A Comparison of VoIP Performance Evaluation on different environments Over VPN Multipoint Network

Adel Alharbi, Ayoub Bahnasse, and Mohamed Talea

Laboratory LTI, Faculty of Sciences Ben M'sik, University Hassan II, Casablanca, 9167 Morocco

Summary

VPN Multipoint network is a kind of modern networking that allows the creation of dynamic private IP tunnels between multiple sites automatically، quickly and with less configuration. Like other networks, it is possible to implement various applications on it, such as VoIP application. VoIP is a technique for transmitting voice data over the Internet, many work have been conducted to evaluate the performance of VoIP on different networks by using various environments such as simulation modeling, emulation and laboratory experiment. In order for previous environments to help us in the exact assessment, it is very important that their results match as closely as possible with the reality results. In this paper, we compared between their results for the performance evaluation VoIP on VPN Multipoint network. In the presence of Security. The comparison was performed in terms of average delay, average jitter, average packet loss ratio and average MOS score.

Key words:

VPN multipoint, VoIP, Delay, Jitter, Packet loss, MOS, Simulation, Emulation, Security

1. Introduction

In the past decade, VoIP [1] (Voice over Internet Protocol) is a rapidly growing technology that enables transport of voice over data networks such as internet. This growth is due to the integration of VoIP system over the existing networking infrastructure [2] and low cost. VoIP comes as an answer to the call users who want to benefit of the same speed and quality of service as the network users already have [3]. 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 such as VPN Multipoint. The VPN Multipoint technology is uses mGRE, NHRP, IPSec and routing protocols to create VPNs:

- mGRE:

The mGRE is a mechanism for encapsulating any network layer protocol over any other network layer protocol, mGRE can transport a wide variety of protocols (for example, IP unicast, multicast, and broadcast) but they are static it means that a specification of combination of source and destination of each tunnel is required, mGRE interface is introduced, which serves as a "one-to-many" interface for creation of multiple hub-and-spoke tunnels, mGRE allows multiple destinations (for example, multiple spoke sites) to be grouped into a single multipoint interface.

- Next Hop Resolution Protocol (NHRP):

Next Hop Resolution Protocol (NHRP) [4] is a layer 2 address resolution protocol and cache, like Address Resolution Protocol (ARP) .NHRP is used by a branch router called spoke connected to a non-broadcast ,multi-access (NBMA) sub-network to determine the IP address of the "NBMA next hop" physical address (Public address). Spokes called Next-Hop Client(NHC) is send a registration to the headend router called Hub as their Next-Hop Server (NHS) that contains the tunnel IP address and the NBMA address .NHS creates an entry in its NHRP cache and returns a registration reply towards the Spokes. NHRP permits mGRE tunnel endpoint to get every others physical IP address.

- IPSec Protocol:

Security issue will arise as long as IP networks are developed on shared public communication infrastructure. Data encryption has been presented as a potential solution to the security problems with VoIP call. The IPSec protocol [5] was designed and created by the IETF as the security architecture for the Internet Protocol IP. IPSec is based on two encapsulating 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 [6]. The IPsec protocol operates in two modes, transport mode and tunnel mode, the transport mode does not change the initial header and it is inserted between the network layer and the transport layer of the OSI model. Whereas the Tunnel mode is the default mode, this mode protects the entire IP packet and wraps the original packet, encrypts it, then adds a new IP header before sending it to other sites.

- Routing protocols :

These protocols are used to ensure optimal routing of data [7], [8] and are "responsible" for creating of routing tables and supporting their content [9]. Fig.1 illustrates an

Manuscript received April 5, 2017
Manuscript revised April 20, 2017

example of VPN Multipoint Network consisting of 2 BRANCHs and 1 Headquarters, Branch have a static permanent mGRE tunnel to the Headquarters, and dynamic temporary tunnels between them.

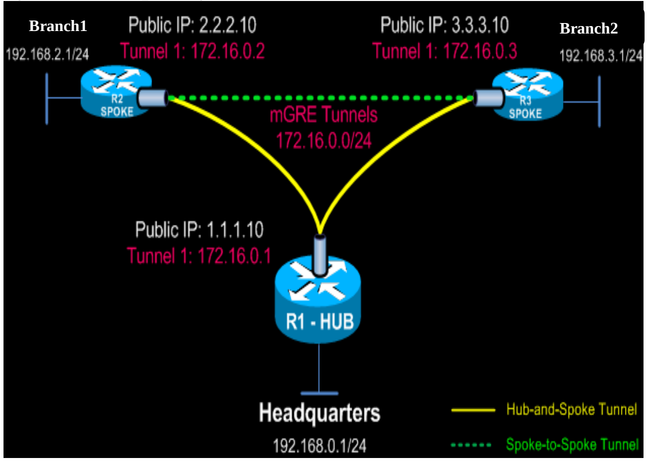


Fig.1 An example of VPN Multipoint Architecture

But when sending voice traffic over IP network, a number of factors contribute to overall voice performance as perceived by an end user. The factors determine voice performance include the MOS [10] (Mean Opinion Score), Perceived voice quality can be measured by a subjective quantity MOS, which varies from 1 (worst) to 5 (best) [4] packet loss, delay and delay variation (jitter). There are three experimental techniques used in the design and validation of the performance of network and application: simulation, emulation and real network testing. All three techniques have unique benefits and drawbacks However, they need not be viewed as competing techniques — using more than one technique and comparing the results obtained can help evaluate better.

2. Related Works

Several works was conducted assessing the performance of VoIP traffic on simulation environment over IP network, MPLS network, Dynamic Multipoint VPN networks, Wireless LAN and WAN network using OPENT [11]–[14], and also over wireline and wireless networks using Network Simulator 2 (ns-2) [15]. Some works are applied many tools such as (GNS3, OPNET) to checks the effect of VoIP traffic over VPN network [16]. Other works implementing simulating and real network for analyzing VOIP [17]. Nevertheless, no work was compared the results obtained, if they were as closely matched as possible with the reality results, this is a good motivation to complete and to enhance the work by comparing the results of performance evaluation of VoIP on VPN Multipoint network using various environments: Simulation, emulation, and in the lab experiment. In the presence of Security.

The paper is organized as follows: in the section 3 we will discuss the tools of work, simulator and emulator, in the section 4 shows the bench test where all the testing was implemented (audio conferences), and in the section 5. We will explain our final results. And we will conclude on the last section.

3. Tools, simulator and emulator

To develop our test, we used the following tools: Netmeeting as the Conferencing software, Omnipeek as the packet sniffer, fillezilla as FTP server and client. Netmeeting was used as the VoIP client as it allows for peer-to-peer communication and we used encryption algorithms through a VPN Multipoint Network. Each packet carrying voice data travelling between the sender and receiver was captured using Omnipeek. The Omnipeek output was the four factors – delay, jitter, MOS and packet loss. In order to be able create the BRANCHs and Headquarters, the PC has:

(i) Processor: Intel Core Duo (or its equivalent), two Ethernet Card,
(ii) Memory: 1GB RAM,
(iii) Space on hard Disk 50 MB,
(iv) Operation system: Linux Ubuntu 14.04 LTI desktop,
(v) Connection: 100 Mbps bandwidth for the LAN and WAN.

The simulation tools is the second environment, are useful for modelling and evaluating network protocols and traffic, provides a repeatable and controlled environment for network experimentation. It is easy to configure and allows a protocol to be constructed at some level of abstraction, making simulation a rapid prototype-and evaluate environment and was possible using the GNS3.

GNS3 is graphical network simulator[18] uses simulation and emulation to allows users to design a network topology based on specific models of different network. In order for it to function, it is dependent on three other programs that must run simultaneous: Dynamips (the core for GNS3 that emulates IOS CISCO image), Dynagen (text-based software that is necessary to Dynamips) and Qemu (open source emulator and virtualization tool).

The emulator [19] is the third environment network. Emulation is the replacement of a real world device with a model at a well-defined interface for the purposes of allowing controlled responses from the emulated real world device. The emulation is "complete" if all the interfaces are present, and the resulting observed behavior matches that of the real world device.

4. Test Scenarios

4.1 Real Network and Results

For assess the performance of VoIP application in VPN Multipoint Network using real work environment, the test network was designed and implemented in a laboratory as shown in Fig.2.The Linux router or Cisco router represented Headquarters called HUB, whereas LANs network are represented by two PCs. PC1 represented client 1 and PC2 represented client 2, both connected via a cables Ethernets to Linux routers or Cisco routers called spokes. PC1 connected Spoke1 and PC2 connected Spoke2. The PCs of LAN as a telephone was possible using Windows NetMeeting utility and this is entirely a real time VoIP traffic and has installed on them.

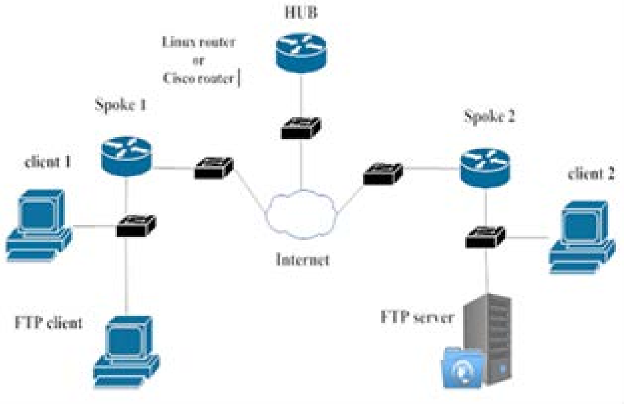


Fig.2 Real Network Topology

In the laboratory scenario, the topology implementation was conducted by establishing a VPN Multipoint tunnel between two clients, and they were successfully contacted. In order to protect the VoIP communication, the encryption protocol AES (Advanced Encryption System) was implemented in our network. AES protocol is the fastest and secure encryption protocol [20]–[22]. It uses a variety of different key length of 128, 192 and 256 bits. For this reason, the encryption protocol AES chosen to lead this assessment, and Hmac-SHA as the integrity mechanism.

for appreciate the behavior of the real time traffic under different traffic loads, we added FTP server generated TCP-FTP traffic through a large files download of 5 G Bytes, we also injected high ICMP traffic load through sending large pings (10000 bytes size). Client FTP was connected with FTP server to download the files through a FTP session. The protocols for multimedia traffic were G.723.1 [23, p. 1] generated by Netmeeting, describes a dual-rate speech coder for multimedia communications. Calls are made between two Netmeeting utility on clients 1 and 2 attached to opposite ends of the LAN, and testing consisted on capturing the VoIP packets that traveled from Client1 with the use of the Omnipeek sniffer. We only considered the VoIP packets coming from the Netmeeting. So as to evaluate the voice perform, we established five real time audio conference. Every audio conference lasted 2 minutes, during that time all multimedia packets were captured making a total of 10 minutes of audio conference packets. The performance assessment was dependent on Average delay, Average Jitter, Average packet loss, Average MOS, they were captured by Omnipeek. The results obtained were.

Table 1: Results VoIP Performance in Real Network

Network parameters	Value
Average one way delay at VoIP receiver (ms)	59.2
Average Jitter of VoIP receiver (ms)	11.4
Average packet loss of VoIP receiver (%)	0.6
Average MOS of VoIP receiver	3.48

4.2 Simulation Moudling and Results

GNS3 is used as the platform for the performance studies. In the scenario of simulation, we used four routers from the Cisco 3700 series platform. Three routers represented the HUB, Spoke1 and Spoke2, one router acted as Internet infrastructure. The two PCs connected Spoke1 and Spoke2. The VPN Multipoint was implemented within three routers (R1, R2 and R3), we used the same configuration in lab experiment. Router has special menu where you can modify certain information. The network topologies for the scenario is shown in Fig.3.

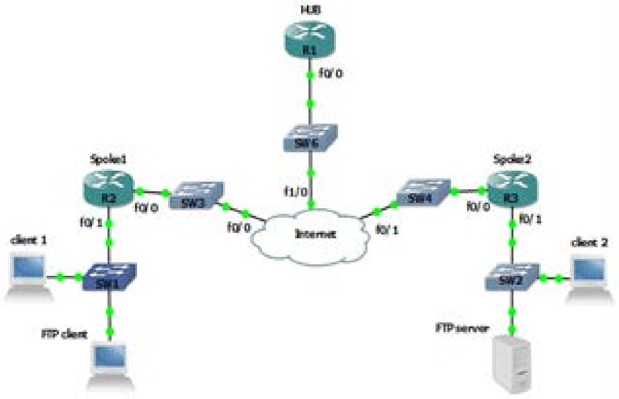
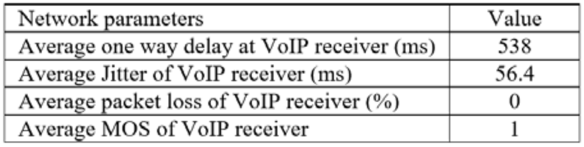


Fig.3 Simulation Network Topology

Once the network is created and works, you can proceed to analyze it with Omnipeek sniffer. To start the capture of packet, you need to choose the interface you are using for the capture. VoIP communication was initiated between client 1 and client 2, and VoIP packets were captured by Omnipeek that came from Client1. The results obtained were:

Table 2: Results VoIP Performance in Simulation Moudling Network



Network parameters	Value
Average one way delay at VoIP receiver (ms)	538
Average Jitter of VoIP receiver (ms)	56.4
Average packet loss of VoIP receiver (%)	0
Average MOS of VoIP receiver	1

4.3 Emulation and Results

Emulation testbed for a VoIP scenario is established using once again GNS3. The scenario was created consisting of five PCs. The three PCs were a virtual machines, they were running on a Linux OS based on the Ubuntu 14.04 desktop distribution which acted like a routers, and were installed Quagga and Zebra Linux daemon which responsible to generate routing protocols such as RIP, OSPFv3 and BGP , and were installed racoon which responsible to generate security parameters . And two PCs were installed with VMware Workstation with two images .This means that every PC represented client. Both clients were installed with Windows XP SP3, were generated voice traffic by using Netmeeting utility. All machines were configured
with dual- socket, quad-core 2.1GHz Intel processors, 400 MB of RAM, and 100 Mbps Broadcom NICs. The scenario was to test the performance VoIP between the traffics transfer from a client 1 to client 2 through a VPN Multipoint Network tunnel. The network topologies for the scenario is shown in Fig.4:

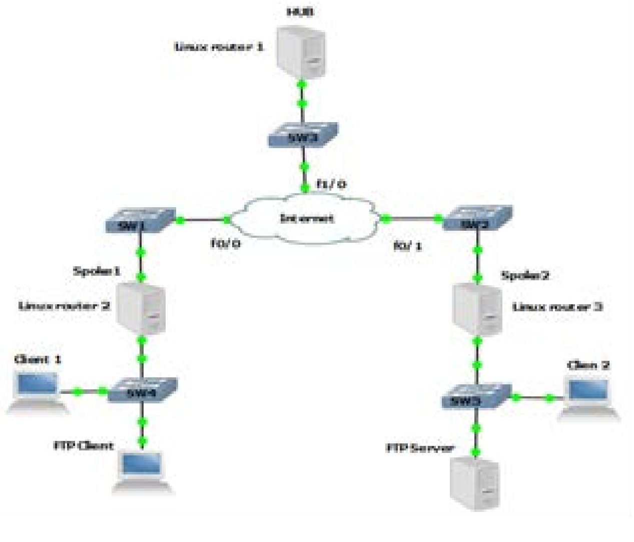
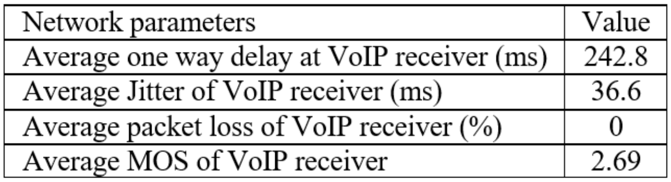


Fig.4 Emulation Network Topology

The packet transfer between VoIP source and receiver is captured using network analyser Omnipeek. The results obtained were:

Table 3: Results VoIP Performance in Emulation Network



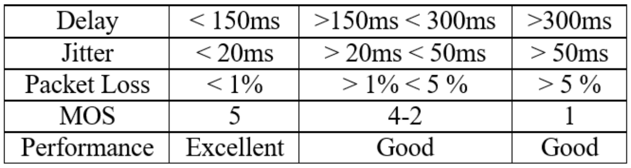
Network parameters	Value
Average one way delay at VoIP receiver (ms)	242.8
Average Jitter of VoIP receiver (ms)	36.6
Average packet loss of VoIP receiver (%)	0
Average MOS of VoIP receiver	2.69

Delay, jitter, packet loss and MOS recommended by the ITU (International Telecommunications Union) for performance from excellent to poor.

5. Results and Discussion

Before presenting and analyzing the results of our study, a presentation of possible VOIP values for delay, jitter, packet loss and MOS recommended by the ITU (International Telecommunications Union) for performance from excellent to poor.

Table 4: ITU Recommended Values for VoIP



Delay	< 150ms	>150ms < 300ms	>300ms
Jitter	< 20ms	> 20ms < 50ms	> 50ms
Packet Loss	< 1%	> 1% < 5 %	> 5 %
MOS	5	4-2	1
Performance	Excellent	Good	Good

Fig.5 shows the results obtained by degree of delay for three environments settings. As the diagram shows, implementing the simulation environment generates higher delay, about 98%, compared with lab environment, and about 45%, compared with emulation environment. On the other hand, Implementation of emulation was have delay acceptable. The graph also indicates that the implementation of lab environment, the degree of latency is lower compared to a simulation and emulation environment. This figure reveals that implementing a simulation is the worst performing evaluation in terms of delay, while lab environment has the least degree of delay.

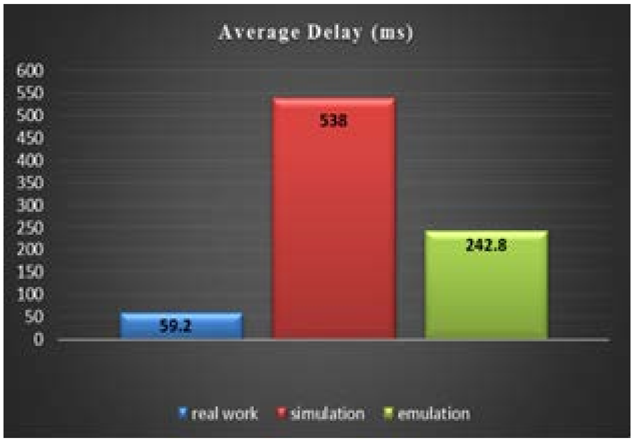


Fig.5 Average Delay in three environments

Fig.6 shows the degree of jitter ratios. It could be noticed that the delay variation (jitter) is approach to 56.4 ms for simulation, 36.6 ms for emulation, and 11.4 ms for lab environment. The jitter is high for simulation, whereas the jitter is acceptable for emulation, remained around 36.6 ms .In a lab environment, the degree of jitter is reduced drastically. Our experiments show that using a lab environment generally has a lower degree of jitter compared with simulation and emulation. The management plan is composed of four agents: (i) Subscriber Agent, (iii) Policy Definition Agent, and (iv) Policy Attr

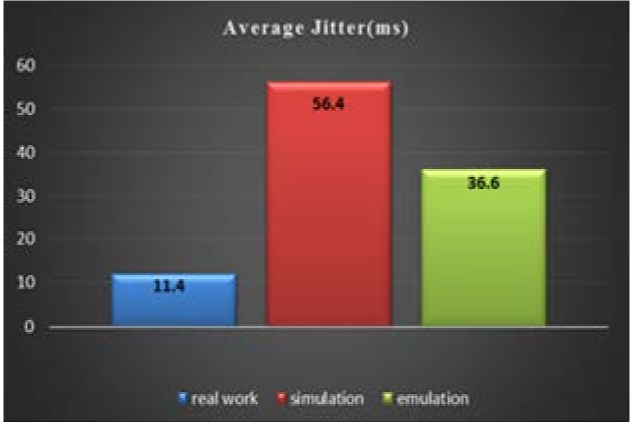


Fig.6 Average Jitter in three environments

The third important parameter considered was the packet loss. As seen in Fig.7 the packets loss was similar, about 0 %, for simulation and emulation environments. In the lab environment generated less than 1% of packet loss, which has always been in the limit of the requirements of VoIP.

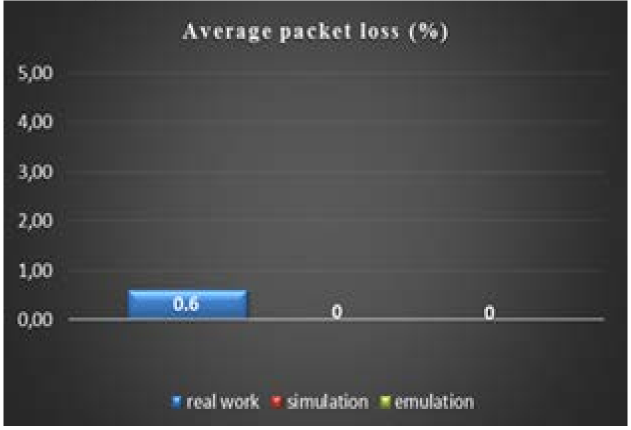


Fig.7 Percentage of packet loss

Fig.8 illustrate the MOS on three scenarios, we can notice that the lab test had the best MOS value, whereas the simulation has the worst MOS value. At emulation environment, testbed results were close with the lab results.

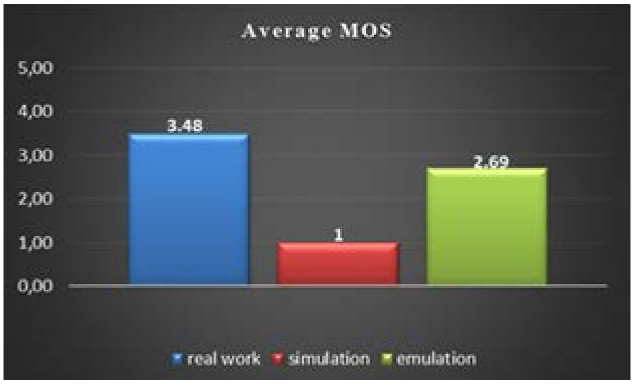


Fig.8 Average MOS

6. Conclusion

In this project, we have evaluated the performance of VoIP under different environment. The implementation was by using simulation modeling, emulation and laboratory experiment over VPN Multipoint Network with VoIP application. The results obtained of the three environments were compared successfully conducted. Overall, the performance of emulation and lab was slightly convergent. On one hand, the evaluation of VoIP in a Jitter parameter using emulation and lab testbed was lower than the simulation. Furthermore, we found that the delay parameter for simulation results may not evaluate the performance VoIP correctly. We can also observe that the result of MOS in lab work and emulation was close to each other, and it is far from simulation. For packet loss, results showed that the percentage of packet loss in simulation and emulation were similar about 0% , while they were different from the result obtained in lab work, but it does not effect on VoIP performance. On the basis of previous comparisons, we can conclude that the laboratory environment provides the good assessment for the Performance VoIP over VPN Multipoint Network under VoIP traffic encryption.

References

[1] A. Prakash, “Voice Over Internet Protocol (VoIP)”.
[2] J. Davidson, Voice over IP fundamentals. Cisco Press, 2006.
[3] H. P. Singh, S. Singh, J. Singh, and S. A. Khan, “VoIP: State of art for global connectivity—A critical review,” J. Netw. Comput. Appl., vol. 37, pp. 365–379, 2014.
[4] J. Luciani, D. Katz, D. Piscitello, B. Cole, and N. Doraswamy, “NBMA next hop resolution protocol (NHRP),” 1998.
[5] K. Seo and S. Kent, “Security architecture for the internet protocol,” 2005.
[6] S. Kent, “IP encapsulating security payload (ESP),” 2005.
[7] R. Asati, M. Khalid, A. E. Retana, D. Van Savage, and P. P. Sethi, System and method for using routing protocol extensions for improving spoke to spoke communication in a computer network. Google Patents, 2013.

[8] H. Chen, “Design and implementation of secure enterprise network based on DMVPN,” in Business Management and Electronic Information (BMEI), 2011 International Conference on, 2011, vol. 1, pp. 506–511.

[9] J. Doyle, “Dynamic Routing Protocols,” CCIE Routing TCPIP, vol. 1, no. 8, 2001.

[10] [10] I. Recommendation, “800, Methods for subjective determination of transmission quality,” Int. Telecommun. Union, 1996.

[11] M. Babu, “Performance Analysis of IPSec VPN over VoIP Networks Using OPNET,” Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 2, no. 9, 2012.

[12] A. A. Eskandar, M. R. Syed, and M. B. Zarei, “SIP over IP VPN: Performance Analysis,” in Proceedings on the International Conference on Internet Computing (ICOMP), 2014, p. 1.

[13] [13] R. S. Naoum and M. Maswady, “Performance Evaluation for VOIP over IP and MPLS,” World Comput. Sci. Inf. Technol. J. WCSIT, vol. 2, no. 3, pp. 110–114, 2012.

[14] [14] A. M. Alsahlany, “Performance analysis of VOIP traffic over integrating wireless LAN and WAN using different codecs,” ArXiv Prepr. ArXiv14072025, 2014.

[15] A. Bacioccola, C. Cicconetti, and G. Stea, “User-level performance evaluation of voip using ns-2,” in Proceedings of the 2nd international conference on Performance evaluation methodologies and tools, 2007, p. 20.

[16] A. Ashraf, M. Wasim, and A. R. Sattar, “Efficient Implementation of VoIP Over VPN wrt Packet Delay and Data Security.” Int. J. Multidiscip. Approach Stud., vol. 3, no. 5, 2016.

[17] B. Enache and I. Giea, “A Method for Implementing, Simulating and Analyzing a Voice over Internet Protocol Network.” Acta Electroteh. vol. 56, no. 3, 2015.

[18] J. Grossman, B. Marsili, C. Goudjil, and A. Eromenko, GNS3 graphical network simulator. 2013.

[19] “Emulator - Wikipedia.” [Online]. Available: https://en.wikipedia.org/wiki/Emulator#Emulation_versus_simulation. [Accessed: 23-Mar-2017].

[20] A. Nadeem and M. Y. Javed, “A performance comparison of data encryption algorithms,” in Information and communication technologies, 2005. ICICT 2005. First international conference on, 2005, pp. 84–89.

[21] P. Ding, “Central Manager: A Solution to Avoid Denial Of Service Attacks for Wireless LANs.” IJ Netw. Secur., vol. 4, no. 1, pp. 35–44, 2007.

[22] D. S. A. Elminaam, H. M. Abdual-Kader, and M. M. Hadhoud, “Evaluating the performance of symmetric encryption algorithms.” IJ Netw. Secur. vol. 10, no. 3, pp. 216–222, 2010.

[23] I. ITU, “723.1: Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s,” Telecommun. Stand. Sect. ITU, 1996.

Adel ALHARBI received his B.Sc. degree in electronic and communication from Mohamed Khaider University, Algeria, in 2004 and 2010 and M. Sc. degrees in electronic from the Hassan II University, Morocco, in 2014 and 2016 respectively. Currently, he is a Ph.D student in Hassan II University, Morocco. He is a member of the Information Treatment Laboratory in the faculty of science Ben M′sik, Morocco.

Ayoub BAHNASSE Ph.D. on Networks and telecommunication, received the master degrees, in 2013 and 2017 respectively. Actually a researcher associate on LTI laboratory, Software Engineering and Telecommunications Team at Ben M’sik faculty of sciences Reviewer on ELSEVIER journals. His research fields are: Security of networks, mobile learning, Wireless Sensor networks, QoS of networks, MPLS, IMS and NGN.

Mohamed TALEA received his Ph. D. degree in physics from Poitiers University, France, in 2001, he obtained a Doctorate of High Graduate Studies degree from the Hassan II University, Morocco, in 1994. Currently, he is a Professor in the department of physics at Hassan II University, Morocco, and he is the Director of Information Treatment Laboratory. He has published about 20 refereed journal and conference papers. His research interest covers Systems engineering, security of system information.