Evaluation of the Scalability of the Protected Multipoint Dynamic VPN by IPsec in a WiMax Network

Najib El Kamoun[†], Ayoub BAHNASSE[††], and Faycal BENSALAH[†]

[†]lab STIC, Faculty of Sciences El Jadida, Chouaib Doukkali University, El Jadida, Morocco
[††]Lab LTI, Faculty of Sciences Ben M'SIK, Hassan II of Casablanca University, Casabanca, Morocco

Summary
Wireless network technologies, specifically 802.16e technology, have been imposed recently thanks to the wide range, the broadband and especially the mobility offered compared to other wireless networks. However, this technology like other wireless, suffers from several weaknesses especially in terms of security and quality of service. The IPsec standard can be used to mitigate security deficiency, but this standard adds additional latencies to the network and the applications being transported. Some work has addressed and studied the effect of site-to-site IPsec VPN tunneling on the same networks. However, with modern networks, which can contain a very large number of WiMax antennas, these VPN tunnels cannot guarantee and respond easily to scalability. The DMVPN technology meets this limit, it allows to create multiple IPsec VPN tunnels in an automatic, dynamic and with a minimum of configuration. Based on our research, no scientific work has done a comparative study on the impact of conventional VPN and DMVPN technology on the performance of the 802.16e network. This was a motivation for us to complete the previous work, while responding to the issues that we have defined. These studies were conducted under OPNET Modeler, we used Voice over IP applications using the G.729 codec. The evaluation criteria are: WiMax delay, throughput and convergence time. Regarding VOIP we chose as metric: jitter, end-to-end delay, loss rate and MOS score.

Key words:
DMVPN, VPN, IPsec, WiMax, VOIP

1. Introduction

In recent years, we have seen a very strong trend in the use of digital communications technologies (ICT). Like wired networks, wireless is an inherent complement to fixed broadband networks by adding the necessary mobility element to areas with high throughput demands. Wireless networks are expected to replace wireline broadband in some geographical areas while they should be extended to other areas where wired infrastructure is not economically viable.

1.1 WiMax IEEE 802.16e

The IEEE 802.16 standard [1], known as WiMax Worldwide Interoperability for Microwave Access, is a high-speed wireless and long-distance WMAN connection. It authorizes a flow of 70 Mb / s on maximum 50 km. In addition to the point-to-point mode, the WiMax can also work in point-to-multipoint mode, that is to say the infrastructure mode that is known for Wi-Fi, or the same operation as 2G technologies, 3G mobile phone. Thus, as in 2G, a base station named BTS (Base Transeiver Station) or BS (Base Station) sends to the clients and receives their requests, then transmits them to the network of the service provider. WiMax technology is used today in the Moroccan university to ensure interconnection between several institutions and the site of the presidency.

WiMax mobile, also called IEEE 802.16e [2], mobile WIMAX provides the ability to connect mobile clients to the Internet. Thus it opens the way to mobile telephony over IP or more broadly mobile broadband services. The mobile WIMAX would allow to move while remaining connected to the Internet, this via a mobile device equipped with a WIMAX card. In other words, to move in the entirety of a covered area via a central antenna without disconnection. Subsequently WIMAX will move from one coverage area to another without disconnection.

1.2 DMVPN IPsec

Dynamic Multipoint Virtual Private Network "DMVPN" [3] [4] technology provides fully meshed connectivity between multiple sites in a dynamic, fast and automatic way. DMVPN offers scalability [5]; that is, by adding a new BTS the old ones did not undergo any additional modifications. The DMVPN architecture is mainly composed of two types of HUB and SPOKE equipment, the HUB equipment called master of the topology plays a key role in the creation of tunnels between various SPOKEs, the connection between a HUB and the SPOKES must be performed by permanent tunnels, however, the link between SPOKE is provided by dynamic tunnels created on demand [6]. The basic architecture of DMVPN is illustrated in Figure 1:

Manuscript received December 5, 2017
Manuscript revised December 20, 2017

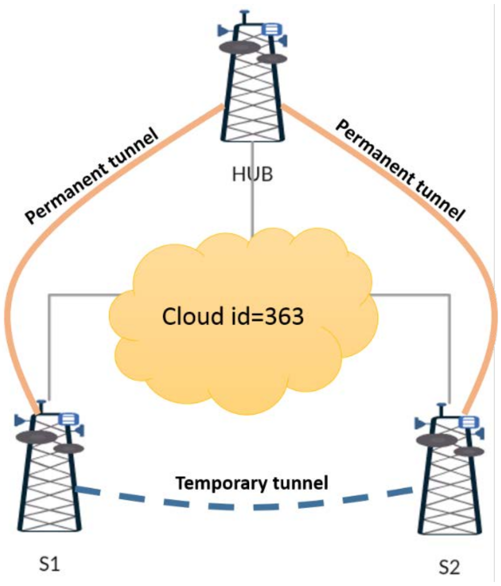


Fig. 1 DMVPN network example

The DMVPN solution relies on several protocols; Multipoint Generic Routing Encapsulation "mGRE", [7] Next-Hop Resolution Protocol "NHRP" [8], Internet Protocol Security [9] "IPsec" and Dynamic Routing Protocols [10] [11] [12].

- mGRE allows you to create multiple VPN connections on a single tunnel interface.
- NHRP works on a client / server principle. The Hub acts as a server that will store a database of tunnel addresses and physical addresses of Spokes.
- IPsec a protocol that guarantees the integrity and authentication of data, confidentiality is on demand. IPsec exploits two sub-protocols [13]: ESP (Encapsulation Security Payload) and AH (Authentication Header), the first guaranteeing the three fundamentals of security namely confidentiality, integrity and authentication, the second only guarantees the first two fundamentals. IPsec can optionally operate in two modes: the transport mode used to secure machine-to-machine connections and the tunnel mode between two sites. Regardless of the two possible AH / ESP protocols, two modes are possible, tunnel or transport. In the transport mode, one can choose the protocol AH, ESP or both. In the tunnel mode, you have to choose between the AH or ESP protocol. This mode creates a new IP packet encapsulating the one to be transported [14].

Several research studies have addressed the problem of the impact of encryption on the performance of an 802.16 and 802.11 network [15] [16] [17]. According to our research, no scientific work has addressed the impact of the IPsec protocol on the 802.16e network taking into account the increase in the number of intermediate equipment. Some work has addressed and studied the effect of site-to-site IPsec VPN tunneling on the same networks. However, with modern networks, which can contain a very large number of WiMax antennas, these VPN tunnels can not guarantee and easily follow the scalability. The DMVPN technology meets this limit, it allows to create multiple IPsec VPN tunnels in an automatic, dynamic and with a minimum of configuration. Based on our research, no scientific work has done a comparative study on the impact of conventional VPN and DMVPN technology on the performance of the 802.16e network.

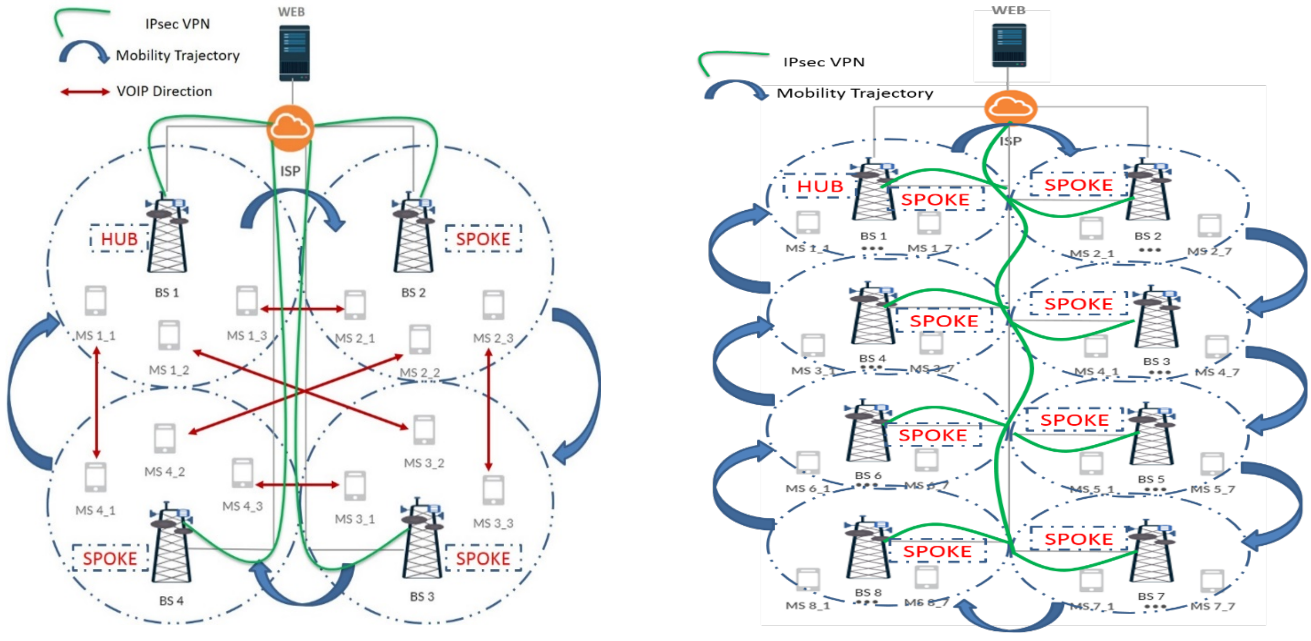
This paper complement above works by including the new VPN technology, the application simulated is VOIP, evaluation criteria fixed are :Jitter, Latency, Loss Rate and score MOS.

The rest of the paper is organized as following; Section 2 will be reserved for the discussion of evaluation scenarios, in Section 3 we will discuss obtained results and we will conclude on the fourth section.

2. Simulation environment

2.1 Experimental model

By default, evaluating scalability is complicated because several criteria must be considered, such as the number of BTSs, the different IPsec protocols, and the number of sites. In order to evaluate the scalability we realized five scenarios, we increased the number of BS by 4. The topology realized under OPNET Modeler 14.5 is illustrated through figure 2:



(a)

(b)

Fig. 2 Experimental model

2.2 Experimental parameters

As evaluation traffic, we used VOIP. The codec used is G.729 [18] because it is less bandwidth consuming than G.711. Also, it is used to get quality telephony [19].

Concerning the configuration of the network, the modulation technique used is OFDM with a gain of 15dBi and a power of 500mW. The IPsec protocol was used for the security of exchanges between BTS, so the IPsec mode used is Transport, the AES, SHA, DH 2 and Pre-shared Key protocols were chosen. Based on research on the impact of internal routing protocols on VOIP, EIGRP was the most recommended and best suited for fast and reliable real-time application routing, for this reason we used it for the whole scenarios realized.

Concerning the connections between equipment, in this simulation we used the SONET OC3 PPP cables between the BTS HUB and ISP, DS3 was used on each SPOKE. the server connection is guaranteed by a 10GigabitEthernet cable

The evaluation criteria are summarized in the table below.

Table 1: Table captions should be placed above the table

Criteria	***Signification***
Latency	The delay between the sending of a packet from the source until its reception, this delay encompasses the following deadlines: Registration with the BS or AP + processing + the queue + Propagation.
MOS[20]	Mean Opinion Score's acronym allows to evaluate the quality of the voice. This score ranges from 1 to 5, where 5 is the perfect quality, this score is influenced mainly by the codec to use and the rate of loss.
Loss Rate	The amount of traffic received versus the traffic sent. In a wireless network such as WiMax, the VOIP loss rate should not exceed 3% for quality telephony
Jitter	If two consecutive packets leave the source node with time stamps t1 & t2 and are played back at the destination node at time t3 & t4, then: jitter = (t4 - t3) - (t2 - t1) Negative jitter indicates that the time difference between the packets at the destination node was less than that at the source node.

3. Obtained results and discussion

3.1 MOS Score

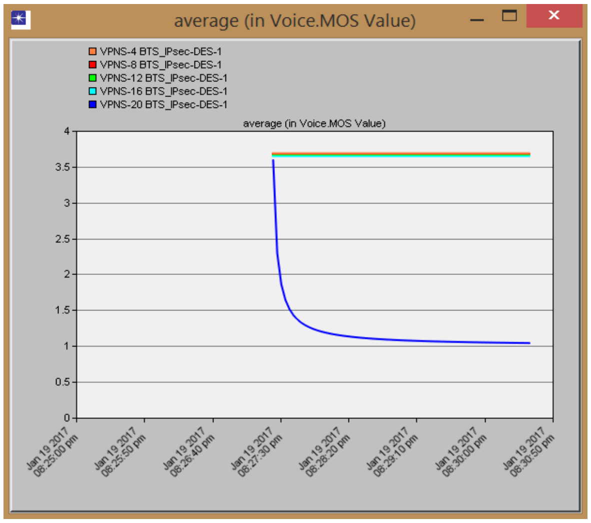


Fig. 3 MOS Score

The result of Figure 3 illustrates the MOS score of the five scenarios ranging from 4 BTS to 20 BTS connected by DMVPN technology. From a first reading we find that the MOS score of the 20 BTS scenario has reached a critical threshold of 1, which implies that the quality is not acceptable. This is due to the number of tunnel connections established in this scenario. In addition, the task of encryption will be much more complex, since the BTS antenna must maintain several tables SAD and SPD for each destination. note that the exemplary quality of the VOIP by the CODEC used is 3.5. 3.2 Latency

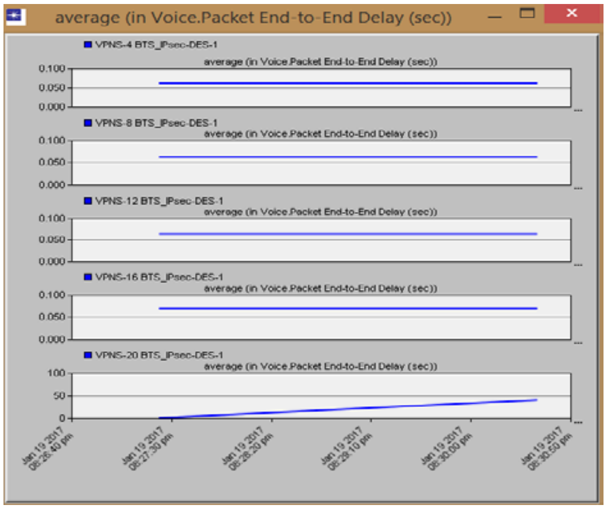


Fig. 4 VOIP Latency

The result of Figure 4 illustrates the end-to-end delay of VOIP in all scenarios. We see the same thing as the previous scenario, the end-to-end delay of the last scenario far exceeded the recommended value of 300 msec. A small imperceptible difference is observed between the different scenarios of 4, 8, 12 and 16 BTS. This difference does not influence in any way the quality of the VOIP. This remarkable increase in the end-to-end delay in the last scenario can be interpreted by the congestion of the Internet link and especially the excessive delay of the encryption and decryption in communicating sites.

3.3 Jitter

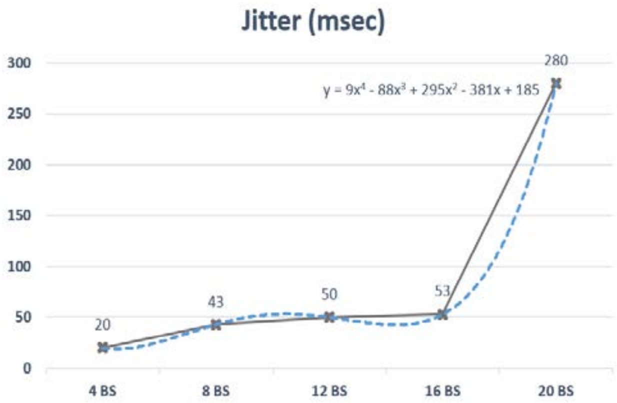


Fig. 5 VOIP Jitter

The result of Figure 5 illustrates VOIP jitter in all scenarios. We find that jitter up to 16 BTS scenario. The BS scenario reaches a very intolerable value of 280 msec, this is justified by the delay in the queue due to the encryption layer. We can say that the variation of the jitter is too high in these scenarios. This variation follows the following formula: y = 9x4 - 88x3 + 295x2 - 381x + 185

3.4 Loss Rate

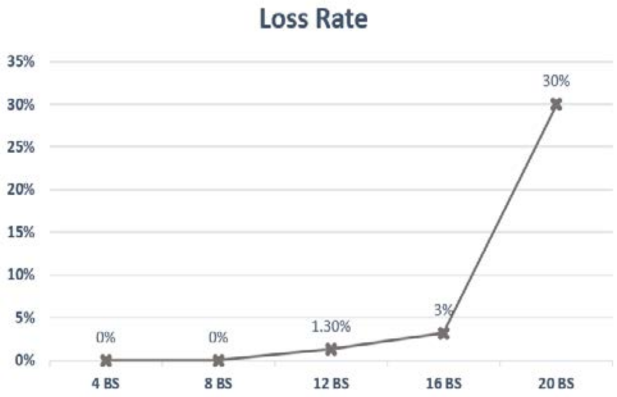


Fig 6 VOIP Loss Rate

The result of Figure 6 illustrates the loss rate of VOIP in all scenarios. The results obtained confirm those preceded. The loss rate up to 16 BS scenario was acceptable, while beyond this number this rate becomes unacceptable for the same reasons as latency and jitter.

4. Conclusion

In this paper we evaluated the Scalability of the protected Multipoint Dynamic VPN by IPsec in a WiMax Network. The study was conducted under OPNET Modeler, VOIP traffic was used to evaluate performance. We have created five scenarios in each one we increase the number of BTS in the order of 4. The results obtained have shown that the increase in the number of IPsec tunnels has a direct influence on the performance of the whole system. The evaluation focused on jitter, latency, MOS score and loss rate. We have shown that the quality of VOIP was: perfect in scenarios of 4, 8 up to 12 BTS, acceptable in scenario 16 BTS and completely unacceptable in the scenario of 20 BTS.

References

[1] WiMAX-Part M. I: A technical overview and performance evaluation. InWiMAX forum 2006 Aug (Vol. 1, No. 7).

[2] Xiao Y. Energy saving mechanism in the IEEE 802.16 e wireless MAN. IEEE Communications Letters. 2005 Jul;9(7):595-7.

[3] Ayoub BAHNASSE and Najib EL KAMOUN, Policy-based Management of a Secure Dynamic and Multipoint Virtual Private Network. Global Journal of Computer Science and Technology. 2014 Jan 1;14(8-E):63.

[4] Ayoub BAHNASSE and Najib EL KAMOUN, “Policy-Based Automation of Dynamique and Multipoint Virtual Private Network Simulation on OPNET Modeler” International Journal of Advanced Computer Science and Applications(IJACSA) 5(12), 2014.http://dx.doi.org/10.14569/IJACSA.2014.051201.

[5] Bahnasse, A., & El Kamoun, N. (2015). Study and Analysis of a Dynamic Routing Protocols' Scalability over a Dynamic Multi-point Virtual Private Network. International Journal of Computer Applications, 123(2).

[6] BAHNASSE, A., & ELKAMOUN, N. (2015). Study and evaluation of the high availability of a Dynamic Multipoint Virtual Private Network. Revue MéDiterranéEnne Des TéLéCommunications, 5(2).

[7] Sullenberger ML, Vilhuber J, inventors; Cisco Technology, Inc., assignee. Method and apparatus for establishing a Dynamic Multipoint encrypted Virtual Private Network. United States patent US 7,447,901. 2008 Nov 4.

[8] Luciani J, Katz D, Piscitello D, Cole B, Doraswamy N. NBMA next hop resolution protocol (NHRP). 1998.

[9] Bahnasse A, El Kamoun N. Security of Dynamic and Multipoint Virtual Private Network. International Journal of Computer Science and Information Security. 2016 Jul 1;14(7):100.

[10] Bensalah F, El Kamoun N, Bahnasse A. Analytical performance and Evaluation of the Scalability of Layer 3 Tunneling Protocols: Case of Voice Traffic Over IP. International Journal of Computer Science and Network Security (IJCSNS). 2017 Apr 1;17(4):361.

[11] Bensalah F, El Kamoun N, Bahnasse A. Evaluation of tunnel layer impact on VOIP performances (IP-MPLS-MPLS VPN-MPLS VPN IPsec). International Journal of Computer Science and Network Security (IJCSNS). 2017 Mar 1;17(3):87.

[12] Bensalah F, El Kamoun N, Bahnasse A. Scalability Evaluation of VOIP over Various MPLS Tunneling under OPNET Modeler. Indian Journal of Science and Technology. 2017 Aug 9;10(29).

[13] Bahnasse A, Talea M, Louhab FE, Laafar S, Harbi A, Khiat A. SAS-IMS for smart mobile security in IP multimedia subsystem. InProceedings of the 2017 International Conference on Smart Digital Environment 2017 Jul 21 (pp. 35-41). ACM.

[14] Alharbi A, Bahnasse A, Talea M. A Comparison of VoIP Performance Evaluation on different environments Over VPN Multipoint Network. International Journal of Computer Science and Network Security (IJCSNS). 2017 Apr 1;17(4):123.

[15] Sithirasenan, E., & Almahdouri, N. (2010, June). Using WiMAX for effective business continuity during and after disaster. In Proceedings of the 6th International Wireless Communications and Mobile Computing Conference (pp. 494-498). ACM.

[16] Dogaru, C. T., & Petrescu, T. (2009). WIMAX 802.16 Network–Secure Communications. UPB Sci. Bull., Series C, 71(2).

[17] BALU, J., & SENTHIL, D. S. T. (2014). SECURE DATA TRANSMISSION OVER WIMAX NETWORKS USING VPN TECHNOLOGY IN REALTIME ENVIRONMENTS. International Journal of Computer Science and Mobile Computing, Vol.3 Issue.2, February- 2014, pg. 202-211

[18] Rec, I. T. U. T. (1996). G. 729: Coding of speech at 8 kbit/s using conjugate structure algebraic-code-excited linear-prediction (CS-ACELP). Mars, 18, 22.

[19] Daengsi, T., Wutiwiwatchai, C., Preechayasomboon, A., & Sukparungsee, S. (2012, January). A study of VoIP quality evaluation: User perception of voice quality from G. 729, G. 711 and G. 722. In Consumer Communications and Networking Conference (CCNC), 2012 IEEE (pp. 342-345). IEEE.

Najib Elkamoun Ph.D, professor higher education degree at Faculty of sciences El Jadida.in the dept. of physics. Researcher member on STIC laboratory, header of Network and Telecommunications team. His research interest includes, NGN, MPLS , Networks, QoS on mobile networks, wireless networks, networks and telecommunications.

Faycal Bensalah received the Master degrees, Network and telecommunication, from Faculty of sciences El Jadida in 2014. Network administrator at Chouaib Doukkali University, Actually a Ph.D Student on STIC Laboratory on Faculty Of sciences El Jadida, Network and Telecommunications team. His research interest are : SDN ,NGN, MPLS , Networks, QoS on mobile networks, wireless networks, networks and telecommunications.

Ayoub BAHNASSE Since joining the Software Engineering and Telecommunications Team, on LTI Laboratory, Faculty of Sciences Ben M'SIK, University Hassan II Casablanca, Ayoub BAHNASSE has been involved with studies related New Generation Networks, Networks security and Mobile Learning. Before joining University, BAHNASSE obtained Ph.D degree on University Chouaïb DOUKKALI El Jadida on 2016. Actually BAHNASSE was awarded as an outstanding reviewer on Elsevier Computer Network journal and technical program committee on several international conferences: Recent Trends in Computer Science and Electronics, EAI International Conference on Technology, Innovation, Entrepreneurship and Education. My research fields are not limited only on: Security, mlearning, Wireless networks, QoS , IMS and NGN, ioT, smart city, MPLS