THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Application and Research on Performance Analysis and Security Implementation in Hybrid Networks

Kamini
Research Scholar, IK GUJRAL Punjab Technical University, Jalandhar, Punjab, India
Rajiv Mahajan
Professor, IK GUJRAL Punjab Technical University, Jalandhar, Punjab, India

Abstract:
Background/Objectives: Security in wireless and wired networks is a serious issue in IT industry because of its performance, capacity and cost. It concern with the secure transmission of traffic between the networks elements. As compare to wired network, wireless net- work security somewhat more concentrating. It covers a gigantic of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. In order to solve to problem of WAP gap for wireless devices like mobile phone and personal digital assistant, in this paper, introduces the performance analysis of wireless and wired network to provide the end to end security. Methods: The main idea is to propose the enhanced protocol to overcome the security gap using opnet modeler as simulation tool. In this model two scenarios are discussed. First scenario is based on communication from wireless device to gateway and second scenario is based on gateway traffic to wired server. Different simulation results based on various parameters like delay, throughput, and re-transmission attempts for wireless networks. Findings and Improvements: A simulation environment was developed to measure various parameters including the traffic received, traffic send, response time is considered for server side applications in wired networks. Furthermore, security parameters are implemented on the firewall to improve the end to end security for hybrid networks. As a result the proposed protocol is observed to be better for wireless network for the parameter considered.

Keywords: *Opnet, security, hybrid, firewall, gateway*

1. Introduction

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 wireless devices are characterized by low bandwidth rate, low Power consumption and small in size and weight. When mobile device wants to connect through the internet all the communication passes through the gateway which act as intermediate between the WAP devices and web server. The WAP gateway used the proxy server for encoding and decoding the content to reduce the size of data which are going to transfer through the wireless link. End to End security is the important concept which deals with providing the end to end secure line between the wireless and wired devices. When any e-commerce transaction takes place through mobile device then there is risk of security and privacy issues. Due to this problem a security protocol has been introduced named WTLS (wireless transport layer security). [1] Discussed about the security architecture for WAP devices and other attributes of WTLS protocol. There are some issues with WAP and WTLS security protocol. Privacy and security is not provided by the wireless devices.In their research they have discussed about the security weakness of WAP and WTLS and propose some of the measurement with using WAP. They have discussed in the paper about the suitable situation of using WAP or not.[2] have explained about the WTLS handshake protocol which is implemented using C++ and its performance measurements are done using Nokia 7650 as client and open source kannel gateway as the WAP gateway.[3] have presented the WTLS handshake protocol is a cryptographic protocol that perform authentication and key establishment for secure WAP communication and protocol is introducing named AKC including key authentication and confirmation of key possession.[4] have focused on the various mode of wireless communication which include satellite communication,cellular networks, cordless systems and other wireless devices. [5] Represents the two end to end security supported protocols. In this paper they have discussed about the industry implemented protocol known as WTLS and ITLS. The current specification of WTLS does not provide end to end security and WTLS enables the gateway that leak plaintext during data transmission to the server. This research proposes the modified ITLS that will increase ITLS performance in addition to providing the same security level for the current ITLS. [6] have explained the time required for execute the necessary cryptographic operations to set up a WTLS connection on a palm OS device with both ECC based public key cryptography as well as with RSA

based public key cryptography. [7] Have described the security of systems along with importance of the digital signature and hashing message algorithms. [8] Discussed that in wireless network channel are unreliable and its network energy is very limited and it's become necessary that protocol should designed in such a way which can optimize the error recovery. [9] discussed about the security of WTLS is analyzed. [10] described the limitation of wireless sensor network such as battery energy, transmission rate, processing hardware and memory parameters which get interact with specific operational context. [11] Give an explanation of the implementation of trust system in network security. [12] Have elucidate the SSL/TLS servers become swamped to perform public key decryption operations when the simultaneous requests increase quickly. [13] Represent architecture design for hardware implementation of the WTLS is proposed to improve the security and integrity. [14] Have state about the technology security of WEP products which provide the wireless link between the clients and access points. [15] Have explicate about the security an issue for sensors networks and then present its related security problem includes threat, risks and its characteristics. [16] Have clear security issues in mobile computing. Many security protocols are being proposed for different application like wireless application protocol, 802.11 etc. [17] have discussed different versions of security protocols for wireless devices. The gateway introduces a security hole which renders WAP unsuitable for any security sensitive devices. [18] Have focused on the functionality model of WAP gateway along with various fundamental aspects of the WAP model. They have discussed about the wireless networks over the internet technologies according to some security issues. [19] Have discussed the development of wireless sensor network application was motivated by the military applications, industrial and consumer applications. [20] Have represents the different way for security aspects for the constrained application protocol are analyzed with respect to wireless sensor networks.

2. Two Stage Security Protocol for Wireless and Wired Network

WTLS: Wireless Transport Layer Security is a part of WAP stack. WAP communication is used in mobile devices and it resides between the WTP and WDP layer of WAP protocol hierarchy stack. WAP used data encryption method to encrypt the data and all the communication passes though the gateway to the server. The WTLS is derived from TLS/SSL.The WTLS is a security layer which is used below the transaction layer and above the transport layer. The WTLS is used for providing the security, privacy and integrity and authentication. The WTLS is a security layer used for wireless devices like mobile phones. The WTLS is integrated with WDP (Wireless Datagram Protocol) which is used for transferring the data over the wireless networks

2.1. Hierarchy Architecture of WAP is as follows

The WAP top layer is known as presentation layer which describe how to present the data. The presentation layer is responsible for delivery of data through the wireless device for WAP and wired devices for web server. Encryption and decryption is also done at this level too. The presentation layer includes the WML, WMLScript, and WBMP. The WML is wireless markup language and its is a scripting language used for providing the communication through the WAP devices. The WMLScript is used by the JavaScript. The WBMP is WAP bitmap format and it is used for black and white images. The next layer is known as binary presentation formats named WBXML and WML Script. The content written in the wireless markup language is encoded into the binary format before the actual transmission take place at the server. The third layer is known as session layer which is used for maintaining the session between the client and server. The session protocol includes WSP/B and WSP. The session layer protocol works as request reply protocol. The transaction layers include the WTP protocol. The WTP for wireless networks are similar to TCP/IP protocol. The next layer is known as security layer. The security is maintained by using the WTLS protocol. The next layer is known as data transport layer using protocol WDP.The WDP is wireless datagram protocol and its is known as connection less protocol. The minimum requirement for developing for WAP applications is web server and simulator. The internet connection

Is required to running WAP server. The wireless markup language is required to running WAP applications. Moreover, at client side WAP enabled mobile phone is required for testing the applications. The Default IIS server or apache server can be used as web server in window or Linux operating system. The protocols used in WAP are based on internet protocol like HTTP and TCP but due to limited bandwidth and low memory in mobile phone these protocol have optimized use.

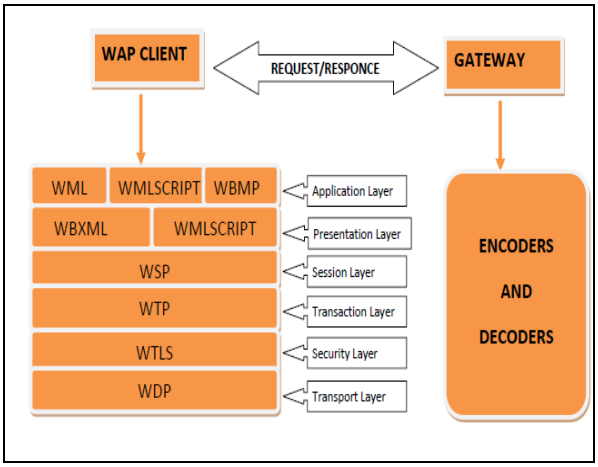

Figure 1: Wap Stack Hierarchy

2.2. Hierarchy Architecture of TLS is as follows

TLS: Transport Layer Security Protocol is used at web server side and it is used to provide security, authentication and authorization for wired networks. The session is maintained with the client on the flowing of data between two parties include client and server. The TLS protocol works on two layer. Layer 1 is called as TLS record protocol known as TCP to check whether the connection maintained between the two parties is reliable or not. Layer 2 is known as TLS handshake protocol is used for providing the authentication between the server and client and used for negotiation between the two parties along with some cryptographic techniques. In protocol hierarchy the topmost layer is application layer which includes HTTP, FTP, Telenet, SSH, RTP. The next layer is known as transport layer which include TCP, UDP, DCCP, SCTP. The third layer is known as network layer for internet protocol. The fourth layer is known as link layer which is used for internet connection. The TLS security layer is used below the application layer and above the network layer. Each layer has upper layer protocol and lower layer protocol. The main function of upper layer to provide the service to lower layer.

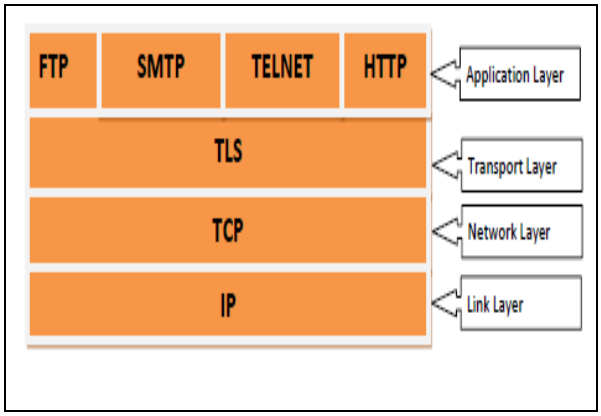

Figure 2: TLS STACK HIERARCHY

2.3. Authentication Types is as Follows

- Category A is called class1 authentication known as (Anonymous authentication). Here client and server are communicating each other without knowing. Any client can connect to any server and any server can connect to any client without exchanging certificates.
- Category 2 is called Class 2 authentication known as (Server authentication). The client authenticates about the server and form the server side digital certificates is providing to the client.
- Category 3 is called Class 3 known as (Server and client authentication): This is two way communications where client and server both have the information about each other.

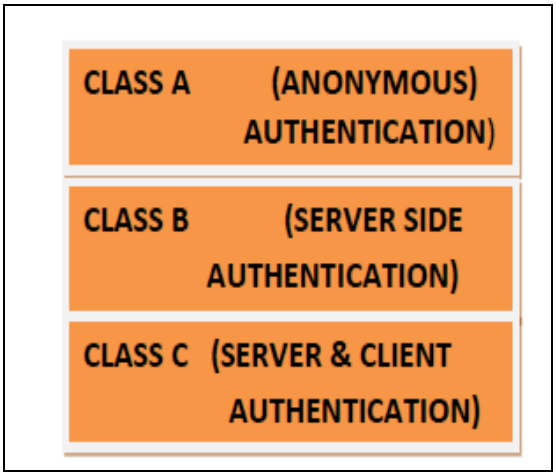

Figure 3: Authentication Types

The main purpose of handshake to maintain the session between the client and server. The connection can be either wireless or wired. The protocol used for the connection less service is known as UDP and connection used for wired service is known as TCP. In case of TCP connection an acknowledgement is pass through the server to client about the delivery of data, In the case of UDP protocol no acknowledgment is send for the server side.

2.4. Existing Protocols for Network Security

SSL was originally developed at Netscape to enable ecommerce transaction security on the Web, which required encryption to protect customers' personal data, as well as authentication and integrity guarantees to ensure a safe transaction [21]. SSL is designed to facilitate communication channel between two peers, providing mechanisms for secure key ex- change, authentication, encryption, and integrity. It aims to be resilient to man-in-the-middle attacks, eavesdropping, replay attacks, and statistical attacks. While SSL can authenticate two sides of the conversation, in practice it is typically only the server that authenticates it [22]. The Secure Socket Layer (SSL) protocol was designed to ensure secure communications between two entities over untrusted networks. The SSL protocol provides authentication based on the X.509 public key infrastructure, protects data confidentiality using symmetric encryption, and ensures data integrity with cryptographic message digests. SSL is commonly used for securing websites and mail servers, preventing passive network attackers from eavesdropping or

replaying the client's messages, and is generally considered security best practice for websites. By enabling encryption, Websites can easily prevent the eavesdropping of unencrypted confidential data [23].

TLS began in 1994 as the secure socket layer feature of Netscape web browser.TLS and content encryption can both be used to secure email communications. The TLS implementation differs from a conventional TLS implementation in that it is included within a bare PC application that manages its own CPU tasks, directly interfaces to the hardware, and communicates with network protocols without using a standard socket interface. SSL/TLS server support for forward secrecy was introduced at major sites such as SNS at the end of last year, so servers enabling forward secrecy are increasing [24].

WTLS

The WTLS (Wireless Transport Layer Security) protocol is the security layer of the WAP (Wireless Application Protocol) [25]. It is becoming the de facto standard for providing privacy, data integrity, and authentication for applications in cellular phones and other small wireless terminals [26]. Wireless Transport Layer Security is used to provide security services in the WAP environment developed by WAP forum. WTLS provides privacy, data integrity and authentication between two communicating entities. WTLS is Based on TLS architecture and incorporates new features such as datagram service, optimized handshake and dynamic key refreshing. The WTLS is in these ways optimized for low-bandwidth with a relatively long latency [27]. Forward secrecy and user anonymity are provided in the WTLS for the wireless Internet communications. Forward secrecy can be built by using Diffie-Hellman key agreement with random numbers in the Hello messages, and user anonymity by employing the sign encryption scheme to the Client Key Exchange and Certificate Verify procedure. The wireless sensor network consists of low cost, large scale and low power consumption nodes [28]. Different types of security attacks, threats and challenges involved are also taken into consideration.

The below design is given for the proposed protocol. The WTLS is inherited from the TLS along with some common features. The security protocol used by the wireless devices is known as WTLS and the protocol used by the wired devices is known as TLS. The handshake takes place between both security protocols using the intermediate called gateway. The main working of gateway is to encrypt all the wireless traffic and then decrypt it to get it ready to send at web server. The concept of marshaling and un-marshalling is used in between the gateway. 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 gateway, the encryption/decryption techniques take place. The marshalling is used for encryption and un-marshalling is used for decryption. Two times encryption and decryption is required for sending the data at web server. This two encryption and decryption waste the time and memory space. Due to the security issues in the wireless devices the data can be hacked in between the gateway. To solve this problem proposed idea is given based on hybrid design which combine the feature of wireless and wired security protocol. Initially handshaking process takes place between WAP client to WTLS security gateway and encryption and decryption initiate here. Secondly all communication passes from the gateway to wired server.

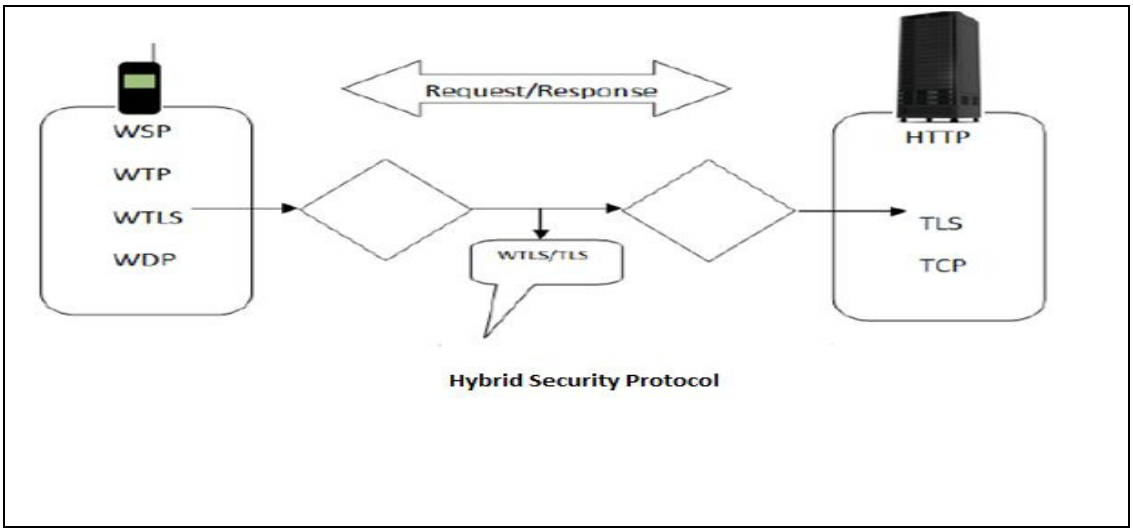

Figure 4: hybrid security protocol Architecture design

The following are the steps involve in the WTLS handshake working.

1. The client sends the Client Hello message to WAP gateway
2. The gateway replies with the Hello message to client along with server certificate, server key exchange, and Certificate request.
3. The client uses the information replied by server to authenticate server.

The client sends the change cipher spec notification to gateway to indicate that the client will start using the new session keys for hashing and encrypting messages.For wireless devices the gateway acts as server. The gateways transfer all the WAP traffic to web server. But for the client the data is arriving from the web server through intermediate by using encryption and decryption.

2.4.1. The Handshake Working for Web Server

The following are the steps involve in the TLS handshake working.

1. The wap gateway sends the Client Hello message to Web server
2. The server replies with the Hello message to WAP gateway along with server certificate, server key exchange, and Certificate request.
3. The gateway uses the information replied by server to authenticate server.
4. The gateway client sends the change cipher spec notification to web server to indicate that the client will start using the new session keys for hashing and encrypting messages.
5.

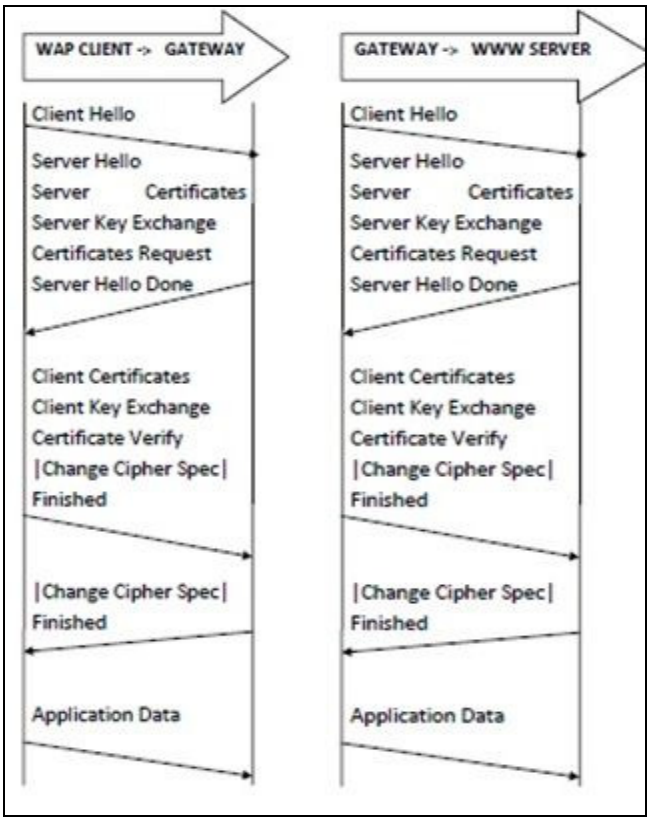

Figure 5: Handshaking from WAP client to WAP gateway and WAP gateway to WWW Server

The above diagram represents how the handshaking perform from gateway to www server by maintaining the session. For web server like www the gateway acts as client. The gateways encrypt all the WAP traffic to web server and now it is decrypted by the web server for further communication.

2.4.2. Methodology and Performance Evaluation

2.5. Simulation Model

The simulation was implemented using opnet modeler 14.5 (Educational Version). OPNET modeler is the simulation tool available for design any kind of network model is a network. OPNET will generate the traffic as defined in attributes set by user and will generate results like utilization, load, delay, throughput etc

2.5.1. Scenario I: Gateway Encryption for Wireless Client

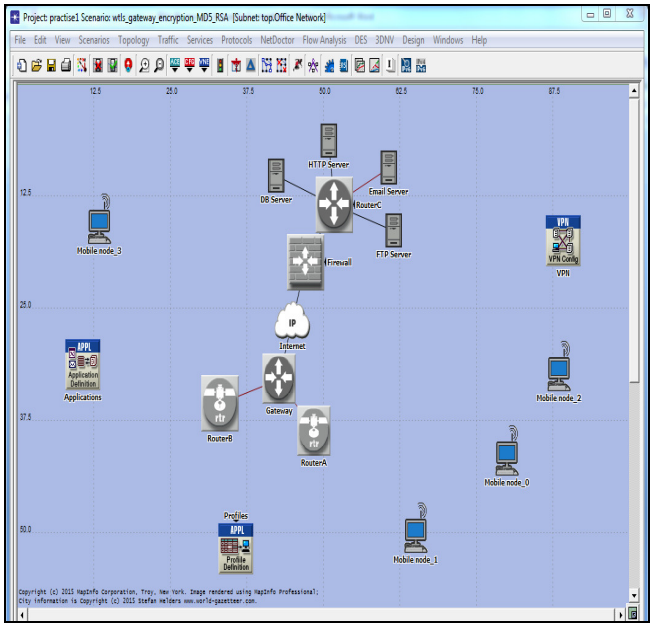

Figure 6: Wireless WTLS gateway encryption using MD5 and RSA

The above simulation model consists of following parameters

1. 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. This workstation requires a fixed amount of time to route each packet, as determined by the "IP Forwarding Rate" attribute of the node. Packets are routed on a first-come-first-serve basis and may encounter queuing at the lower protocol layers, depending on the transmission rates of the corresponding output interfaces.
2. 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.
2. "Application Specification": Specifies applications using available application types. You can specify a name and the corresponding description in the process of creating new applications. For example, "Web Browsing (Heavy HTTP 1.1)" indicates a web application performing heavy browsing using HTTP 1.1. The specified application name will be used while creating user profiles on the "Profile Config" object.
3. "Voice Encoder Schemes": Specifies encoder Parameters for each of the encoder schemes used for generating Voice traffic in the network.

3. Profile config (1): The "Profile Config" node can be used to create user profiles. These user profiles can then be specified on different nodes in the network to generate application layer traffic. The application defined in the "Application Config" objects are used by this object to configure profiles. Therefore, you must create applications using the "Application Config" object before using this object. You can specify the traffic patterns followed by the applications as well as the configured profiles on this object.
4. VPN (1): Defines Virtual Private Network(VPN) attribute configuration details for tunneling supported at the IP layer.
5. wlan_ethernet_router_adv (2): This is a wireless lan based router with one Ethernet interface.
6. ethernet4_slip8_gtwy (1): The ethernet4_slip8_gtwy node model represents an IP-based gateway supporting four Ethernet hub interfaces, and eight serial line interfaces. IP packets arriving on any interface are routed to the appropriate output interface based on their destination IP address. The Routing Information Protocol (RIP) or the Open Shortest Path First (OSPF) protocol may be used to dynamically and automatically create the gateway's routing tables and select routes in an adaptive manner.
7. ip32_cloud node (1): The ip32_cloud node model represents an IP cloud supporting up to 32 serial line interfaces at a selectable data rate through which an IP traffic can be modeled.
8. ethernet2_slip8_firewall (1): The ethernet2_slip8_firewall node model represents an IP-based gateway with firewall features and server support. Hence, it can be also called as a multi homed-server firewall node. It supports two Ethernet and eight serial line interfaces at selectable data rates. IP packets arriving on any interface are routed to the appropriate output interface based on their destination IP address. The Routing Information Protocol (RIP), the Open Shortest Path First (OSPF), the Border Gateway Protocol (BGP) or the Interior Gateway Routing Protocol (IGRP) protocols may be used to automatically and dynamically create the gateway's routing tables and select routes in an adaptive manner
9. ethernet_server_adv (4): The ethernet_server_adv model represents a server node with server applications running over TCP/IP and UDP/IP. This node supports one underlying Ethernet connection at 10 Mbps, 100 Mbps, or 1 Gbps. The operational speed

is determined by the connected link's data rate. The Ethernet MAC in this node can be made to operate either in full-duplex or half-duplex mode. Note that when connected to a Hub, it should always be set to "Half Duplex". A fixed amount of time is required to route each packet, as determined by the "IP Forwarding Rate" attribute of the node. Packets are routed on a FCFS basis and may encounter queuing at the lower protocol layers, depending on the transmission rates of the corresponding output interface.

2.5.2. Scenario II: Firewall encryption for wired server

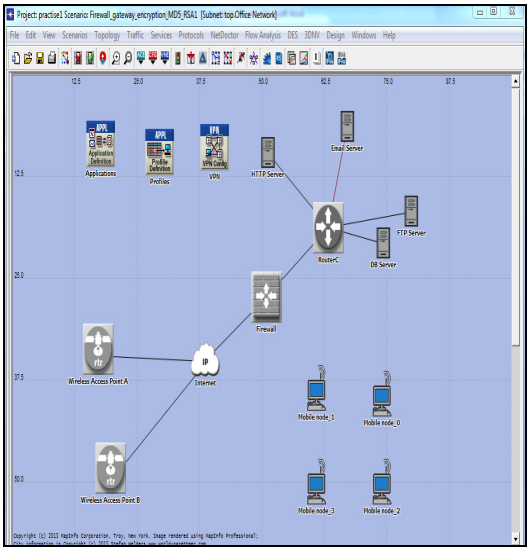

Figure 7: Firewall encryption using MD5 and RSA

The above simulation model consists of following parameters

1. wlan_wkstn_adv(4)
2. Application config, profile config,VPN(1)
3. wlan_ethernet_router_adv(2)
4. ip32_cloud node(1)
5. ethernet2_slip8_firewall(1)
6. ethernet_server_adv(4)

We have taken different parameters to study the performance of hybrid networks

2.6. Simulation Analysis

- Delay: It is observed from fig. that delay overhead in WTLS gateway is slightly higher than the firewall gateway. Delay is calculated in form of seconds. When the gateway encryption is used for wireless client then delay is higher. Similar to wired traffic delay is in lower order when firewall encryption is used.

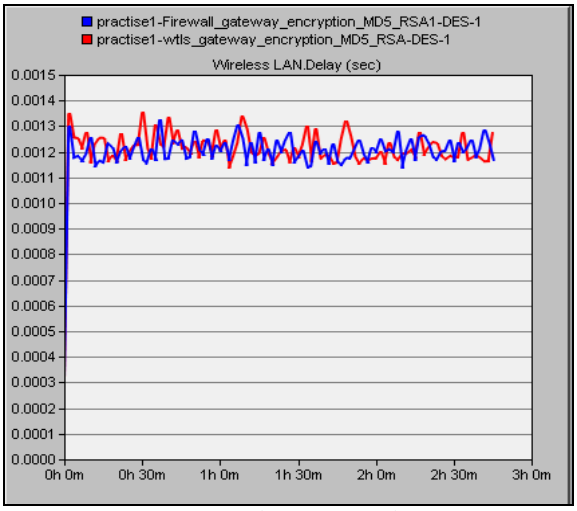

Figure 8: Wireless LAN Delay (Sec)

- Throughput: As observed from below figure that throughput with gateway encryption is lower than the firewall encryption. With gateway encryption the maximum throughput is 120,000 bits in 60 minutes. On the other side for firewall encryption the maximum throughput is 105,000 bits in 60 minutes.

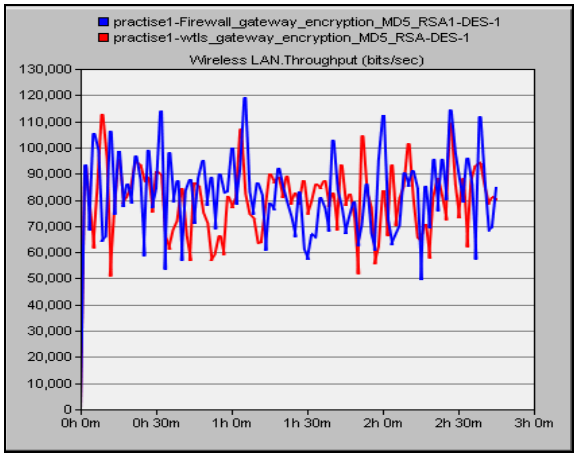

Figure 9: Wireless LAN throughput (bits/sec)

- Media Access Delay: It is observed that media access delay is higher is case of WTLS gateway encryption and lower in firewall encryption. In fig media access delay for WTLS gateway encryption is 0.00054(sec). Similar to firewall gateway encryption media access delay is 0.00047(sec)

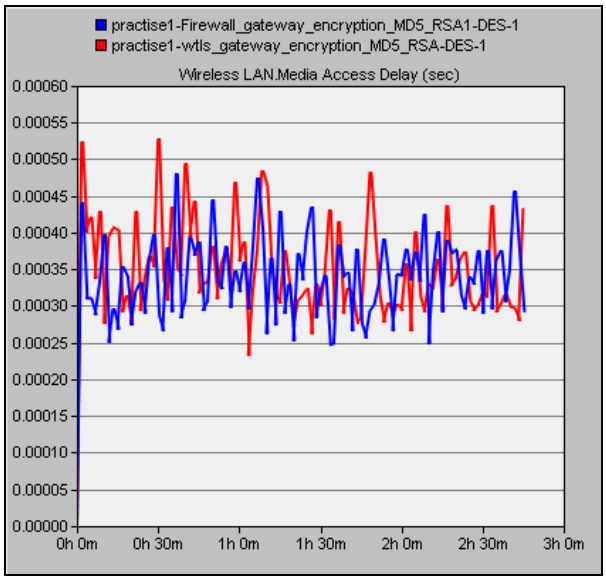

Figure 10: Wireless LAN Media Access Delay

2.7. Server DB Query Traffic Sent and Received

DB query traffic received means average bytes per second forwarded to the database query Application by the transport layer in this node. In Fig the average traffic received for WTLS gateway encryption is 127 bytes and firewall encryption is 138 bytes.

DB query traffic sent means average bytes per second submitted to the transport layer by the Database Query Application in this node. In Fig the average traffic received for WTLS gateway encryption is 8000 bytes and firewall encryption is 8600 bytes.

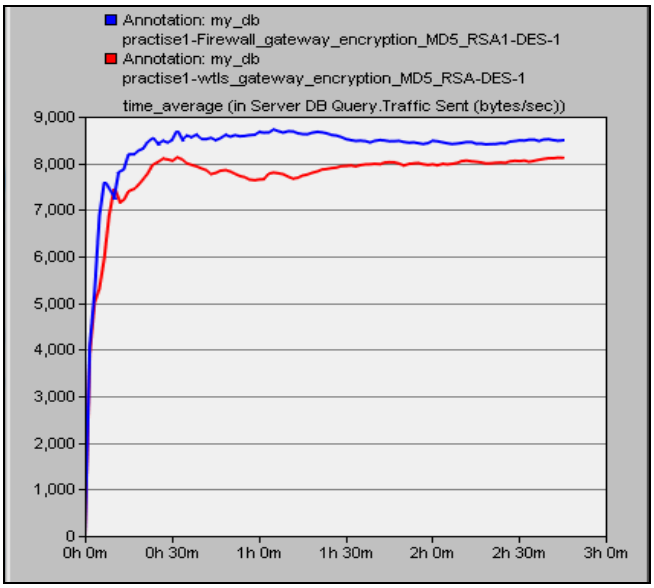

Figure 11: Time Average in server DB query traffic sent (bytes/sec)

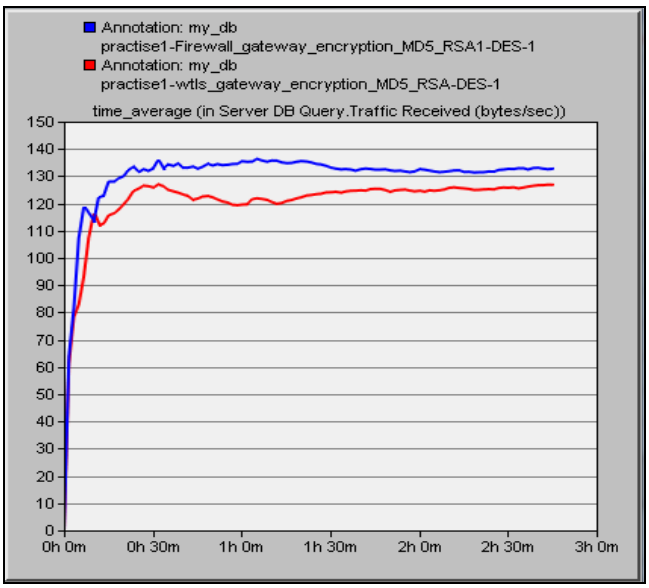

Figure 12: Time average in server DB query traffic received (bytes/sec)

2.8. Time Average in Client FTP Download Response Time

It is observed from below figure that average time for client ftp download response time for WTLS gateway encryption is 0.45 sec and firewall gateway encryption is 0.50 sec. Therefore, firewall encryption performs better as compare to gateway encryption. Time beyond the sending a request and receiving the response packet for the FTP application in this node. it is measured from the time a client application sends a request to the server to the time This time includes signaling delay for the connection setup and tear-down. This statistic is written after the connection is closed.

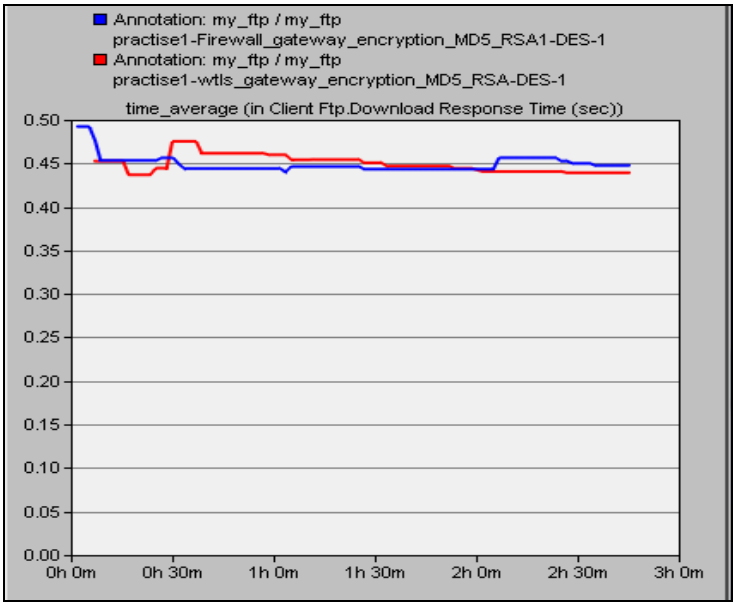

Figure 13: Time average in client ftp download response time (se

3. Conclusion

We have identified and analyze the security holes in between the wireless client and WAP gateway using opnet modeler 14.5 as simulation tool. We plan for having multiple scenarios with different parameters. Based on opnet we have experiments the results on various wireless factors like delay, throughput, media access delay web application like https, email, ftp and DB server with various factors like packets sent and received by client and server. The results show that with firewall security mechanism wireless networks perform better as compare to gateway security.

This paper also presented and implemented the proposed model for hybrid security protocol architecture for wired and wireless devices. Moreover, the comparison based on the performance of Transport layer security and Wireless Transport Layer Security with proposed protocol has done in this paper.

4. References

i. Singelée, Dave, and Bart Preneel. "The wireless application protocol (WAP)." Cosic Internet Report (2003).
ii. BAYOGLU, BURAK. Performance evaluation of WTLS handshake protocol using RSA and elliptic curve cryptosystems. Diss. Sabanci University, 2004.
iii. Moon, Jongcheol, et al. "A HANDSHAKE PROTOCOL ANALYSIS OF WAP WTLS.".
iv. Eduardo B. Fernandez, Imad Jawhar, Maria M. Larrondo-Petrie, and Michael VanHilst, "An overview of the security of wireless networks". Technical Report. Dept. of Computer Science and Engineering Florida Atlantic University. Version 19-Nov-2004.
v. Kim, Younhee, and Chun-kit Wong. "Comparison of WTLS and ITLS in Wireless end-to-end secure network (December 2002)."
vi. Daswani, Neil. "Cryptographic execution time for WTLS handshakes on palm OS devices." Certicom Public Key Solutions (2000)..
vii. Ganeshkumar, K., and D. Arivazhagan. "Generating a digital signature based on new cryptographic scheme for user authentication and security." Indian Journal of Science and Technology 7.S6 (2014): 1-5.
viii. Ghaffari, Ali, and Leyla Azari. "Proposing a novel method based on network-coding for optimizing error recovery in wireless sensor networks." Indian Journal of Science and Technology 8.9 (2015): 859.
ix. Sami Jormalainen, Jouni Laine.Security in the WTLS.Computer Science and Engineering Helsinki University of Technology.1999.11
x. Mohammadi, Ramin, and Ali Ghaffari. "Optimizing reliability through network coding in wireless multimedia sensor networks." Indian Journal of Science and Technology 8.9 (2015): 834.
xi. M.Thiyagarajan, Chaitanya Raveendra, V. Thiagarasu,"Web Service Authentication and Multilevel Security",Indian Journal of Science and Technology,2015 July, 8(15).
xii. Pateriya, R. K., et al. "A Proposed Algorithm to improve security & Efficiency of SSL-TLS servers using Batch RSA decryption." arXiv preprint arXiv:0907.4994 (2009).
xiii. N.Sklavos,P.Kitsos,K.Papadopoulos,O.Koufopavlou.Design Architecture and Performance Evaluation of the Wireless Transport Layer Security. The journal of supercomputing,36,33-50,2006
xiv. Miller, Sandra Kay. "Facing the challenge of wireless security." Computer 34.7 (2001): 16-18.
xv. Mayank Sarogi.Security in wireless Sensor Networks. Department of Computer Science. University of Tennessee, Knoxville saraogi AT cs.utk.edu.
xvi. Chaitanya Pullela et al., "Component based Architecture for Mobile Information Access", International Conference on Parallel Processing (ICPP 2000), August 2000, 14 citations.
xvii. Juul, Niels Christian, and Niels Jørgensen. "Security issues in mobile commerce using WAP." 15th Bled Electronic Commerce Conference. 2002.
xviii. Hamarsheh, Qadri. "Wireless Gateway Programming Model." Perspective Technologies and Methods in MEMS Design (MEMSTECH), 2010 Proceedings of VIth International Conference on. IEEE, 2010.
xix. Devasena, A., & B. Sowmya. "Wireless Sensor Network in Disaster Management." Indian Journal of Science and Technology [Online], 8.15 (2015): n. pag. Web. 23 Feb. 2016
xx. Madhumitha, P., B. Johnsema, and D. Manivannan. "Domination of Constrained Application Protocol: A Requirement Approach for Optimization of Internet of Things in Wireless Sensor Networks." Indian Journal of Science and Technology 7.3 (2014): 296.
xxi. Emdadi, A., R. Karne, and A. L. Wijesinha. "Implementing the TLS Protocol on a Bare PC." Computer Research and Development, 2010 Second International Conference on. IEEE, 2010.
xxii. Yuji Suga, "SSL/TLS Servers Status Survey about Enabling Forward Secrecy", NBIS, 2014, 2014 17th International Conference on Network-Based Information Systems (NBiS), 2014 17th International Conference on Network-Based Information Systems (NBiS) 2014, pp. 501-505
xxiii. Markku Juhani Olavi Saarinen,"Attacks against the WAP WTLS protocol",CMS 99 proceedings of the IFIP TC6/TC11 joint working conferences on secure information networks:communication and multimedia security pages 209-215.
xxiv. Yuanyuan, Cui, et al. "Cryptanalysis and improvement of a WTLS handshake protocol with user anonymity and forward secrecy." High Technology Letters, Beijing 15 (2005): 6-10.
xxv. Kwak, Dong Jin, et al. "A WTLS handshake protocol with user anonymity and forward secrecy." Mobile Communications. Springer Berlin Heidelberg, 2003. 219-230.
xxvi. Pateriya, R. K., et al. "A Proposed Algorithm to improve security & Efficiency of SSL-TLS servers using Batch RSA decryption." arXiv preprint arXiv: 0907.4994 (2009)..
xxvii. Jonsson, Jakob, and Burton S. Kaliski Jr. "On the Security of RSA Encryption in TLS." Advances in Cryptology—CRYPTO 2002. Springer Berlin Heidelberg, 2002. 127-142.
xxviii. Ghaffari, Ali. "Designing a wireless sensor network for ocean status notification system." Indian Journal of Science and Technology 7.6 (2014): 809.
xxix. Durairaj, M., and A. Manimaran. "A study on security issues in cloud based e-learning." Indian Journal of Science and Technology 8.8 (2015): 757-765.