ANALYSIS OF SECURITY ISSUES ON THE PERFORMANCE OF WIRELESS LOCAL AREA NETWORK IEEE 802.11

Nahom Abishu[1], Dr. A. Senthil Kumar[2], Andualem Alemu Zemedun[3]
[1]Lecturer, Department of Computer Science & Engg., Hawasa University, Ethiopia
[2] Assistant Professor, School of Computing and Informatics, Dilla University, Ethiopia
[3]Lecturer, School of Computing and Informatics, Dilla Univesity, Ethiopia

Abstract

The Performance of the WLAN is determined by various factors such as wireless standards, security protocols, encryption techniques, transmission power, communication protocols, coverage area and wireless attacks. This research is focused to analyze the performance level impact of security protocols, wireless standards, wireless attacks, and threats and vulnerabilities on WLAN using Wireshark network protocol analyzer. The study considered a variety of security protocols (such as WEP, WPA, WPA2) with different encryption techniques (AES, TKIP) over various standards of WLAN (802.11n, 802.11n/g, 802.11n/g/b). Comprehensive experimental measurements and analysis has been done in terms of throughput, delay, response time and error rate for TCP streams and network variations to demonstrate the performance level impact of security protocols, wireless standards and wireless attack in wireless local area networks. As a result, the study showed that WEP authentication and WPA security with TKIP encryption significantly affect performance in WLAN. However, WAP2 with AES encryption and IEEE 802.11n/g standard found good on wireless LAN performance. Thus, the study recommends wireless network should be configured with best suit security protocols, encryption techniques and wireless standards.

Keywords: attacks, security protocols, threats, vulnerabilities, wireless standards.

1. INTRODUCTION

In the age of Wireless Communication, the number of wireless devices connected with internet is growing rapidly and communication of confidential data over the internet is becoming more frequent every day. This is due to freedom of mobility for users by releasing the constraint of physical connections as well as increase in usage of mobile devices such as laptop computers and handhelds. Besides these advantages, inherent broadcast nature of wireless networks has raised security concerns [1], [2], [3]. Wireless networks are susceptible to many attacks since interception and eavesdropping of data in transit is possible for anyone with access to wireless network [4], [5]. Security is very much essential in tele-healthcare applications [6]. Such security issues necessitate the need to apply security mechanisms to protect the communications at the expense of system resource. Meanwhile, security services are not free as security protocols consume valuable system resources.

Thus, providing high level of security becomes a concern in mobile environments in which system resources are very limited [2]. The system resources, which are of concern in mobile wireless environments, include such as bandwidth, memory, processing power and devices, such as computer laptops and handhelds, which operate on battery power. Devices cannot implement system programs with high computational requirements, because system programs developed for mobile wireless networks must be resource efficient. Therefore, there is an acute need to quantify and analyze the performance overhead introduced by security protocols so that appropriate security services

can be provided in mobile wireless environments.

Beside the rapid growth of device connectivity and high needs of transmitting confidential data over the network, performance of wireless network is becoming low due to different determinant factors such as transmission power of access point, security protocols, coverage area, communication protocols, wireless attacks, wireless standards and threats and vulnerabilities of networking devices.

Regarding factors affecting performance in Wireless LAN some researches were conducted on transmission power, communication protocols and security protocols such as WEP, WPA and WPA2 [2], [3] . The above studies found that transmission power of access points, security protocols such as WEP and WPA significantly affect performance of WLAN specifically security protocol affects throughput, Furthermore; they recommended that it needs further study on other security issues that affect performance in wireless local area network like wireless standards, wires attack, wireless coverage area, and threats and vulnerabilities.

There is insufficiency of studies which focused on security issues that affect performance in wireless LAN like wireless standards, security protocols, wireless attack, and threats and vulnerabilities. Due to this reason, this research is focused to assess comprehensively about the factors that affect performance in Wireless Local Area Network. Thus, circumstances initiated the researcher to launch a study on the issue.

Therefore, this research analyze security protocols, wireless standards, wireless Attack, and threats and vulnerabilities that impact the performance of WLAN evaluating metrics of performance such as throughput, delay, response time and TCP error in the wireless network.

1.1 Wireless Network Performance

The performance of a network is determined by certain factors and some of them interact to provide overall performance results. Performance results vary depending on the choice of hardware device, software application and network topology [7].

According to [2], [3] the performance of wireless network is determined by certain factors such as: threats and vulnerabilities, security protocols, transmission power of access points, communication protocols, wireless standards, coverage area and wireless attack

1.1.1 Threats and Vulnerabilities

Security threats: When talking about threat it can be any person or event that can cause the damage of data or network. Threats can also be natural for example wind, lightning, flooding or can be accidental, such as accidentally deletion of file [8], [9].

Security vulnerabilities: Vulnerabilities defined as the weakness in any network that can be exploited by a threat. Recently almost in all areas network technologies have been applied, such as banking, tax, E-Commerce. These applications are consist of different network devices and computers and it is very important to protect these applications and devices from malicious hackers so that chances to exploit the vulnerabilities may reduce. There are different hardware and software tools available in the market to protect against these attacks, such as firewalls, Intrusion Detection Systems (IDS), antivirus software and vulnerability scanning software. However the usage of these hardware and software cannot guarantee the network against attacks. “The only truly secure system is that which is powered off – and even then I have my doubts”, a quotation by a leading security expert. According to the statistic from the reports of Computer Emergency Response Team/Coordination Center (CERT/CC), the number of exploited vulnerabilities increased dramatically [10]. [11].

1.1.2 Wireless Network Security Attacks

Wireless network security attack is the techniques that can be applied to violate both confidentiality and integrity or only confidentiality and only integrity [12]. This section explains various types of security attack techniques. According to [12] different types of security attacks are described below:

Unauthorized access: Once the attacker gets the access to the network, he/she is able to initiate some other types of attacks or use network without being noticed.

Man in the middle attack enables data reading from the session or modifications of the packages with violate integrity of the session. There are several ways to implement this type of attack. One way is when attacker disrupts the session and does not allow for the station to establish communications again with the Access

Point (AP). Station tries to establish session with the wireless network through AP, but can do that only through the workstation of the attacker pretending to be AP. At the same time, the attacker establishes connection and authentication with the AP.

In High-jacking type of attack, the attacker deprives the real owner of the authorized and authenticated session.

Denial of Service (DoS): An attacker tampers with the data before it is communicated to the sensor node. It causes denial of service attack due to wrong or misleading information. Jamming is one of DoS attack on network availability. It is performed by malicious attackers who use other wireless devices to disable the communications of users in a legitimate wireless network.

1.1.3 WLAN Security Protocols

To avoid these threats and to improve the security of the wireless networks various companies collaborated to make the Wi-Fi alliance to make the robust security protocol. Initially they came with the new security protocol for wireless networks known as Wi-Fi Protected Access (WPA). The need for enhanced security in wireless networks has led to the development of diverse security protocols such as Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2), and Wired Equivalent Protocol (WEP), which has led to increase in confidentiality, integrity and authenticity [13]. Although security protocols provide the services listed previously, the network performance can be affected by the deployment of such protocols.

1.1.4 Wireless LAN Standards

Wi-Fi is a wireless local area network that enables portable computing devices to connect easily to the Internet. Standardized as IEEE 802.11 a/b/g/n, Wi-Fi approaches speeds of some types of wired Ethernet [14]. The IEEE 802.11 is a set of standards for wireless local area network (WLAN) computer communications in the 2.4, 3.6 and 5 GHz frequency bands [15]. The 802.11a, b, g, and n standards are the most common for home wireless access points and large business wireless systems.

2. Materials and Methods

2.1 Experimental Setup

The test bed has been developed in a single cell environment including five wireless devices that supports 802.11 and one Access Point to configure client-server architecture in a wireless connection. One laptop was configured as a server and the second as a client in the network.

Figure 2.1 : Experimental set up

Third laptop was configured as a rouge access point installed with attacking application for the purpose of penetration testing. The access point is connected with Cisco switch and the mobile nodes were connected to D-Link Access Point (DAP1360) to provide wireless connectivity. The mobile node obtains a new IP address using DHCP to access the network.

In this experiment, wireless security protocols (WEP, WPA and WPA2) with different authentication and encryption techniques(TKIP and AES), IEEE 802.11 wireless network standards(such as 802.11n, 802.11n/g and 802.11n/g/b), threats and vulnerabilities and wireless attack were analyzed by measuring the most common metrics of network performance

like throughput, delay, response time and TCP error.

Software used in the setup the environment: Xampp server, Wireshark and Netsparker were installed. Web applications were deployed on the Xampp server and using Wireshark and netsparker vulnerability of the network and application deployed on the server were analyzed. Finally, using wireshark attack was exploited on the server and performance of the network was analyzed.

Experiment setup made for performance analysis by calculating throughput, delay, TCP error and response time by applying some variations of security mechanisms like WEP, WPA and WPA2 with different authentication and encryption methods i.e. TKIP and AES on the wireless Local Area Network. The throughput is defined as a parameter for the measurement of the amount of data transmitted over wireless LAN in a predefined period of time. The response time is the time required for traffic to travel between two points or the time interval between a user's request for using services and the time till the connection is established. Throughput has been measured in KB/sec and Response time in seconds.

2.2 Experimental Procedures and Analysis

Five different experiments as shown below have been done to evaluate the impact of security issues on the performance of WLAN.

Experiment 1**:** wireless access point (AP) is configured on different IEEE 802.11 standards without security protocols, authentication and encryption.

Experiment 2: WEP authentication

Scenario 1**:** WEP authentications with 64-bit. The researcher configured the Access Point by enabling WEP 64-bit with 802.11n/g and 802.11/n/g/b separately and measured throughput, delay, response time and TCP error.

Scenario 2: WEP authentications with 128-bit is configured with each wireless standard and performance metrics were measured.

Experiment 3**:** WPA-Personal authentication with TKIP and AES Encryption

Scenario 1: WPA-Personal authentication with TKIP Encryption is configured with each wireless standard (802.11n, 802.11n/g, 802.11n/g/b) and performance metrics were measured.

Scenario 2**:** WPA-Personal authentication with AES Encryption. The researcher configured wireless Access Point by enabling WPA with AES encryption techniques for IEEE802.11n,802.11n/g and 802.11n/g/b standards and performance metrics were measured.

Experiment 4: WPA2 Personal authentications with TKIP and AES Encryption

Scenario 1: a WPA2-Personal authentication with TKIP Encryption. To evaluate the performance of a wireless network WPA2 security and TKIP encryption were implemented with three wireless standards namely 802.11n/g/b, 802.11n/g and 802.11n. Thus, throughput, latency, response time and TCP error were measured.

Scenario 2: a WPA2-Personal authentication with AES Encryption. To evaluate the performance of a wireless network WPA2 security and AES encryption are implemented with three wireless standards namely 802.11n/g/b, 802.11n/g and 802.11n. Hence, throughput, latency, response time and TCP error were measured.

Experiment 5: Analyzing wireless attack by finding vulnerabilities of network

To analyze the effect of wireless attack on the performance of wireless LAN, threats and vulnerabilities of wireless network were checked using netsparcker and wireshark. Using the vulnerabilities of the network, attacks were exploited to deny service form a server.

3. Experimental Results

a) Throughput analysis

The average throughput significantly increase in a network configured without security and when WPA2 with AES encryption is implemented but significantly low in a wireless network WEP authentication is implemented (Table 1).

Table 1: shows the average throughput (KB/s) of IEEE 802.11 standards with security protocols.

IEEE 802.11 Standards	No security	WEP 64-bit	WEP 128- bit	WPA with TKIP	WPA with AES	WPA2 with TKIP	WPA2 with AES
802.11n	1557.06	N/A	N/A	963.74	7.18	986.25	1351.96
802.11n/g	1266.46	511.33	661.01	833.13	967.60	1039.65	1034.24
802.11n/g/b	1276.79	2.94	732.47	900.95	1274.69	780.16	1337.64
Average	1366.77	257.14	696.74	899.27	749.82	935.35	1241.28

As it is shown on Figure 2, highest average throughput is yield when wireless standard IEEE 802.11n/g is implemented and significantly low in IEEE 802.11n wireless standard.

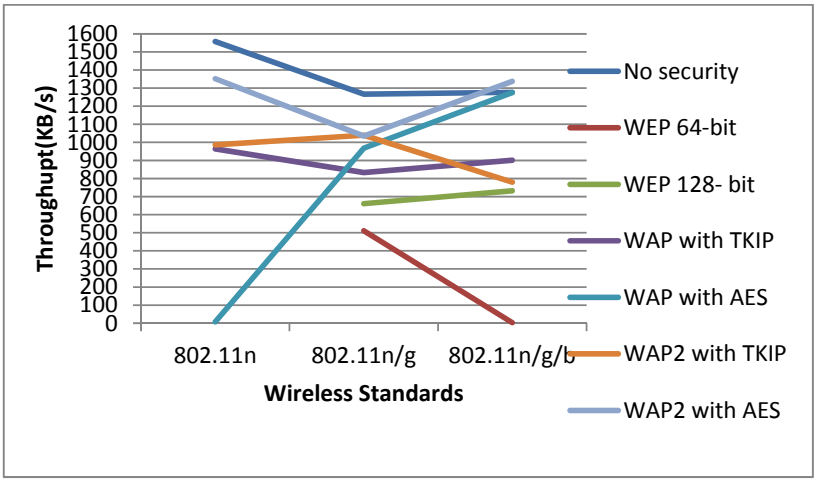

Figure 2: Average throughputs (KB/s) of IEEE 802.11 standards with wireless Security protocols.

b) Delay analysis

In this experiment the average delay time, significantly low in a wireless network configured without security and from wireless networks configured with security, WPA2 with AES encryption yields low delay time (9.71s) and significantly high in a wireless network configured with WAP and TKIP encryption techniques (Table 2).

Table 2: shows the average delay (s) of 802.11 standards with wireless security protocols

IEEE 802.11 Standards	No security	WEP 64-bit	WEP 128 bit	WPA with TKIP	WPA with AES	WPA2 with TKIP	WPA2 with AES
802.11n	2.62	N/A	N/A	15.59	5.43	8.59	10.22
802.11n/g	5.02	5.12	5.84	16.82	23.16	1.23	15.00
802.11n/g/b	11.5	29.37	13.92	24.44	7.52	19.94	3.91
Average	6.38	17.25	9.88	18.95	12.04	9.92	9.71

The lowest average delay time was obtained in a wireless network configured with IEEE 802.11n wireless standard and the highest average delay was 15.8s produced when wireless network configured with IEEE 802.11n/g/b standard (Figure 3).

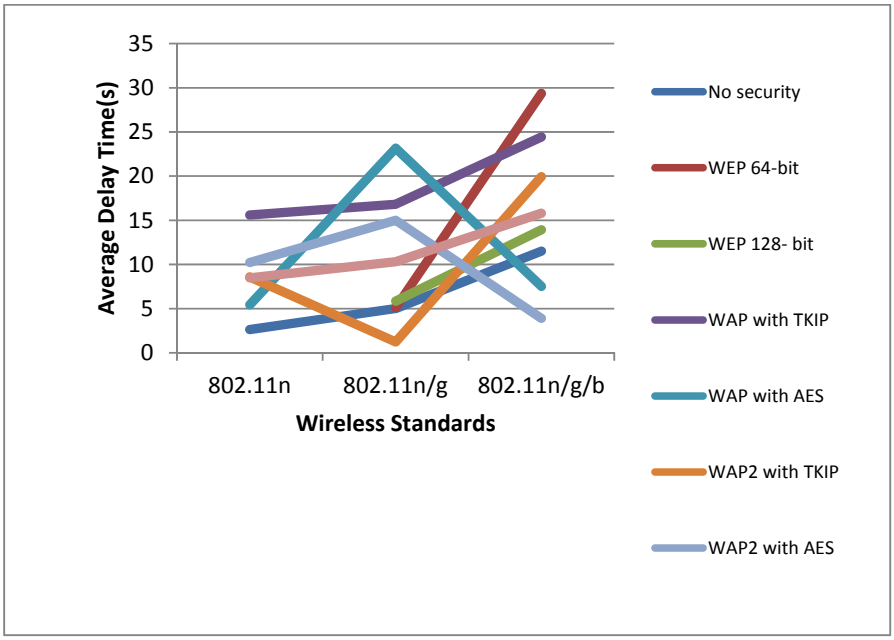

Figure 3: Average delay times (s) of IEEE 802.11 standards with wireless security protocols.

c) Response time analysis

From the experiment result shown that, the lowest average response time was yield in a wireless network configured with WEP 128-bit authentication and the highest average response time was obtained when WAP2 security with TKIP encryption implemented in a wireless network (Table 3).

Table 3: shows the average response time(s) of 802.11 standards with wireless security protocols

IEEE 802.11 Standards	No security	WEP 6-bit	WEP 128 bit	WPA with TKIP	WPA with AES	WPA2 with TKIP	WPA2 with AES
802.11n	3.5	N/A	N/A	14.43	1.0	20.1	7.44
802.11n/g	2.4	3.0	1.0	13.53	17.07	1.0	7.13
802.11n/g/b	6.38	7.8	1.0	4.95	14.25	14.49	11.91
Average	4.09	5.4	1.0	10.97	10.77	11.86	8.83

Experimental result showed that, lowest average response time was yield in a wireless network configured with IEEE 802.11n/g and highest average response time was obtained in a wireless network configured with IEEE 802.11n standard (Figure 4).

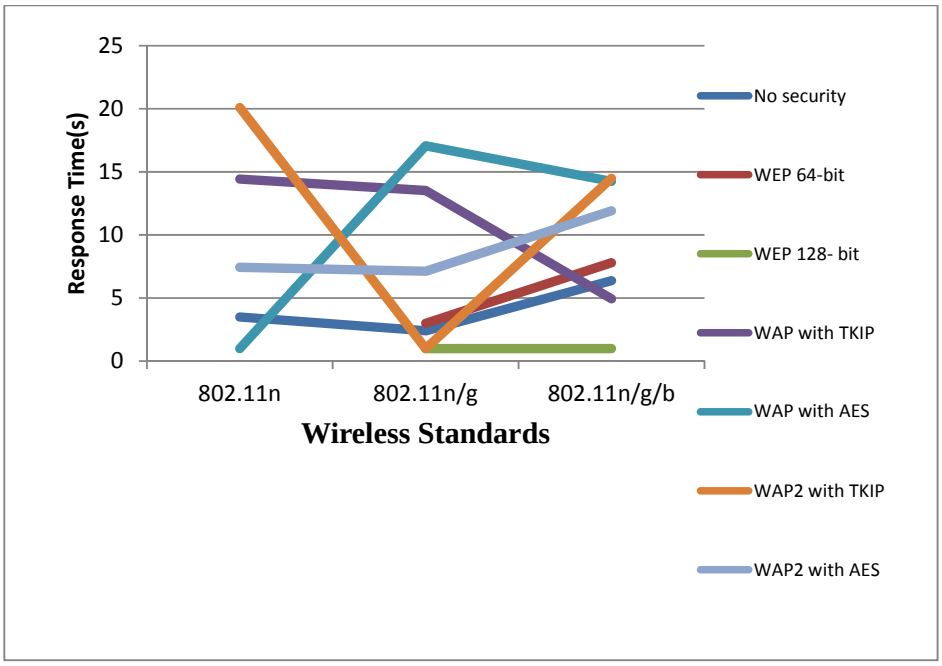

Figure 4: Average response times (s) of IEEE 802.11 standards with wireless Security protocols

d) TCP Error analysis

It is observed that, average TCP error rate is high in a wireless network configured without security and from networks configured with security protocols, the average error rate was found high in a network configured with WPA2 and TKIP encryption and lower in WPA with AES encryption (Table 4).

Table 4: shows the average error rate (pkts/sec) of 802.11 standards configured with wireless security protocols

IEEE 802.11 Standards	No security	WEP 6-bit	WEP 128-bit	WPA with TKIP	WPA with AES	WPA2 with TKIP	WPA2 with AES
802.11n	26.06	N/A	N/A	14.35	1.29	15.41	10.07
802.11n/g	12.83	17.89	3.08	9.53	16.02	6.8	6.18
802.11n/g/b	29.71	19.6	7.17	5.52	10.0	44.45	17.27
Average	22.87	18.75	5.13	9.8	9.1	22.22	11.84

Lowest average error rate (10.33pkts/sec) was yield in a wireless network configured with IEEE 802.11n/g standard and the highest error rate (19.10pkts/sec) was obtained in wireless network configured with IEEE 802.11n/g/b standard (Figure 5).

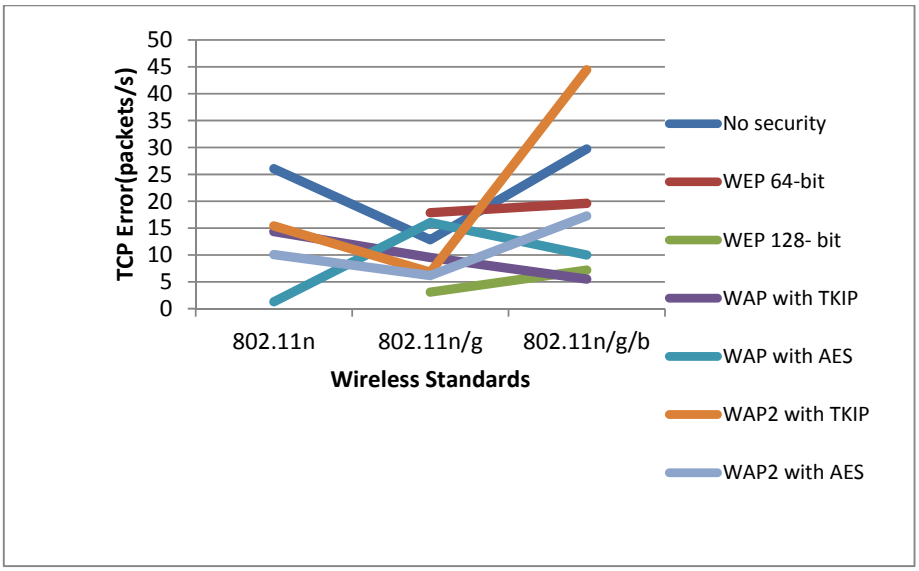

Figure 5: Average TCP errors (pkts/sec) of IEEE 802.11 standards with wireless Security protocols.

The experimental result showed that, a network configured with a security decrease throughput by 41.72%, delay increased by 49.23%, response time increased by 49.75% and error rate decreased by 49.75% (Table 5). This shows that performance significantly decrease in a network configured with security.

Table 5: Shows summary result of secured and unsecured network performance

	Average Secured	Unsecured	Difference %
Throughput (KB/s)	796.6	1366.77	41.72
Delay (s)	12.96	6.38	49.23
Response Time (s)	8.14	4.09	49.75
Error Rate (pkts/sec)	12.81	22.87	43.99

As it is shown in Table 6, from secured wireless network, WAP2 with AES encryption yields good throughput (1241.28KB/s), delay (9.1s) and response time (8.83).

Table 6: shows summary performance of security protocols

	No security	WEP 64-bit	WEP 128- bit	WPA with TKIP	WPA with AES	WPA2 with TKIP	WPA2 with AES
Average throughput (KB/s)	1366.77	257.14	696.74	899.27	749.82	935.35	1241.28
Average delay (s)	6.38	17.25	9.88	18.95	12.04	9.92	9.71
Response time (s)	4.09	5.4	1	10.97	10.77	11.86	8.83
Error rate (pkts/sec)	22.87	18.75	5.13	9.8	9.1	22.22	11.84

Table 7: Shows summary result of wireless standards performance

	802.11n	802.11n/g	802.11n/g/b
Throughput (KB/s)	881.91	901.92	900.81
Delay (s)	8.49	10.31	15.8
Response Time (s)	9.29	6.45	8.68
Error Rate (pkts/sec)	13.44	10.33	19.1

e) Wireless Attack analysis

To exploit wireless attack, vulnerabilities of a network and applications were analyzed using netsparker, wireshark and netsh command. Using the vulnerability of wireless network found attacker was connected with "ciscolab" network. The, by using netsparker the vulnerability of FTP server is identified and the attacker started sniffing FTP password using Wireshark. The result demonstrated that, wireless network performance significantly decrease by wireless attack. It is observed that in attacked wireless network environment, average throughput decrease by 39.12%, average delay time increased 19.56% and error rate increased by 17.49% (Table 8).

Table 8: shows impact of wireless attack on network performance

Performance Metrics	Before Attack	After Attack	Difference (%)
Average Throughput (Kb/s)	359.52	219.13	39.12%
Average Delay(s)	6.52	10.79	39.56%
Average Error Rate(Packet/s)	588.81	713.62	17.49%

The graph bellow showed that, throughput of wireless network significantly decreased due to attack exploited on the wireless network. When the number of requests for FTP service is increased the throughput of the network significantly decreases (Figure 6).

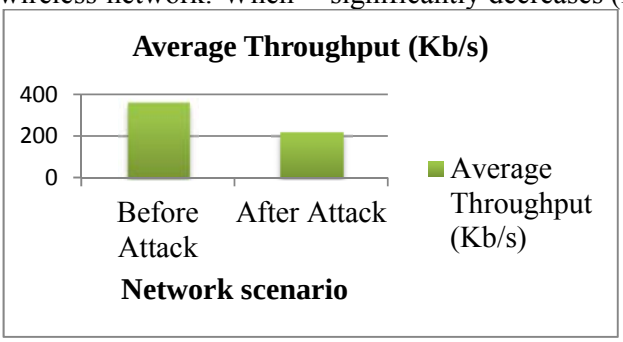

Figure 6: Shows average throughput of wireless network before and after attack

Wireless network also results communication delay in wireless network. The experimental result showed that communication delay was significantly increase after the network is congested due to attack exploited (Figure 7).

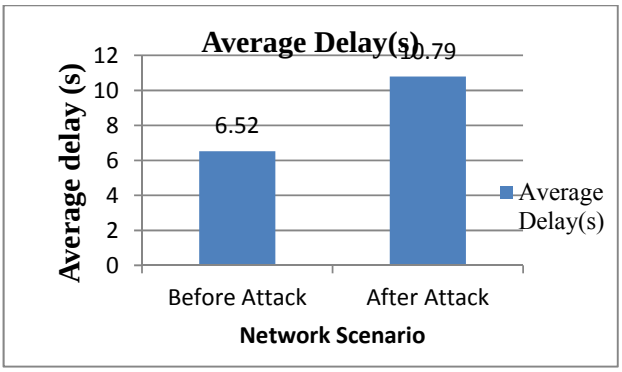

Figure 7 : Shows the average delay of wireless network before and after attack

In a congested network error rate increases significantly. The experimental result on wireless attack showed that error rate of wireless network is increased significantly after the network is congested because of the denial of service attack is exploited (Figure 8).

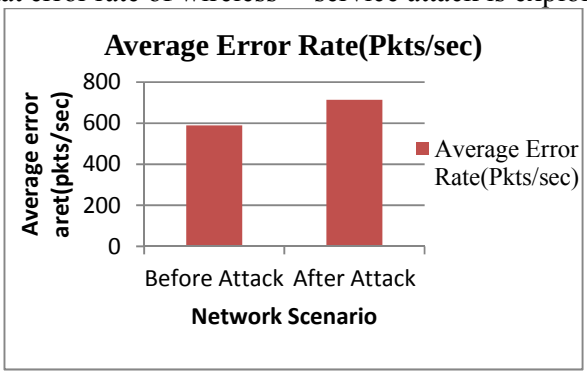

Figure 8: Shows the average error rate of wireless network before and after attack

4. Conclusions

A different combination of WLAN security protocol, wireless standard, wireless attack, threats and vulnerabilities were analyzed and the experimental result showed that the secured network's average throughput was decreased (41.72%), delay time increased (49.23%), response time increased (49.75%) and error rate decreased (34.99%) from un secured network. It was also noticed that from secured network environment, a network configured with WPA2 security and AES encryption yields good average throughput (1241.28KB/s), delay time (9.71s) and response time (8.83s).

The analysis result indicates that, WPA2 with AES encryption yields highest throughput (1351.96KB/s) when configured with IEEE 802.11n standard and low (1034.24KB/s) when configured with IEEE 802.11n/g, but yields good delay, response time and error rate with this standard. On the other hand, the result showed that WPA with AES encryption decrease throughput (749.82KB/s) significantly. It yields the least throughput (7.18KB/s) when configured with 802.11n standard and high (1274.69KB/s) when configured with 802.11n/g/b.

The study showed that IEEE 802.11n/g yields better average throughput (901.92Kb/s), delay (10.31s), response time (6.45s) and error rate (10.33pkts/sec).This standard yields high throughput (1039.24KB/s) and low error rate (6.18s) when configured with WPA2 and AES encryption and low delay (1.23s) and low response time (1s) when configured with WPA2 and TKIP encryption.

From the above statistics, it is possible to conclude that WPA2 security with AES encryption yields good performance in a secured wireless network and 802.11n/g obtained the best standard to boost performance in Wireless network. Configuring WPA2 with AES encryption over 802.11n/g standard found to result better performance on wireless network. The study reveals that the wireless network and services assessed were vulnerable and wireless attacks significantly decrease network throughput by 39.12%, increase delay time 39.56% and increase error rate by 17.49%. Therefore, this research showed that, configuring wireless LAN with right combination of security

and communication protocols with appropriate standards yields a good performance and high security.

5. Recommendations

Based on the research findings, the following possible points recommended

- Wireless network should be configured with compatible security protocols and encryption techniques over best standards.
- System and network administration experts should understand the nature of each security protocols, encryption techniques and standards before implementing them in wireless network configuration.
- Experts should change default configuration on the devices before giving service
- To make wireless network more secure, experts should assess threats and vulnerabilities through penetration tests.

6. Future work

- Future work is opened to analyze the impact of security protocols and standards on performance with infrastructure less wireless LAN such as Ad hoc or wireless sensor networks.
- Since, the WATM standards are developed to implement multimedia streaming data and mobile computing is emerged currently, impacts on WATM is also could be performed.

REFERENCES

[1] Y. Zahur and T. A. Yang, "Wireless LAN Security and Laboratory Designs," Journal of Computing Sciences in Colleges,2004, pp.44–60.

[2] M. Ahmad, S. Taj, T. Mustafa and M. Asri, "Performance analysis of wireless network with the impact of security mechanisms," International Conference on Emerging Technologies, Islamabad, 2012, pp.1-6.

[3] U. Singh and P. Jindal, "Performance Analysis of Secure Wireless Local Area Network Using Test-Bed," Fourth International Conference on Advanced Computing and Communication Technologies, Rohtak, 2014, pp.386-389.

[4] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking, 2001.

[5] D. B. Faria and D. R. Cheriton, "DoS and Authentication in Wireless Public Access Networks," 2001, pp.7–56.

[6] S. Satheeskumaran, and M. Sabrigiriraj. "A new LMS based noise removal and DWT based R-peak detection in ECG signal for biotelemetry applications." National Academy Science Letters 37, no. 4 (2014): 341-349..

[7] Wong, J., "Performance Investigation of Secure 802.11 Wireless LANs: Raising the Security Bar to Which Level," University of Canterbury, Christchurch, NZ, 2002.

[8] Stamatios and V. Kartalopoulos, "Differentiating Data security and Network Security," IEEE International Conference on Communications, Beijing, 2008.

[9] T. Karygiannis and L. Owens, "Wireless Network Security 802.11, Bluetooth and Handheld Devices" National Institute of Technology, Special Publication, pp.800–848, 2002

[10] Yeu-Pong Lai and Po-Lun Hsia, "Using the vulnerability information of computer systems to improve the network security," Journal of Computer Communications, vol.30, Issue 9, 2007, pp.2032-2047.

[11] A. Alruban and E. Everitt, "Two Novel 802.1x Denial of Service Attacks," European Intelligence and Security Informatics Conference, Athens, 2011, pp.183-190.

[12] S. D. Kanawat and P. S. Parihar, "Attacks in Wireless Networks," International Journal of Smart Sensors and Adhoc Networks, 2011.

[13] F. Zdarsky, S. Robitzsch and A. Banchs, "Security analyses of wireless mesh backhauls for mobile networks," Journal of Network and Computer Applications, vol. 34, Issue 2, 2011, pp.432–442.

[14] Umesh Kumar and Sapna Gambhir, "A Literature Review of Security Threats to Wireless Networks," International Journal of Future Generation Communication and Networking, vol.7, Issue 4, 2014.

[15] IEEE Std 802.11, "Revision of IEEE Std 802.11-1999," 2007.