International Journal of Advance in Computer Science & its application – IJCSIA 2018
Copyright © Institute of Research Engineers and Doctors , SEEK Digital Library
Volume 7 : Issue 2 [ISSN : 2250-3765] - Publication Date: 25 June , 2018

Studying The Impact Of Accessing The Wired Network Through Private Wireless Devices Using Wireless Transport Layer Security (WTLS)

Hadeel ImadElDin Abd ElSamad Ahmed, Latifa Sami Hassan Elhakim
Sami Abbas Nagar, Ali.M.A.Ibrahim

***Abstract*— Studies show that, the wireless network is not precisely secured therefore security protocols must be implemented. In this research Wireless Transport Layer Security (WTLS) protocol was used to have secured wireless network with approximately or exactly same performance of wired network. In secured wireless network the unsecured wireless network packets were taken to be simulated in NS2 by adding the Wireless Transport Layer Security (WTLS) protocol using Wi-Fi Protected Access (WPA), and then the secured wireless network was implemented in reality.**

The accuracy between the simulated and actual production obtained was 100% for packet loss, 99.998915 % for average delay and 99.999944% for throughput. Finally, the throughput accuracy between wired and secured wireless network is 77.585955% in reality.

***Keywords*—Reality, NS2, WTLS, Delay, Throughput, Packet loss.**

I. INTRODUCTION

Most organizations and companies prefer using wired devices to keep their network information secured despite the distance limitations and costs. Although Wireless devices capacity and performance has increased exponentially and allow users to access the network remotely within the specified range they have many security threats. Securing wireless devices is necessary with the increase considerations about a secure access to your network using private wireless devices such as personal digital assistant (PDA), Smartphone and IP phone, since it became a critical issue. Smart phones and other handheld devices like PDAs are growing rapidly with their easy to access the Internet by using WIFI, LIFI or mobile data [3].

The wireless devices can access the network by tuning in to the appropriate infrared or radio frequency within the effective distance covered by the access point (Hotspot) to share information between devices [3, 4], wireless networks are less secured because communication signals travel through the air and can be easily intercepted. It protects its data through encryption [5].

The communication network between the wired and wireless device is unfortunately not precisely secured since it can be exposed to malicious attacks. As a result security protocols are applied to avoid those attacks, but a tremendous disadvantage that affects the three metrics which are the delay, throughput, and packet loss occurs after applying these protocols.

This paper aims to access the wired network through private wireless devices. And then adding the security protocol Wireless Transport Layer Security (WTLS) to the wireless network. After that studying the impact of adding the security protocol on the three metrics (Delay, throughput and packet loss) in order to enhance the performance of secured wireless network to have exactly or approximately same performance as wired network.

II. Related work

There are different types of networks that can be accessed and these networks can be divided as follows:

A. *Wired networks:*

Ethernet network which is widely known as wired network is the most common sort of Local Area Network (LAN). A wired framework is essentially an aggregation of no less than two PCs, printers, and different gadgets associated by Ethernet link which has very high speed ranged between (10-100)Mbps or higher[2].

Although the wired network has very high speed of transmission of data and strong security it has also distance limitations and has very high expenses due to physical infrastructure[1, 2]These limitations in the wired network lead to introduction of wireless networks[2].

B. *Unsecured wireless networks:*

The wireless network has capability to access networks remotely [3]. The wireless devices can access the network by tuning in to the appropriate infrared or radio frequency within the effective distance covered by the access point (Hotspot) to share information between devices [1, 4], wireless networks

Latifa Sami Hassan Elhakim
University Of Medical Science And Technology (UMST)
Sudan
latifa_elhakim@hotmail.com

Hadeel ImadElDin Abd ElSamad Ahmed
University Of Medical Science And Technology (UMST)
Sudan
hadeelabushaiba@gmail.com

are less secured because communication signals travel through the air and can be easily intercepted. And this security problem leads to have secured wireless network.

C. Secured wireless networks:

To protect the data from attacks secure communication protocols are used to protect the data through encryption[6].

The demand for security proper implementations is increasing rapidly, thus the need for new applicable protocols were introduced. Secure Socket Layer (SSL), it is a protocol that has the capability to secure any transmission over Transmission Control Protocol (TCP). SSL applied to most web browsers and these browsers used to access web applications. In SSL client does not need client certificate, but each web server has its own digital certificate. In order to make a standardized protocol to all internet community the Transport Layer Security (TLS) protocol was introduced [5]. TLS was the basis of Wireless Transport Layer Security (WTLS) which is security level for Wireless Application Protocol (WAP). WTLS was introduced to reliability and privacy for wireless applications[2].

III. Models and Results:

The research methodology considers the organization of the research design and procedure, and describes the way forward towards achieving the research objectives. In this paper, the traffic flow of wired, unsecured wireless and secured wireless networks will be captured by Wireshark software. NS2 software used in order to simulate three types of networks and then making comparison of reality and simulated results and studying the impact of applying Wireless Transport Layer Security (WTLS) security protocol.

The three metrics were calculated using the following equations:

Average Delay= Total delay/ Count (1)

Delay[i]=Receiving time – Sending time[i] (1.1)

Total Delay= total delay + delay[i] (1.2)

Count= Total Packet (1.3)

i=total packet sequence

Throughput=(ReceivedData * 8)/ Data transmission period (2)

Packet loss= Generated Packet – Received packet (3)

A. MODELLING OF THE PRODUCTION NETWORK IN NS2:

This section includes how data is captured for production (wired) network.

1) Network production:

In this network the data centre was originated from three servers in the virtual machine (VMware) whereas the connection is considered wired installed in windows 8 PC. After connecting the wired network, the WIRESHARK application was utilized for capturing the data and it was installed in windows 8, adjusted to end capturing after 5 minutes and started exactly at the same second as the scenario. The data that captured by WIRESHARK was transferred to excel sheet. 30 packets were sorted out according protocols required and each IP address for forward and reverse link whereas each IP must send and receive for all other IP's if found and taken as a reference to be applied for simulation network. The three metrics (Delay, Throughput and Packet loss) were calculated.

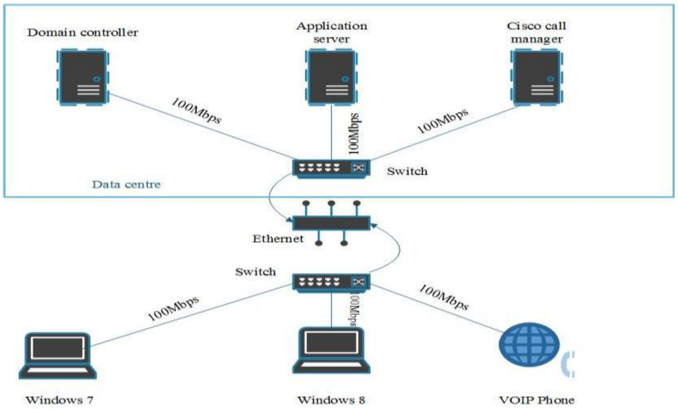


Figure 1. Production (wired) network

a) Scenario:

The data "Scenario" input to the production network was as follows:

1st min: was idle.

2nd min: The call was established between Windows 7 and windows 8.The conversation was as follows:

Windows 7: Hello, I am Latifa.

Window 8: hello Latifa.

Windows 7:the exam is on the 29th of December.

Windows 8:Okay thank you.

3rd min: for uploading the file.

4th min: For downloading the file.

5th min: for finishing the upload and download of the files.

b) Reality Numerical Results:

Suppose that each IP is denoted by an alphabet:

A → 192.168.30.200

B → 192.168.30.129

C → 192.168.30.130

D → 192.168.30.128

E → 192.168.30.131

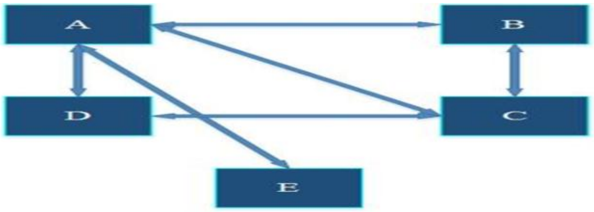


Figure 2. Link between each IP's in production network

TABLE I. THE DELAY BETWEEN EACH LINK AND BANDWIDTH OF THE PRODUCTION NETWORK

Link	Delay	Bandwidth
A-C	0.0794284s	100 MHZ
A-D	26.091218s	100 MHZ
A-E	0.001175s	100 MHZ
B-C	0.000143s	100 MHZ
C-D	24.382191s	100 MHZ

Total Delay= 0.0797284+26.091218+0.001175+0.000143+24.382191 =47.5544554s

Average Delay = 50.5556884/30 = 1.585148s

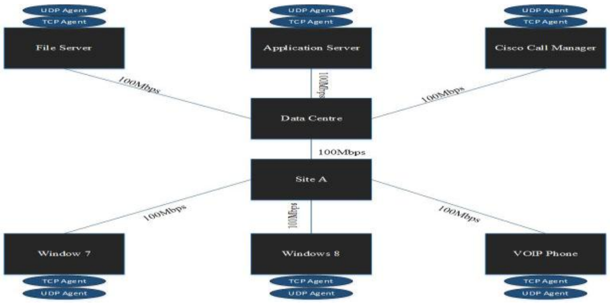
Throughput=21140.00*8/178.660486=946.5999102bps

2) Ns2 Modeling:

After constructing the production network in reality, same network with same parameters setup was built in NS2 simulator and capturing trace file for calculating the three metrics. Links, TCP and UDP agents were created in the network simulator.

The 30 packets in reality were used in simulation. An assumption that all UDP, RTP, SIP packets are Cbr in simulation having an accuracy 100% with the exact same timing and packet size. Whereas the TCP packets are assumed to have a delay of 0.00247s for establishing the link connection with an acknowledgment in return.

Figure 3. Production network in NS2



a) NS2 Numerical results:

Calculation of the three metrics using the same equations of reality:

Packet loss= 0

Average delay= 3.534379774s

Throughput= 946.599624bps

3) Validation and verification:

Due to the results of simulation and reality a comparison was verified to validate the accepted accuracy range of the simulation in order to initiate this model as a reference of comparison with the results generated in both wireless networks, this comparison was as follow:

TABLE II. RELATION BETWEEN SIMULATION AND REALITY RESULTS

Metrics	Wired network in reality	Wired network in Ns2 simulator	Error percentage	Accuracy
Packet loss	0	0	0%	100%
Average delay	3.534308581s	3.534379774s	0.00204340%	99.99868475%
Throughput	946.599910bps	946.599624bps	0.0000302%	99.9999849%

B. *MODELLING THE UNSECURED WIRELESS NETWORK IN NS2:*

This section includes how data is captured for unsecured wireless network.

1) Unsecured wireless Network production:

In this network wireless components were added to the wired network in order to access wired network remotely. The same steps of wired network were followed in this network with addition to using WIFI access point.

a) Reality Numerical Results:

The IP's are donated by the same alphabets.

A → 192.168.30.50

B → 192.168.30.129

C → 192.168.30.51

D → 192.168.30.128

E → 192.168.30.131

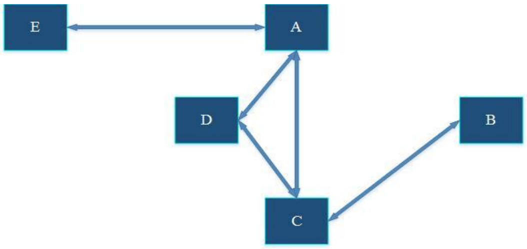


Figure 4. Link between IP's in Unsecured network

TABLE III. THE DELAY BETWEEN EACH LINK AND BANDWIDTH OF THE UNSECURED NETWORK

Link	Delay	Bandwidth
A-B	-	-
A-C	0.199452s	54MHZ
A-D	20.868588s	100MHZ
A-E	0.001217s	100MHZ
B-C	0.000311s	100MHZ
C-D	7.068462s	100MHZ

Total delay = 0.199452+20.868588+0.001217+0.000311+7.068462 =<u>28.156539s</u>

Average delay =28.156539/30 = <u>0.9385513s</u>

Throughput= 23856*8/179.172374 =<u>1065.164209bps</u>

2) Ns2 Modeling:

After constructing the unsecured wireless network in reality, same network with same parameters setup and assumptions in wired NS2 model was built in NS2 simulator.

a) Ns2 numerical results:

Calculation of the three metrics using the same equations of reality:

Packet loss= 0

Total delay = 94.348036s

Average delay= 3.144934533s

Throughput= 1065.164209bps

3) Validation and verification:

Due to the results of simulation and reality a comparison was verified to validate the accepted accuracy range of the simulation in order to initiate this model as a reference of comparison with the results generated in both wireless networks, this comparison was as follows:

TABLE IV. RELATION BETWEEN REALITY AND SIMULATION RESULTS

Metrics	Unsecured wireless network in reality	Unsecured wireless network in Ns2 simulator	Error percentage	Accuracy
Packet loss	0	0	0%	100%
Average delay	3.144919067s	3.144934533s	0.0005871%	99.99868475%
Throughput	1065.164209 bps	1065.164209 bps	0.00%	100%

C. *MODELLING OF THE SECURED WIRELESS NETWORK IN NS2:*

This section includes how data is captured for unsecured wireless network.

1) Ns2 Modeling:

The Wireless network was built in NS2 environment adding to the WTLS security protocol. After building the secured wireless network in simulation environment, the traffic flows between devices was captured and a trace file was obtained to calculate the three metrics (Delay, Throughput and Packet Loss.

a) Ns2 numerical results:

Calculation of the three metrics using the same equations:

Packet loss= 0

Total delay = 96.852071s

Average delay= 3.228402s

2) Secured wireless Network production:

In this network wireless Transport Layer Security (WTLS) protocol was added to the unsecured wireless network. And the encryption used was WPA pre-shared key.

a) Reality numerical results:

The IP's are donated similarly as the unsecured:

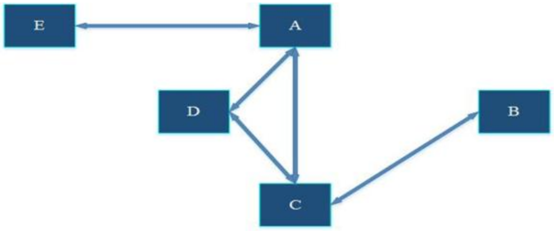


Figure 5. Links between IP's in secured network

TABLE V. THE DELAY BETWEEN EACH LINK AND BANDWIDTH OF SECURED NETWORK

Link	Delay	Bandwidth
A-B	-	-
A-C	0.076617s	54MHZ
A-D	38.177162s	100MHZ
A-E	0.001247s	100MHZ
B-C	0.000147s	100MHZ
C-D	24.5727569s	100MHZ

Total delay = 0.076617+38.177162+0.001247+0.000147+24.5727569 = 62.8279299s

Average delay =62.8279299/30 = 2.09426433s

Throughput= 23832*8/180.409334 =1056.790195bps

3) Validation and verification:

Due to the results of simulation and reality comparison was verified to validate the accepted accuracy range of the simulation in order to initiate this model as a reference of comparison with the results generated in both wireless networks, this comparison was as follows:

TABLE VI. RELATION BETWEEN REALITY AND SIMULATION RESULTS

Metrics	Secured network in Ns2 simulator	Expectation results	Secured wireless network in reality	Error percentage
Packet loss	0	0	0	0%
Average delay	3.228402	3.228415153s	3.228367s	0.00108413%
Throughput	1056.790195 bps	1056.790195 bps	1056.790869 bps	0.00005543%

IV. Conclusion:

In this research, parameters of real traffic data were injected into NS-2 simulator. The error average between the actual production and simulated obtained was 0% for packets sent, 0% for packets loss and 0% packets length. Three metrics are used for validation and enhanced results gave suitable values so as to proceed to the verification stage.

Using these real network parameters, unsecured wireless network was injected in NS2 simulator. The error average between the actual production and simulated obtained was 0% for packet loss, 0.0005871% for average delay and 0% for throughput.

In secured wireless network the unsecured network packets were taken by adding the Wireless Transport Layer Security (WTLS) protocol using Wi-Fi Protected Access (WPA) , and then the secured wireless network was implemented in reality. The error average between the simulated and actual production obtained was 0% for packet loss, 0.00108413% for average delay and 0.00005543%for throughput.

Finally, the throughput accuracy in the reality between wired and unsecured wireless network is 70.386% and between wired and secured wireless network is 66.586% .

As recommendation, is to perform the simulation with Wi-Fi channel instead of the assumption made that the channel was a direct link.

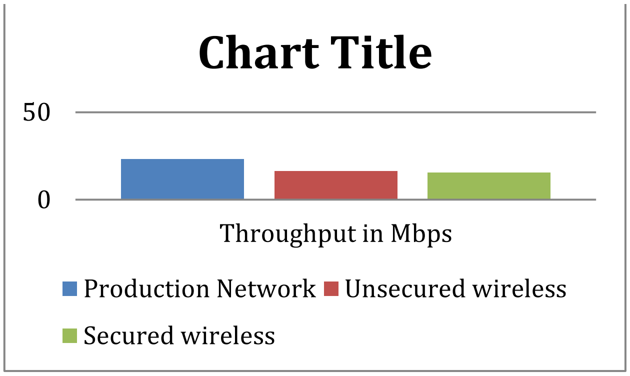


Figure 6. Comparison between throughputs of three networks

Acknowledgement:

We are thankfull for the blessings of our lord Allah Almighty and for keeping us on the right track and guiding us to complete this project successfully.

We would like to convey our gratitude towards our Supervisor, **Dr. Sami Abbas Nagar** for his guidance and endless support throughout the process of completing this project. His patience and insight were very important through this entire period. We would also like to thank our co-supervisor, **T. Ali Maher** for his efforts and time.

We appreciate the help and special support **Prof. Mamoon Mohamed Ali Homida, Dr. ElNazir** and **Dr. Haythem Awad** gave for the completion of this paper.

Finally, we are very gratefull to our family and friends for the unconditional love and encouragement they provided.

References:

[1] G. Urbas and T. Krone, *Mobile and wireless technologies: security and risk factors*: Australian Institute of Criminology, 2006.
[2] J. Muscatello and J. Martin, "Wireless Networks Security," April 20 2005.
[3] "The importance of wireless security," 2008.
[4] E. M. Royer and C.-K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," *IEEE personal communications*, vol. 6, pp. 46-55, 1999.
[5] H. L. McKinley, "SSL and TLS: A Beginners Guide," p. 15, 2003.

About Authors:

Hadeel ImadEldin final year student for BSC degree in electronics engineering, University of Medical Sciences and Technology (UMST)

Latifa Sami Elhakim final year student for BSC degree in electronics engineering, University of Medical Sciences and Technology (UMST)