International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2763
Issue 11, Volume 3 (November 2016) www.ijirae.com

The Difference Impact on QoS Parameters between the IPSEC and L2TP

Alaa Hani Haidar
Dept. of ICT Eng
Maleke Ashtar Univ. of Tech

Mojtaba Houseini
Dept. of ICT Eng.
Maleke Ashtar Univ. of Tech

Abstract* - Many of the networks are existing but little of them that believe the quality and security together, the secure transmission of the information with high quality remains the primary goal of all engineers, which is considered the ideal goal of this theory either in fact, get a high quality of service comes at the expense of security and vice versa, has been expressed networks fiber optic for the best possible speed while maintaining a good level of security. In the Internet network, person-to-person communication can be enhanced with high quality images and videos, and access to information and services on public and private networks will be enhanced by higher data rates, quality of service (QoS), security measures, location-awareness, energy efficiency, and new flexible communication capabilities. So some networks are characterized by the QOS offered in addition to the security that we will discuss extensively later. This distinction is linked to the quality of communication and service over the network and security[1]. The quality of a network is evaluated on the basis of the quality of service, and especially on its security features. The use of security mechanisms is important in knowing the identity, saving the information, and ensuring that there is no tampering.in this research we try to ensure the security for QoS with two different methods using the Tunnel like the L2TP and IPSec that mean the security of layer two and three of OSI model, and we compared the differential impact between the two types of security on QoS parameters.

Keywords – L2TP, VPN, IPSEC and Quality of Service QoS

I. INTRODUCTION

The Security is one of the most important elements in any network and has been discussed by keen technicians since 1960 [2]. We cannot be trusted in any network if it does not take into account the issue of security. In addition to security, there is a new technique which is witnessed by the world of network quality of service and is also considered one of the most important services that are based on the classification of information in order of importance, which it deems appropriate technicians helping to improve communication and send information. But these services must be given something of secrecy and security, and if it does not enjoy a specific level of which they become vulnerable to hacking and interception and damage.

The security is a critical requirement of dependable systems and networks [3], it does not separate works with the QoS, in other words, it affects the quality of independent, non-declared security service and vice versa. Also the security does not come for free and, in general, protection mechanisms require more processing time and causes traffic delay. We have several types of security combined service with a high level of confidentiality and security, in order to reach the nearest state of the ideal. But so far, this ideal has not been reached to integrate security with quality of service parameters, So integrating the security to the quality of the service parameters did not specify what kind of security will be combined although the security elements are also controlled by confidentiality, integrity and other parameters of security. In order to pursue our goal of securing the network, we must improve the weak points of the OSI layers. Through our knowledge in OSI layers, the second layer (data link layer) and the third are considered one of the weakest layers due to its proximity to the physical layer, and thus benefiting from the second layer and the third of OSI Model helps in preventing access to the upper layers [1]

The synchronization of the security and quality of service in the network is a basic requirement, despite the existence of its mutual effect; engineers always seek to create a state close to the ideal in networks where the service and the security both are at the top level.

The security does not separate works with the quality of service, in other words, it affects the quality of independent non-declared security service and vice versa. Also the security does not come for free and, in general, protection mechanisms require more processing time and causes traffic delay. Real time applications such as video conferencing, VoIP, and real-time video need special processing to achieve their goals and to overcome the delay introduced by adding security mechanisms [1].

We have several methods for the QoS security, but in this article we will use the security layer 3 of the OSI model(IPSEC) and layer 2 (L2TP),but every protocol works alone. Then we will build a network that has tow subnet (every subnet has five workstations, one router, one server for the application and one switch), IP cloud for internet connection. The first work it must to build the network, implementation the QoS, implementation the tunnel of L2TP, and the tunnel of IPSEC and last we will run the simulation for compart the result. For the simulation we will use the Opnet simulator program, the last step is the study the difference between the L2TP impact on QoS parameters and the IPSEC impact. This paper presents in Section 2 RELATED WORK., Section 3 IPSec. Section 4 L2TP. Section 5 INTEGRATE THE QoS AND SECURITY (TUNNEL), Section 6 QoS TECHNIC, SECTION 7 SIMULATION and ANALYSE, Section 8 CONCLUSION on open issues and perspectives of this work.

II. RELATED WORK

There are some articles very related to our paper such as the [4] The authors talked about the impact of security on the quality of service through mathematical equations, and the impacts of encryption and authentication on SAL and delay. Finally they concluded, that to get the minimum delay and the highest SAL, they should use an immune algorithm to optimize key length and authentication rate. Their simulation showed that the proposed model is effective to get the optimal solution under different configurations.

In [5], discussed a new type of networking mobile ad hoc network (MANETS) and how to take advantage of the security and quality of service in this type of networks. The new model used for integrating security and Quality of Service (QoS) as one parameter in MANET, is introduced and studied in their research . Their model via cross layer design (CLD) provides an alternative to cooperation between QoS and security.

In [30] the researchers presented an assessment methodology to analyze the performance of different firewall platforms. The performance analysis considers delay, jitter, throughput, and packet loss. The proposed methodology was tested by performing a number of experiments on different types of firewalls, including network-based and personal firewalls. The results showed that network-based firewalls outperformed personal firewalls in all metrics and Cisco ASA achieved better performance than a packet filter, and all the firewalls can protect against the proposed attack, which confirms the idea of using both personal and network-based firewalls to provide layered security. Other results of this study showed that most computer users do not use or configure firewalls on their devices which is a concerning issue for network administrators

The relation between QoS and security is strong, and both QOS and security have a set of parameters, and for this reason we have many possible combinations of parameters, but we must choose the best combinations. These combinations have been presented by Tarik Taleb and Abderrahim Benslimane, where they demonstrated the need for jointly addressing QoS and security requirements. To this end, they devised a network policy framework entitled QoS2 which orchestrates between the conflicting requirements of QoS and security based on a MADM approach (an approach that can be applied using different algorithms for choosing the best decision) running at a global security advisory system. The advisory system assesses current network security conditions based on real-time feedback from different monitoring systems deployed over the network in a hierarchical fashion. They evaluated the performances of their QoS2 mechanism while considering the case study of QoS-sensitive IPTV services. The authors demonstrate that they envisioned QoS2 framework achieves its designed goals.

For utilizing this approach we must pass through three steps: Step one Defining all possible QoS level and security level combinations, Step tow Defining the Decision Matrix (DM) for a user’s connection, Step three Applying a MADM algorithm to find the best alternatives among the available ones. After these steps, the researchers used the Network Simulator (NS3) and the TOPSIS algorithm to select the best set of parameters to meet both the QoS and security requirements. At the end of the article the authors have concluded the impact of security on QoS by two figures (3 and 4) that illustrate the relation between the Buffer Playback rate occupancy and different threat levels.[31]

In [6] the authors proposed a QoS-friendly Encapsulated Security Payload (Q-ESP) to solve problem of IPSec encapsulation security protocol (ESP) that hides much of the information’s in its encrypted payloads, this information is utilized in performing classification appropriately. Finally, they concluded that, in this way they could minimize the possibility of QoS attack to the VPN module, as unconcerned packets will be filtered by the firewall.

In [11] Stefan et al, talked about adding security on QOS architecture, where they said that "until now security has not been recognized as a parameter in QoS architectures and no security-related service classes have been defined". They have made a brief survey of what has been done so far in the area and suggested some potential ways of further progress towards a quality of service concept that would include security aspects. In the research, the authors said that there must be a definition for the security that is needed by the user, and must define a method to arrive at quantitative value. But the authors did not put a method to measure the parameters of QOS and security. Moreover, they did not specify which level of security and QOS must be chosen. In [54] the authors present an improved UGF, named VUGF, to study the simultaneous analysis of multiple QoS indices for an SCA in an algebraic procedure. The VUGF inherits the outstanding advantages that allow one to find the entire MSS performance distribution based on the performance distribution of its elements by using a fast algebraic procedure.

III. IPSEC

A. *Definition:* Internet Protocol security (IPSec) is a framework of open standards for helping to ensure private, secure communications over Internet Protocol (IP) networks through the use of cryptographic security services. IPSec supports network-level data integrity, data confidentiality, data origin authentication, and replay protection. Because IPSec is integrated at the Internet layer (layer 3), it provides security for almost all protocols in the TCP/IP suite, and because IPSec is applied transparently to applications, there is no need to configure separate security for each application that uses TCP/IP.IPSec is the merge some of security algorithms for making sure the security for the network and the connection between the users, the protocol is used on layer 3 of the OSI Model and use the tunnel technique. And it ensures the authentication, packets, security and administration of keys [7].

B. *IPSEC Advantage:* 1-Ensure a strong security between the inside and the outside the LAN In case of use in routers and firewalls. 2- Hidden in front the user 3-Ensures the cryptography, 4-The principal advantage of IPSec is that it offers confidentiality and authentication at the packet level between hosts and networks[7].

C. *IPSEC Characteristics: 1*- involuntary in IPV6 and voluntary in IPV4, 2- Has described a relatively difficult 3- The files of IPSec are long, 4- keys administrator, 5- cryptography algorithms and authentication. 6- Documents of IPSec are very large and are classified as follows: a-Architecture, ESP Encapsulating Security Payload, (AH) Authentication Header

D. *IPSEC Mode: We* have two modes of IPSec transport: 1-IPSec tunnel mode, 2- IPSec transport mode, but in this paper we will talk about the tunnel mode only[7].

1) *IPSEC Tunnel Mode: IPSec* tunnel mode is the **default mode**. With tunnel mode, the entire original IP packet is protected by IPSec. This means IPSec wraps the original packet, encrypts it, adds a new IP header and sends it to the other side of the VPN tunnel (IPSec peer). Tunnel mode is used to encrypt traffic between secure IPSec Gateways, for example, two Cisco routers connected over the Internet via IPSec VPN. Configuration and setup of this topology are extensively covered in our Site-to-Site IPSec VPN article. In this example, each router acts as an IPSec Gateway for their LAN, providing secure connectivity to the remote network:

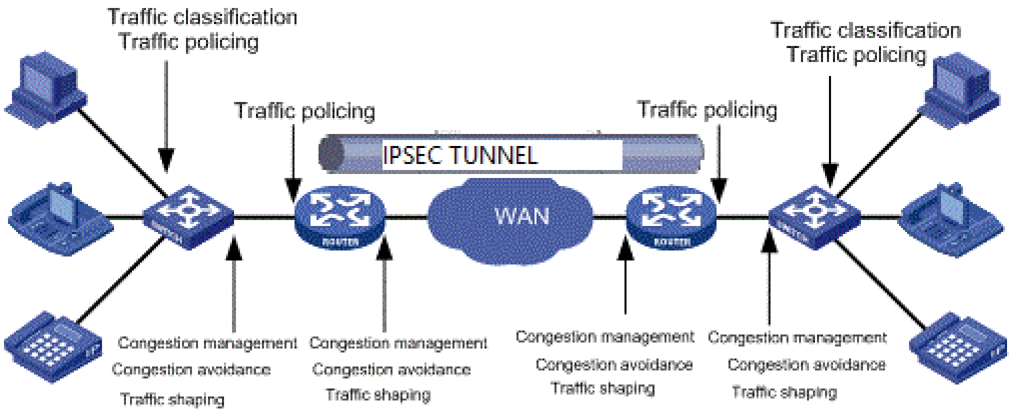


Fig .1 IPSec Tunnel

In tunnel mode, an IPSec header (AH **or** ESP header) is inserted between the IP header and the upper layer protocol. Between AH and ESP, ESP is most commonly used in IPSec VPN Tunnel configuration. The packet diagram below illustrates IPSec Tunnel mode with ESP header**:**

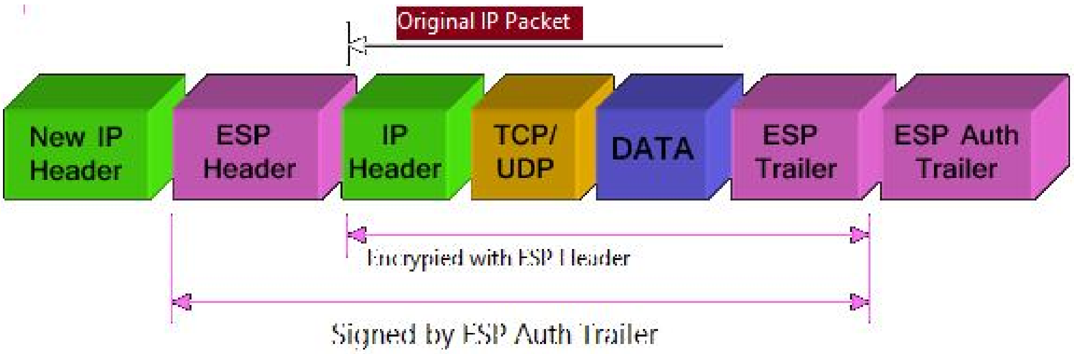


Fig .2 IPSec Packet

L2TP (LAYER 2 TUNNEL PROTOCOL)

A. *Definition.* The data-link layer (Layer 2 of the OSI Model) provides the functional and procedural means to transfer data between network entities with interoperability and interconnectivity to other layers. Network security is only as strong as the weakest link, and Layer 2 is no exception. Applying first-class security measures to the upper layers (Layers 3 and higher) does not benefit your network if Layer 2 is compromised. Tunneling offer a wide range of security features at Layer 2 to protect the network traffic flow and the devices themselves [1]. Through which you can get to the top levels that become safe if this was the security level in addition to its proximity to the level of physics and also the security advantages of the protocols, such as the pole which we will display its advantages

B. *Advantages of L2TP Include***:**

High data security is provided for critical applications.
High-level encryption is used so that critical information is always safe and remains personal.
It provides excellent and efficient connectivity.
It is cost-effective and does not have overhead cost after implementation.
It is reliable, scalable, fast and flexible.
It is an industry-standard best for the corporate sector.
It has the best authorization policy for users with VPN authentication.

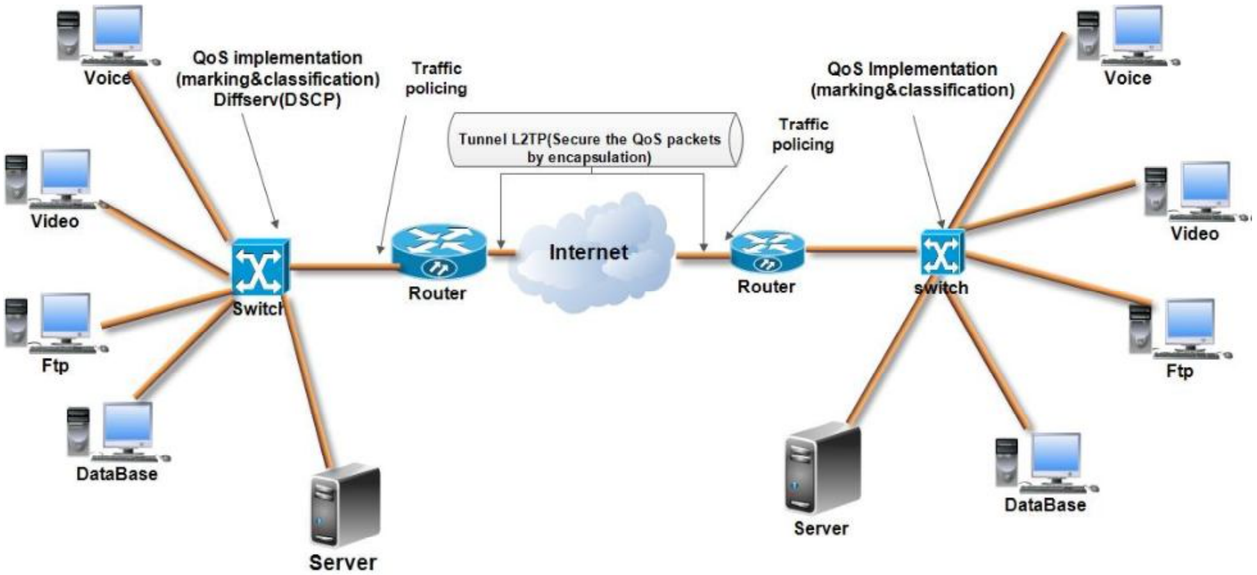

Voice
QoS implementation (marking&classification) Diffserv(DSCP)
Traffic policing
Tunnel L2TP(Secure the QoS packets by encapsulation)
Traffic policing
QoS Implementation (marking&classification)
Voice
Video
Internet
Video
Switch
Router
Router
switch
Ftp
Ftp
DataBase
Server
Server
DataBase

Fig .3 L2TP Tunnel

IV. INTEGRATE THE QoS AND SECURITY (TUNNEL)

The security domain is very wide and complex, and demanding most of the components of the network, so it must to determine the place and the method that we will use in our research, we talked that our research is the QoS' security, therefore, the principal work of the research is about the classification packets that characterizes the QoS and how we can provide the security for that as shown in Fig 4.

Encapsulation of L2TP/IPSec packets consists of two layers:

- *First layer: L2TP encapsulation A PPP frame (an IP datagram) is wrapped with an L2TP header and a UDP header. The following figure shows the structure of an L2TP packet containing an IP datagram.*
- *Second layer: IPSec encapsulation*

The resulting L2TP message is then wrapped with an IPSec Encapsulating Security Payload (ESP) header and trailer, which is an IPSec Authentication trailer that provides message integrity and authentication, and a final IP header. In the IP header is the source and destination IP address that corresponds to the VPN client and VPN server.

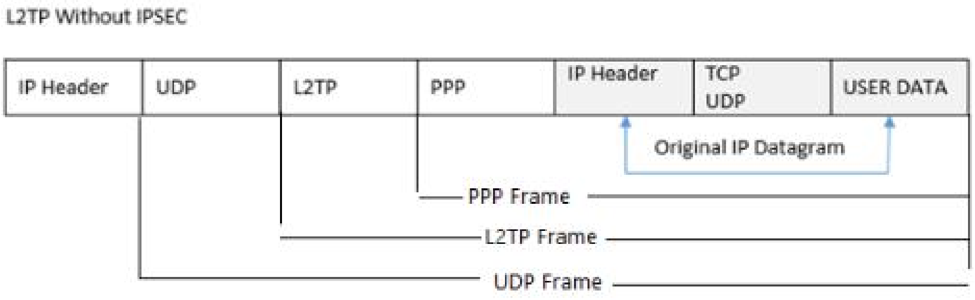


Fig .4 L2TP Packet

V. QOS TECHNIC

QoS, which is defined as the ability of a network to recognize different service requirements of different application traffic flowing through it, and to comply with service level agreement (SLAs) negotiated for each of the applications is absolutely essential in a multi-service network, in order to meet SLAs of different services and to maximize the network utilization. [9]. QoS allows the service provider to utilize a network infrastructure for offering multiple application services, thereby saving the capital and operating costs involved in maintaining multiple networks for each of the applications separately. Although network traffic flows are dynamic in nature, QoS allows the service provider to maximize network resource utilization, thereby increasing their profit. QoS maximizes network resource utilization and optimizes the revenue generation by providing priority access to network bandwidth for high-priority traffic, and by allowing low-priority traffic to gain the bandwidth committed to high-priority traffic in the absence of high-priority traffic

A. QoS Architectures

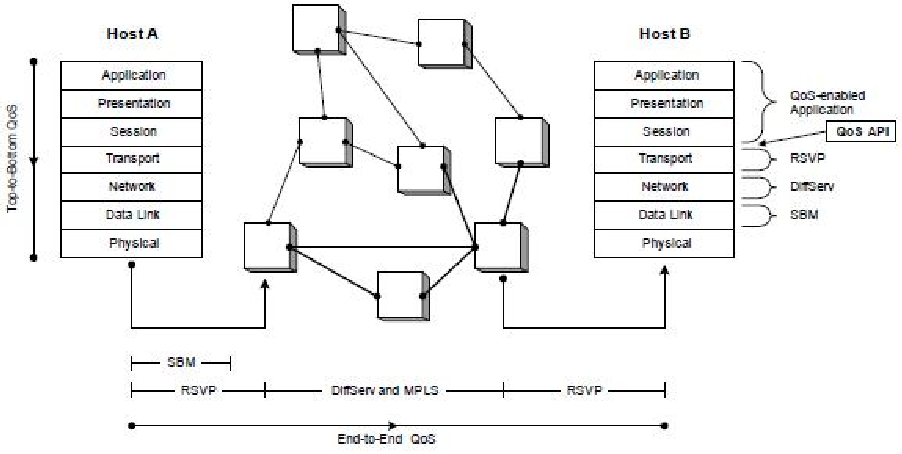


Fig .5 QoS Architectures

B. *QoS Models*

Which model of QoS we will use? We have three models of QoS: Best-effort service, integrated service (IntServ), and differentiated services (DiffServ). In this research, we will choose the DiffServ model because it is a scalable end to end quality of QoS. The DiffServ works on the provisioned-QoS model, where network elements are set up to service multiple classes of traffic with varying QoS requirements. This model uses several protocols such DSCP and other.

Why we will use DiffServ? The major advantages of the Diffserv approach are that it is a good match to the Internet architecture and that it can be initially deployed with a minimalist approach, adding complexity as needed, and it has several important aspects including[8]:

A. It is very important for real time application such voice and video.
B. The scalable end to end quality model.
C. The traffic on Diffserv is grouped into class:
1. A classification process defined at the network edge.
2. Classification can be encoded inside packet itself.

D.An application can’t/doesn’t always conform to/provide “strict” model of resource usage.
E. Is based on assigning each packet to a service support class, marking corresponding treatment into IP header.

VI. SIMULATION

In this research, we used the Opnet simulator to analyze the result, because it is spatial for the network analyze and in this article we studied the difference between the impact of IPSEC tunnel and L2TP tunnel on the QoS parameters, like delay, jitter, loss ratio…

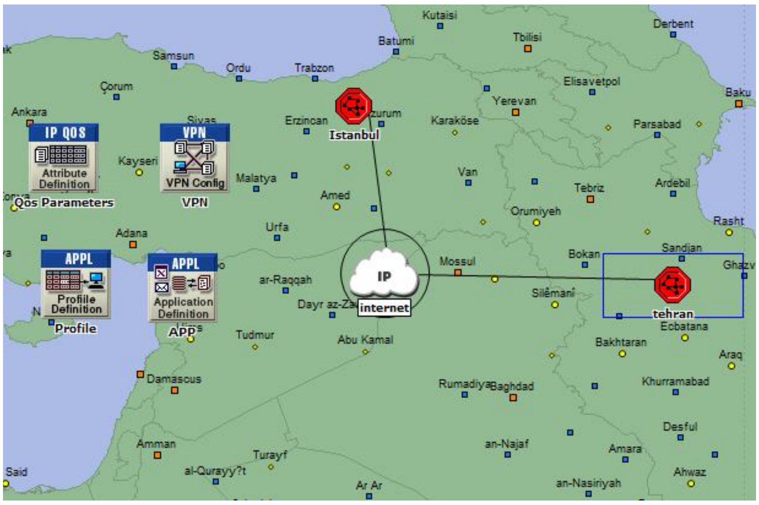


Fig .6

In this network we have 2 scenarios, the first for the L2tp tunnel and the second for the IPSec tunnel and every scenario has, 2 subnets ,IP cloud for internet and 4 nodes model model's, application ,VPN and QoS, for configure the network, the first subnet is in ISTANBUL and the second is in THRAN, this network has the QoS technic to use the different type of data, video, VoIP, HTTP, DB, and FTP.

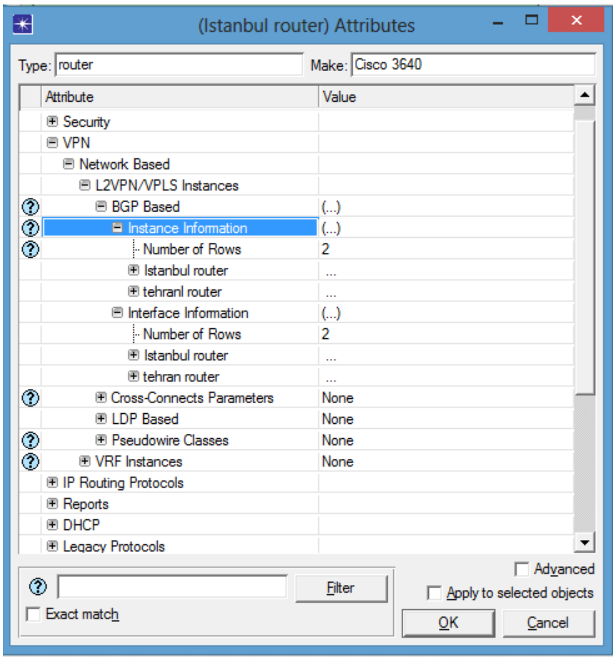
Through this section we will display the process implemented in order to reach the positive results. So we are going to do some basic steps. First, we must build a network with Opnet,. Then we implemented the QoS. After that, we add the security using the security protocols on the data link layer, such as L2TP and we measured the QoS parameters, after we implanted the tunnel of IPSec in order to compare them with the previous results. Finally, we analyzed the variation that occurred as a result of increasing the security to those parameters. So we have the steps below:

Create a network, Implement QoS, Integrate QoS and Security (tunnels), Measure QoS parameters, analyze the differences. We have more than one method: CLI (command line interface), MQC (modular QoS command), CCP (Cisco configuration Professional, Auto QOS: using one command on cisco router for deploying QOS automatic[9].

A.Implementation of the (VPN) over internet network

The VPN consist of the following devices; ten of workstation connected using Ethernet protocols, two switches of 16 ports, two sites routers, and tow Ethernet server, two Ethernet servers, links 10BT and 100BT.

1) *The Implementation of the L2TP : The configure L2TP will be in the routers gateway but the configuration of QoS will be in the switshes,this configuration as shown in the fig (7)*

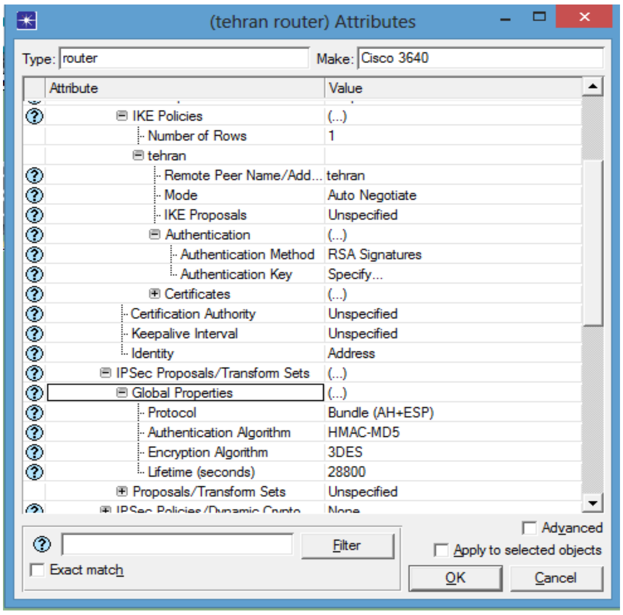

(Istanbul router) Attributes

Type: router Make: Cisco 3640

Attribute	Value
⊞ Security	
⊟ VPN	
⊟ Network Based	
⊟ L2VPN/VPLS Instances	
⊟ BGP Based	(...)
⊟ Instance Information	(...)
Number of Rows	2
⊞ Istanbul router	...
⊞ tehranl router	...
⊟ Interface Information	(...)
Number of Rows	2
⊞ Istanbul router	...
⊞ tehran router	...
⊞ Cross-Connects Parameters	None
⊞ LDP Based	None
⊞ Pseudowire Classes	None
⊞ VRF Instances	None
⊞ IP Routing Protocols	
⊞ Reports	
⊞ DHCP	
⊞ Legacy Protocols	

Fig .7 The configuration of L2tp

2)*The Implementation of the IPSEC :* To configure IPSec protocol must duplicate scenario and first need to remove all parameters that used in L2TP from all routers then select Tehran router click right on it chose edit attribute will open list and chose form it security. The IPSec Parameters can be used to configure the security related parameters on this node. IKE parameter this content internet Key Exchange (IKE) automatically negotiates, IPSec security associations (SAs) and enables IPSec secure communications without costly manual reconfiguration. Fig (8), shows the attributes needed for that connection.


(tehran router) Attributes

Type: router Make: Cisco 3640

Attribute	Value
⊟ IKE Policies	(...)
Number of Rows	1
⊟ tehran	
Remote Peer Name/Add...	tehran
Mode	Auto Negotiate
IKE Proposals	Unspecified
⊟ Authentication	(...)
Authentication Method	RSA Signatures
Authentication Key	Specify...
⊞ Certificates	(...)
Certification Authority	Unspecified
Keepalive Interval	Unspecified
Identity	Address
⊟ IPSec Proposals/Transform Sets	(...)
⊟ Global Properties	(...)
Protocol	Bundle (AH+ESP)
Authentication Algorithm	HMAC-MD5
Encryption Algorithm	3DES
Lifetime (seconds)	28800
⊞ Proposals/Transform Sets	Unspecified
⊞ IPSec Policies/Dynamic Crypto	None

Fig .8

3) *The results of the VPNs using OPNET simulation***:** *OPNET simulator has measurement criteria that can be used to measure the efficiency of the performance and quality of service (QoS) of the implemented networks, the QoS measure can be used with services of voice ,Email, video, Ftp and DB some of these criteria are: Traffic Sent and receive ,Response time (sec) ,Email or file transfer Download response time ,Email or file transfer upload response time , Jitter (sec): Jitter is defined as a variation in the delay of received packets, and MOS is called Mean Opinion Score (MOS). MOS gives a numerical indication of the perceived quality of the media received after being transmitted and eventually compressed using codecs As shown in the fig (16),the jitter (variation in the delay) during the Voice conferencing of the types of networks and the packet loss ratio during the connection.*

DB Download Response(Fig .9) *: time elapsed between sending a request and receiving the response packet. Measured from the time when the Database Query Application sends a request to the server for the time it receives a response packet. Every response packet sent from a server to a Database Query application is included in this statistic.. As shown in figure (9). DB* ***using L2TP*** *is comparatively less than IPSec.*

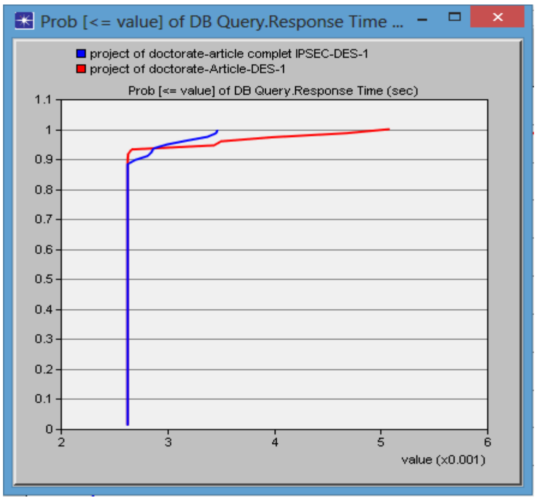


Fig .9 DB Download Response Time

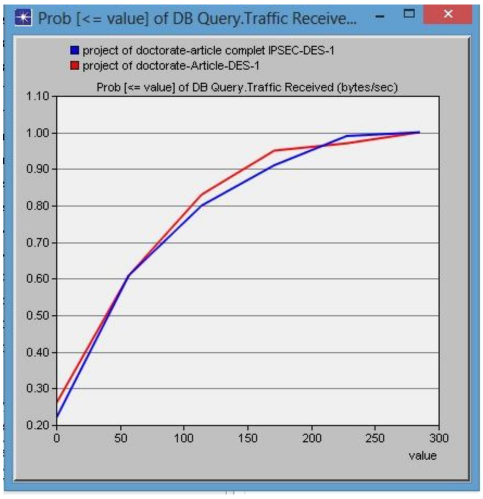


Fig .10 DB Query Traffic receive

DB Query Traffic receives (Fig .10): *Average bytes per second forwarded to all Database Query Applications by the transport layers in the network , here the time is approximately equivalent between the L2TP and IPSec .*

Ethernet Delay (Fig .11) ***:****This statistic represents the end to end delay of all packets received by all the stations. In this result we conclude that the packet of IPSec passes more of the time than L2TP.*

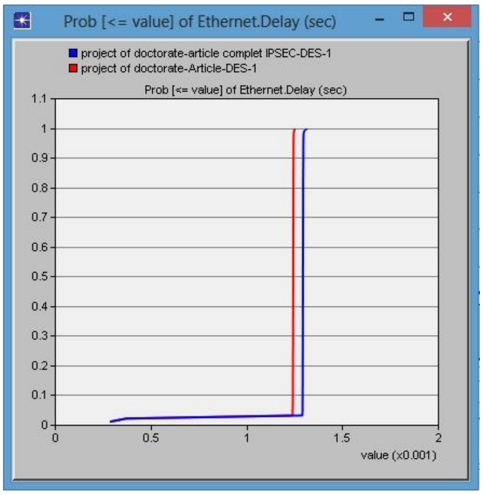


Fig .11 Ethernet Delay

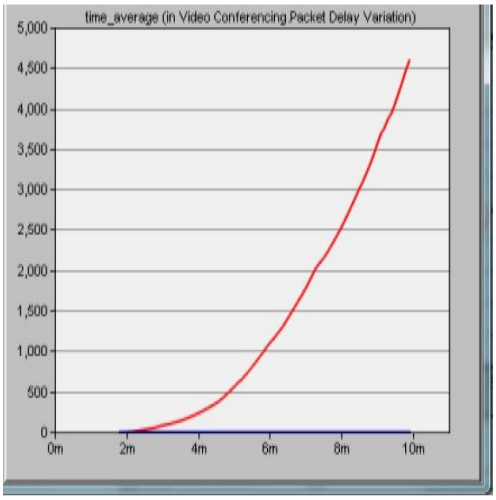


Fig .12 Video conferencing Packet Delay(IPSec)

Video conferencing Packet Delay(IPSec) Fig .12: Variance among end to end delays for video packets. End to end delay for a video packet is measured from the time it is created to the time it is received.

Video conferencing Packet Delay(L2TP) Fig .13: Variance among end to end delays for video packets. End to end delay for a video packet is measured from the time it is created to the time it is received. It is observed from the figure (12,13) that Apparently, the IPsec is comparatively less than the L2TP.

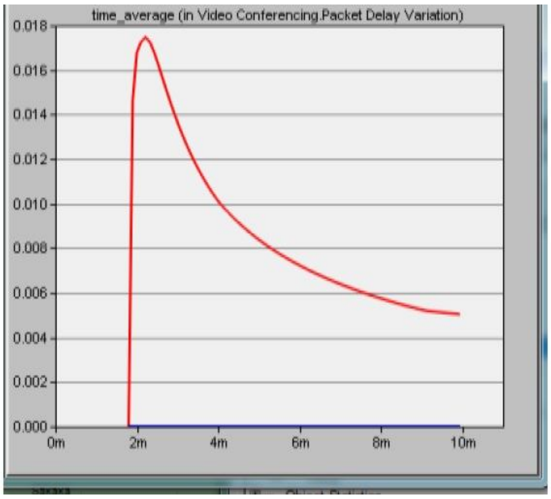


Fig .13 Video conferencing Packet Delay(L2TP)

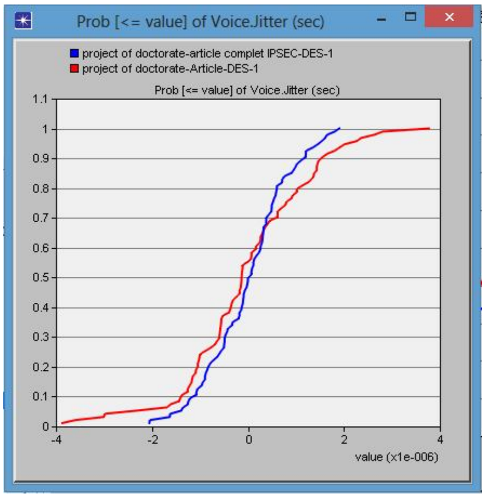
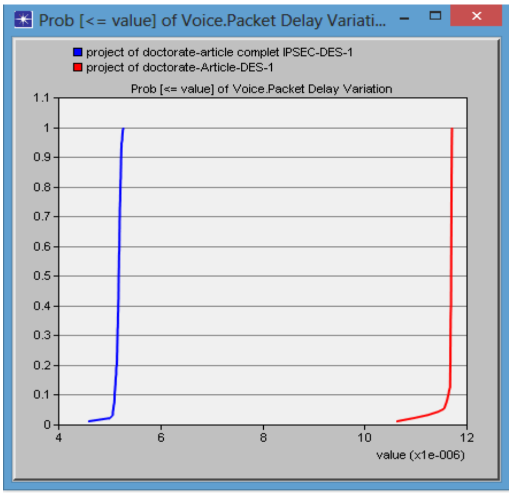


Fig .14 Voice Jitter

Voice Jitter (Fig .14): If two consequetive 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**,** It is observed from the figure (14) that Apparently, the IPsec is comparatively less than the L2TP before 0.5 but atfer 0.5 the L2TP become comparatively less than IPSec .

Mean Opinion Score (MOS) Value Fig .16: gives a numerical indication of the perceived quality of the media received after being transmitted and eventually compressed using codecs. The MOS value on L2TP is high than IPSec so the best is IPSEC Tunnel.



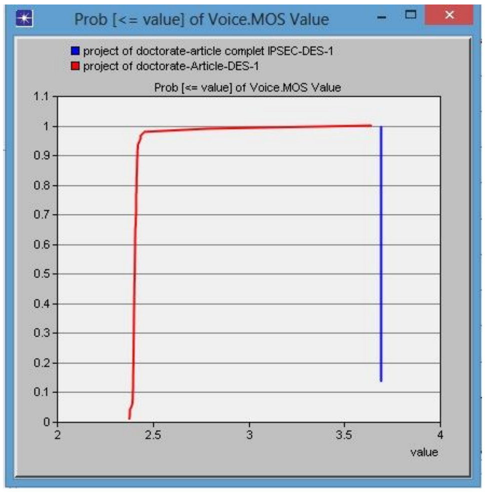


Fig .15 Packet Delay Variation

Fig .16 MOS Value

Packet Delay Variation (Fig .15): Variance among end to end delays for voice packets. End to end delay for a voice packet is measured from the time it is created to the time it is received, this figure illustrates that delay variation on L2tp is less than the IPSec, that mean the voice on L2TP is better and continue during in the first 11 second.

Packet End To End Delay (Fig .17): The total voice packet delay, called "analog-to-analog" or "mouth-to-ear" delay = network_delay + encoding_delay + decoding_delay + compression_delay + decompression_delay Network delay is the time at which the sender node gave the packet to RTP to the time the receiver got it from RTP. Encoding delay (on the sender node) is computed from the encoder scheme. Decoding delay (on the receiver node) is assumed to be equal to the encoding delay.

Compression and Decompression delays come from the corresponding attributes in the Voice application configuration. This statistic records data for all the nodes in the network, this figure illustrates that delay variation on L2tp is less than the IPSec, that mean the voice on L2TP is better and continue for all the users.

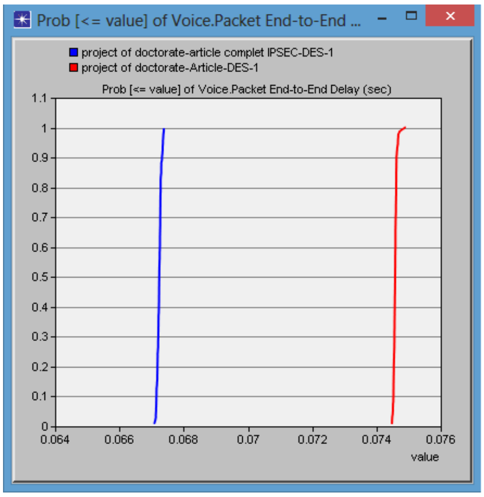


Fig .17 Packet End To End Dlay

VII. CONCLUSION

The rapid development of technology, especially in the field of networking and communications, allows for improved the QoS, and thus increases the speed of transmission of information, but at the same time,the informations has become invulnerable, so the work of engineers is to find a solution to secure at the same time the minimum QoS and high level of security, The primary goal of this work is providing high QoS with VPN using tunneling technique and using security protocols of layers2 of OSI Model and IPSEC layer3, this method is based on the encapsulation technique. With the simulation programme OPNET we showed the differnce impact resulting between the L2TP and IPSEC from adding the security(tunnel) on QoS parameters such delay, jitter, loss and bandwidth.. In our future work we will define which one of the parameters of security that has the most impact on the QoS parameters and then choose the best level of security with the best QoS possible.

REFERENCES

[1] Haidar, A.H., M. Houseini, and M. Kshour, The Analyse of Adding Security on QoS Parameters, International Journal of Innovative Research in Advanced Engineering (IJIRAE), 2014.

[2] http://www.ciscopress.com/articles/article.asp?p=170743 .

[3] Aiash, M., An integrated approach to QoS and security in future mobile networks using the Y-Comm framework. 2012, Middlesex University.

[4] Chen, J., et al. Impact of security on QoS in communication network. in Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC'09. International Conference on. 2009. IEEE.

[5] Cizmar, A., J. Papaj, and L. Dobos, Security and QoS integration model for MANETS. Computing and Informatics, 2012. 31(5): p. 1025-1044

[6] Mostafa, M., et al. Q-ESP: a QoS-compliant security protocol to enrich IPSec framework. in New Technologies, Mobility and Security (NTMS), 2009 3rd International Conference on. 2009. IEEE.

[7] **http://dnsl.ce.sharif.edu**

[8] S Patil1 and A Kumar," Effective Realization of QoS, Network Scalability in Term of Network Security using Symmetric Algorithm", International Journal of Computer Science & Communication Vol. 1, No. 2, July-December 2010, pp. 101-104.

[9] Seo, K. and S. Kent, Security architecture for the internet protocol. 2005

[10] Spyropoulou, E., T. Levin, and C. Irvine. Calculating costs for quality of security service. in Computer Security Applications, 2000. ACSAC'00. 16th Annual Conference. 2000. IEEE.

[11] Lindskog, S. and E. Jonsson. Adding Security to Quality of Service Architectures. in Proceedings of the SS-GRR Conference. 2002.

[12] S Duflos, V Gay, B Kervella1 ,E Horlait1, "Integration of Security Parameters in the Service Level Specification to Improve QoS Management of Secure Distributed Multimedia Services", IEEE, 2005.

[13] Dierks, T. and E. Rescorla: "The TLS Protocol Version 1.1", IETF Internet Draft, Dec. 2004.

[14] ISO, "Information Processing System – Open System Interconnection – Basic Reference Model – Part 2: Security Architecture", International Standard ISO 7498-2, ISO, Feb.1998. .

[15] http://searchwindowsserver.techtarget.com/definition/command-line-interface-CLI

[16] ITU (International Telecommunication union),"Framework and methodologies for the determination and application of QoS parameters, ITU, www.itu.int/rec/T-REC-E.802-200702-I

[17], Irvine, C., et al. Security as a Dimension of Quality of Security Service. in Proc. of the Active Middleware Services Workshop, San Francisco, CA. 2001

[18] Liu, G.Q., et al. A Method of QoS Measurement Based on User Behavior Analysis. in e-Business Engineering, 2009. ICEBE'09. IEEE International Conference on. 2009. IEEE..

[19] Beuran, R., et al., Network quality of service measurement system for application requirements evaluation. SIMULATION SERIES, 2003. 35(4): p. 380-387.

[20] ITU-T Recommendation "Framework and methodologies for the determination and application of QoS parameters",ITU, 2008.

[21] Siler, M. and J. Walrand. Monitoring quality of service: measurement and estimation. in Decision and Control, 1998. Proceedings of the 37th IEEE Conference on. 1998. IEEE..

[22] Dressler, F., A metric for numerical evaluation of the QoS of an Internet connection. Teletraffic Science and Engineering, 2003. 5: p. 1221-1230.

[23] Hayajneh, T., et al., Performance and Information Security Evaluation with Firewalls. International Journal of Security & Its Applications, 2013. 7(6).

[24] Günter, M., T. Braun, and I. Khalil. An architecture for managing QoS-enabled VPNs over the Internet. in Local Computer Networks, 1999. LCN'99. Conference on. 1999. IEEE.

[25] Alexander, D.S., et al., Secure quality of service handling: SQoSH. Communications Magazine, IEEE, 2000. 38(4): p. 106-112.

[26] E. Spyropoulou, T. Levin, and C. Irvine Calculating costs for quality of security service. in Computer Security Applications, 2000. ACSAC'00. 16th Annual Conference. 2000. IEEE.

[27] Irvine, C. and T. Levin. Toward a taxonomy and costing method for security services. in Computer Security Applications Conference, 1999.(ACSAC'99) Proceedings. 15th Annual. 1999. IEEE..

[28] Irvine, C. and T. Levin. Quality of security service. in Proceedings of the 2000 workshop on New security paradigms. 2001. Kang, K.-D. and S.H. Son, Towards security and qos optimization in real-time embedded systems. ACM SIGBED Review, 2006. 3(1): p. 29-34.

[29] 50. Aldini, A. and M. Bernardo, A formal approach to the integrated analysis of security and QoS. Reliability Engineering & System Safety, 2007. 92(11): p. 1503-1520.

[27] L Zhu, F Richard Yu, B Ning,T Tang " A joint design of security and quality-of-service (QoS) provisioning in vehicular ad hoc networks with cooperative communications", Springer, 2013.

[28] Swan, T.L. and D.U. McKinney, Ability to apply different levels of quality of service (QoS) to different sessions in an IPsec tunnel. 2010, Google Patents.

[29] Roch, S. and G. Algie, Dynamic virtual private network (VPN) tunnel quality of service (QoS) treatment. 2000, Google Patents.

[30] Alia, M., et al. Putting together QoS and security in autonomic pervasive systems. in Proceedings of the 6th ACM workshop on QoS and security for wireless and mobile networks. 2010. ACM

[31] Andersson, J.A. and Z. Hossein, QoS in Today's Internet. 2004.

[32] Nieto, A. and J. Lopez, Security and QoS relationships in mobile platforms, in Computer Science and its Applications. 2012, Springer. p. 13-21.

[33] Daoudeyeh, O.M. and R. Hassan, The Necessity of Integrating Security as a QoS Parameter in Mobile Ad Hoc Networks. Research Journal of Applied Sciences, 2014. 9(8): p. 466-473.

[34] Shen, Z. and J.P. Thomas, Security and qos self-optimization in mobile ad hoc networks. Mobile Computing, IEEE Transactions on, 2008. 7(9): p. 1138-1151.

[35] Foley, S.N., et al., Multilevel security and quality of protection, in Quality of Protection. 2006, Springer. p. 93-105.

[36] Jason, J., L. Rafalow, and E. Vyncke, IPsec configuration policy information model. 2003.

[37] He, W. and K. Nahrstedt. An integrated solution to delay and security support in wireless networks. in Wireless Communications and Networking Conference, 2006. WCNC 2006. IEEE. 2006. IEEE.

[38] Irvine, C., et al. Security as a dimension of quality of service in active service environments. in Active Middleware Services, 2001. Third Annual International Workshop on. 2001. IEEE.

[39] Nanji, S. and W. Palter, Tunnel interworking. 2005, Google Patents.

[40] Taleb, T., Y.H. Aoul, and A. Benslimane. Integrating security with qos in next generation networks. in Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE. 2010. IEEE.

[41] Lee, H.-J., et al., QoS parameters to network performance metrics mapping for SLA monitoring. KNOM Rev, 2002. 5(2).

[42] Swander, B.D. and W.H. Dixon, Method and apparatus for traversing a translation device with a security protocol. 2008, Google Patents.

[43] Sharma, M., et al., System and method for secure network roaming. 2008, Google Patents..

[44] Mishra, A., Security and quality of service in ad hoc wireless networks. 2008: Cambridge University Press.

[45] Fenton, N. and J. Bieman, Software metrics: a rigorous and practical approach. 2014: CRC Press.

[46] D Gaiti," Network Control And Engineering For QoS, Security And Mobility", IFlP TC6/ WG6.2 & WG6.7 Conference on Network Control and Engineering for QoS, Security andMobility, 2002, Paris, France

[47] R Burnett, A Brunstrom, A. Nilsson," Communication, Media and Information Technology", Printed and bound in Great Britain by TJ International, ISBN 0-470-86863-5, 2003

[48] Tang, S.-Y., P. Muller, and H. Sharif, WiMAX security and quality of service: an end-to-end perspective. 2011: John Wiley & Sons.

[49] A. Rachedi, ., et al., A secure mechanism design-based and game theoretical model for manets. Mobile Networks and Applications, 2010. 15(2): p. 191-204.

[50] Doerr, C. and P. Smith, Resilience and Survivability for future networking: framework, mechanisms, and experimental evaluation. ResumeNet Deliverable D, 2010. 2: p. 1b.

[51] G.A. Fink et al., A metrics-based approach to intrusion detection system evaluation for distributed real-time systems. 2002, DTIC Document

[52] Bari, F. and V. Leung. Multi-attribute network selection by iterative TOPSIS for heterogeneous wireless access. in 2007 4th IEEE Consumer Communications and Networking Conference. 2007.

[53] F Dressler," A Scalable Environment for Quality of Service Measurements in the Internet. in Proceedings of 2nd IASTED International Conference on Communications, Internet, and Information Technology (CIIT 2003), Scottsdale, AZ, USA. 2003. Citeseer.

[54] N, X., et al., Analyzing Comprehensive QoS with Security Constraints for Services Composition Applications in Wireless Sensor Networks. Sensors, 2014. 14(12): p. 22706-22736.

[55] Mengual Galan, L. and L. Enciso Quispe, Analysis of QoS parameter in AODV a DSR in mobile Ad Hoc networks. 2012.