International Journal of Future Generation Communication and Networking
Vol. 9, No. 1 (2016), pp. 71-78
http://dx.doi.org/10.14257/ijfgcn.2016.9.1.07

Performance Analysis of Wireless Network Throughput and Security Protocol Integration

Paschal A. Ochang[1]* and Phil Irving[2]

[1]*Department of Computer Science, Federal University Lafia, Nasarawa State, Nigeria*
[2]*Department of Computing, Engineering and Technology, University of Sunderland, Sunderland, United Kingdom*
[1]*paschal.ochang@fulafia.edu.ng*, [2]*phil.irving@sunderland.ac.uk*

Abstract

Wireless network security protocols are essential for enhancing security, privacy and confidentiality. However, network security protocols also require network resources in other to carry out authentication of users through the use of encryption keys and packet encryption. It is therefore relevant to investigate the effects of the amount of resources used by recommended wireless network security protocols in other to determine if user quality of experience and user quality of service is affected by the implementation wireless network security protocols. Our research investigates and examines the effect of security protocols on wireless network performance. The Wi-Fi Protected Access 2 - Pre-Shared Key (WPA2-PSK) was used as the security protocol in focus while throughput was the network performance feature that was analyzed. Experiments were carried out which showed that throughput in a non-secured Wireless Local Area Network (WLAN) is a bit higher than throughput in a secured WLAN. Our research contributes to the future development of WLAN protocols with low network resource consumption in other to contribute to improved network performance.

Keywords*: WLAN, Throughput, encryption, TCP, WPA2-PSK, Wireless Security*

1. Introduction

Wireless networks have continued to advance in the world of networking due to the seamless benefits they offer to users. This has led to the deployment of wireless networks in campuses, airports, offices and other public areas (Hayajneh et al., 2012). These advantages offered by wireless networks are due to the fact that users can be mobile while assessing information that is fixed. Wireless networks use the air as a medium of transmission unlike wired networks that use wires as the medium of transmission, therefore this means that the medium of transportation is accessible to everybody (Choi, 2012) which points to the fact that security becomes an essential feature in wireless networks. Wireless networks are open to many attacks or threats such as eavesdropping, spoofing and denial (Isaac and Mohammed, 2007). The need for enhanced security in wireless networks has led to the development of diverse security protocols such as Wi-Fi Protected Access (WPA) and Wired Equivalent Protocol (WEP), which has led to increase in confidentiality, integrity and authenticity (Zdarsky et al., 2011). Although security protocols provide the following services listed previously, the network performance can be affected by the deployment of such protocols.

Much emphasis has been laid on the need to implement security on wireless networks, but low emphasis has been placed on the effect of the security protocols on the performance of wireless network. (Tasoluk and Tanrikulu, 2011) showed that security protocols use encryption keys to secure information which might take a long time for a

ISSN: 2233-7857 IJFGCN

hacker to crack. These keys are usually used for authentication and cryptography when a client is trying to connect to a wireless network, and it involves exchanging of keys between an access point and the client. The action of cryptography entails that security and authentication keys have to be set up at all end points (Rachna and Patel, 2011) which involves a client or node trying to connect to the network acting as one point and the network node in charge of security acting as another point. Previous research has shown that for every encryption a decryption must be carried out, this is also supported by Pitchaiah et al (2012) who demonstrated the complex methods of encryption and decryption adopted by the Advanced Encryption Standard (AES) Algorithm, therefore encryption and decryption can be said to be processor intensive which is supported by Si et al. (2012) who showed that deploying a security protocol that uses Symmetric Key Cryptography on a wireless sensor Network (WSN) link can affect the energy consumed by a node and a particular number of CPU cycles are required to carry out encryption. The action carried out by the authentication and cryptographic procedures of these protocols tend to utilize network and system resources such as bandwidth, processing power, and memory. Furthermore, hand held and mobile devices may also experience a drain in battery performance (Agarwal and Wang, 2005).

Considering the fact that the security protocols utilize network resources, legitimate traffic may encounter low quality of service (QoS), therefore this can be reflected in a hypothesis H1 which can be stated as follows:

H1: There is a significant effect on the throughput performance of wireless networks due to the implementation of security protocols.

While the null hypothesis H0 can be stated as follows:

H0: There is no significant effect on the throughput performance of a wireless network due to the implementation of security protocols.

Various factors determine good quality of service; these factors include delay, throughput, latency and bandwidth. Muogilim et al. (2011) implemented a method of securing network traffic using a virtual private network (VPN) and internet protocol security (IPSec), although the results showed that the method enhances security, it also showed that the throughput of the network was affected, although it offered a better security.

The main objective of this paper is to analyze if the introduction of a security protocol on a network affects the performance of a network in a negative manner resulting in low quality of service. In other to address the research question stated above, an experimental analysis is carried out to test for H1. The experimental analysis involves applying a well-known security protocol called The Wi-Fi Protected Access 2 - Pre-Shared Key (WPA2-PSK) over a Wireless Local Area Network (WLAN) while analyzing the performance of the network in terms of throughput, while the second scenario also involves carrying out an analysis on a WLAN without the implementation of any security protocol while also analyzing performance in terms of network throughput. Therefore in other to carry out the experimental analysis, an experimental test bed is set up which consist of a miniature wireless network .The results from the experimental analysis will serve as a baseline for comparison in other to determine H1.

The rest of this paper is arranged as follows: Section 2 discusses basic WLAN security protocols and gives a summarized overview of WPA2-PSK which will be the security protocol used for analysis, section 3 discusses factors that determine network performance and a summary overview is given on throughput, which will be the network performance feature that will be used for analysis. Section 4 discusses the experimental setup and conducted experiments. Section 5 analyses the experiment results while section 6 gives a reflective summary and conclusion of the paper.

2. WLAN Security Protocols

Many protocols have been developed to tackle WLAN security and some of these include the Wired Equivalent Protocol (WEP), Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) (Barka and Boulmalf, 2007). However, WPA2-PSK will be used for the experimental analysis.

2.1. Wi-Fi Protected Access 2 - Pre-Shared Key

WPA2-PSK which is also referred to as WPA2 Personal is a security protocol designed for the IEEE 802.11i standard. It allows the use of a plain-English passphrase of 8 to 63 characters rather than using an encryption key. Through the use of Temporary Key Integrity Protocol (TKIP) the passphrase is combined with the Service Set Identifier (SSID) of the network to generate a new key per packet, therefore through this method a unique encryption key is generated for each wireless client and these encryption keys are constantly changed. Therefore WPA2-PSK is used because it offers better security features and is highly recommended.

3. Network Performance

The performance of a network is determined by certain factors such as delay, throughput, latency and overhead. For our experimental analysis the network performance feature that will be used in the experimental set up will be the throughput of the network. Throughput can be classified as the volume or amount of data or traffic that can flow through a network at a given time (Muogilim et al., 2011). Throughput can be used to measure network efficiency and performance in the sense that a low throughput offers low network performance and vice versa.

4. Experimental Testbed Setup

This section involves the implementation of experimental test scenarios for the purpose of testing for H1 and H0. Two tests scenarios are actually adopted; the first involves measuring the throughput of a network over 4 nodes with a security protocol enabled, while the second test scenario involves measuring the throughput of a network over 4 nodes without a security protocol enabled.

The bandwidth of the access points is set at 10Mbps in other to provide enough bandwidth for the traffic, while the data or packet size to be sent was set at 1400 bytes. The wireless network standard used was 802.11n and this was set to be uniform on all the access points in other to achieve the same network performance on all the access points.

4.1. Security Test Scenario

In the first test scenario, all the access points are networked together using the Cat5e cables, the first laptop which is labeled as L1 is connected to the first access point which is labeled as A1 via a wireless connection and WPA2-PSK security protocol is also enabled on A1. The distance between L1 and A1 is set at 6 metres in other to ensure high signal strength while limiting the influence of external factors on the experiment such as low signal strength and signal fading as these might also affect throughput. The second laptop which is labeled as L2 is also connected to AP1 via a wireless connection using the same distance of 6 metres. In other to generate network traffic, LanTraffic which is a software capable of generating network traffic was used to generate TCP traffic from L1 through A1 to L2. The Wireshark network protocol analyzer which is a network analyzer software is used to analyze the TCP traffic and measure throughput. After throughput is determined, L2 is then disconnected from A1 and connected to the second access point A2 and WPA2-PSK security protocol is also enabled on A2. TCP Traffic is generated

from L1 which flows through A1 and A2 to L1 and throughput is also measured. The same process carried out above is also repeated through AP3 and AP4 and network throughput levels are measured respectively.

4.2. No Security Test Scenario

In this test scenario the same process carried out in the security test scenario is also applied, but in this case WPA2-PSK security protocol is not applied on any of the access points. The network is not secured in any manner and TCP traffic is generated from L1 to L2 while measuring the throughput and L2 is disconnected and connected to the next access point respectively until the throughput is determined for all respective access point connections.

5. Experimental Result and Analysis

In this section the experimental results are presented and analyzed. Experimental data are presented when a security protocol is applied to a network and when no security protocol is applied.

Table 1. Average Throughput of TCP Traffic When WPA2-PSK is Applied to the Wireless Network

	Over 1 WPA2-PSK Secured access point	Over 2 WPA2-PSK Secured access point	Over 3 WPA2-PSK Secured access point	Over 4 WPA2-PSK Secured access point
Average throughput of TCP Traffic	1188Kbps	1010Kbps	966Kbps	910Kbps

Table 2. Average Throughput of TCP Traffic When No Security Protocol is Applied to the Wireless Network

	Over 1 non Secured access point	Over 2 non Secured access point	Over 3 non Secured access point	Over 4 non Secured access point
Average throughput of TCP Traffic	1228Kbps	1039Kbps	998Kbps	930Kbps

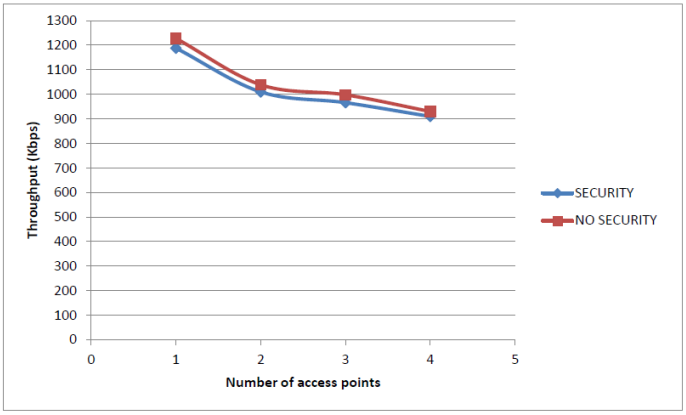

Figure 1. Throughput Achieved Over Number of Access Points with Security and No Security

Table 1 shows the throughput when WPA2-PSK security is applied to the network and Table 2 shows the throughput when no security is applied, while Figure 1. shows a graph of both throughput levels against the number access points in which the TCP traffic was passed through. They is a considerable degradation in the throughput attained in both test scenarios, which is as a result of increase in delay, latency, interference and increase in traffic delivery distance.

5.1. Throughput 1

As It can be seen that when traffic is sent from L1 to L2 over one access point (A1) that has WPA2-PSK security activated, the throughput attained is 1188Kbps while when the same amount of traffic is sent through the access point without security activated a throughput of 1228Kbps is attained that means throughput improved by 40Kbps (1228Kbps-1188Kbps) without security.

5.2. Throughput 2

When traffic is sent from L1 to L2 over two access points(A2) with security activated, the throughput is reduced from 1188Kbps to 1010Kbps, while when the same amount of TCP traffic is sent from L1 to L2 through two access points without security activated the throughput attained was 1039Kbps which is lower than the first throughput attained when the traffic is passed over only one access point without security which is 1228Kbps, but it is greater than the throughput attained when TCP traffic is passed over two access points with security enabled by 20Kbps (1039Kbps-1010Kbps).

5.3. Throughput 3

When L2 is connected to the third access point (A3) in a WPA2-PSK secured scenario the throughput attained is 966Kbps while when it is connected to A3 in a non-secured mode throughput is 998Kbps, therefore throughput improved by 32Kbps

5.4. Throughput 4

The throughput achieved on connecting L2 to the fourth access point A4 and activating WPA2-PSK security is 910Kbps, while without activating security the throughput is 930Kbps which shows a 20Kbps improvement in throughput.

5.5. Statistical Analysis

A paired or dependent T-test is also used to analyze the throughput in other to determine the significance of the test, also to determine if the mean of the throughput value when WPA2-PSK security is applied to a wireless network is statistically different from the mean of the throughput value when no security is applied to a wireless network.

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	SECURED	1018.50	4	120.182	60.091
	NONSECURED	1048.75	4	127.675	63.838

Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	SECURED & NONSECURED	4	1.000	.000

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	of the Difference Lower	of the Difference Upper			
Pair 1	SECURED - NONSECURED	-30.250	8.261	4.131	-43.396	-17.104	-7.323	3	.005

Figure 2. Statistical Analysis Result

From the T-Test in Figure 2, it can be seen that the p value is less than 0.5; this means that there is a statistically significant difference between the mean throughputs of when security is applied on a wireless network and when no security is applied, therefore H1 which is the alternative hypothesis is selected.

6. Conclusion

In other to develop more advanced methods of providing wireless network security it is therefore important to analyze the effects of current protocols on network performance which will enable the development of enhanced versions of wireless network protocols. In this paper an experimental procedure was implemented to actually determine if wireless network performance is affected by the implementation of security protocols and if the effect was significant. WPA2-PSK security protocol was used while throughput was the basis for performance. It was realized that throughput in a secured scenario was lower than in an unsecured scenario, it was also noticed that over more access point's throughput in both scenarios depreciated but the throughputs in the secured scenario were lower than that of the non-secured scenario, this is because of the behavior of the WPA2-PSK security protocol which adds encryption keys to the packets containing the traffic being sent thereby increasing the packet sizes. However, our research did not take into account proper analysis of the encryption headers in an encrypted packet which might be a cause of reasonable overhead. Although the performance of a network is affected by the implementation of security, this does not eliminate the need for the introduction of security in a wireless network in other to ensure confidentiality, privacy and integrity, but it calls for the development of security protocols with efficient use of network resources.

References

[1] A. Agarwal and W. Wang, "Measuring performance impact of security protocols in wireless local area networks", In 2nd International Conference on Broadband Networks, IEEE, **(2005)**, pp. 625–634, Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1589663.

[2] E. Barka and M. Boulmalf, "On the Impact of Security on the Performance of WLANs", Journal of Communications., vol. 2, no. 4, **(2007)**, pp.10–17.

[3] M. Choi, R. Robles, C. Hong and T. Kim "Wireless Network Security: Vulnerabilities, Threats and Countermeasures", International Journal of Multimedia and Ubiquitous Engineering., vol. 3, no. 3, **(2008)**, pp.77–86.

[4] T. Hayajneh, S. Khasawneh, B. Jamil and A. Itradat, "Analyzing the Impact of Security Protocols on Wireless LAN with Multimedia Applications", In SECUREWARE 2012, The Sixth International Conference on Emerging Security Information Systems and Technologies, **(2012)**, pp. 169–175.

[5] B. Issac and L. Mohammed, "War Driving and WLAN Security Issues—Attacks, Security Design and Remedies", Information Systems Management, vol. 24, no. 4, **(2007)**, pp. 289–298. Available at: http://www.tandfonline.com/doi/abs/10.1080/10580530701585831.

[6] O. Muogilim, K. Loo, and R. Comley, "Wireless mesh network security: A traffic engineering management approach", Journal of Network and Computer Applications., vol. 34, no. 2, **(2011)**, pp. 478–491. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1084804510000627.

[7] M. Pitchaiah, P. Daniel and Praveen, "Implementation of Advanced Encryption Standard Algorithm", International Journal of Scientific & Engineering Research, vol. 3, no. 3, **(2012)**, pp. 1–6. Available at: www.ijser.org/researchpaper%5CImplementation-of-Advanced-Encryption- Standard-Algorithm.pdf.

[8] H. Rachna and M. Patel, "Encryption And Key Management Approach With In-Network Processing In Wireless Sensor Network And Security Analysis", World Journal Of Science & Technology., vol. 1, no. 12, **(2011)**, pp. 46–49.

[9] L. Si, Z. Ji and Z. Wang, "The Application of Symmetric Key Cryptographic Algorithms in Wireless Sensor Networks", Physics Procedia, vol. 25, **(2012)**, pp. 552–559. Available at: http://www.sciencedirect.com/science/article/pii/S187538921200541X.

[10] B. Tasoluk and Z. Tanrikulu, "A Weakest Chain Approach To Assessing The Overall Effectiveness Of The 802.11 Wireless Network Security", International Journal of Wireless & Mobile Networks (IJWMN), vol. 3, no. 1, **(2011)**, pp. 1–8.

[11] F. Zdarsky, S. Robitzsch and A. Banchs, "Security analysis of wireless mesh backhauls for mobile networks", Journal of Network and Computer Applications., vol. 34, no. 2, **(2011)**, pp. 432–442. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1084804510000640.

