CGC International Journal of Contemporary Technology and Research
ISSN: 2582-0486 (online) Vol.-2, Issue-2 DOI: 10.46860/cgcijctr.2020.06.26.120

Performance Test of WAP Gateway over Web Server Using OPNET

Kamini[1*], Ravinder Singh[2]
[1]Chandigarh Group of Colleges Landran,Mohali
[2]Beant College of Engg & Tech (Diploma Wing)
Email id:*Kamini_girdhar08@hotmail.com

***Abstract*: The Security for the portable devices such as mobile phones,iPad and laptops becoming extremely important day by day.The intermediates such as gateway are the main source for communication through wireless media. In today's era, maintaining the transport level security amongst cellular devices like mobile phones and PDA(Personal Digital Assistant) become the most burning issue.During communications of smart phones with the web server through broadband method pass communication through the gateway known as Wireless Applications Protocol. The main purpose of WAP gateway is to transfer all the protocol used in WAP to the protocols used on the internet server. The WAP proxy server uses marshalling and unmarshalling methodology for the content to reduce the size of the data that has been sent through the wireless link. Further, the communication between the mobile phones and wireless application protocol is secured by using the security protocol called WTLS. The communication between the WAP gateway and web server is secured through the TLS/SSL security protocols. This paper simulates an assessment of wireless and wired networks using OPNET simulation tools. 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 how the end to end security takes place between wireless clients to web servers using hybrid security protocol.**

***Keywords*: OPNET; Security; WAP; Server.**

I.INTRODUCTION

As per current market scenario many of the applications are evaluated through the wireless devices like mobile phones and personal digital assistants in every digitalarea like commercial, medical, manufacturing and other. The main reason behind this mode of change is due to big access to the internet through wireless devices; security has become the important issue. In contemporary societies the mode of sharing the resources using mobile phones around the world becomes very important. The advanced facilities of mobile devices allow the user to buy the products, pay for products, surf the internet, surf and manage various bank accounts anywhere without moving to a specific location [1].

A user with mobile use always demand for a higher speed internet at lower prices, and rigid on moto "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 threat in such heterogeneous networks is the possibilities of roaming for administrative fields to which a mobile client home user service does not have a well standard 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 connected at any time at anywhere, demand in the development of wireless networks. 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 created 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 are 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 confined to sources 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 privacy, an applied method that ensures a private end to end transfer is defined [14]. As a result, the RSA encryption method on the client side is very less expensive, whereas the corresponding decryption applied on the server side is much more 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 realtime 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].

II. PROBLEM FORMULATION

The motivation behind this research work is that in today scenarios all wireless telecommunication networks generated traffic in the air is followed by encrypted However end to end transport layer security is not provided between the wireless devices and web internet server [21]. The current system based on twice encryption and decryption is used for establishment the communication between the mobile end users and a server supporting web applications. Besides this, when data arrives at the gateway through the mode of WAP standard protocol again due to security data is encrypted and decrypted for wireless and reuse the concept of Re-encrypted by gateway when the transaction has to pass through the mode of wired media. At this time of Re-encryption, the data can be modified by any of the unauthorized user [22, 23]. The main thought behind this research is to design a hybrid security protocol that will maintain a single secure channel for end to end communication.

III. OBJECTIVES OF STUDY

i. To examine and analyse the security holes in between the wireless client and WAP gateway.
ii. To propose an Enhanced Protocol to overcome the security holes.
iii. To build and implement the proposed composite security protocol architecture for mobile devices and web servers.
iv. To comparative analyse the performance of Transport layer security and Wireless Transport Layer Security with proposed protocol.
v. To support the improvement of the end to end Security in hybrid networks.

Table I: Used phase information

Transaction Detail	Phase Name	Start Phase After	Source	Destination
Transaction #1	Transaction #1	Application Starts	Originating Source	Proxy Server
Transaction #2	Transaction #2	Previous Phase Ends	Proxy Server	NA
Transaction #3	Transaction #3	Previous Phase Ends	Proxy Server	Main Server
Transaction #4	Transaction #4	Previous Phase Ends	Main Server	NA
Transaction #5	Transaction #5	Previous Phase Ends	Main Server	Proxy Server
Transaction #6	Transaction #6	Previous Phase Ends	Proxy Server	Originating Source

IV. RESEARCH METHODOLOGY

To achieve the set of objectives, our research focused on the performance measuring from wireless client to wired server with implementation of 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 with RSA encryption methods. Secondly, the transferring of Firewall gateway TLS encryption using message digest algorithm.To simulate the results Opnet is a wide and powerful software which provides the various possibilities to simulate entire heterogeneous networks with various protocols. Our research focused on algorithms implementation in various phases.

First phase: This phase contains the basic layout of the network with client node and server node.
Second Phase: In this phase we have configured the network with a set of applications. The profile configuration is used to create user profiles. We have also defined the use of Virtual Private Network (VPN) features for the configuration details for tunneling supported at the IP layer.
Third Phase: In this phase we have created scenarios for wireless and wired networks with different sets of attributes.
Fourth Phase: In this phase we have implemented the hybrid security protocol by applying the security at the web server.
Fifth Phase: In this phase we have done simulation with different scenarios with different types 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

V. SCOPE & SIGNIFICANCE OF STUDY

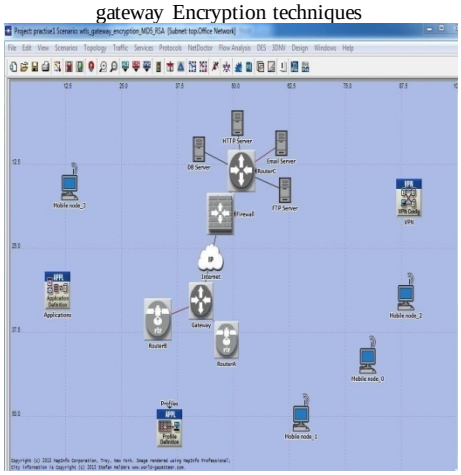
A.Simulation Environment and Parameters

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 the client side and server side model. The gateway is used to pass all encryption data from wireless client to web internet server. The analysed results are based on different parameters based on throughput, wireless LAN delay, FTP uploading /downloading response time and DB query traffic sent and received etc. OPNET is a wide and powerful simulation software which signifies the possibility to simulate the heterogen mode of networks with various available protocols. Originally this software was developed for the need of the 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 a large network environment via software

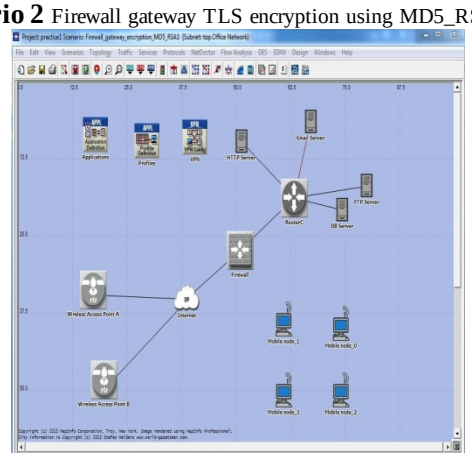
CGC International Journal of Contemporary Technology and Research
ISSN: 2582-0486 (online) Vol.-2, Issue-2 DOI: 10.46860/cgcijctr.2020.06.26.120

B. Simulation Results

Scenario 1 Wireless client mobile communication using WTLS gateway Encryption techniques



Scenario 2 Firewall gateway TLS encryption using MD5_RSA



Scenario 3 Response Time Calculation

The Response Time graph displays the time taken by an instance of the Profile to complete. It is calculated as a sum of time taken to complete each transaction.

The graph shows a value of 40 sec which is the composite sum of:

(i) Query Request Generation delay on workstation (Transaction 1): 5 sec
(ii) Query Processing delay on Proxy Server (Transaction 2): 10 sec
(iii) Query Request Generation delay on Proxy Server (Transaction 3): 5 sec
(iv) Query Processing delay on Main Server (Transaction 4) : 10 sec
(v) Query Request Generation delay on Main Server (Transaction 5): 5 sec
(vi) Query Request Generation delay on Proxy Server (Transaction 6): 5 sec

c. Combined graph for phase

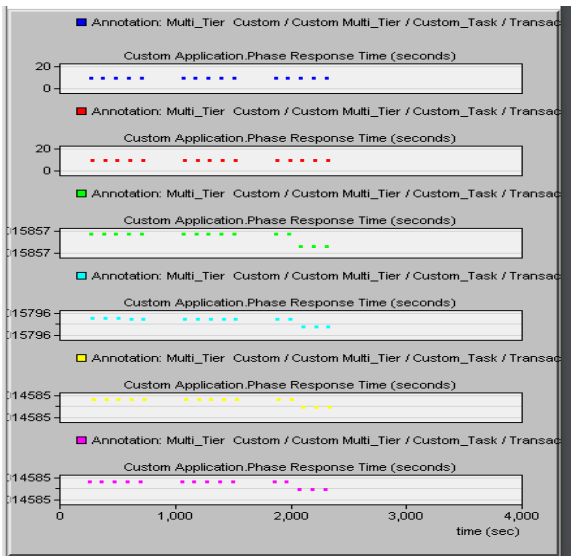


Fig. 1. Combined graph to represent Response time

A. Throughput of wireless client and wired server

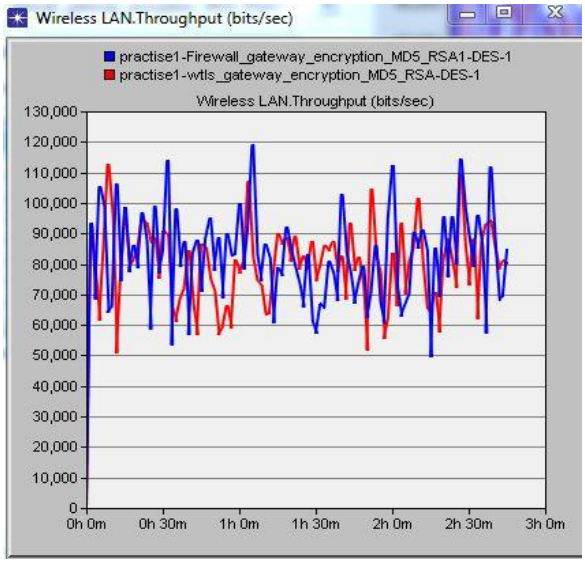


Fig. 2a. Throughput of wireless client and wired server

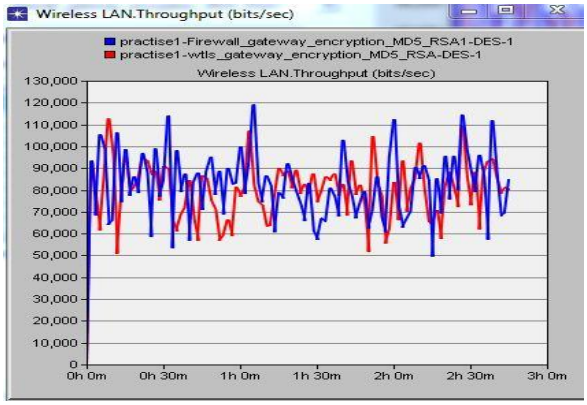


Fig. 2b. Network Throughput of wireless client and wired server

Network throughput is really an effective amount of profitable message delivery across a mobile communication stream with different network types, such

as EthernetBits per second (bit / s or bps), data packets per time slot, or data packets per second are the unit of the throughput. These data can be transmitted by a real and logical link, or sometimes by a specific routing protocol. The output that can be machine or aggregate is the sum of bit rates in all terminals that are transmitted through a network.

B. *Delay*

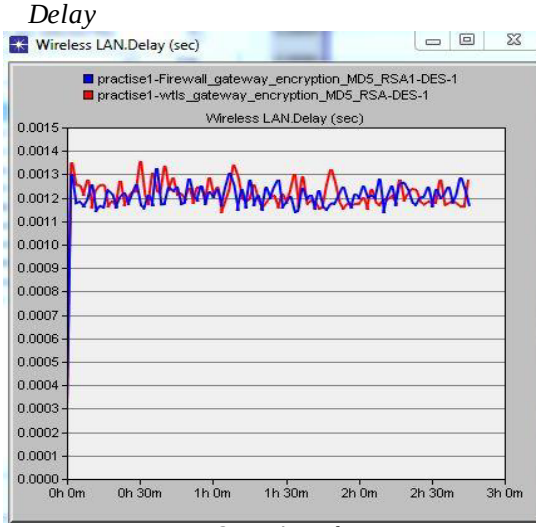


Fig. 3. WLAN Delay

The delay in the network is defined as the how long it takes for data bits to mitigate from one mode to other mode over a network. The units for delay are seconds. Delay can differ a bit depending on the location of the communication node. In fig, it is obvious that the significant delay to the WTLS gateway is higher compared to the firewall encryption, resulting in data delay from one server to the other.

C. *Load in wireless local area network*

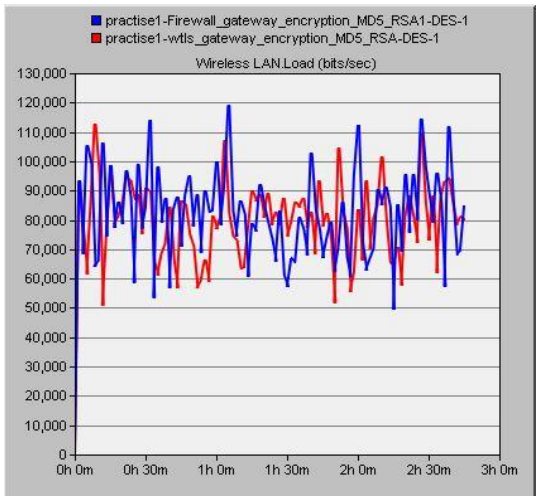


Fig. 4. Load in wireless local area network

Load in both the scenario and gives the idea that firewall gateway load is higher than the WTLS gateway which is present in the above given figure. The highest load value in the WTLS gateway is 120,000 bits per second and the minimum value is 49,000 bits per second. On the contrary, the Firewall gateway encryption is 110,000 bits per second and the minimum value is 51,000 bits per second.

D. Wireless LAN Media Access Delay

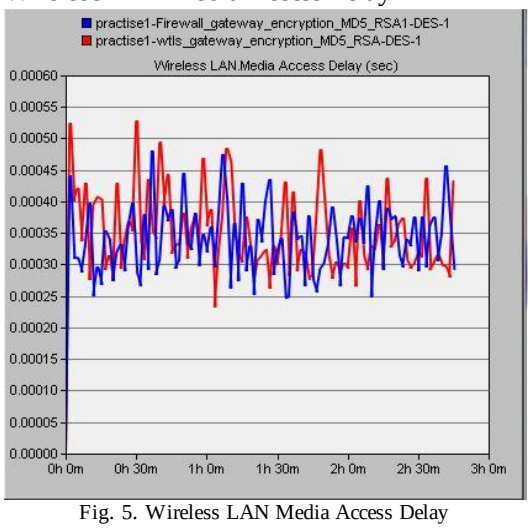


Fig. 5. Wireless LAN Media Access Delay

The idea that the Delay in wireless LAN media access is in the form of seconds is shown in the above-mentioned figure. It also reveals that in both scenarios and results the delay for media access shows that the delay level is highest in the case of WTLS gateway encryption and weak in the case of firewall encryption. WTLS gateway encryption has a maximum value of 0.00053 sec and a minimum value of 0.00024 sec. The other side of the maximum value for firewall encryption is 0.00046 sec and 0.00025 sec lowest.

E. *DB query traffic received*

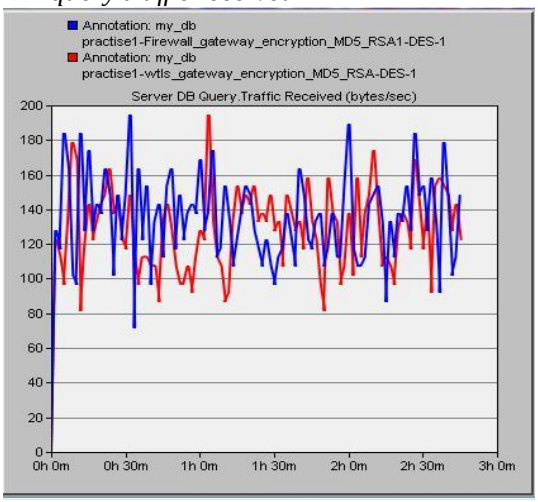


Fig. 6. DB query traffic received

F. *DB query traffic sent*

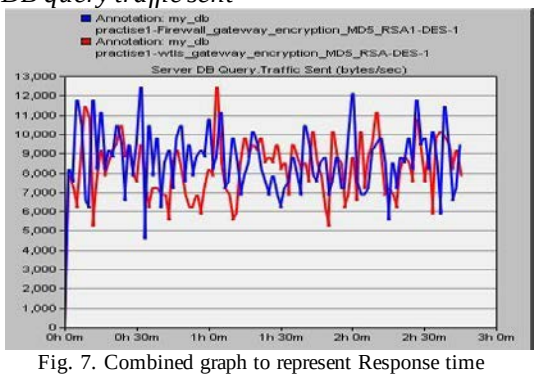


Fig. 7. Combined graph to represent Response time

G. *FTP server traffic received*

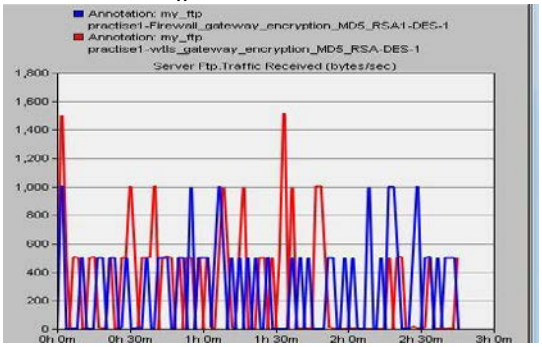


Fig. 8. FTP server traffic received

H. *FTP server traffic sent*

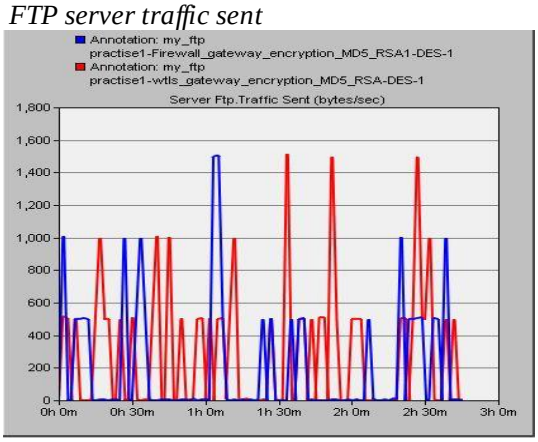


Fig. 9. FTP server traffic sent

I. *Firewall to Router Throughput*

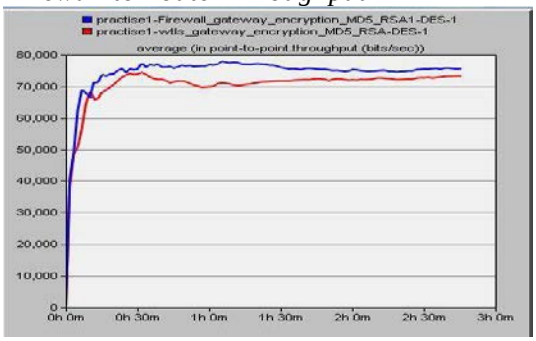


Fig. 10. Firewall to Router Throughput

VI. CONCLUSION

The paper has been defined on the simulation modeling of mobile devices and web server devices. Today mobile is accessed by most of the people in daily life just by its functionality of less utilization of bandwidth, tiny nature in size and limited power consumption. The WTLS security layer is used for wireless devices and TLS is the 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 communicating through the gateway to the 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 the proposed protocol analysed the performance of wireless and wired security models with the help of OPNET simulation tool. At the end, the security measures result of both security protocols are judged on the basis of parameters like delay, throughout, data sent and received etc.

Table II: Comparison Table for Simulation Results

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

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).

[2] Gustafsson E, Jonsson A. Always best connected. Wireless Communications,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).

[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] M.Shaikhan,A.Sobhani,M.E.Kalantari," Modification of Mobile Web Shopping Protocol Using GAA and Analysis by Colored Petri Nets",SATCCN,2011WAP Forum, Wireless Application Protocol Architecture Specification, WAP-210-WAPArch-200100712-a, 12-July- 2001 version, latest version is available athttp://www.wapforum.com.

[8] 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).

[9] 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).

[10] 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).

[11] 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).

[12] 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).

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

[14] M.Holbal,T,Welzer," An Improved Authentication Protocol Based on One-Way Hash Functions and Diffie-Hellman Key Exchange", International Conference on Availability, Reliability and Security,2009.

[15] M. Csernai and A. Gulyas, "Wireless adapter sleep scheduling based on video qoe: How to improve battery life when watching streaming video?" in Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on, 31 2011-aug. 4 2011, pp. 1-6.

[16] 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. 2016

[17] Rikure T, Jurenoks A. WIRELESS NETWORK TECHNOLOGIES IN TRANSPORT AREA: SECURITY AND E-LEARNING APPLICATIONS. Wireless technologies, security, wireless enabled teaching, application, IEEE. 2019 Feb;802.

[18] LAN MAN Standards of IEEE Comp. Soc., "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification," 1999

[19] W. A. Arbaugh, "An Inductive Chosen Plaintext Attack Against WEP and WEP2. 2001," IEEE 802.11 Working Group, Task Group I (Security), 2002.

[20] D. Verma and P. Singh, "Efficient Authentication and Privacy Mechanism to protect legitimate Vehicles in IEEE 802.11p Standard," Int. J. Mod. Educ. Comput. Sci., vol. 11, no. 1, pp. 39–44, 2019.

[21] Z. Qian and Z. Ya-Qin, "Cross-Layer Design for QoS Support in Multihop Wireless Networks," Proc. IEEE, vol. 96, no. 1, pp. 64–76, 2008

[22] S. Sattar, H. K. Qureshi, M. Saleem, S. Mumtaz, and J. Rodriguez, "Reliability and energy-efficiency analysis of safety message broadcast in VANETs," Comput. Commun., vol. 119, no. June 2017, pp. 118–126, 2018

[23] N. Shankar, W. Arbaugh, and K. Zhang, "A Transparent Key Management Scheme for Wireless LANs Using DHCP," HP Laboratories, Palo Alto, CA, 2001.