This full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET 2017 conference.

Design of Secured WLAN by Using "Packet Filtering Firewall"

Haider Mohammed Turki Al-Hilfi,[1] Bassam Abdulmunem Salih[2] and Ion Marghescu[3]
[1,3]Department of Telecommunication, Faculty of Electronics, Telecommunication & Information Technology
University "Polytechnic" of Bucharest
[2]Electrical Engineering, Dept. Kufa University, Najaf, Iraq

***Abstract*—Due to the rapid demands for using wireless Local Area Network (WLAN), the security issues of WLAN becomes an important factor and interesting research area. This paper deals with the security of WLAN that designed for university of Baghdad. It consists of three buildings. The designed WLAN supports four types of services, these are: HTTP, FTP, Email and DB. The security issue that adopted, analyzed and investigated in this paper is the (packet filtering firewall system). The modeling and simulation of the designed WLAN are implemented using OPNET 14.5 modular simulator. For analysis and comparison purposes, the network is designed and simulated in two scenarios. These scenarios are: first the network is designed without using firewall protection, and second using firewall with packet filtering. After the modeling and simulation of the designed WLAN comprehensive analyses and comparisons are performed on the network at various conditions of operation with different types traffic being applied. The obtained results showed enhanced performance of WLAN security by using the proposed packet filtering firewall scheme. The delay is reduced also due to filtering of undesired packets.**

***Index Terms*—WLAN secured, Packet filtering system, OPNET 14.5.**

I. Introduction

WLAN—Several years of continuous research has led to the development of features whereby concerns about network security are gradually being addressed and resolved. Security issues related to WLAN are a major concern for all. While WLAN solutions address most of these concerns, the network is vulnerable to attacks even when there is a packet encryption. In a wireless network connection, these attacks pick up information carried by the packages. A security software has recently been developed by a wireless technology infrastructure specialist, which blocks radio signals from unauthorized access points and thus protects the wireless network from interference at the RF signal level. The micro-scanning technology makes each access point to act both as monitor and as a Wi-Fi access point [7], [9].

Firewalls protect both the wired and wireless LANs from unauthorized access. Firewalls are programmers configured in the proxy servers that define the security policy for the network. The function of the Firewall is to screen the packets so as to allow or disallow their receipt. It does so for each packet header, by matching the information, based on the predetermined packet filtering rules and accordingly determines whether to forward or discard the packets [6].

The filtering of the packets is done in the IP layer. The design of the network infrastructure and security of information technology are important elements for security of the wired and wireless networks. A well designed infrastructure ensures protection of information from unauthorized access and protects important data and software applications. Data and information security applications are the basic demand for network security, as unauthorized access can corrupt the data and cause damage to devices. With the rapid growth of WLAN technology, security of the network has assumed utmost importance and the insufficiencies of the basic security services offered by the IEEE 802.11 standard is a serious cause for concern. It has therefore become increasingly important to develop the next generation wireless multimedia applications. This research intends to explore alternative measures for new security solutions to keep pace with the growing demands [7], [9].

This article is organized as follows: Section II. In section relative works. In Section III. The proposed secured WLAN using "firewall and VPN" is presented. Section III. Gives details related to the OPNET 14.5 WLAN simulation model. Section IV. Includes a discussion of the simulation results and a comparative analysis. Section V. Concludes this article.

II. Related Works

There exists a large body of research on firewalls, such as [1–5]. In [9], performance analysis of the firewalls, their importance in protecting networks. The authors [10], investigate the performance of the firewall and impact on the network performance. The authors [12], studying the effect of implementing the firewall on the network performance and how using parallel firewalls. The authors [15], Emphasis is on the relationship between network security and performance by the firewall. The authors [16], packet filter (PF) firewall, ccheckpoint SPLAT and Cisco ASA in a testing environment with laboratory-generated traffic. In this paper, secured WLANs using "packets filtering firewall " model is used based on the part of the model proposed in [9], [15], [16].

The model is implemented by using Opnet 14.5 modular. WLAN network is modeled, and then simulated network for the two different scenarios and analyze the results and evaluate the effects of the use of the firewall with WLANs.

978-1-5090-4442-9/17/$31.00 ©2017 IEEE

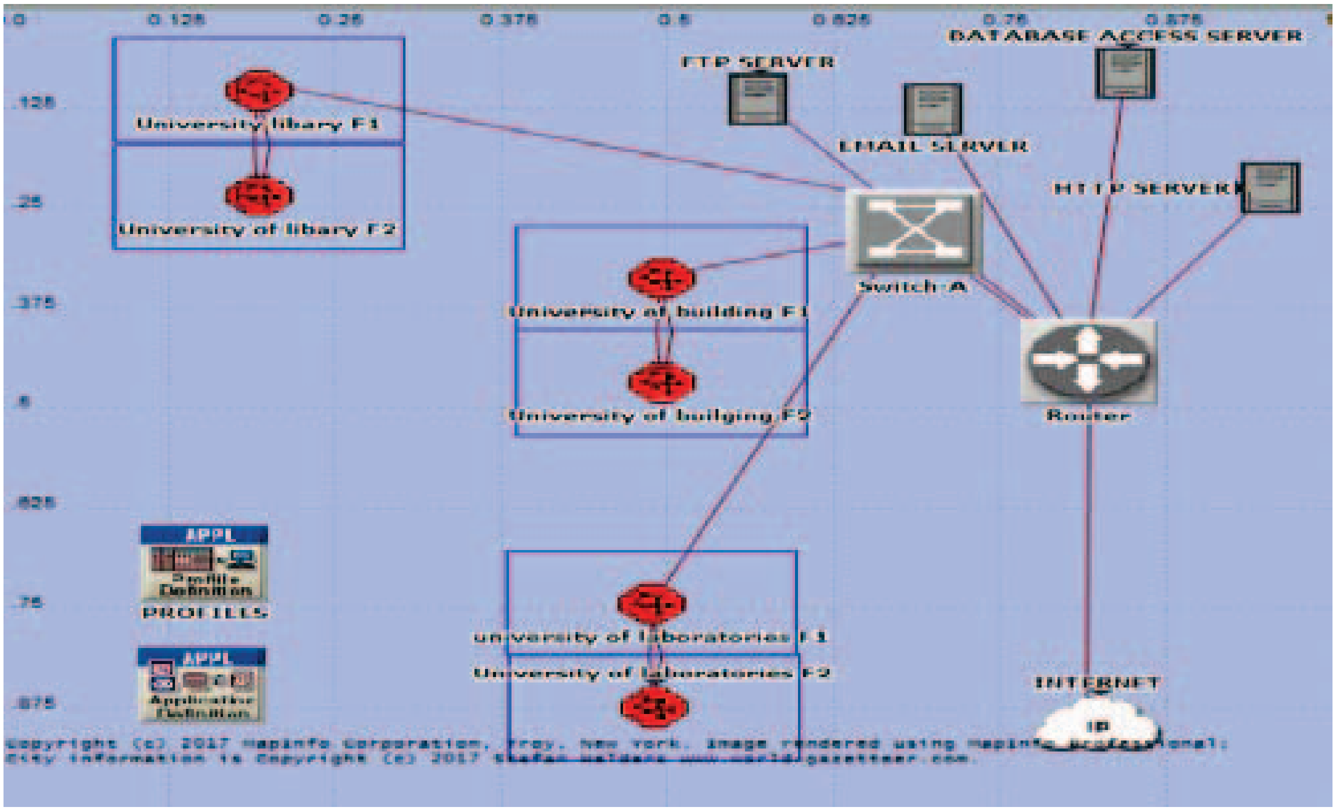
0
0.125
0.25
0.375
0.5
0.625
0.75
0.875
.125
.25
.375
.5
.625
.75
.875
DATABASE ACCESS SERVER
FTP SERVER
EMAIL SERVER
HTTP SERVER
University libary F1
University of libary F2
University of building F1
University of builging F2
Switch A
Router
APPL
Profile Definition
PROFILES
APPL
Application Definition
university of laboratories F1
University of laboratories F2
INTERNET
IP
Copyright (c) 2017 MapInfo Corporation, Troy, New York. Image rendered using MapInfo Professional;
City information is Copyright (c) 2017 Stefan Helders www.world-gazetteer.com

Fig. 1. The simulation of scenario A “without firewall”.

III. The Opnet 14.5 WLAN Simulation Model

In this section, the network topology which consists of the two scenarios are described. These are scenario “Without firewall” and scenario “With firewall”. The proposed design creates a secured WLAN to provide security to the University of Baghdad, which consist of the three buildings “University building”, “University library” and “University laboratories”, each building consist of two floors and each floor has 32 workstations divided between two access points (AP1and AP2) that configured as two BSS. The WLAN network that supports four types of the servers HTTP, FTP, EMAIL, and database, the customers in the each building can use limited services through (send/receive packets). As shown in Table I.

The proposed design is adopting (packet filtering system) for each building and also provide high security for WLANs. The modeling and simulation of WLANs are implemented using OPNET 14.5 modular simulator. Two scenarios of WLANs are designed, implemented and analyzed. These scenarios are “Without firewall WLAN” and “With firewall”. The simulation model of scenarios A and B model is shown in Figs. 1 and 2.

A. Scenario A: Without Firewall

In this scenario A the network topology consists of 6 subnets, each 2 subnets are connected together through PPP-DS3. These subnets are connected through PPP-DS3 to switch A. The latter is connected through PPP-DS3 to the router which connected through PPP-DS3 to IP cloud. The router also connected through PPP-DS3 to the four servers services (HTTP, FTP, EMAIL, and database). In the scenario “without firewall”. All users can use all applications and services on the network with full traffic between clients and servers. The simulation of scenario A model is shown in Fig. 1.

TABLE I
Scheme of the (Packets Firewall System) for WLANs Secured.

Firewall name	Location	Services permitted
Firewall A	IP cloud	HTTP & Email
Firewall B	University of library (F1,F2)	HTTP, Email and FTP
Firewall C	University of building (F1,F2)	HTTP, Email, FTP, and Database access (DB)
Firewall D	University laboratories (F1,F2)	FTP

B. Scenario B: With Firewall

In this scenario B, packet filtering is the most basic form of security mapping. The routing software can establish the license based on the source address, destination address or port number of the packet. Filtering the known port number can prevent or allow Internet protocols. The network topology consists of 6 subnets, each 2 subnets representing the one building. Each 2 subnets are connected together through PPP-DS3 to the firewall. These firewalls are connected through

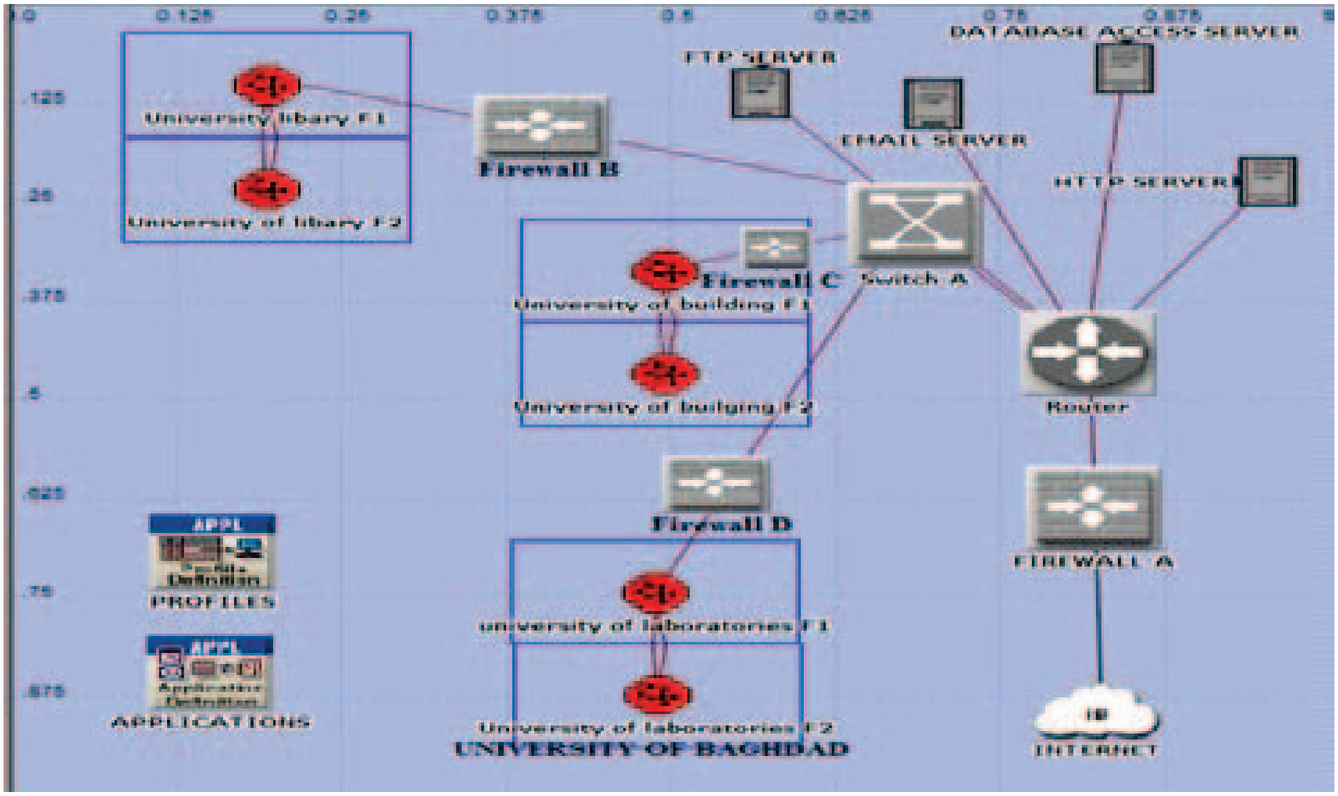

Fig. 2. WLAN model scenario“with firewall”.

PPP-DS3 to switch A. The latter is connected through PPP-DS3 to the router which connected through PPP-DS3 to firewall A which is connected through PPP-DS3 to IP cloud. The router also connected through PPP-DS3 to the four servers are: (HTTP, FTP, EMAIL, and database). The simulation of scenario B model is shown in Fig. 2.

The clients in the University Library is authorized to use all the services except database service, while the clients in the University laboratories is authorized them to use only FTP service, therefore, the clients in the University building is authorized them to use services only (HTTP, FTP, EMAIL, and DB).either, the IP could use services are: (HTTP and EMAIL in university private network). As shown in Table I. In this Wireless LAN model, the “packet filtering system” to secure and protect the database resource on the main server from any unauthorized access. In addition, the “packet filtering system” the manager the data traffic on the network and keep a big ratio of the “Wireless LAN system” capacity.

IV. Simulation Results and Comparative Analysis

In this section, comparisons, and analysis the response time is presented for the two scenarios are: “without firewall” and “with firewall”. Throughput is a refers to how much data traffic in bits/sec can be transferred and received successfully from one location to another in a given amount of time. The impact of using the scenario “With firewalls” in the “Wireless local area network” are clear via packet filtering system for the certain services so because of the difference in throughput between the two cases. The evaluation result of the system shown the throughput value in the scenario “with firewalls” is less productive than that of the scenario “without firewalls” because the firewalls are will prevent the unauthorized traffic between the three buildings and the IP cloud and the servers. It is found that throughout value in case of “Without firewall” and “With firewalls” at the operation time of 14 min:42 s, are 4,250,000 b/s and 1,500,000 b/s respectively. These results are shown in Table II and Fig. 3.

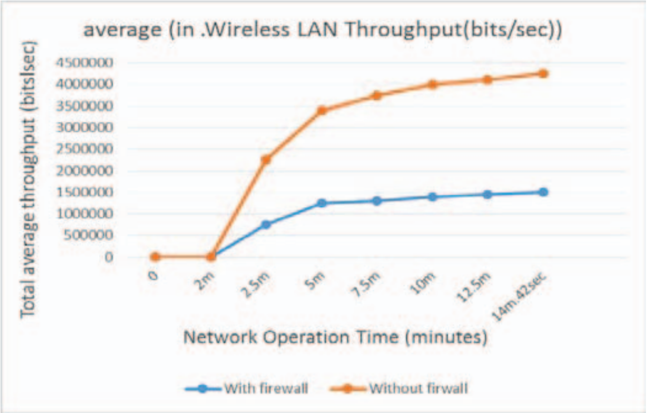

Fig. 3. Wireless LAN. throughput.

TABLE II
WLAN Model Responsible Time.

Cases	Without firewall	With firewall
Throughput at time 14 min:42 s	4,250,000 (b/s)	1,500,000 (b/s)
Delay at time 14 min:23 s	0.0569 s	0.0301 s
Database traffic received at time 14 min:23 s	882.25 (B/s)	353.24 (B/s)
Email traffic received at time 14 min:23 s	2750 (B/s)	1890 (B/s)
FTP traffic received at time 14mim:23 s	11 900 (B/s)	14 600 (B/s)
HTTP traffic received at time 14 min:23 s	1100 (B/s)	14 600 (B/s)
Firewall A database traffic received at time 14 min:23 s	1150.196 (B/s)	0
Firewall A Email traffic received at time 14 min:23 s	3036.28 (B/s)	1232.34 (B/s)
Firewall A FTP traffic received at time 14 min:23 s	13 250.196 (B/s)	0
Firewall A HTTP traffic received at time 14 min:23 s	1150.186 (B/s)	650.5 (B/s)

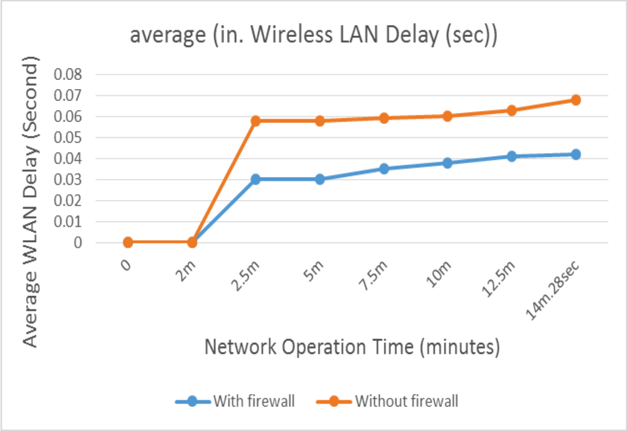

Fig. 4. Wireless LAN. delay.

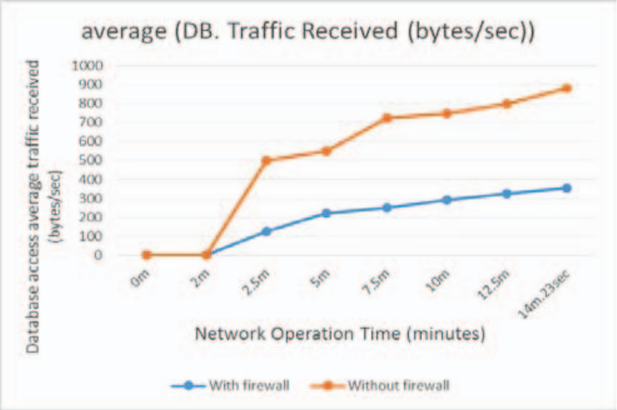

Fig. 5. Wireless LAN. DB. access, traffic received.

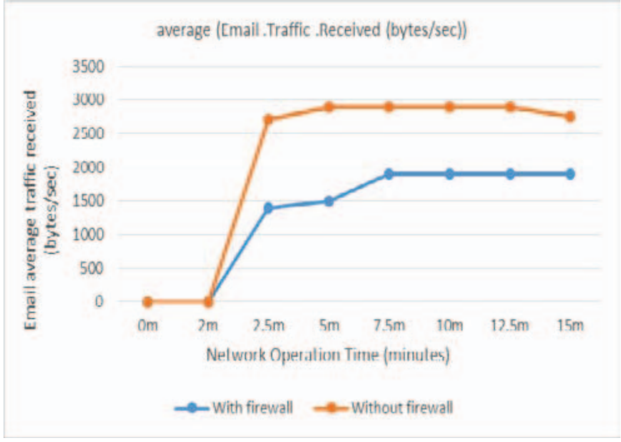

Fig. 6. Wireless LAN. Email traffic received.

Fig. 4 the evaluation result of system shown the delay value in scenario "With firewalls" is less delay than that scenario "Without firewall" because the "packet data" suffers from many delays between client and server as in "Propagation delay" and so, processing the delay, at each (node). While there too much a delay due increasing in queuing (delay) at the routers. It is found that the delay value is equal for both scenarios at operation time 2 min. after that, the delay in scenario "without firewalls " jumps to the maximum that is higher than scenario "With firewalls" at the operating time 0.0803 s and 0345 s, after few minutes of operation time, the delay in both scenarios decreased to an approximate level and refers the delay at the operation time of 14 min:28 s which is 0.0569 s for without firewalls whereas 0.0301 s for with firewalls.

Fig. 5 shows the average database traffic received. The evaluation results of the system showed the database traffic in two scenarios when use scenario "Without firewalls" are higher than that scenario "With firewalls" due to the "filtering action" of the firewalls. There is a big difference between the two scenarios because three firewalls from four firewalls had filtered the packets of database service. During the "operation time" the data traffic will gradually raise for both cases. It is found that the "database traffic" received in cases of scenario "Without firewall" and scenario "With firewall" at operation time 2 min are 361.25 B/s, 142.6 B/s while at the operation time of 14 min:23 s are 882.25 B/s, 353.24 B/s.

Fig. 6 shows the average email traffic received. The evaluation result of the system shown the traffic in scenario "With firewall" is less than that in scenario "Without firewall" because of the "packet filtering action" of the firewall which reduces the data traffic between the client and the server, therefore, reduces traffic in the network.

Fig. 7 shows the average FTP traffic received. The evaluation result of the system shown the FTP traffic in scenario "Without firewalls " is less than that scenario "With firewalls" due of the clients in the "University of laboratories " is authorized to use only (FTP) packets and will prevent other applications packets, Hence other applications packets will equal zero according to the (carrier sense multiple access with collision avoidance) access method. So, FTP will be the bigger size than other applications and increase in FTP traffic.

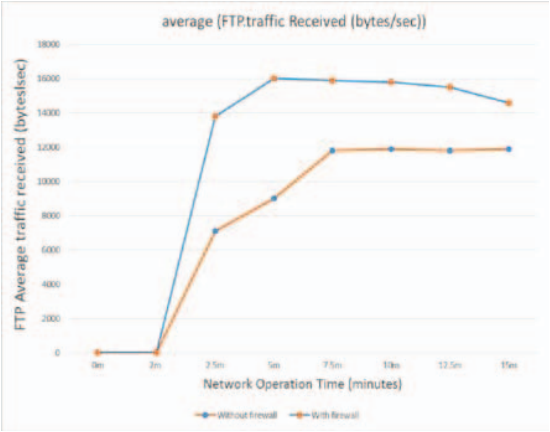

Fig. 7. Wireless LAN. FTP traffic received.

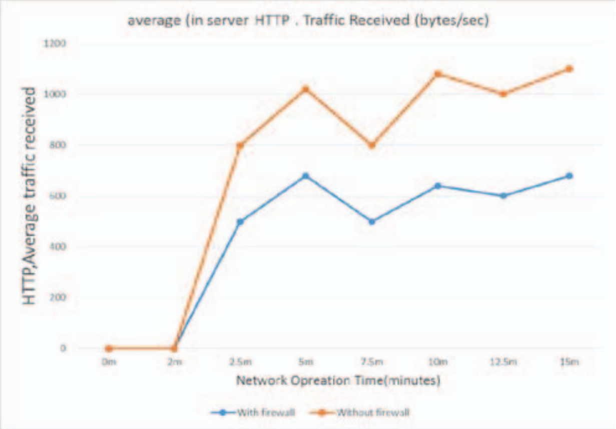

Fig. 8. Wireless LAN. HTTP traffic received.

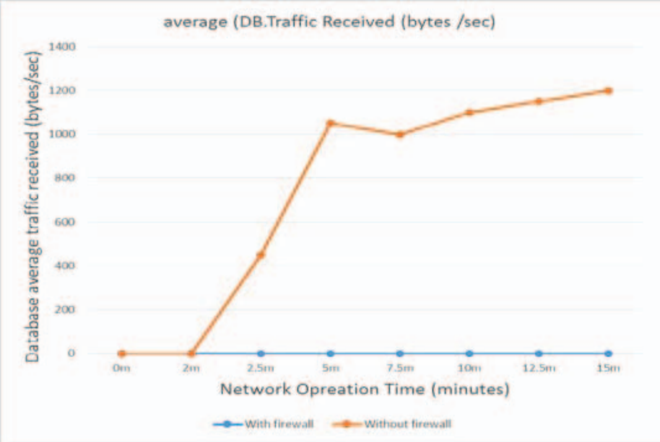

Fig. 9. Wireless LAN. (Firewall A) database traffic received.

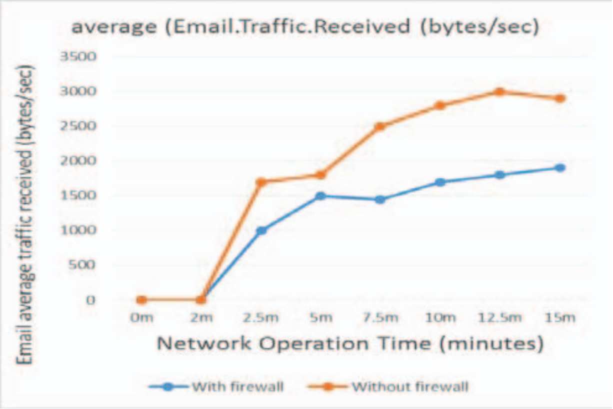

Fig. 10. Wireless LAN. Firewall A: Email traffic received.

Fig. 8 shows the average HTTP traffic received. The evaluation result of the system shown the HTTP traffic in scenario “Without firewalls” is higher than that scenario “With firewalls” because the firewall D protects the “University laboratories” is will not be allowed HTTP packets filters to the transfer through “University laboratories”.

Fig. 9 shows the “Firewall A” database traffic received. The firewall A of responsibility is the protection of data traffic between the router and IP cloud and also prevented the database traffic with IP cloud. The evaluation result of the system shown the “Firewall A” database traffic in scenario “With firewalls” equal to zero because “Firewall A” is prevented data traffic between the database server and IP cloud, while in scenario” Without firewall” there will be data traffic between the database server and IP cloud. It is found the database traffic in “Firewall A” in scenario “Without firewall” at the operating time of 12 min:50 s is 1150.196 B/s.

Fig. 10 shows the “Firewall A” Email traffic received. The “firewall A” of responsibility is the protection of data traffic between the router and IP cloud and also filtering the data traffic between Email with IP cloud. The evaluation result of the system shown the “Firewall A” Email traffic in scenario “With firewalls” is less than that scenario “Without firewall” because in scenario of “Without firewalls” there will be more connection with servers and other nodes while scenario “with firewall” will be less connection and also the firewalls there is in “University laboratories” which filters the email packets. It is found the Email traffic in “Firewall A” in scenario “Without firewall” and scenario “With firewall” at the operating time of 13 min:7 s are equal to 3036.28 B/s and 1932.34 B/s respectively.

Fig. 11 shows the “Firewall A” FTP traffic received. The “firewall A” of responsibility is the protection of data traffic between the router and IP cloud (internet) and also prevented the FTP traffic with IP cloud. The evaluation result of the system shown the “Firewall A” FTP traffic in scenario “With firewalls” equal to zero because “Firewall A” is prevented data traffic between the FTP server and IP cloud. While in scenario “Without firewall” there will be data traffic between the FTP server and IP cloud. It is found the FTP traffic in ”Firewall A” in scenario “Without firewall” at the operating time of 12 min:50 s is 13250.196 B/s.

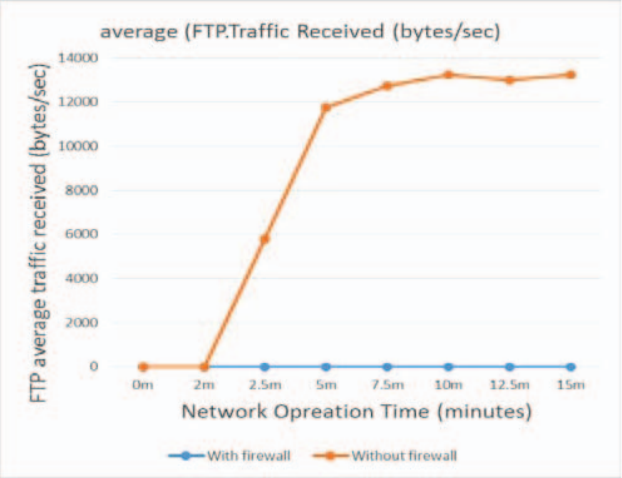

Fig. 11. Wireless LAN. “Firewall A” FTTP traffic received.

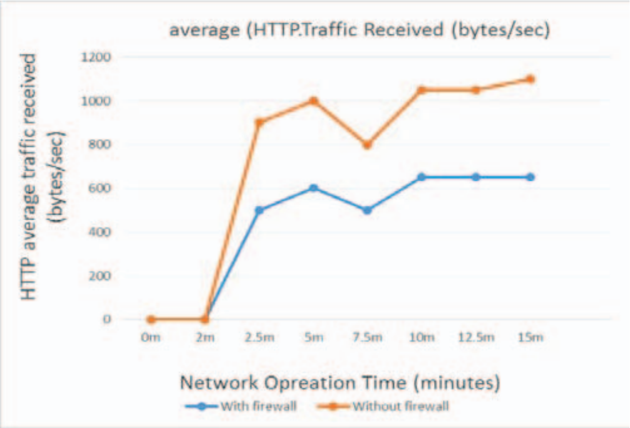

Fig. 12. Wireless LAN. (Firewall A) HTTP traffic received.

Fig. 12 shows the “Firewall A” HTTP traffic received. The “firewall A” of responsibility is the protection of data traffic between the router and IP cloud and also filtering the HTTP traffic and allowed to send and receive the packet traffic to/ from IP cloud then the network. The evaluation result of the system shown the “Firewall A” HTTP packets in scenario “Without firewalls “is higher than scenario” With firewall” because of “Firewall A” is filtering data traffic between the HTTP packets and IP cloud. It is found the HTTP traffic in “Firewall A” in scenario “Without firewall” and “With firewall” at the operating time of 12 min:50 s are 1150.196 B/s, 650.5 B/s respectively.

V. Conclusions

This paper introduced the design of secured WLAN using the “packets filtering system” technology that implemented by OPNET 14.5 Modeler. The proposed network is simulated and analyzed to investigate the impact of packets filtering system security technology on throughput and received data traffic, in addition to delay on the network through individual nodes. It is found that “packets filtering system ” is a fit way to secure and protect WLANs by decreasing the data traffic on the network and check the security required. The following conclusions are pointed out:

1) Using the packets filtering system in WLANs decreases the delay and throughput on the network but also increases the security of the network. The decreased delay on the network is due to filtering of unwanted packets
2) Packet filtering system uses as a security system and also as traffic management system on the network.
3) Packet filtering system can save important percentage of the total capacity of the network by expanding the area of deployment of the network, improving “quality of service”, and adding additional clients.

Acknowledgements: I would like to begin by thanking Allah for making all this possible. Second, I would like to thanks, “Republic of Romania”. I am grateful for all the support received whilst researching and writing up this article. There are so many to thank. First and foremost I want to express my sincere gratitude and appreciation to my supervisor Prof. Ion Marghescu Ph.D. Department of Telecommunication, Faculty of Electronics, Telecommunication & Information Technology, University “Polytechnic” of Bucharest. His words of encouragement, quiet urgings and careful reading of all of my writing will never be forgotten and also all committee members discussion.

References

[1] K. Khakpour, Liu, *Firewall fingerprinting and denial of firewalling attacks*, IEEE 2017.
[2] W. Lingbo, *A firewall of two clouds: preserving outsourced firewall policy confidentiality with heterogeneity*, IEEE 2016.
[3] S. Dhaval, “Enhanced SDN security using firewall in a distributed scenario,” in *(ICACCCT)* 2016.
[4] K. Sukhveer and K. Karamjeet, “Implementing open flow based distributed firewall,” in *InCITe* 2016.
[5] C. Thawatchai, *An improvement of tree-rule firewall for a large network: supporting large rule size and low delay*, IEEE 2016.
[6] S. Amina, “An accurate FDD-based approach for discovering Distributed Firewalls Misconfigurations,” IEEE2016.
[7] T. Hailu and K. Mesfin, *Application aware firewall architecture to enhance performance of enterprise network*, IEEE 2015.
[8] Y. Siddeep and W. Shayma, “Firewall and VPN investigation on cloud computing performance,” *(IJCSES)*, vol. 5, no. 2, Apr. 2014
[9] A. Tagwa and B. Amin, “The impact of firewall security for wireless performance,” *(IJSR)*, 2013.
[10] Z. Mohd, Y. Muhammad, and M. Abdullatif, “Performance analysis of application layer firewall,” in *(ISWTA) IEEE* 2012.
[11] M. Aruna, K Harsh, and P. Raju, “Impact of firewall and VPN for securing WLAN,” vol. 2, no. 5, May 2012.
[12] S. Nassar, A. El-Sayed, and N. Aiad, “Improve the network performance by using parallel firewalls,” in *Networked Computing (INC), 2010 6th International Conference on*, 2010, pp. 1–5.
[13] MyungKeun Yoon, Shigang Chen, and Zhan Zhang, “Minimizing the maximum firewall rule set in a network with multiple firewalls,” in *Proc. IEEE Transactions on Computers*, vol. 59, no. 2, pp. 218–230, Feb. 2010.
[14] K. Scarfone and P. Hoffman, *Guidelines on firewalls and firewall policy*, Gaithersburg, MD, USA: National Institute of Standards and Technology, 2009.
[15] H. Garantla and O. Gemikonakli, “Evaluation of firewall effects on network performance,” School of Engineering and Information Sciences, Middlesex University, London, 2009.
[16] S. S. T. Chirag, and T. Rajesh, “Performance evaluation and comparative analysis of network firewalls,” 382424, India, 2009.