International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 9 • Number 45 • 2016

Performance Analysis of WAP Gateway Over Web Server Using OPNET

Kamini[a] and Rajiv Mahajan[b]

[a]*(Research Scholar) Computer Applications I.K. Gujral Punjab Technical University Kapurthala, India*
E-mail: Kamini_girdhar08@hotmail.com
[b]*Computer Science & Engineering, I.K. Gujral Punjab Technical University Kapurthala, India*
E-mail: Rajivmahajan08@gmail.com

Abstract : Security for wireless devices is becoming important day by day. When internet connection is available for mobile devices all the communication pass through some intermediates. The end to end security is the major issues in wireless security devices like mobile phone and PDA(Personal Digital Assistant).When mobile device wants to communicate to the web server through internet the all the communication pass through the WAP gateway. This WAP gateway translates all the protocol used in WAP to the protocols used on the internet. The WAP proxy server use encoding and decoding technique for the content to reduce the size of the data that has been sent through the wireless link. The communication between the mobile phones and wireless application protocol is secured by using the security protocol is called WTLS .The communication between the WAP gateway and web server is secured through the TLS/SSL security protocols. This paper presents an evaluation study of wireless and wired network using OPNET simulation tool. This paper simulated 2 different scenarios comparing wireless mobile client communication using WTLS gateway MD5_RSA encryption and Firewall gateway TLS encryption using MD5_RSA.The investigation results shows that how the end to end security take place between wireless client to web server using hybrid security protocol.

Keywords : *OPNET; Security; WAP; Server*

1. INTRODUCTION

In today most of the applications are accessed through the wireless devices like mobile phones and personal digital assistant in any of the area like commercial, medical, manufacturing and other. Due to big accessing of internet through the wireless devices the security has become the important issue. In modern societies the sharing of resources using the mobile phones throughout the world becomes very important. The advanced facilities of mobile device allow the user to buy the products, pay for products, internet surfing and manage various back accounts anywhere without moving to specific location [1].

A mobile user always asks for a higher speed at lower prices, and demands to be "Always Best Connected" [2].Mobile networking promises its users to use fully functionality of anything, anytime, anywhere [3].The wireless internet evolution support for accessing anything from mobile networking at any time. A main challenge in such heterogeneous networks is the chances of roaming for administrative domains to which a mobile client home domain does not have a well established roaming agreement [4, 5].over the last few years wireless networks based on IEEE 802.11 standard have experienced remarkable growth. This has happened because of releasing the IEEE 802.11 standard, low cost hardware and high data rate and speed [6].

The fast growth of wired and wireless technologies, as well as increased in the demand of mobile users to get connect at any time at anywhere, demand in the development of wireless networks. The main feature of wireless technology is small in size and its portability. In today' time various distributed application peoples use network communication channels to communicate with each other. The end to end communication is possible only with the use of protected encryption and decryption methodology. Privacy, security and authentication is provided by security protocols. Hotspot operators offer wireless Internet in public places like cafes, restaurants, hotels and airports. A Wi-Fi community called FON has more than 7 million hotspots worldwide [7].

The extensive use of mobile communication has creates an important demand for value added services.WAP is a framework for developing applications to run over wireless networks.WAP is developed by the international industry wide organization called WAP forum [8]. The next is Transport Control Protocol (TCP), the most used transport control protocol, works well over wired networks. As many wireless networks is deployed, TCP should be altered to work for both wired and wireless networks. TCP model is designed especially for congestion control in wired networks; it cannot detect any non-congestion related data packet loss from wireless networks [9]. Both the communications for wireless and wired were developed to be based on link to link and working with the same protocols, based on IEEE 1451.0-2007 [10]. As wireless mesh networks are deployed on the base of a new concept named hybrid internetworks, i.e., internetworks that contain both wired mesh networks and wireless mesh networks. Routing is most challenging today that arise in hybrid internetworks: indeed, while specific routing protocols are typically designed for wired communication on one hand and for wireless communication networks on the other hand, it has been seen that work with a one routing protocol to manage a hybrid internetwork as a whole an built several advantages [11]. Wireless sensor networks (WSN) are ad-hoc mobile networks with the sensors have limited number of resources and communication capacity [12] A Radio Frequency Identification Device (RFID) permits a very good identification technique for a large number of tagged objects without any physical or visual contact [13]. With the privacy, an applied method that ensures a private end to end transfer is defined [14]. As a result RSA encryption method in the client side is very less expensive, whereas the corresponding decryption applied on server side is much expensive because its private component is much larger [15]. A self-optimizing wireless data network which can optimize the network performance by itself at run time [16]. The latest generation of wireless projectors has made possible of real-time communication between a room-full of business class executives or students a reality [17]. Wireless technologies promise to provide even more features than any other network and functions in the next few years [18].but both of these methods are identity-based verification mechanisms [19]. A large number of organizations, based on literature theory, believe that the security provided by their deployed wireless access points is enough to prevent unauthorized user access and use [20].

2. PROBLEN FORMULATION

The motivation behind this research work is that in current wireless telecommunication networks, all the traffic is in the air is encrypted but end to end security is not provided between the wireless devices and WWW server. In existing system double encryption and decryption is used for providing the communication between the mobile devices and a web server. On the other hand when transaction arrives at the gateway Through the WAP the data is encrypted and decrypted for wireless and again it will be Re-encrypted by gateway when the transaction has to pass through the wire. At this time of Re encryption the data can be hacked by any of the unauthorized user. The use of the Internet and mobile phones may integrate the satellite, radio and audio video communication. The main idea behind this research is to develop a hybrid security protocol that will provide a single secure channel for end to end communication.

3. OBJECTIVES OF STUDY

1. To identify and analyze the security holes in between the wireless client and WAP gateway.
2. To propose an Enhanced Protocol to overcome the security holes.
3. To design and implement the proposed composite security protocol architecture for wired and wireless devices.
4. To compare the performance of Transport layer security and Wireless Transport Layer Security with proposed protocol.
5. To improve the end to end Security in hybrid networks.

4. RESEARCH METHODOLOGY

To achieve the set of objectives, our research focused on the performance measuring from wireless client to wired server with implementation the method of hybrid security protocol .In this research we have considered two types of scenarios. Firstly, comparing wireless mobile client communication using WTLS gateway MD5_ RSA encryption. Secondly, Firewall gateway TLS encryption using MD5_RSA.To simulate the results Opnet is wide and powerful software which provide the various possibility to simulate entire heterogeneous in networks with various protocols. Our research focused on algorithms implementation in various phases.

First phase: This phase contains the basic layout of network with client node and server node.

Second Phase: In this phase we have configured the network with set of applications .The profile configuration is used to create user profiles. We can specify the traffic patterns followed by the applications as well as the configured profiles on this object. We have also defined the Defines Virtual Private Network (VPN) attribute configuration details for tunnelling supported at the IP layer.

Third Phase: In this phase we have created scenarios for wireless and wired network with different set of attributes.

Fourth Phase: In this phase we have implemented the hybrid security protocol by applying the security at web server.

Fifth Phase: in this phase we have done simulation with different scenarios with different type of security protocol.

Sixth Phase: Result is compared with all scenarios on the basis of parameters like delay, throughput, and traffic sent and received; HTTP and FTP downloaded Response time

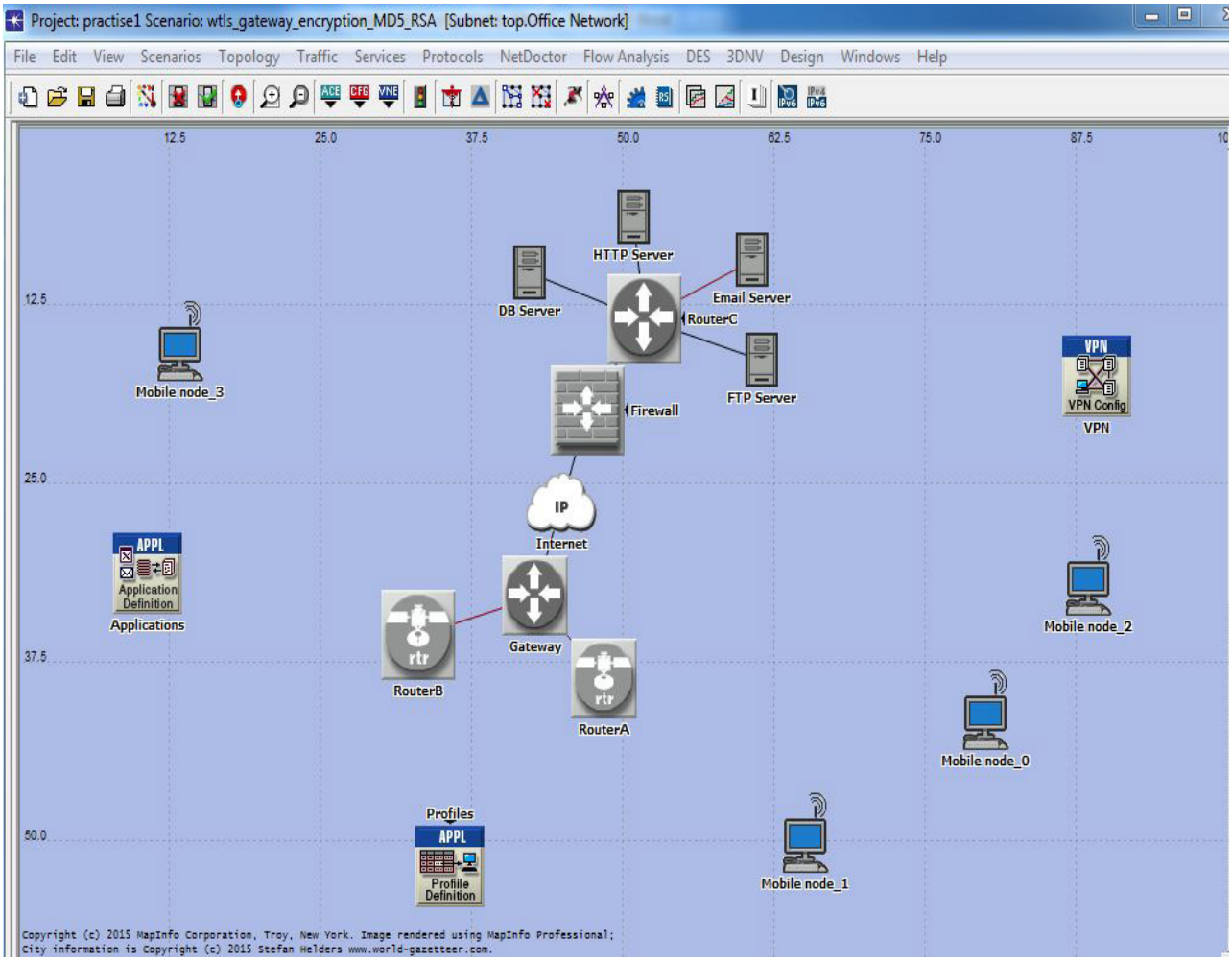
5. SCOPE AND SIGNIFICANCE OF STUDY

5.1. Simulation Environment and Parameters

The model is developed using the OPNET simulation environment. The network diagram is created with 4 client node and 4 server nodes. Encryption and decryption is applied on client side and server side model. The gateway is used to pass all encryption data from wireless client to wired server. The simulation results are based on throughput, delay, FTP uploading and downloading response time and DB query traffic sent and received etc. OPNET is wide and powerful simulation software which enables the possibility to simulate entire heterogeneous networks with various protocols. Originally this software was developed for the need of military but now it has become the world leading commercial network simulation tool. OPNET simulation operates at packet level it contains a huge library of accurate models of commercially available fixed network hardware and protocols. This tool is used to create large network environment via software.

5.2. Simulation Results

Scenario 1. Wireless client mobile communication using WTLS gateway MD5_RSA encryption



Figurue 1

Scenario 2: Firewall gateway TLS encryption using MD5_RSA

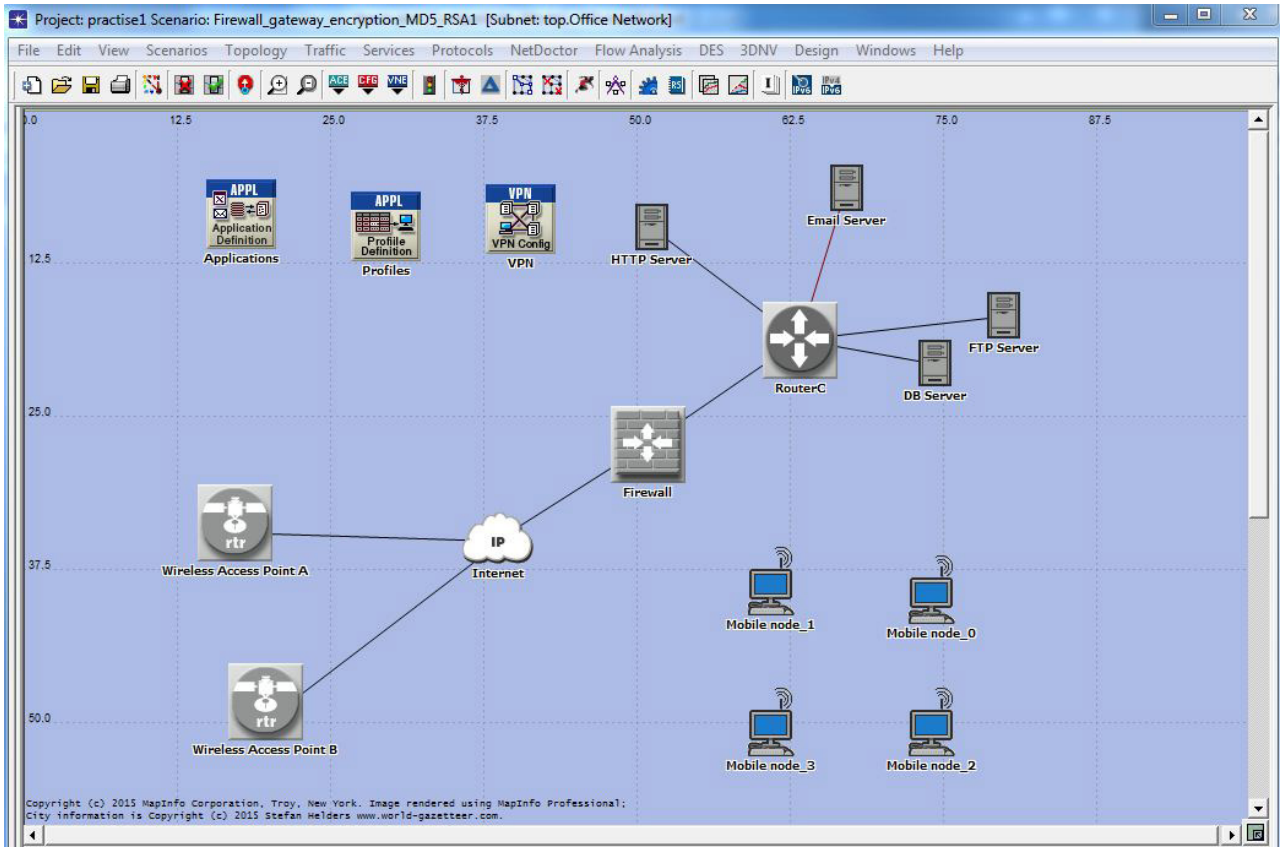


Figure 2

(*a*) Throughput of wireless client and wired server

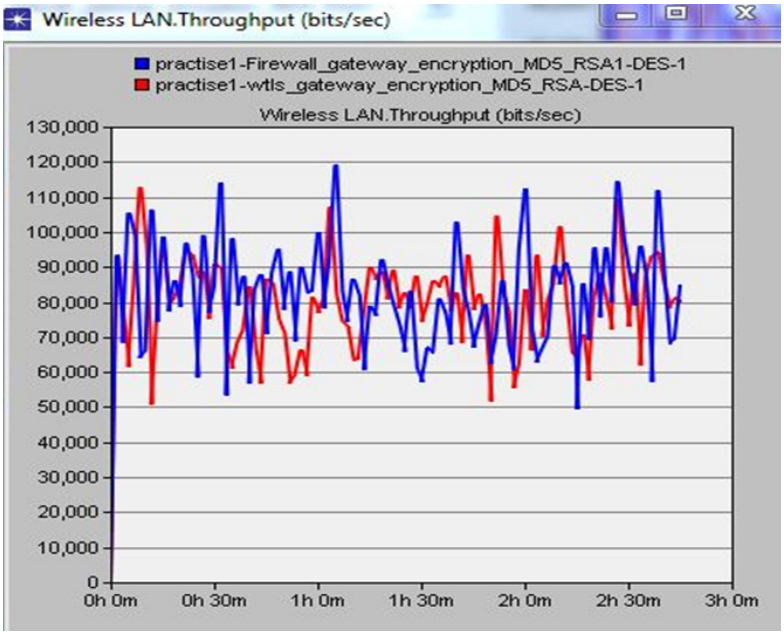


Figure 3

(*b*) Delay

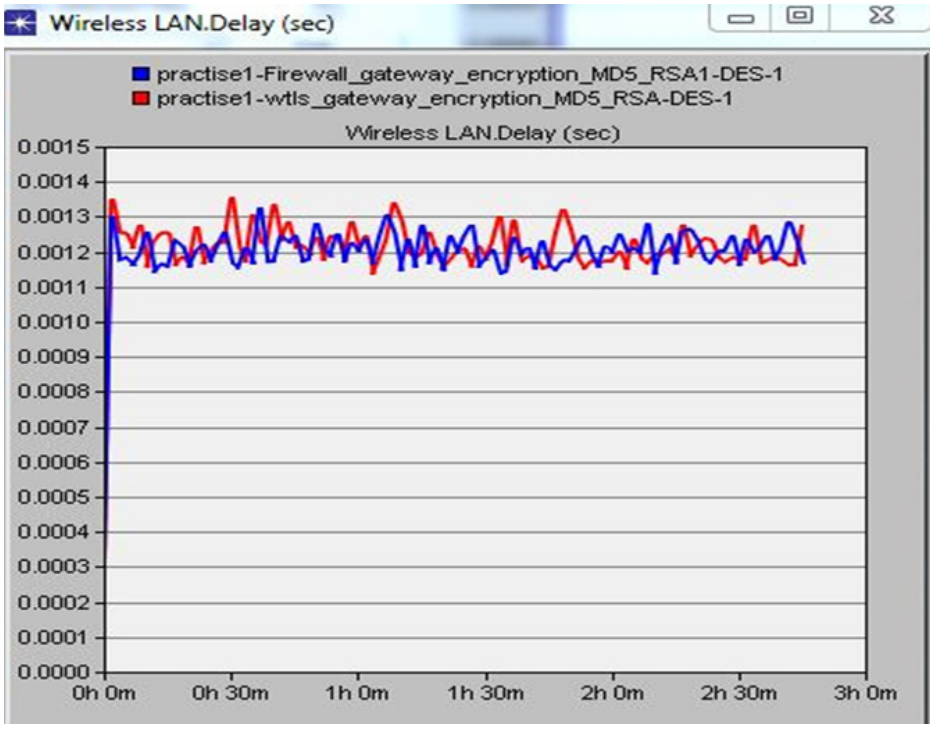


Figure 4

(*c*) Load in wireless local area network

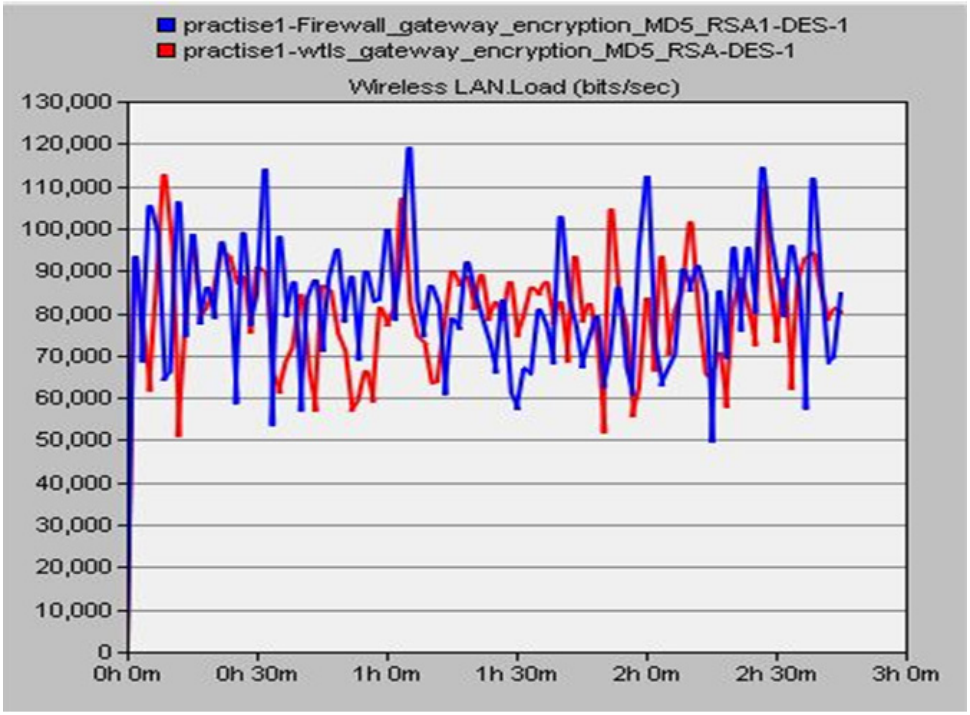


Figure 5

(*d*) Wireless LAN Media Access Delay

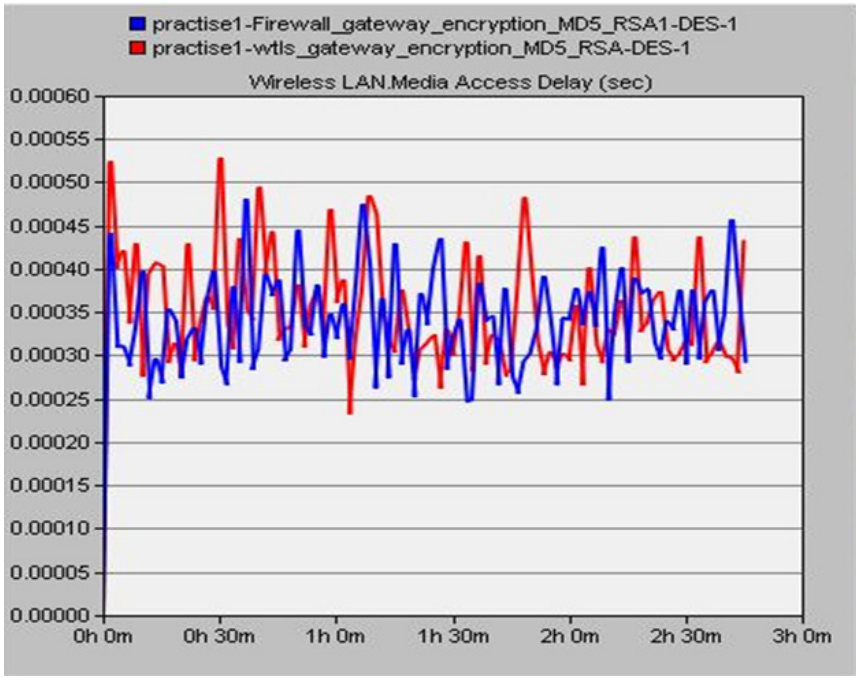


Figure 6

(*e*) DB query traffic received

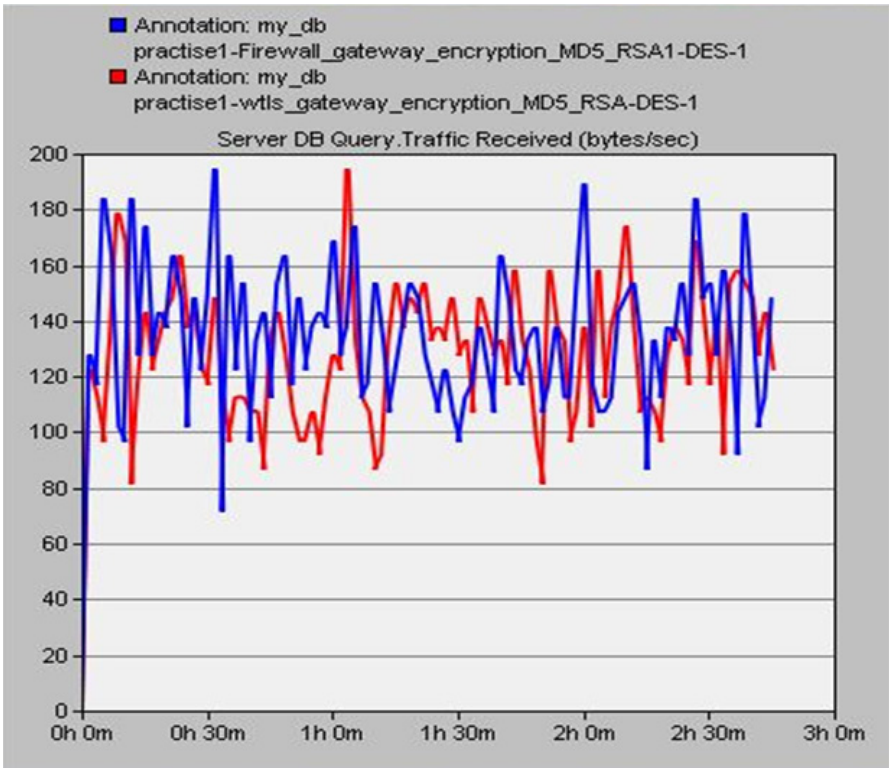


Figure 7

(*f*) DB query traffic sent

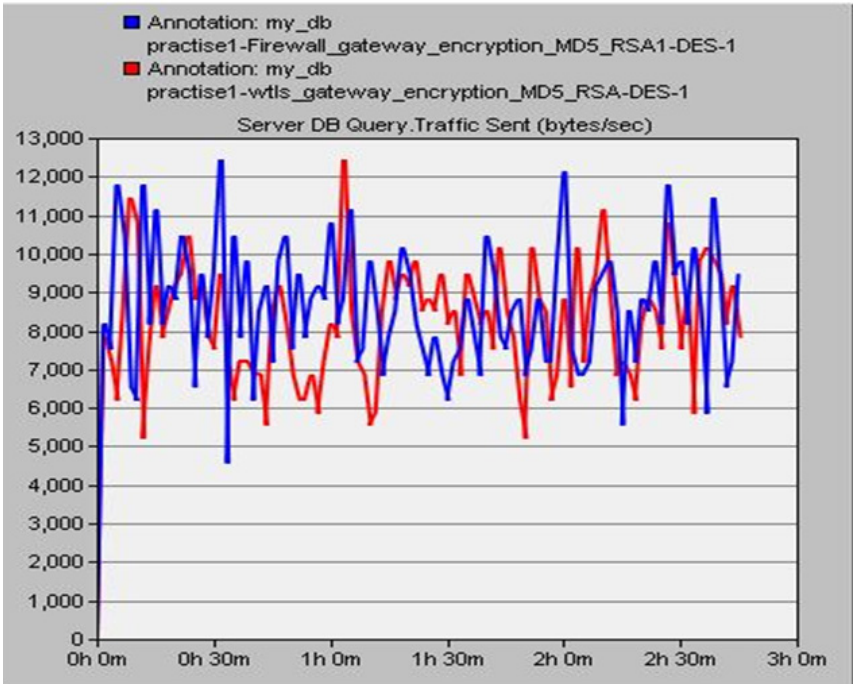


Figure 8

(*g*) FTP server traffic received

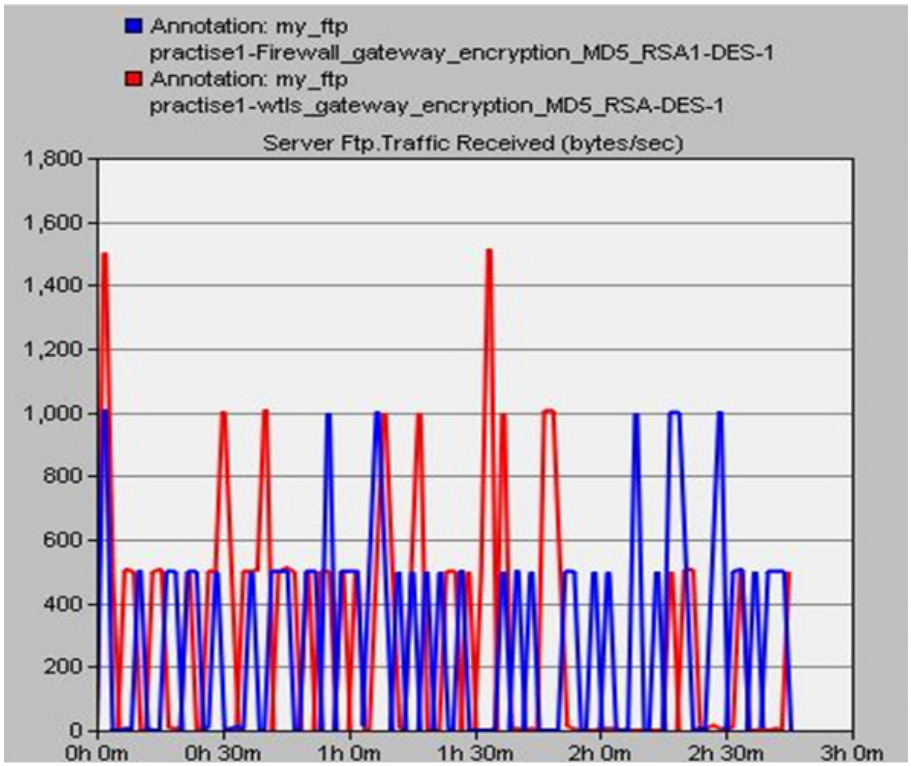


Figure 9

(*h*) FTP server traffic sent

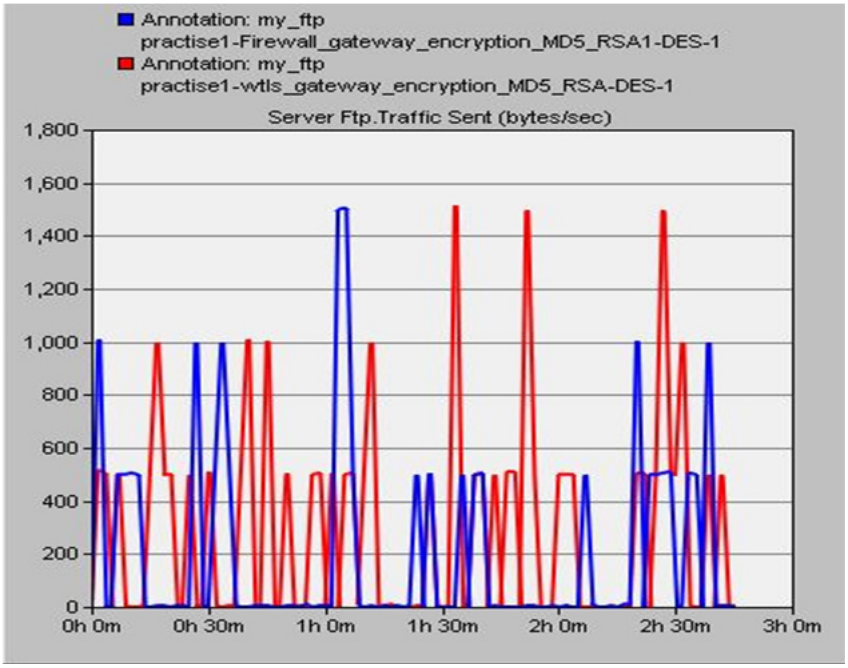


Figure 10

(*i*) Firewall to Router Throughput

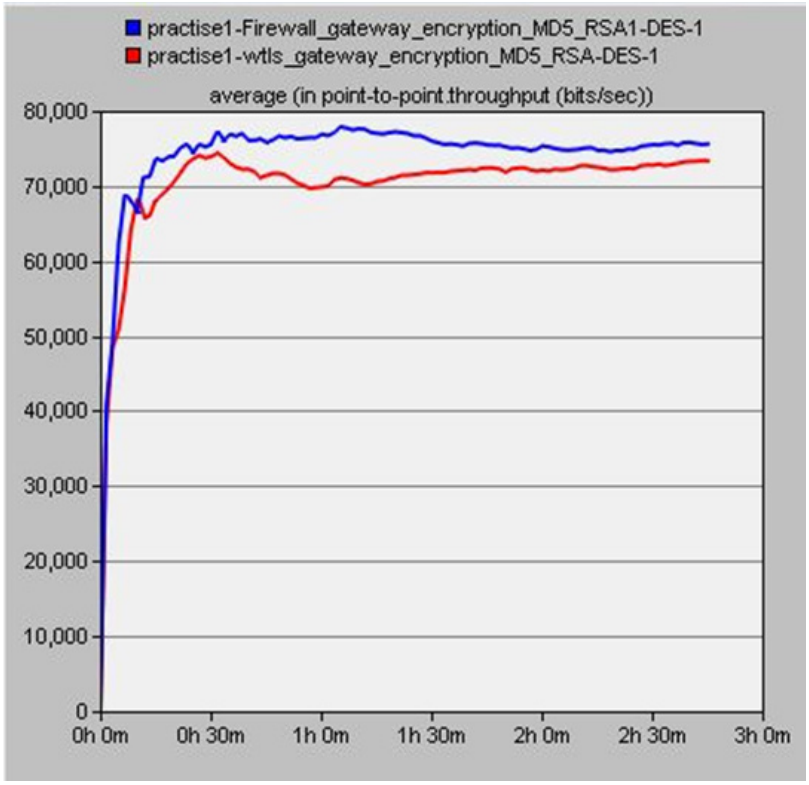


Figure 11

6. COMPARISON TABLE FOR SIMULATION RESULTS

Table 1

Parameters	*WTLS MD5_RSA*	*TLS MD5_RSA*	*Hybrid Protocol*
Throughput	90 Bits/Sec	120 Bits/Sec	120 Bits/Sec
Delay	0.0013 Sec	0.0012 Sec	0.0012 Sec
Load in WLAN	120,000 bits per sec	110,000 bits per sec	110,000 bits per sec
WLAN Media Access Delay	0.00053 sec	0.00046 sec	0.00046 sec
DB Query Traffic Received	197 bits per sec	199 bits per sec	199 bits per sec
DB Query Traffic Sent	12500 bytes per sec	12000 bits per sec	12000 bits per sec
FTP Server Traffic Received	1500 bytes per sec	1000 bytes per sec	1000 bytes per sec
FTP Server Traffic Sent	1550 bytes per Sec	1600 bits per sec	1600 bits per sec
Firewall to Router Throughput	70,000 Bits/Sec	75,000 Bits.sec	75,000 Bits.sec
Firewall to Router Channel Utilization	4.5 Sec	5 Sec	5 Sec

7. CONCLUSION

This paper have focused on the simulation modeling of wireless devices and wired devices. Today mobile is accessed by most of the person in daily life just because of its features like low bandwidth, small in size and limited power consumption. The WTLS security layer is used for wireless devices and TLS is security layer used for wired devices. During the communication between the wireless devices and the gateway the encryption and decryption are used for WTLS protocol .Again while communicate through the gateway to web server re-encryption is required. This re-encryption leads to the problem of WAP gap. To remove this WAP gap the architecture design for the WTLS and TLS need to be modified.

In this paper we have analysed the performance of wireless and wired security model with the help of OPNET simulation tool. We the analysed the results of both security protocol on the basis of parameters like delay, throughout, data sent and received etc.

REFERENCES

[1] Rehunathan D, Bhatti S. Application of virtual mobile networking to real-time patient monitoring. InTelecommunication Networks and Applications Conference (ATNAC), 2010 Australasian 2010 Oct 31 (pp. 124-129). IEEE.

[2] Gustafsson E, Jonsson A. Always best connected. Wireless Communications, IEEE. 2003 Feb;10(1):49-55.

[3] Tanenbaum A.S. "Computer Networks," Prentice Hall India (PHI), November 1998.

[4] Tuladhar SR. Inter-Domain Authentication for Seamless Roaming in Heterogeneous Wireless Networks (Doctoral dissertation, University of Pittsburgh).

[5] Tuladhar SR, Caicedo CE, Josh JB. Inter-domain authentication for seamless roaming in heterogeneous wireless networks. InSensor Networks, Ubiquitous and Trustworthy Computing, 2008. SUTC'08. IEEE International Conference on 2008 Jun 11 (pp. 249-255). IEEE.

[6] IEEE Computer Society LAN MAN Standards Committee. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications.FON. (2012). Fon Passes 7 Million Hotspots. Available: www.fon.com,Access date: 22/02/2013.

[7] FON. (2012). Fon Passes 7 Million Hotspots. Available: www.fon.com,Access date: 22/02/2013.

[8] WAP Forum, Wireless Application Protocol Architecture Specification, WAP-210-WAPArch-200100712-a, 12-July- 2001 version, latest version is available athttp://www.wapforum.com.

[9] Joe I, Lee J. An Enhanced TCP Protocol for Wired/Wireless Networks. InINC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on 2009 Aug 25 (pp. 531-533). IEEE.

[10] Tércio Filho AS, Silva AC, Grout IA, Rossi SR. Network node with wireless and wired interfaces: Nios II processor and uClinux to development of a NCAP embedded (IEEE 1451.1) with two interfaces, wireless (IEEE 1451.5) and wired (IEEE p1451. 2). InInstrumentation and Measurement Technology Conference (I2MTC), 2011 IEEE 2011 May 10 (pp. 1-6). IEEE.

[11] Fuertes JA, Philipp M, Baccelli E. Routing across wired and wireless mesh networks: Experimental compound internetworking with OSPF. InWireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International 2012 Aug 27 (pp. 739-745). IEEE.

[12] Dellutri F, Me G, Strangio MA. Local authentication with bluetooth enabled mobile devices. InAutonomic and Autonomous Systems and International Conference on Networking and Services, 2005. ICAS-ICNS 2005. Joint International Conference on 2005 Oct 23 (pp. 72-72). IEEE.Karthikeyan, Sindhu, and Mikhail Nesterenko. "RFID security without extensive cryptography." Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks. ACM, 2005

[13] Karthikeyan S, Nesterenko M. RFID security without extensive cryptography. InProceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks 2005 Nov 7 (pp. 63-67). ACM.

[14] Palmgren K. Diffie-Hellman Key Exchange: A Nonmathematicians explanation. ISSA J. 2006 Oct.Complete WAP Security from Certicom pages 5-12

[15] Complete WAP Security from Certicom pages 5-12

[16] Csernai M, Gulyás A. Wireless adapter sleep scheduling based on video qoe: How to improve battery life when watching streaming video?. InComputer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on 2011 Jul 31 (pp. 1-6). IEEE.Shie-Yuan Wang; Chin-Liang Chou, "The Effects of Using Roadside Wireless Repeaters on Extending Path Lifetime in Vehicle-Formed Mobile Ad Hoc Networks on Highways," in Systems, Man and Cybernetics, 2006. SMC '06. IEEE International Conference on , vol.3, no., pp.2069-2074, 8-11 Oct. 2006

[17] Shie-Yuan Wang; Chin-Liang Chou, "The Effects of Using Roadside Wireless Repeaters on Extending Path Lifetime in Vehicle-Formed Mobile Ad Hoc Networks on Highways," in Systems, Man and Cybernetics, 2006. SMC '06. IEEE International Conference on , vol.3, no., pp.2069-2074, 8-11 Oct. 2006

[18] Rikure T, Jurenoks A. WIRELESS NETWORK TECHNOLOGIES IN TRANSPORT AREA: SECURITY AND E-LEARNING APPLICATIONS. Wireless technologies, security, wireless enabled teaching, application, IEEE. 2005 Feb;802.

[19] Arbaugh WA, Shankar N, Wan YJ, Zhang K. Your 80211 wireless network has no clothes. Wireless Communications, IEEE. 2002 Dec;9(6):44-51.Gupta, Er Anuj K., B. Lonia, and Er Vikas Gupta. "WIRELESS TECHNOLOGIES–AN OVERVIEW."

[20] Gupta, Er Anuj K., B. Lonia, and Er Vikas Gupta. "WIRELESS TECHNOLOGIES–AN OVERVIEW."