International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 10, Volume 2 (October 2015) www.ijirae.com

The Analyse of Adding Security on QoS Parameters

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

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

Mohamad Kshour
School of Electrical and Computer
Univerity of Tehran

Abstract— 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. In this paper we propose a new method for securing the QoS parameters using layer2 of OSI Model, and analyse the impact resulting from adding the security on QoS parameters such delay, jitter, loss and bandwidth.

Keywords— Quality of service; security; measure ; Quality of service parameters; security parameters

I. INTRODUCTION

A computer network is a telecommunication's network that allows computers to exchange data. In computer networks, networked computing devices transfer data in the form of packets to each other, along data connections (network links). The connections between nodes are established using either cable media or wireless media. The best-known computer network is the Internet.

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.

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.

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]. Poor security mechanism selection and placement can reduce the performance of a carefully queued network. Inappropriate service level selection can leak extra information about the importance of packets in the traffic stream, but clever manipulation of quality of service parameters might even help to reduce leaking of information through covert channels.

The protection of exchanges is usually achieved using security mechanisms and protocols. However, adding security to a service increases the resource consumption and the delay of the exchange and so decreases the quality of the service [2]-[4].

To select the security parameters, we based our work on the ISO 7498-2 Recommendation, which describes in details the different security services and mechanisms available for each OSI layer, and the IPsec and TLS security protocols, which are mainly used to secure the Internet, unlike QoS evaluation, security is not an absolute quantity and no quantitative approach exists to evaluate it. [5]-[7] and [17]. In this paper we will use tunneling without IPsec protocol (layer 3) but with L2tp protocol (layer 2), which means using the layer 2 of OSI Model.

This paper presents in Section 2 the related work. Section 3 QoS component. Section 4 security and QoS . Section 5 a new model of network that join the security and QoS. Section 6 simulation and analyse. Section 7 concludes on open issues and perspectives of this work.

II. RELATED WORK

There are some researches related to the study of Security and QoS tradeoffs, where each has developed a specific scenario such as scientific method or simulation method.

In [1] 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.

There are some articles very related to our paper such as the [17]. 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 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 configuration.

In [19], 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 this integration the authors provide a new way of how QoS and security related services could be provided in parallel, and also provide new ideas of how new models could be designed to provide different service types. Through this research, the designed model can be used for different service types or for different applications. Based on the collected results, the authors stated that the new model that integrated the new modified security service vector (SSV) model with CLD (the dynamic source routing protocol (DSR)+SSV CLD), has reduced the processing time as compared with standard DSR model and the DSR + SSV model. The presence of delay and packet processing delay in the results of their research indicates that integrating the modified SSV model with CLD results in an insignificant increase of delays in the MANET network, and also an increase in the total processing delays.

Finally, when the performance of implemented modified SSV and CLD model in MANET was simulated, comparable results were achieved in the DSR model. Deviations were caused by the modified SSV activity and physical parameters of the MANET network.

In our work we talked about layer 2 of OSI Model and about VPN (virtual private network). These concepts are referred by [20] that describes an architecture for the management of QOS enabled VPN over internet. The architecture focuses on two important issues of VPNs: security and Quality-of-Service (QoS). The security achieved in VPNs is based on IPSec tunnels. But in our work the security will be based on layer 2 of OSI Model not on layer 3, in other word not on IPSec but on L2TP. This architecture is based on a generalization of the bandwidth broker concept introduced in the DiffServ environment, and it allows for automated service configuration because the architecture framework includes a service broker hierarchy. An instantiation of the framework allows a user to set up, change, and modify VPNs including parameters such as security and QoS related parameters. Finally the authors arrived to result that "This architecture forms the basis of the implementation of a demonstrator scenario currently being implemented." VPN is one of some methods for security on network, but dynamic Virtual Private Network (VPN) tunnel is the method used by [29].

They present that Dynamic Quality of Service (QoS) treatment of traffic within a secure Virtual Private Network (VPN) tunnel is provided by attaching a QoS marker to data traffic at an ingress end of the VPN tunnel. By querying a policy database the QoS marker is obtained, during tunnel setup the policy data base can be queried by a VPN Gateway at an ingress end of the tunnel and/or at any time following tunnel setup to obtain updated QOS information. This updated QoS information is then propagated through the VPN tunnel to a VPN gateway at the opposite end of the VPN Tunnel, so that it can be used for egress processing of the tunnel. After this introduction the authors present the working mechanism with some figures and scenario of the interaction between VPN getaways and others device such NIU, NSP, PS. Finally they suggested a method of providing dynamic Quality of Service (QoS). 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. QoS Component

A. QOS definition

QOS "Quality of service" 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 SLAs (service level agreement) 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. [7]

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 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 [7]

Some very important issues related to the QoS, are specified by International Telecommunication Union (ITU) and collected in [13]:

1-QoS requested by the user / customer((QoSR), QoS requirements: QoS requested by a user or by one or more segments of the population users who have the same needs in terms of quality of operation.
NOTE - The needs of users can be expressed in descriptive terms (criteria) and listed in terms of priority and a preferred value must be given to each criterion. The provider of Service then translates the services into numerical parameters and values [8].

2-QoS offered by the service provider: A statement of the level of quality expected to be offered to the customer by the service provider.
QoS delivered/achieved by the service provider: A statement of the level of the actual quality achieved and delivered to the customer.

3-QoS perceived by user/customer: A statement expressing the level of quality that customers believe they have experienced.

4-QoS parameter: A definition of the scope of a QoS criterion with clear boundaries and explicit measurement method to enable a quantifiable or qualifiable value to be assigned.

B. QoS Architectures

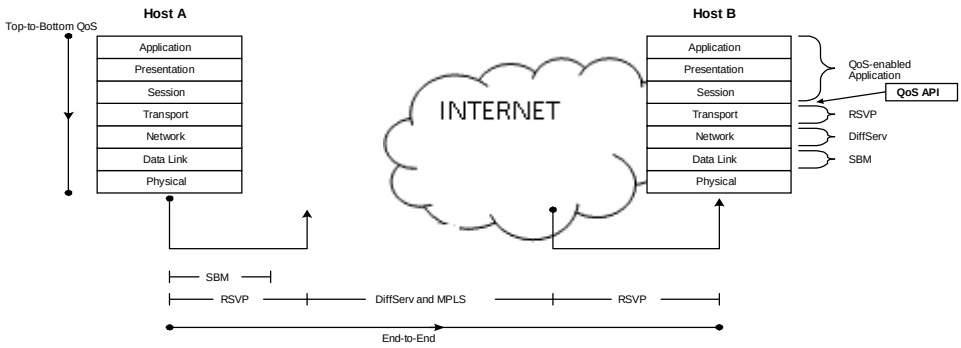

Fig.1 QoS Architectures

C. QoS Parameters

In this section we present parameters that are mostly used to describe QoS requirements of IP traffic and QoS provided by IP networks. According to IETF (Internet Engineering Task Force), the Quality of Service refers to the nature of the packet delivery service provided, as described by parameters such as achieved bandwidth, packet delay, and packet loss rates… In fact, different applications may have different interpretations of their QoS requirements.

D. QoS Models

There are two QoS architectures used in IP networks when designing a QoS solution which are the IntServ and DiffServ models. The QoS service models differ by two characteristics:

1-How the models enable applications to send data.

2-The way in which networks attempt to deliver the respective data with a specified level of service.

A third method of service is the best-effort, which is essentially the default behavior of the network device without any QoS , The best-effort is the standard form of connectivity without any guarantees. This type of service, in reference to catalyst switches, uses first-in, first-out (FIFO) queues, which simply transmit packets as they arrive in a queue with no preferential treatment.. In summary, the following list restates these three basic levels of service for QoS: Best-effort service, integrated service, and differentiated services [9].

IV. SECURITY AND QOS

Security is one of the most important elements in any network and has been discussed by keen technicians since 1960 [10]. 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.

That is why engineers and technicians are seeking to reach the best services provided by the network through quality 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, and we seek through this paper to analyze and study increasing security on QoS, and analyzing the variation of their parameters values, and the impact of each of the security parameters on the results. Therefore, we want to view if any of security parameters have a direct impact on QoS parameters such as the Effect of Encryption and Authentication on Delay [16].

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 others parameters of security. In order to pursue our goal of securing the network, we must improve the weak points of OSI layers. Through our knowledge in OSI layers, the second layer (data link layer) is considered one of the weakest layers due to its proximity to the physical layer, and thus benefiting from the second layer of OSI Model helps in preventing access to the upper layers.

After that, we measured again all parameters QoS in order to compare it with the previous values and to study and analyze the changes occurring from the increased security to the quality of service parameters. This analysis was based on the results that we reach through simulation and mathematical equations.

V. A NEW MODEL OF NETWORK JOINING QOS AND SECURITY

Through this section we'll show the way in which we will use it or hind steps to reach the positive results. So we are going to do some basic steps. First thing to do is to build a network with Opnet. Second step we measured the parameters of QoS. Third step adding the security using the security protocols on data link layer such L2TP, fourth step we measured again those parameters, then comparing them with the previous results, and studying and analyzing the variation that occurred as result of increasing the security to those parameters. So this article passed the following steps:

1-Create network and simulation
2-Install QOS
3-Measure QOS parameters
4- Adding the Security on QOS parameters in the new model.
5-Measure QoS parameters

A. Create network:

we created a network by a simulation program this network contain more types of data such as video, audio, file.

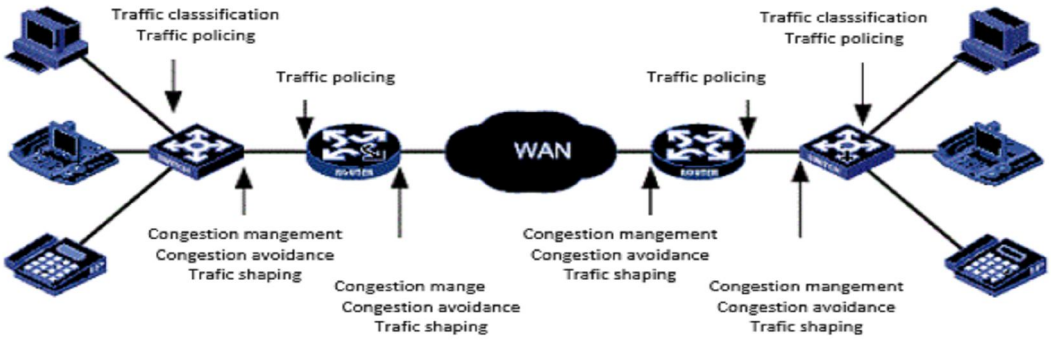

Figure-2 QoS Network

B.2 - Install QOS:

we had several methods for deploying QOS but we used one of them :

2.1 CLI (command line interface): A command-line interface or command language interpreter (CLI, is a means of interacting with a computer program where the user (or client) issues commands to the program in the form of successive lines of text (command lines), use the command by IOS[7].

2.2 MQC (modular QOS command): Modular Quality of Service Command Line Interface (Class-map + policy –map + service-map), creation groups of QOS using class-map, policy-map, and service-map. (This method that we used)

2.3 CCP (Cisco configuration Professional): using a program by windows configuration replacement command line.

2.4 Auto QOS: using one command on cisco router for deploying QOS automatic.

C. 3- QOS's parameters Measure

We had several methods for the measurement of QOS parameters:

3.1 A Method of QoS Measurement Based on User Behavior Analysis [11].

3.2 Method using Fast Ethernet taps to monitor full-duplex traffic and programmable network interface cards to extract all the information needed to compute the network QOS parameters: latency, jitter, packet loss and throughput [12].

3.3 Estimation and measuring using an algorithm that collects a histogram of the occupancy of a single-server FCFS queue at packet arrival times, and infers the loss rate and delay distribution from such measurements [14].

3.4 A Metric for Numerical Evaluation of the QOS : this is a method which allows one to use measured QOS values and the application requirements to compute a numerical representation for the service quality[15].

Delay: is the difference between send time and receive time.

The one-way delay (Δt_{OWD}) as follows: $\Delta t_{OWD} = t_{resv} - t_{sent}$.

Jitter: Variation is the difference between packet delay from end-to-end $\Delta t_{jitter} = \max_{k} \left(\left| \frac{\sum_{i=0}^{n} \Delta t_{OWDi}}{n+1} - \Delta t_{OWDk} \right| \right)$

We used this method because it has a numerical representation that helps us compare the result of simulation method.

D. Adding the Security on QOS parameters in new model

In different ways Security and QOS can be joined together. For example in mobile ad hoc we have securing the QOS routing protocol, Quality of security service (QoSS).

Currently, there are some studies that talked about the existence of IT spending on layer 3 to benefit from IPsec in order to secure the encryption. In this paper we presented a new method of security for QoS using the tunnel on layer2 of OSI Model . The primary goal of this work is providing high quality of service with VPN using tunneling technique and using security protocols of layers2 of OSI Model, this method is based on the encapsulation technique(as show in figure 4), that is the process of encapsulating the packets inside an additional header before tunneling. This additional header contains the routing information necessary to send the encapsulated payload through the intermediate internetwork(as show in figure 5). This information is essential because the payload is sent through a network (protocol) different to the network in which the data was created. In Layer 2 (which uses frames as the unit of exchange) tunneling, both PPTP and L2TP do encapsulation in a PPP (Point-to-Point Protocol) . In Layer 3 (which uses packets as the unit of exchange) tunneling, IPSec tunnel mode encapsulates IP (Internet Protocol) packets with an additional IP header.

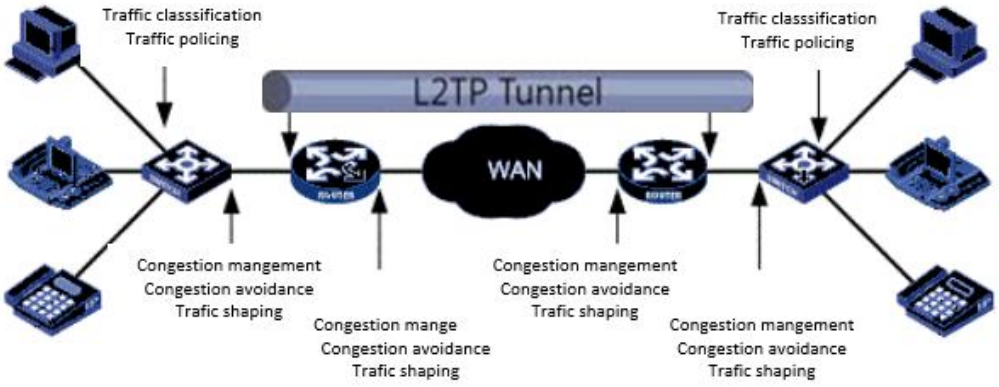

Fig. 3 QoS with the Tunnel Technic

With the rapid growth of IP networks in the past years, high-end switching has played one of the most fundamental and essential roles in moving data reliably, efficiently, and securely across networks. The tunnels are the leader in the switching market and major players in today's networks.

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.

So security will become one of QOS's parameters, in which the parameters of QOS will become (delay, jitter, loss, reliability, throughput, bandwidth, and security).

Understanding and preparing for network threats is important, and hardening Layer 2 is becoming imperative. Tunnel is continuously raising the bar for security, and security feature availability at Layer 2 is no exception. The sections that follow highlight the Layer 2 security features available on tunnel with QoS [37].

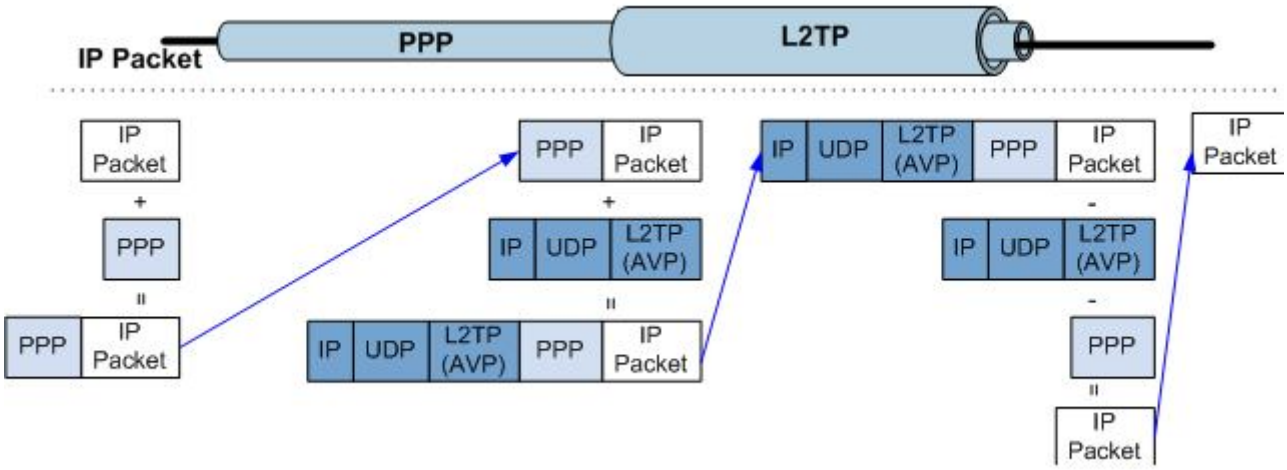

Fig. 4 The Encapsulation in L2TP Protocol.

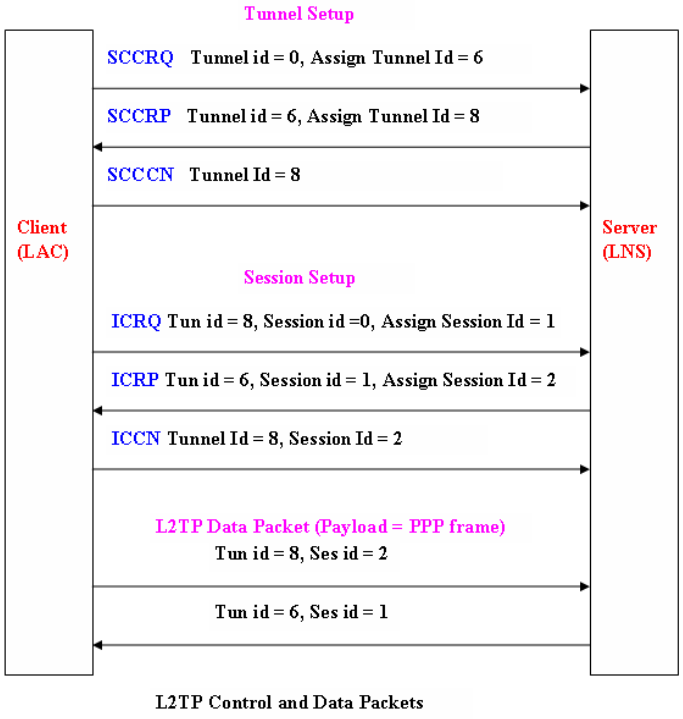

Figure.5 L2TP Control and Data Packets

VI. WHY WE CHOOSE LAYER 2 OF OSI MODEL

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

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.

VII. SIMULATION AND ANALYSE

Through the simulation that we did over the simulation program, a significant change was found in the delay Jetter values and other parameters of QoS, because of adding the security across tunnel technique where it should not exceed the required rate delay values. Figure.5 shows a significant delay that leads to disconnecting sometimes, especially if the connection was an audio connection. The parameters that values the quality of service before and after the increase of security, matched almost with values that we achieved though mathematical equations that we previously mentioned, and this is what gives credibility to the simulation and our findings.

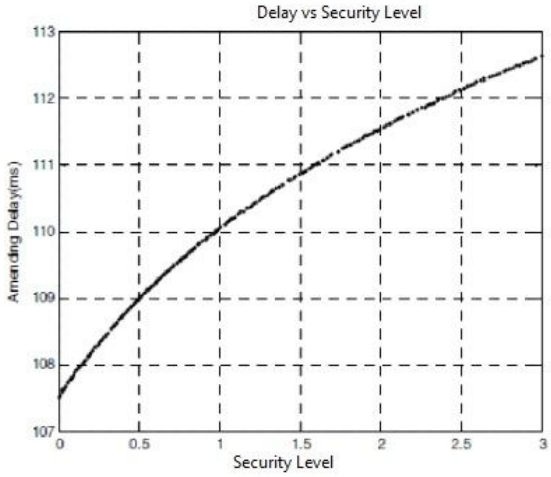

Fig. 6 The Variation of the Amending Delay Verse the Security Level.

VIII. CONCLUSION AND FUTURE WORK

Security is one of the most important elements in any network and has been discussed by keen technicians. Any network cannot be trusted 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 this paper we presented a new method security for QoS using the tunnel on layer2 of OSI Model . The primary goal of this work is providing high quality of service with VPN using tunneling technique and using security protocols of layers2 of OSI Model, this method is based on the encapsulation technique. With the simulation programme OPNET we showed the impact of adding security on QoS and the match between the result of simulation and the result of equation numeric. 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]. 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.

[2]. 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.

[3]. 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

[4]. 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.
[5]. Dierks, T. and E. Rescorla: "The TLS Protocol Version 1.1", IETF Internet Draft, Dec. 2004.
[6]. ISO, "Information Processing System – Open System Interconnection – Basic Reference Model – Part 2: Security Architecture", International Standard ISO 7498-2, ISO, Feb.1998.
[7]. Seo, K. and S. Kent, Security architecture for the internet protocol. 2005.
[8]. http://searchwindowsserver.techtarget.com/definition/command-line-interface-CLI
[9]. 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
[10]. http://www.ciscopress.com/articles/article.asp?p=170743.
[11]. Lindskog, S. and E. Jonsson. Adding Security to Quality of Service Architectures. in Proceedings of the SS-GRR Conference. 2002.
[12]. 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..
[13]. Beuran, R., et al., Network quality of service measurement system for application requirements evaluation. SIMULATION SERIES, 2003. 35(4): p. 380-387.
[14]. ITU-T Recommendation "Framework and methodologies for the determination and application of QoS parameters",ITU, 2008.
[15]. 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..
[16]. Dressler, F., A metric for numerical evaluation of the QoS of an Internet connection. Teletraffic Science and Engineering, 2003. 5: p. 1221-1230.
[17]. 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.
[18]. Hayajneh, T., et al., Performance and Information Security Evaluation with Firewalls. International Journal of Security & Its Applications, 2013. 7(6).
[19]. Cizmar, A., J. Papaj, and L. Dobos, Security and QoS integration model for MANETS. Computing and Informatics, 2012. 31(5): p. 1025-1044
[20]. 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.
[21]. Alexander, D.S., et al., Secure quality of service handling: SQoSH. Communications Magazine, IEEE, 2000. 38(4): p. 106-112.
[22]. 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.
[23]. 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..
[24]. 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.
[25]. 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.
[26]. 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.
[27]. 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.
[28]. Roch, S. and G. Algie, Dynamic virtual private network (VPN) tunnel quality of service (QoS) treatment. 2000, Google Patents.
[29]. 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
[30]. Andersson, J.A. and Z. Hossein, QoS in Today's Internet. 2004.
[31]. Nieto, A. and J. Lopez, Security and QoS relationships in mobile platforms, in Computer Science and its Applications. 2012, Springer. p. 13-21.
[32]. 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.
[33]. 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.
[34]. Foley, S.N., et al., Multilevel security and quality of protection, in Quality of Protection. 2006, Springer. p. 93-105.
[35]. Jason, J., L. Rafalow, and E. Vyncke, IPsec configuration policy information model. 2003.

[36]. 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.
[37]. 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.
[38]. Nanji, S. and W. Palter, Tunnel interworking. 2005, Google Patents.
[39]. 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.
[40]. Lee, H.-J., et al., QoS parameters to network performance metrics mapping for SLA monitoring. KNOM Rev, 2002. 5(2).
[41]. Swander, B.D. and W.H. Dixon, Method and apparatus for traversing a translation device with a security protocol. 2008, Google Patents.
[42]. Sharma, M., et al., System and method for secure network roaming. 2008, Google Patents..
[43]. Mishra, A., Security and quality of service in ad hoc wireless networks. 2008: Cambridge University Press.
[44]. Fenton, N. and J. Bieman, Software metrics: a rigorous and practical approach. 2014: CRC Press.
[45]. 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
[46]. 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
[47]. Tang, S.-Y., P. Muller, and H. Sharif, WiMAX security and quality of service: an end-to-end perspective. 2011: John Wiley & Sons.
[48]. 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.
[49]. Doerr, C. and P. Smith, Resilience and Survivability for future networking: framework, mechanisms, and experimental evaluation. ResumeNet Deliverable D, 2010. 2: p. 1b.
[50]. G.A. Fink et al., A metrics-based approach to intrusion detection system evaluation for distributed real-time systems. 2002, DTIC Document
[51]. 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.
[52]. 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.
[53]. 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.
[54]. Mengual Galan, L. and L. Enciso Quispe, Analysis of QoS parameter in AODV a DSR in mobile Ad Hoc networks. 2012.
[55]. 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.
[56]. Aiash, M., An integrated approach to QoS and security in future mobile networks using the Y-Comm framework. 2012, Middlesex University..