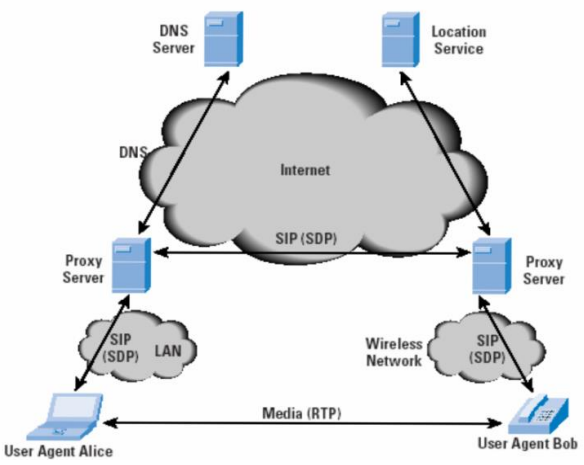

Fig. 2. SIP components

E. Virtual Private Network (VPN)

The VPNs are responsible for providing a secure connection through a public network like the internet. VPN employs a functionality known as IP tunnel that is a virtual point to point link between two end nodes, which may be located in different networks with number of intermediate networks in between [9].

There are a number of different tunneling protocols such as GRE (Generic Routing Encapsulation), PPTP (Point-to-pint Tunneling Protocol), L2TP (layer 2 Tunneling Protocol), IPsec (IP security) and SSTP (Secure Socket Tunneling Protocol).

GRE is a tunneling protocol developed by Cisco and provides encapsulation of a wide range of network layer protocols inside point to point links. GRE tunnels are normally established between a source and destination router with packets encapsulated with GRE header [8]. Fig. 3 illustrates packet encapsulation in GRE.

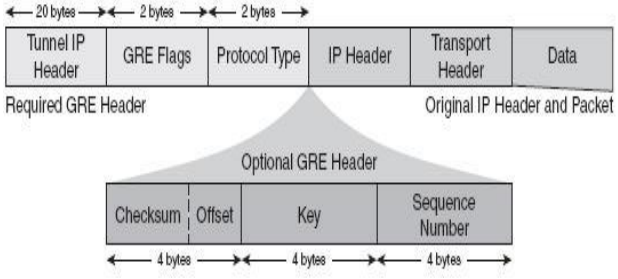

Fig. 3. Packet Encapsulation in GRE

III. Methodology

For the purpose of this research we employed simulation to conduct the research. Simulation is valid approach to model a real scenario or a system. By simulating a system expected behavior of the system under different conditions can be studied. Simulation is valid approach to model a real scenario or a system. By simulating a system expected behavior of the system under different conditions can be studied. In this study we utilized OPNET Modeler as the simulation tool. OPNET Modeler is powerful simulation tool which has been adopted by researchers (and also in the industry), offering a complete simulation and development environment for simulation and modeling the communication networks. OPNET Modeler provides discrete event simulation feature, which can be used to study the performance and behavior of a model. By utilizing OPNET Modeler's GUI, different hypothetical scenarios can be configured and studied. For modeling and simulation of a network topology, OPNET Modeler offers three main editors at network level, Node level and Process level. Network-level editor provides high level modeling for deisgn and creation of the network(s) to be studied. Node-level editor can be used to model and define the behvaoir and flow structure of ineteranl modules within a network level componet. Procees-level editors repersents Finite State Machine decsitiptions and C/C++ source codes realted to each state of the process model [16].

In this section we describe the simulation process and the network topology. OPNET Modeler version 17.5 was used as our simulator. Created and configurated Network topology in this work is shown in fig. 4.

The network topology, shown in fig.4 represents three network segments or sites, namely A, B, and C. Each network segment has a router, an access layer (Layer 2) switch. Site-A (bottom-right) and Site-B (bottom-left), each, has one IP phone device (generating VOIP traffic) and one PC (generating data traffic. Site-C (top-center) has either a H.323 Gatekeeper or a SIP-Proxy Server (based on the running signaling protocol in different scenarios) and one server, which will receive and send packets to and from PCs located in site A and B. Each site (network segment) is connected via IP network cloud (resembling Internet). In this work we studied and evaluated impact of different factors such as signaling protocols (i.e. H.323 and SIP), VPN Tunneling protocols (i.e. GRE), and voice codecs (i.e. G.711 and G.723) –as identified by prior research- that play a role in quality of a VOIP communication. There are two general network scenarios: 1) with VPN tunneling and 2) without VPN tunneling. VPN tunneling protocol used in this experiment is GRE. Each of the scenarios is simulated with two different profiles, namely, data and voice. As the names suggest a voice profile was assigned to each IP phone and the data profile was assigned to each PC. Data profile included mix traffic of such applications as Web, Email, Database and File Transfer. IP phones were configured to strictly communicate to each other and PCs were configured to send/receive traffic to/from the Server located in Site-C (top-center).

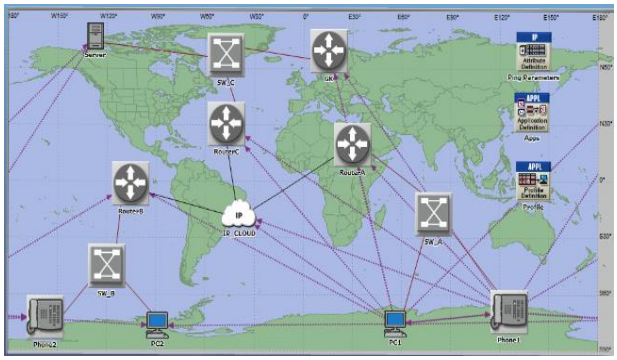

Fig. 4. VOIP simulated Network Configuration

To exlude impact of scuch factors as network congestion of we chose to configure and generate light traffic pattern during simulation in all scenarios (i.e. with VPN and without VPN). Data traffic was generated and sent in serial order throughout the simulation with unlimited repetitions and applications running simultaneously. In the case of voice traffic, 15 phone calls were generated in serial order; each call had a duation of 180 seconds. Configured profiles for Data traffic are shown in fig. 5 and fig. 6, respectively. Fig. 7 and 8 repserenst voice Codec atributes for G.711 and G.723 Codesc, respectovely. Lastly, fig. 9, represents global configuration and IP addressing scheme where VPN tunnel is established.

DATA	
Profile Name	DATA
Applications	(...)
Number of Rows	5
Database Access (Light)	...
Email (Light)	...
Video Conferencing (Light)	...
Web Browsing (Light HTTP1.1)	
Name	Web Browsing (Light HTTP1.1)
Start Time Offset (seconds)	uniform (5,10)
Duration (seconds)	End of Last Task
Repeatability	(...)
Inter-repetition Time (seconds)	exponential (300)
Number of Repetitions	Unlimited
Repetition Pattern	Serial
File Transfer (Light)	...
Operation Mode	Simultaneous
Start Time (seconds)	uniform (100, 110)
Duration (seconds)	End of Last Application
Repeatability	Once at Start Time

Fig. 5. Configured Data Profile

Profile Configuration	(...)
Number of Rows	2
VOIP	
Profile Name	VOIP
Applications	(...)
Number of Rows	1
Voice over IP Call (PCM Quality)	...
Operation Mode	Serial (Ordered)
Start Time (seconds)	constant (60)
Duration (seconds)	End of Last Application
Repeatability	(...)
Inter-repetition Time (seconds)	constant (60)
Number of Repetitions	constant (15)
Repetition Pattern	Serial

Fig. 6. Configured VOIP Profile

Fig. 7 and Fig. 8 show voice Codec attributes running during simulation.

Attribute	Value
Voice Encoder Schemes	(...)
Number of Rows	46
PCM	...
PCM	
Codec Type	PCM
Name	G.711 (silence)
Frame Size (secs)	10 msec
Lookahead Size (secs)	0 msec
DSP Processing Ratio	1.0
Coding Rate (bits/sec)	64 Kbps
Speech Activity Detection	Enabled
Equipment Impairment Factor (Ie)	unknown
Packet Loss Robustness Factor (Bpl)	default

Fig. 7. G.711 voice Codec attribute

MP-MLQ	
Codec Type	MP-MLQ
Name	G.723.1 6.3K (silence)
Frame Size (secs)	30 msec
Lookahead Size (secs)	7.5 msec
DSP Processing Ratio	1.0
Coding Rate (bits/sec)	6.3 Kbps
Speech Activity Detection	Enabled
Equipment Impairment Factor (Ie)	15
Packet Loss Robustness Factor (Bpl)	16.1

Fig. 8. G.723 Voice Codec attributes

Fig. 9, represents global configuration and IP addressing scheme where VPN tunnel is established.

Preview

	Subnet ID	Member Address	Member Node	Interface Name	Is Router?
1	10.1.2.0/24	10.1.2.1	RouterB	Tunnel0	Yes
2	10.1.1.0/24	10.1.1.1	RouterA	Tunnel0	Yes
3	192.168.3.0/24	192.168.3.1/24	RouterC	IF0	Yes
4	192.168.1.0/24	192.168.1.10/24	Phone1	IF0	No
5		192.168.1.11/24	PC1	IF0	No
6	192.168.2.0/24	192.168.2.10/24	Phone2	IF0	No
7		192.168.2.11/24	PC2	IF0	No
8		192.168.2.1/24	RouterB	IF0	Yes
9	192.1.3.0/24	192.1.3.1/24	RouterC	IF10	Yes
10		192.1.3.2/24	IP_CLOUD	IF1	Yes
11	192.168.3.0/24	192.168.3.10/24	GK	IF0	Yes
12		192.168.3.11/24	Server	IF0	No
13	192.168.1.0/24	192.168.1.1/24	RouterA	IF0	Yes
14	192.1.2.0/24	192.1.2.1/24	RouterB	IF10	Yes
15		192.1.2.2/24	IP_CLOUD	IF0	Yes
16	192.1.1.0/24	192.1.1.1/24	RouterA	IF10	Yes
17		192.1.1.2/24	IP_CLOUD	IF2	Yes

Fig. 9. Global Configuration – VPN Established

IV. Results

In the first set of simulation experiment (i.e. Experiment.1HHO: scenario 1.1 and scenario 1.1.V), H.323 signaling protocol in combination with G.711 voice Codec in a homogenous network environment (i.e. voice traffic, in this study) was configured and impact of VPN (GRE tunnel, in this study) was investigated. Result analysis of the experiment showed that VPN, in this case GRE tunnel, in this set of experiment, did not show a significant impact on end-to end delay and jitter, But GRE Tunnel increased call setup time by 0.4 Seconds. Call quality (MOS) also was not affected by GRE Tunnel. In the second set of simulation experiments (i.e. Experiment.1HHE: scenario 1.2 and scenario 1.2.V), H.323, in conjunctions with G.711 in a heterogeneous network environment (i.e. data, mixed with voice traffic) was configured and impact of VPN (GRE tunnel, in this study) was examined. In this set of experiment (i.e. Experiment.2HHE), call set up time was increased slightly with GRE Tunnel, but end-to-end delay and voice quality remained unchanged (same as pervious experiment). In this set of experiment, however negative jitter was observed. Based on the findings from Experiment.1HHO and Experiment.1HHE, the end-to-end delay time in Experiment.1HE, where GRE Tunnel is established, was much greater than that of Experiment.1HHO, where no GRE Tunnel was in place. Likewise, MOS value in Experiment.1HHE was much greater than MOS value in Experiment.1HHO. Based on the comparative result analysis of Experiment.1HHE and Experiment.1HHO, the end-to-end delay and MOS value were not acceptable in a non-ideal (heterogeneous) network environment. Table 4, summarizes result analysis of impact pf GRE Tunnel in Experiment.1HHO and Experiment.1HHE.

In the next set of experiments (i.e. Experiment.2SHO: scenario 2.1 and scenario 2.1.V), in order to experiment and evaluate impact of GRE Tunnel on a SIP-based VOIP communication, we configured SIP signaling protocol and G.711 voice Codec in a homogeneous network environment (i.e. voice traffic, in this study). Result analysis of this experiment (i.e. Experiment.2SHO) showed no indication that GRE Tunnel may lead to

lowering the VOIP performance in terms of end-to-end delay, call setup time, jitter and MOS. Subsequently we performed the next set of experiment (i.e. Experiment.2SHE: scenario 2.2 and scenario 2.2.V) in which SIP was configured as the choice of signaling protocol and G.711 was configured as the voice Codec, in a heterogeneous network environment, where non-VOIP traffic (i.e. web, email, database, and FTP generated along with voice traffic in the network. Based on result analysis of this experiment (Experiment.2SHE), GRE Tunnel didn't increase QoS parameters, under investigation (i.e. end-to-end delay, call setup time, and MOS value). However, in this experiment, similar to Experiment.2HHE, we noticed a negative jitter value. In summary, performance values for Experiment.2SHE (scenario 2.2 and scenario 2.2.V) indicated that GRE Tunnel did not bring any performance issues (excluding observance of negative jitter values) in both homogeneous and heterogeneous network environments. However, in a heterogeneous (non-ideal) network environment, performance values are not acceptable. For example in scenario 2.2 and 2.2.V, the values for end-to-end delay were 5 seconds. Likewise MOS call values were 1.0 (one). According to standard voice quality measures (as outlined in tables 1 and table 3), the values for the non-ideal environment (in this study, scenarios 1.2, 1.2.V, 2.2, and 2.2.V) indicated a poor VOIP quality. Table 4, summarizes result analysis of impact pf GRE Tunnel in Experiment.2HSO and Experiment.2HSE. Table 5, provides a summary of comparative analysis on impact of GRE tunnel on different VOIP call quality measure in different scenarios (i.e. H.323 vs. SIP and homogenous vs. heterogeneous network environments).

Table 4. Result Summary- Experiment.1HHO and Experiment.1HHE

Experiment	Scenario	Signaling Protocol	Voice Codec	Traffic Type	VPN Established [Yes/No]	QOS Performance [Delay][CST*][MOS**]	Result
1HHO	1.1	H323	G.711	Homogeneous	No	Acceptable [delay: 250 ms, CST: 1.9 sec, MOS: 2.85]	VPN didn't show a significant impact on call quality
1HHO	1.1.V	H323	G.711	Homogeneous	Yes	Acceptable [delay: 250 ms, CST: 2.3 sec, MOS: 2.8]	
1HHE	1.2	H323	G.711	Heterogeneous	No	Poor [delay: 3400 ms, CST: 1.9 sec, MOS: 1.5]	VPN didn't show a significant impact on call quality. Call QOS measures are very poor when traffic is heterogeneous
1HHE	1.2.V	H323	G.711	Heterogeneous	Yes	Poor [delay: 3400 ms, CST: 2.0 sec, MOS: 1.5]	
2SHO	2.1	SIP	G.711	Homogeneous	No	Acceptable [delay: 250 ms, CST: 19 sec, MOS: 2.85]	VPN didn't show a significant impact on call quality
2SHO	2.1.V	SIP	G.711	Homogeneous	Yes	Acceptable [delay: 250 ms, CST: 22 sec, MOS: 2.85]	
2SHE	2.2	SIP	G.711	Heterogeneous	No	Poor [delay: 5000 ms, CST: 32 sec, MOS: 1]	VPN didn't show a significant impact on call quality. Call QOS measures are very poor when traffic is heterogeneous
2SHE	2.2.V	SIP	G.711	Heterogeneous	Yes	Poor [delay: 5000 ms, CST: 32 sec, MOS: 1]	

* CST: Call Setup Time
* *MOS: Mean Opinion Score

In this study we also performed a comparative analysis on impact of GRE Tunnel on performance of VOIP communications, where H.323 is the signaling protocol, in a homogenous environment between G.711 and G.723 voice Codecs. Based on result of this comparative analysis, G.723 showed higher end-to-end delay and lower voice quality (in terms of MOS value). G.711, despite consuming more bandwidth, showed better performance (i.e. significantly lower end-to-end delay and higher MOS value) as compared with G723.

When we performed a comparative analysis on impact of GRE Tunnel on performance of VOIP communications, where SIP is the signaling protocol, in a homogenous environment between G.711 and G.723 voice Codecs, G.711, despite consuming more bandwidth, showed a performance equal to that of G.723. Table 6,

summarizes results of comparative analysis on impact of GRE Tunnel on H.323-based versus SIP-based VOIP communications.

Table 5. H.323 vs. SIP and GRE Tunnel Impact

Experiment	Scenario	Signaling Protocol	Voice Codec	VPN Established [Yes/No]	Traffic Type	QOS Performance [Delay][CST*][MOS**]	Result
1HHO	1.1.V	H323	G.711	Yes	Homogeneous	Delay: 250 ms	VPN didn't show a significant impact on call quality. Call QOS measures are very poor when traffic is heterogeneous
1HHE	1.2.V				Heterogeneous	Delay: 3400 ms	
1HHO	1.1.V	H323	G.711	Yes	Homogeneous	CST: 2.3 sec	
1HHE	1.2.V				Heterogeneous	CST: 2.0 sec	
1HHO	1.1.V	H323	G.711	Yes	Homogeneous	MOS: 2.8	
1HHE	1.2.V				Heterogeneous	MOS: 1.5	
2SHO	2.1.V	SIP	G.711	Yes	Homogeneous	Delay: 250 ms	VPN didn't show a significant impact on call quality. Call QOS measures are very poor when traffic is heterogeneous
2SHE	2.2.V				Heterogeneous	5000 ms	
2SHO	2.1.V	SIP	G.711	Yes	Homogeneous	CST: 22 sec	
2SHE	2.2.V				Heterogeneous	CST: 32 sec	
2SHO	2.1.V	SIP	G.711	Yes	Homogeneous	MOS: 2.85	
2SHE	2.2.V				Heterogeneous	MOS: 1	

* CST: Call Setup Time
** MOS: Mean Opinion Score

Table 6. G.711 vs. G.723, on H.323-based vs. SIP-based VOIP communication

Signaling Protocol	Voice Codec	Traffic Type	VPN Established [Yes/No]	QOS Performance [Delay][CST*][MOS**]	Result
H323	G.711	Homogeneous	Yes	Acceptable [delay: 250 ms, CST: 2.3 sec, MOS: 2.8]	G.711, despite consuming more bandwidth, showed better performance (i.e. significantly lower end-to-end delay and higher MOS value) as compared with G723
H323	G.723	Homogeneous	Yes	Poor [delay: 310 ms, CST: 2.0 sec, MOS: 1.8]	
SIP	G.711	Homogeneous	Yes	Acceptable [delay: 250 ms, CST: 22 sec, MOS: 2.85]	G.711, despite consuming more bandwidth, showed a performance equal to that of G.723
SIP	G.723	Homogeneous	Yes	Acceptable [delay: 250 ms, CST: 22 sec, MOS: 2.85]	

* CST: Call Setup Time
* *MOS: Mean Opinion Score

V. Conclusion and Future Works

In this paper OPNET Modeler 17.5 was used to simulate behavior of a VOIP communication running over a GRE VPN tunnel. Analysis of the result of this study indicated that VPN (in this experiment GRE Tunnel), didn't lead to a significant increase in such quality of service (QoS) performance factors as: end-to-end delay, call setup time, or a decrease in call MOS value. However, in a non-ideal (heterogeneous) network environment, where voice and non-voice traffic coexist together, performance values for end-to-end delay, call setup time and call MOS are not acceptable according to the current standards of voice communication. No significant evidence was found to suggest that such poor results in the heterogeneous network environment can be

attributed to GRE Tunnel. So, it can be concluded that heterogeneity of the network traffic, rather than use and deployment of a GRE Tunnel can be the factor responsible for lowering quality of VOIP in such network settings. We believe that deploying Quality of Service (QoS) features in a network environment can improve quality of VOIP performance. Hence, further experiments evaluating performance of VOIP communications over IP VPN in a non-ideal network environment, where QoS parameters are configured, can provide a better insight pertaining possible performance improvements in VOIP call quality in a non-ideal VPN protected network. In addition, in order to reduce the number of factors impacting performance quality of a VOIP communication, we chose to generate light volumes of voice and non-voice (data) traffic in this experiment. In future works, role of congestion, a common issue in a non-ideal network environment, may also be examined. Therefore, experiments with different traffic distribution pattern, resembling a real life scenario may be insightful for us. Simulation of VOIP over IP VPN in a non-ideal packet switched network, combined with congestion issue and deployment of QoS parameters can provide more realistic figures relating to a real network environment.

REFERENCES

[1] Shankar R. R. Performance Analysis of Different Codecs in VoIP Using SIP in Mobile and Pervasive Computing, 2008.

[2] Gouda I.Salama, M. Elemam Shehab, A. A. Hafez, M. Zaki. Performance Analysis of Transmitting Voice over Communication Links Implementing IPsec in 13th International Conference on AEROSPACE SCIENCES & AVIATION TECHNOLOGY, ASAT- 13,May 2009.

[3] Dalgic, Ismail, and Hanlin Fang. "Comparison of H. 323 and SIP for IP Telephony Signaling." Proc. of Photonics East, Boston, Massachusetts. Vol. 3845. 1999.

[4] Kazemitabar, Haniyeh, et al. "A survey on voice over ip over wireless lans."World Academy of Science, Engineering and Technology 71 (2010): 352-358.

[5] Liu, Hong, and Petros Mouchtaris. "Voice over IP signaling: H. 323 and beyond." Communications Magazine, IEEE 38.10 (2000): 142-148.

[6] Cisco Systems. "Understanding H.323 Gatekeepers", Jul 20, 2006

[7] Ibrahim S. I. Timothy J. Performance Analysis of VoIP over BGP/MPLS VPN Technology in PGNet, 2011.

[8] Ferguson, Paul, and Geoff Huston. "What is a VPN?." April 1998.

[9] Kosta, Y.P.; Dalal, U.D.; Jha, R.K., Security Comparison of Wired and Wireless Network with Firewall and Virtual Private Network (VPN) in Recent Trends in Information, Telecommunication and Computing (ITC),March 2010. pp.281,283

[10] R. Barbieri, D. Bruschi and E. Rosti, Voice over IPsec: Analysis and Solutions in Computer Security Applications Conference and Proceedings. 18th Annual, Dec2002.

[11] Muhamad Amin. A.H. VOIP PERFORMANCE MEASUREMENT USING QoS PARAMETERS in The Second International Conference on Innovations in Information Technology (IIT'05), 2005.

[12] Khaled Alutaibi and Ljiljana Trajković. Performance Analysis of VoIP Codecs over Wi-Fi and WiMAX Networks. In http://www2.ensc.sfu.ca/~ljilja/papers/OPNETWORK, 2012.

[13] J. Yu and I. Al-Ajarmeh, Call admission control and traffic engineering of VoIP in The Second International Conference on Digital Telecommunications (ICDT 2007) in San Jose, California, USA, July 2007. pp. 11–16.

[14] Schulzrinne, Henning, and Jonathan Rosenberg. "A Comparison of SIP and H. 323 for Internet Telephony." Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV). sn, 1998.

[15] A. Asadi Eskandar, Mahbubur R Syed, and M.B. Zarei. SIP over IP VPN: Performance Analysis. In proceedings of WorldComp2014.

[16] Ricardo Reis, "discrete even simulation with application to computer communication system performance" in Information Technology: Selected Tutorials, Volume 157 of IFIP Advances in Information and Communication Techno, Springer, 2006, pp. 289-295.

Authors' Profiles

Aria. Asadi Eskandar earned his Bachelor's degree in Business Administration from Payam Noor University, Isfahan, Iran in the year 2006. Subsequently, he earned his MBA degree, in Multimedia University, Cyberjaya, Malaysia in the year 2011. He continued his education with a Master of Science degree in Information Technology and graduated in the year 2015 from Minnesota State University, USA. He worked as a Network Administrator in IT industry from 2001 to 2006. He is currently employed by a multinational technology and management consulting company in the USA. Deep passion in applied research, aspired him to embark on academic research activities alongside pursuing his career in IT industry.cased.

Mahbubur. R. Syed is currently a professor of Computer Information Science Department at Minnesota State University, Mankato (MSU), USA. He has more than 30 years of experience in teaching, in industry, in research and in academic leadership. He has more than 30 years of experience in teaching, in industry, in research and in academic leadership. Earlier he worked at the North Dakota State University in USA, Monash University in Australia, Bangladesh University of Engineering and Technology (BUET) in Bangladesh and in Hungary. He was a founding member of the Department of Computer Science and Engineering at BUET and served as Head of this Department during 1986-92. He received the UNESCO/ROSTSCA' 85 award for South and Central Asia region in the field of Informatics and Computer Applications in Scientific Research. He has co-edited several books in the area of e-commerce, software agents, distance education, multimedia systems and networking.

Bahareh. Zarei. M has bachelor's degree from Bahonar University of Kerman in the field of Computer Science and her M.Sc degree from Putra Universiti Malaysia in the field of distributed networks in 2014. She is now PhD student in TU Chemnitz in the Distributed and Self Organizing Systems research group. At the moment she is working on web engineering and linked data research topics.

