IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

Improvement in Security Architecture for Hybrid Networks in Wireless and Wired Devices for End to End Security

Kamini [*], Rajiv Mahajan[2], Ravinder Singh[3]

[1,2,3]I.K. Gujral Punjab Technical University Kapurthala, India

[*]*Corresponding Author: kamini_girdhar08@hotmail.com, Tel.: +91-9530565694*

DOI: https://doi.org/10.26438/ijcse/v7i4.167173 | Available online at: www.ijcseonline.org

Accepted: 12/Apr/2019, Published: 30/Apr/2019

***Abstract*—** Security for wireless devices is turning into vital 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 contrivances like mobile phone and PDA(Personal Digital Assistant).When mobile contrivance wants to communicate to the web server through internet the all the communication pass through the Wireless Application Protocol gateway. This Wireless Application gateway protocols interprets all the convention utilized in Wireless Application gateway to the protocols utilized in the cyber world. The Wireless Application Protocol 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 utilizing the safety protocol is termed Wireless Transport layer security. The communication between the WAP entrance and net server is secured through the TLS/SSL security protocols. This paper presents an evaluation study of wireless and wired network utilizing OPNET simulation implement. This paper simulated 2 different scenarios comparing wireless mobile client communication utilizing Wireless Transport Layer Security gateway with MD5_RSA encryption and Firewall gateway TLS encryption utilizing MD5_RSA.The analysis results shows that how to provide the point to point security between wireless client to web server by proper utilizing the hybrid security protocol.

***Keywords*—Opnet, Security, WAP, Gateway**

I. INTRODUCTION

In today most of the applications are accessed through the wireless contrivances like mobile phones and personal digital assistant in any of the area like commercial, medical, manufacturing and other. Due to immensely colossal accessing of internet through the wireless contrivances the security has become the paramount issue. In modern societies the sharing of resources utilizing the mobile phones throughout the world becomes very paramount. The advanced facilities of mobile contrivance sanction the utilize to buy the products, pay for products, internet surfing and manage sundry back accounting anywhere without peregrinating to categorical location [1].

A versatile utilizer continuously inquires for a better speed at lower costs, and injuctively authorizes to be "Always Best Associated" [2].Mobile networking promises its users to utilize plenarily functionality of anything, anytime, anywhere [3].The wireless internet evolution support for accessing anything from mobile networking at any time. A fundamental challenge in such heterogeneous systems is the chances of meandering for authoritative spaces to which a portable client domestic space does not have a well set up wandering passive [4,5]. Over the final few a long time remote systems predicated on IEEE 802.11standard have experienced surprising amplification. This has unfolded since of giving up the IEEE 802.11 standard, moo taken a toll equipment and tall information rate and speed [6].

The expeditious magnification of wired and wireless technologies, as well as incremented in the ordinate dictation 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 minute in size and its portability. In today' time sundry distributed application peoples use network communication channels to communicate with each other. The terminus to culminate communication is possible only with the utilization of forfended encryption and decryption methodology. Privacy, security and authentication are provided by security protocols. Hotspot administration offer wireless Internet in public places like cafes, restaurants, hotels and airports. A Wi-Fi community called FON has more than 7 million hotspots ecumenical [7].

The considerable utilization of mobile transmission has engenders a consequential request for value integrated accommodations. Wireless Application Protocol is a framework for developing applications to run over wireless networks.WAP is expand by the international industry wide organization called WAP forum [8]. The next is Convey Control Protocol (TCP), the most used convey control protocol, performs better over wired networks. As many wireless networks are deployed, TCP should be altered to work for both wired and wireless networksTCP demonstrate is outlined particularly for clog co ntrol in wired systems; it cannot distinguish any non-congestion
cognate information parcel misfortune from remote systems [9]... Both the communications for remote and wired were created to be predicated on interface to connect and working with the same conventions, predicated on IEEE [10] 1451.0-2007. As wireless mesh networks are deployed on the base of an incipient concept designated hybrid internetworks, i.e., internetworks that contain both wired work networks and remote work networks. Routing path is most challenging today that arise in hybrid internetworks: indeed, while categorical routing protocols are typically designed for wired communication on one hand and for wireless communication networks on the other hand, it has been optically discerned 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 constrained number of resources and communication capacity [12]. A Radio Frequency Identification Contrivance (RFID) sanctions a very good identification technique for an immensely colossal number of tagged objects without any physical or visual contact [13]. With the privacy, an application procedure that contains a private end to culminate transfer is defined [14]. As a result RSA encryption method in the client side is very less sumptuous, whereas the corresponding decryption applied on server side is much extravagant because its private component is much more sizably voluminous [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 authentic-time communication between a room-full of business class executives or students an authenticity [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-predicated verification mechanisms[19]. An immensely colossal number of organizations, made their predication on literature theory, trust that the security provided by their deployed wireless access points is much enough to obviate unauthorized access and use[20].

II. PROBLEM FORMULATION

The motivation behind this research work is that in current wireless telecommunication networks, all the traffic is in the air is encrypted but point to point security is not distributed 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 Wireless Application Protocol, first all the data is encrypted and decrypted at gateway for wireless and again it will be Re-encrypted by gateway when the transaction has to transfer through the wired traffic. At this time of Re-encrypted 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.

III. 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.

IV. 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 method is used for generating user profiles. We can mention the ongoing traffic patterns followed by the applications as well as the configured profiles on this object. We have also discussed the Virtual Private Network (VPN) with attribute configuration details for the purpose of tunnelling supported at the Internet protocol 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 various parameters such as delay, throughput, and traffic sent and received through networks; HTTP and FTP downloaded Response time

V. RESULT OUCOME

a. To identify and analyze the security holes in between the wireless client and WAP gateway.

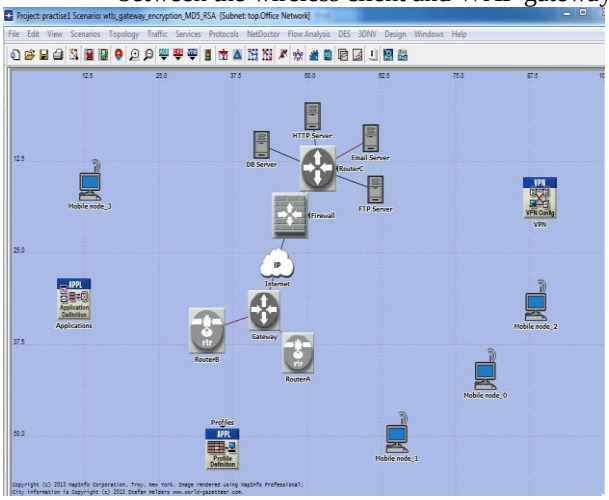


Figure 1:Wireless client mobile communication using WTLS gateway MD5_RSA encryption/decryption

In the above situation four wireless mobile node are created for wireless communication and four server node are created for transferring the data at server .All wireless translation pass through the Wireless Application Protocol gateway which act as intermediate between wireless mobile(WTLS) and wired server(TLS) .The encryption and decryption is applied in gateway then again encryption and decryption is applied at server and wired communication and the double encryption and decryption are used in existing system between the mobile devices and a web server. On the other hand when transaction arrives at the gateway Through the Wireless Application Protocol the data is encoded and decoded 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 which results in security holes in between the wireless client and WAP gateway.

b. To propose an Enhanced Protocol to overcome the security holes

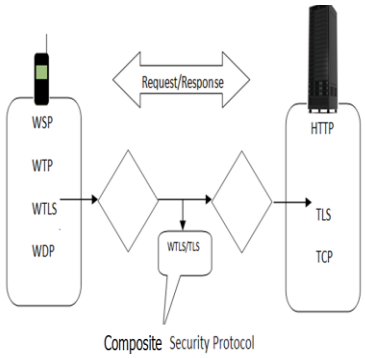


Figure 2: Composite Security Protocol

In the above scenerio all the wireless traffic arrived at the intenet (wired server) and The concept of marshaling and un-marshalling is used at web server. The marshalling means convert all the traffic of wireless into that form which can be easily understood by web server. When wireless data is arrived at the server, the encryption/decryption techniques take place .The marshalling is used for encryption and un-marshalling is used for decryption.

C. To design and implement the proposed composite security protocol architecture for wired and wireless devices

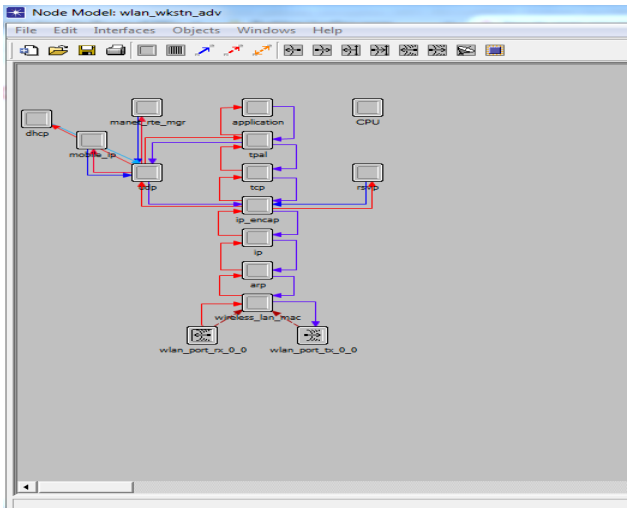


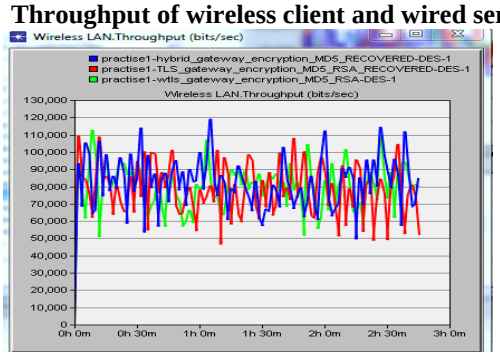
Figure 3: OSI design model of composite security protocol

- wlan_wkstn_adv (4): The wlan_wkstn_adv node model represents a workstation with client-server applications running over TCP/IP and UDP/IP. The workstation supports one underlying Wlan connection at 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps
- Application config(1): The "Application Config" node can be used for the following specifications:
  1. "ACE Tier Information": Specifies the different tier names used in the network model. This attribute will be automatically populated when the model is

created using the "Network->Import Topology->Create from ACE..." option. The tier name and the corresponding ports at which the tier listens to incoming traffic are cross-referenced by different nodes in the network.

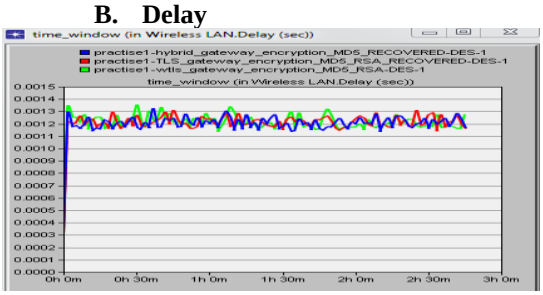
- Profile Config (1): The "Profile Config" hub can be utilized to create user profiles. These user profiles can then be specified on diverse nodes in the network to generate application layer traffic activity
- VPN (1): Defines Virtual Private Network(VPN) attribute configuration details for tunneling supported at the IP layer
- Wlan_ethernet_router_adv (2): This is a remote lan based switch with one Ethernet interface.
- ethernet4_slip8_gtwy (1): The ethernet4_slip8_gtwy node model show an IP-based gateway supporting four Ethernet center interfaces, and eight serial line interfaces. IP packets arriving on any interface are steering to the suitable output interface based on their goal IP address
- ethernet2_slip8_firewall (1): The ethernet2_slip8_firewall node model shows an IP-based door with firewall highlights and server back. Thus, it can be moreover called as a multi homed-server firewall node. It supports two Ethernet and eight serial line interfaces at selectable data rates
- ethernet_server_adv (4): The ethernet_server_adv model demonstrate a server node with server applications running over TCP/IP and UDP/IP. This node supports one basic Ethernet association at 10 Mbps, 100 Mbps, or 1 Gbps. The operational speed is decided by the associated link's information rate.

A. Throughput of wireless client and wired server



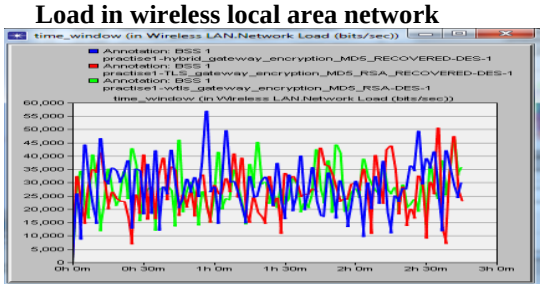
Throughput In wireless communication of different sorts of systems, such as Ethernet, network throughput is the average rate of fruitful message conveyance over a communication channel. The throughput is ordinarily measured in bits per second (bit/s or bps) or in data packets per second or data packets per time slot. These data may be conveyed over a physical or logical link, or pass through a certain network hub

B. Delay



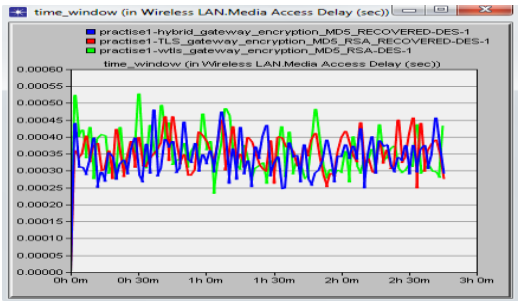
The delay of network implies how much time is required for bit of information for the data to travel across the network from one mode to another mode. It is computed in terms of seconds' .delay may contrast small bit depending on the area of the particular pair of communicating nodes. In fig it is clear that delay in WTLS and TLS gateway is higher as compare to Hybrid which results in delay of data to across from one network to another.

C. Load in wireless local area network



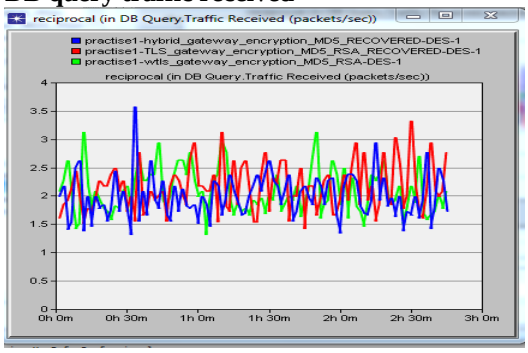
The above figure shows the load in both the framework and this make it clear that load of Hybrid is higher than WTLS and TLS gateway .The highest value of load in WTLS gateway is 110,000 bits per sec and TLS value is 109,000 bits per sec .On the other side for Hybrid gateway encryption the maximum value is 110,000 bits per sec and minimum value is 51,000 bits per sec.

D) **Wireless LAN Media Access Delay**



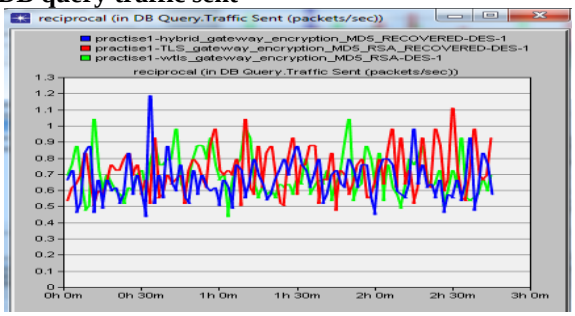
The above fig shows the media access delay for wireless LAN in form of seconds. The above figure shows the media access delay in three scenario and results shows that the frequency of delay is highest in case of WTLS ans TLS gateway encryption and low in case of Hybrid encryption. The maximum value of WTLS gateway encryption is 0.00055 sec and for TLS is 0.00046 sec. The other side for Hybrid encryption maximum value is 0.00040 sec

E) **DB query traffic received**



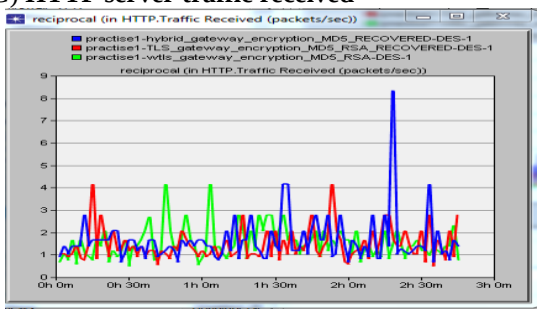
The above fig shows the DB query traffic received in both the scenario and it is clear that DB query traffic response of Hybrid gateway is higher than WTLS and TLS gateway .The highest value of load in WTLS gateway is 3.1 packets per sec and TLS value is 3.2 packets per sec .On the other side for Hybrid gateway encryption the maximum value is 3.7 packet per sec .

f) **DB query traffic sent**



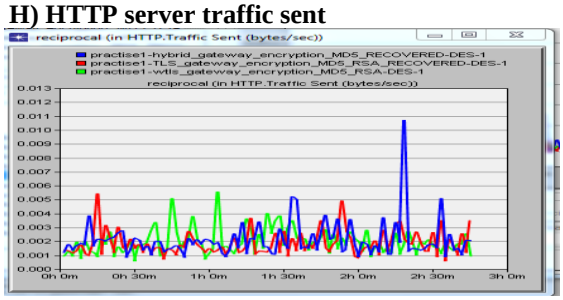
The above fig shows the DB query traffic sent in both the scenario and it is clear that DB query traffic response of Hybrid gateway is higher than WTLS and TLS gateway .The highest value of load in WTLS gateway is 1.0 packets per sec and TLS maximum 1.1 packets per seonds .On the other side for Hybrid gateway encryption the maximum value is 1.2 packets per sec .

G) **HTTP server traffic received**



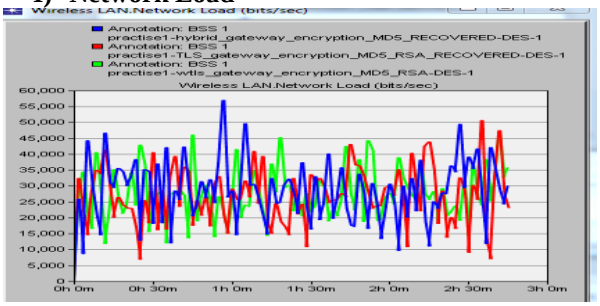
The above fig shows the HTTP traffic received in both the scenario and it is clear that HTTP traffic response of Hybrid gateway is higher than WTLS/TLS gateway .The highest value of load in Hybrid gateway is 8.2 packets per sec and On the other side for WTLS/TLS gateway encryption the maximum value is 4.1 packets per seconds.

H) HTTP server traffic sent



The above fig shows the HTTP server traffic sent in both the scenario and it is clear that HTTP server traffic response of hybrid protocol is in increasing order of WTLS and TLS gateway .The highest value of load in WTLS gateway is 0.006 bytes per sec and TLS is 0.005 bytes per sec .On the other side for Hyrid Protocol encryption the maximum value is 0.010 bytes per sec.

I) Network Load



The above fig shows that network load of hybrid protocols greater as compared to WTLS and TLS.In the above

scenerio the maximum value of network load is 58000 and very low in WTLS and TLS around 40000.Greater network load results in greater performance.

E. To Improve the end to end Security in hybrid networks.

For our simulation model we have setup three different scenerio

- Wireless client mobile communication using WTLS gateway MD5_RSA encryption/decryption
- Firewall gateway TLS encryption using MD5_RSA encryption/decryption
- Hybrid Gateway encryption MD5 _RSA & DES2 encryption/decryption

Scenerio 1: Wireless client mobile communication using WTLS gateway MD5_RSA encryption/decryption

- Application Configuration :

We add a new application by adding a new row and configured the new row for HTTP,DB,FTP etc.

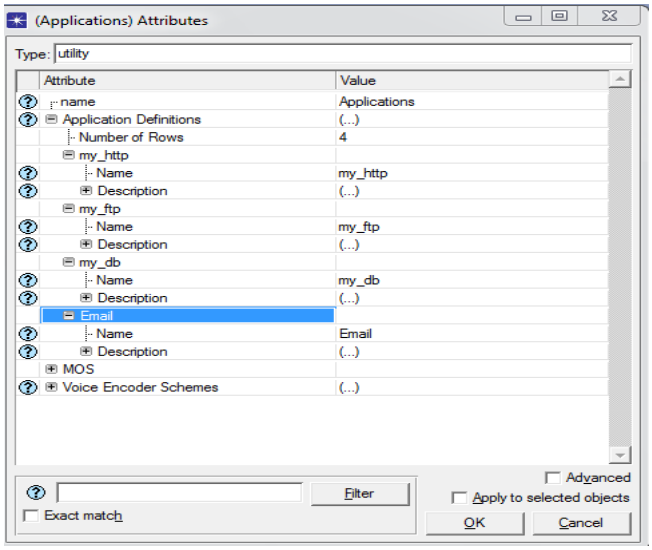


Figure4: Application Configuration

- Profile Configuration:

We configured the Profile Config module to use the sample profile for FTP,HTTP and DB

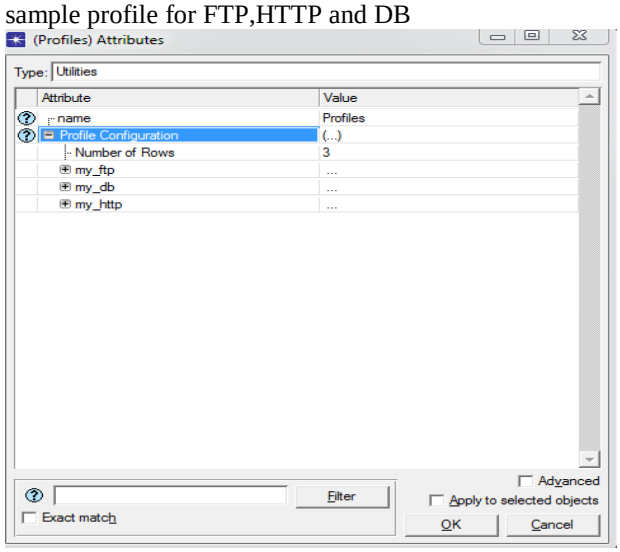


Figure5: Profile Configuratuon

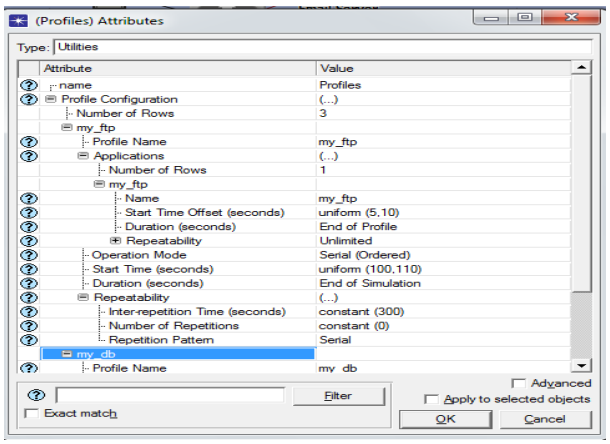


Figure6: Profile attribute for FTP

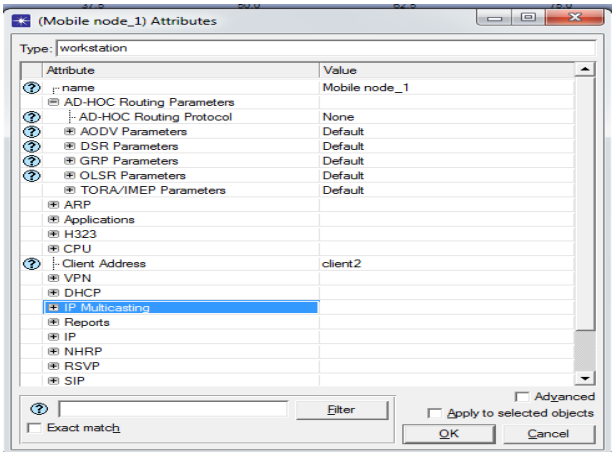


Figure7: Mobile client profile attributes

Scenerio 2: Firewall gateway TLS encryption using MD5_RSA encryption/decryption

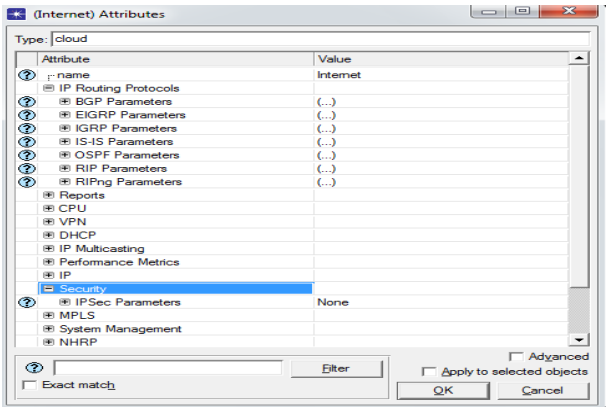


Figure8: IP Configuration

CONCLUSION

This paper has emphasis on the reenactment modeling of remote gadgets and wired gadgets. Nowadays versatile is gotten to by most of the individual in existence fair since of its highlights like moo transmission capacity, little in measure and constrained control utilization. The WTLS security layer is utilized for remote gadgets and TLS is security layer utilized for wired gadgets. Amid the communication between the remote gadgets and the door the encryption and decoding are utilized for WTLS convention .Once more whereas communicate through the portal to web server re-encryption is required. This re-encryption leads to the issue of WAP hole. To evacuate this WAP hole the architecture plan for the WTLS and TLS got to be modified. In this paper we have examined the execution of remote and wired security show with the assistance of OPNET recreation apparatus. We the examined the comes about of both security convention on the premise of parameters like delay, all through, information sent and gotten 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, 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.

[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..

[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 at http://www.wapforum.com

[9] Inwhee Joe; Jaehyung Lee, "An Enhanced TCP Protocol for Wired/Wireless Networks," in INC, IMS and IDC, 2009. NCM '09. Fifth International Joint Conference on , vol., no., pp.531-533, 25-27 Aug. 2009

[10] Filho, T.A.S.; da Silva, A.C.R.; Grout, I.A.; Rossi, S.R., "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)," in Instrumentation and Measurement Technology Conference (I2MTC), 2011 IEEE , vol., no., pp.1-6, 10-12 May 2011

[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.; Gianluigi Me; Strangio, M.A., "Local Authentication with Bluetooth enabled Mobile Devices," in Autonomic and Autonomous Systems and International Conference on Networking and Services, 2005. ICAS-ICNS 2005. Joint International Conference on , vol., no., pp.72-72, 23-28 Oct. 2005

[13] 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

[14] Diffie Hellman Key Exchange –A Non –Mathematician's Explanation. Global Knowledge-Expert reference series of white papers. Link available at http://www.recursosvoip.com/docs/english/WP_Palmgren_DH.pdf

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

[16] Csernai, M'rton; Gulyas, A., "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 , vol., no., pp.1-6, July 31 2011-Aug. 4 2011

[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, Tatiana, and Alexey Jurenoks. "WIRELESS NETWORK TECHNOLOGIES IN TRANSPORT AREA: SECURITY AND E-LEARNING APPLICATIONS." Wireless technologies, security, wireless enabled teaching, application, IEEE 802 (2005).

[19] Arbaugh, W.A.; Shankar, N.; Wan, Y.C.J.; Kan Zhang, "Your 80211 wireless network has no clothes," in Wireless Communications, IEEE , vol.9, no.6, pp.44-51, Dec. 2002

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

Authors Profile

Ms Kamini is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computational Applications, Department of Electronic and Communication,. SHe has 9 years of teaching experience and 3 years of Research Experience.She is life time Member of CSI.

