Research Journal of Applied Sciences, Engineering and Technology 3(9): 910-913, 2011
ISSN: 2040-7467

Submitted: June 22, 2011 Accepted: August 27, 2011 Published: September 20, 2011

# A Formal Evaluation of the Security Schemes for Wireless Networks

Shadi R. Masadeh and Nidal Turab
Faculty of Information Technology Applied Sciences University,
Isra University Amman, Jordan

**Abstract:** Information security is a critical issue in the wireless network, because the transmission media is open (no physical control on the air). Any wireless device equipped with wireless interface can use and share the airwave transmission medium with other users. For protection purposes, several security mechanisms have been developed over years. This paper provides systematic evaluation of different security schemes used in wireless networks: WEP, TKIP, WPA, AES and WPA2. A formal comparison is made between these security algorithms for different settings such as different data types, different packet sizes and traffic loads.

**Key words:** Advanced encryption standard (AES), temporal key integrity protocol (TKIP), Wi-Fi protected access (WPA), Wi-Fi protected access 2 (WPA2), wired equivalent privacy (WEP)

## INTRODUCTION

This study presents an evaluation of the most important security protocols used in WLANs. We identify their strength and weaknesses from the security point of view and the impact of these security protocols on network performance.

Wireless local area networks have important role for users and organizations. The wide spread for using wireless networks makes the need for protection of transferred data because the transmission media is open (no physical control on the air). For protection purposes, multiple security techniques have been developed over years, these security protocols differ in the degree of security they provide. In addition to the fact that they are not completely secure, they influence substantially on the performance of the network. Any security protocol or approach used in WLAN should provide the following characteristics (Anrech, 2002): Confidentiality, authentication and integrity.

Wired Equivalent Privacy (WEP) (Nedier Janvier Senat, 2003) was designed to make the wireless networks as secure as the wired networks. WEP uses RC4 symmetric encryption algorithm with 40 bit or 104 bit key, CRC-32 data integrity, shared key authentication and no anti reply protection. Some of the WEP security problems are:

Weak encryption, offline dictionary attacks, message deletion, Man in the Middle attack (MITM), Denial-of-Service attacks (DoS). The WiFi Protected Access (WPA) (Wong Stanley, 2003) was implemented by the WiFi alliance. WPA adopts The Temporal Key Integrity Protocol (TKIP) for encryption and includes packet integrity (a.k.a Michael), preshared key or IEEE 802.1x for authentication and packet number is used for reply protection. WPA suffers also from security problems (when using preshared key) like: Off line dictionary attacks, Message Deletion, Man in the Middle attack (MITM), Denial-of-Service attacks (DoS).

AES (Daemen, 2001) has a particular encryption key used for both cryptography and authentication. AES block size consists of 128-bits and this means that there are 1048576 bytes per packet. It is much more than the required maximum packet length for WLAN (the maximum packet length of WLAN is 2312 bytes).

IEEE 802.11i (A.K.A WPA2) (Changhua, 2006): 802.11i overcomes most of the security problems of the WLAN. For encryption IEEE 802.11i uses TKIP (to support legacy wireless devices) and AES-CCMP (which requires extra hardware), for authentication WPA2 uses 802.1x/EAP for authentication and Michael Message Integrity Check for Message Integrity. WPA2 may suffer from MITM attack.

This study evaluates the performance of different encryption algorithms used in wireless networks. The evaluation will be conducted in terms of different data types (audio, video and text), different packet sized and different traffic loads (light, medium and heavy).

## LITERATURE REVIEW

Many researches had studied the performance of WLAN. Nedier Janvier Senat (2003) studied the performance of the TCP, UDP for IEEE 802.11b when using WEP and WPA security protocols. Also they studied the performance of IEEE 802.11b WLAN for FTP and HTTP protocols under WEP and WPA security protocols was evaluated in [Site mirror software was used to simulate the WEB site in the experiments. Muhammad *et al*. (2009) investigated the performance of 802.11b

**Corresponding Author:** Shadi R. Masadeh, Faculty of Information Technology Applied Sciences University, Isra University Amman, Jordan

WLANs using a saturated environment for different data rates and packet sizes in an error free environment. Diana *et al*. (2009) studied the performance of selected symmetric encryption algorithms; such as AES, DES, 3DES, RC6, Blowfish and RC2. They concluded that Blowfish has better performance than other encryption algorithms used.

Fernando *et al*. (2005) showed that the effect of the encryption algorithm do not have a significant effect on the total energy consumed by the protocol but the authentication methods , such as EAP, have a significant impact on energy consumption. Shaneel *et al*. (2009) studied the performance of wireless IEEE802.11n using four operating systems; the performance is tested for both TCP and UDP protocols. Wireless security encryption methods (WEP-64, WEP-128, WPA and WPA2) were used; that study shows that performance is depending in the operating system

## EXPERIMENTAL DESIGNS

This study aims to identify the relationship between performance and security for WLANs using different encryption protocols WEP, TKIP, WPA, AES and WPA2. This part of our paper is composed of two stages:

- First stage, was carrying to study the impact of the most commonly used traffic messages (TCP and HTTP) on the performance of the WLAN,
- Second stage is to carry out analysis of the different experiments:
- Analyze the effect of the security mechanisms on the performance of the WLAN
- Analyze the impact of fixed packets length on the performance of the WLAN.

**WLAN implementation:** The following four security mechanisms combinations were selected to show the most important security mechanisms available for WLAN.

- WEP 128-bit: 128-bit encryption and authentication is used
- WPA (using TKIP for encryption)
- WPA Shared Key authentication with key management while AES protocol is used for encryption. This combination of the WPA-PSK for authentication and key management and the strongest encryption algorithms AES, provides simplicity of implementation and configuration while offering an acceptable level of security
- WPA2 (using AES): digital certificates are used for authentication and AES is used for encryption

**Experimental results and analysis:** The aim was to investigate some factors that influence network throughput; we studied the effect of the following factors: network bandwidth, traffic type and packet length on the network throughput under various WLAN security protocols.

- The measured performance obtained from four repetitive tests for each security mechanisms was evaluated. The experiments were divided into thre :
- The first experiment investigated the network efficiency under various different security protocols on network performance for TCP protocol
- The second experiment aimed to study the network performance under the security protocols mentioned in the previous section for HTTP protocol.
- The influence security protocols on the network performance using variable packet size for TCP protocol was studied in the third set of experiments, the number of packets used is 80000 packets.

For the first and second sets of experiments, two bandwidths were used to send data to from the wireless client to the access point: 11 MB/Sec, to represent a normal traffic; 60 MB/Sec, the IEEE 802.11g standard maximum speed is 54 MB/Sec so that 60 MB/Sec represents a congested traffic. Congested wireless network means that the wireless clients sends much more data than the bandwidth between it and the access point can handle.

- We used the following hardware components within the network architecture
- Wireless client: Laptop Intel Dual core 3GHz with 4GB RAM; OS Windows VISTA

Wireless AP and client adapter software necessary for wireless communications to the access point; that

Table 1: Network performance (in MB/Sec) for TCP

| | Traffic type and performance percentage loss | | | |
|---|---|---|---|---|
| | Band 11 MB/Sec | | Bandwidth 60 MB/Sec | |
| Security mechanism | TCP | Loss-TCP% | TCP | Loss-TCP% |
| WEP 128 | 9.402 | 6.619893 | 14.59 | 4.686630369 |
| WEP/TKIP | 9.181 | 8.582593 | 14.49 | 5.291591047 |
| WPA/AES | 9.176 | 8.769980 | 14.86 | 5.053236540 |
| WPA2/AES | 8.114 | 17.05861 | 14.11 | 7.314555550 |

Table 2: Network performance (in MB/Sec) for HTTP

| | Traffic type and performance percentage loss | | | |
|---|---|---|---|---|
| | File size = 60 MB | | File size = 11 MB | |
| Security mechanism | HTTP | Loss-HTTP% | HTTP | Loss-HTTP% |
| WEP 128 | 21.0100 | 5.951871 | 17.958 | 17.564210 |
| WPA/TKIP | 21.1435 | 4.331085 | 17.780 | 19.506871 |
| WPA/AES | 21.4915 | 3.712857 | 17.780 | 19.506871 |
| WPA2/AES | 19.83375 | 10.42152 | 18.550 | 15.815604 |

Table 3: network performance and the performance percentage loss for different packet sizes using TCP

| | Security protocol | | | |
|---|---|---|---|---|
| Packet length | WEP 128 | WPA/TKIP | WPA/AES | WPA2/AES |
| 100 | 9.5142222 | 11.133783 | 8.9688032 | 9.2773260 |
| Loss 100% | 27.18593 | 13.145144 | 12.575437 | 27.239703 |
| 500 | 15.235248 | 12.311861 | 12.312058 | 12.185968 |
| Loss 100% | 3.6091434 | 1.9045393 | 2.0439463 | 2.4717696 |
| 1000 | 14.329081 | 14.259481 | 17.219938 | 14.899059 |
| Loss 100% | 2.1353535 | 2.3715727 | 2.8090016 | 3.5356911 |
| 1300 | 18.210782 | 18.168265 | 18.073107 | 19.901487 |
| Loss 100% | 1.4789696 | 1.4901054 | 1.7964110 | 2.4625298 |
| 1540 | 12.740245 | 14.650515 | 14.554718 | 13.488653 |
| Loss 100% | 9.1537510 | 2.5624431 | 2.8532630 | 2.9296756 |

provides mutual authentication to the access point and client via EAP authentication.

All the experim ents were conducted in a clean laboratory environment (there was no any radio interference from any device with wireless devices, no obstacles between AP and wireless clients and they were very close to each other to eliminate any delay factor).

**Network performance under various security protocols for TCP protocol:** The measured network performance as expressed in (MB/Sec) for TCP protocol under different security mechanisms is in Table 1. The table also shows the percentage performance lost for different security mechanisms with reference to no security case.

**Network performance under various security protocols for HTTP protocol:** A web page containing two files of sizes 11 MB for normal traffic and 60 MB for congested traffic was used. This web page was stored on the WEB server and then downloaded by the wireless client using HTTP protocol.

The measured network performance as expressed in (MB/Sec) for HTTP protocol under different security protocols is in Table 2. The table also shows the percentage performance lost for different security protocols with reference to no security case.

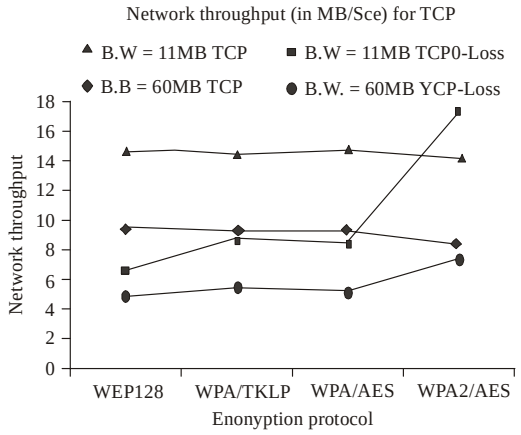


Fig. 1: Network throughputs for TCP protocol

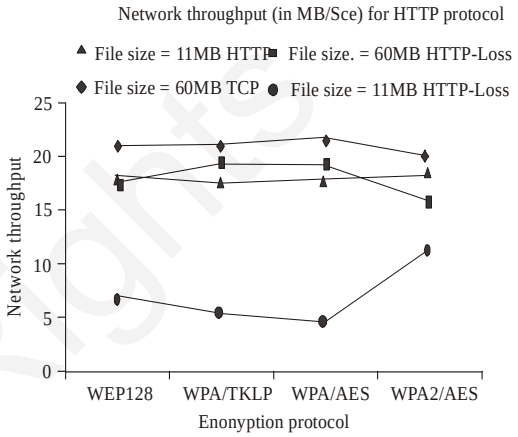


Fig. 2: Network performance (in MB/Sec) for HTTP protocol

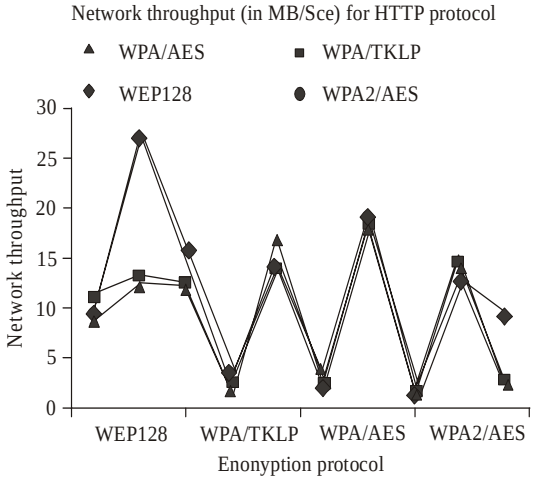


Fig. 3: Percentage performance loss for different packet lengths

**Network performance under various security protocols using various packet lengths:** TCP traffic with 54 MB/Sec and packet lengths of 100, 500, 1000, 1300

and 1540 bytes were chosen to simulate traffic consisting out of short, normal and long packets.

Network performance (in MB/Sec) for TCP protocol for congested network traffic with the percentage performance lost with reference to the no security are in Table 3 and the results are illustrated graphically in Fig. 3.

## DISCUSSION AND CONCLUSION

From Fig. 1, 2 it is clear that the network performance (throughput ) decreases as the security level increases for both congested and normal traffic, as expected, the reason is that different authentication, encryption create different levels of performance overload. WPA2/AES generates the longest delay and decreased throughput, because of mutual authentication and key management. A comparison between the delay caused by the authentication mechanisms in a descending order is WPA2/AES> WPA/AES> WPA/TKIP >WEP. Congested network traffic results in better performance than the normal network traffic as it utilizes all available bandwidth. The percentage performance lost of congested network for TCP protocol varies between 4.6 and 7.3%; the percentage performance lost of normal network traffic for TCP protocol varies between 6.6 and 17.05%. The same situation is applied for HTTP.

The following results obtained from our experiments:

- WEP gives best network performance at all key sizes WPA gives moderate network performance
- WPA2/AES gives the least network performance due to the extra required processing of the authentication, encryption, and creation of the security associations.
- WPA2/AES requires extra hardware and software implementations (e.g. AAA server and support of CCMP and AES).
- From Fig. 3 we can notice that packet size of 1300-byte gives the best network throughput for all security mechanism, the percentage performance lost for TCP packet of 1300 bytes long varies between 1.4 and 2.4%; which is the less than any percentage performance lost for other packet lengths.
- For a packet length of 1500 bytes the packets were fragmented (Fig. 3), because the configuration of the networking devices used in our experiments was set up to fragment packets of 1500 bytes and larger. The Maximum Transmission Unit (MTU) is the size of the largest packet which that network can transmit before fragmentation occurs, which yields to network performance decreases.

## ACKNOWLEDGMENT

The authors are grateful to the Applied Science Private University, Amman, Jordan, for the partial financial support granted to this research project (Grant No –DRJS-2011-20).

## REFERENCES

Anrech, M. and A.A. William, 2002. An Initial Security and Improvements for IEEE 802.11i. Retrieved from: http://www.isoc.org/isoc/conferences/ndss/05/proceedings/papers/NDSS05-1107.pdf.

Changhua, H. and C.M. John, 2006. Security Analysis and Improvement for IEEE 802.11x standard. Retrieved from: http://www.cs.umd.edu/~waa/1x.pdf.

Daemen, J. and V. Rijmen, 2001. Rijndael: The advanced encryption standard. Dobb's J., March, 26(3): 137-

Diana, S.A., Elminaam, H.M. Abdul Kader and M.M. Hadhoud, 2009. Energy efficiency of encryption schemes for wireless devices. Int. J. Comp. Theory Engine., 1(3): 1793-8201.

Fernando, C., C. Osorio and K. McKay, 2005. A Trade off Between Energy and Security in Wireless Networks. Proceedings of SDR05 Technical Conference and Product Exposition, IEEE802.11g, Retrieved from: http://standards.ieee.org/getieee802/download/802.11g-2003.pdf. IEEE802.11i, http://standards.ieee.org/getieee802/download/802.11i-2004 .pdf.

Muhammad, U.N., U. Nauman and K. Hussain, 2009. Performance analysis of wireless local area networks. Int. J. Comp. Theory Engine., 1(2).

Nedier Janvier Senat, 2003. IEEE 802.11 wireless LAN Security Performance using Multiple Clients. Retrieved from: http://www.cosc.canterbury.ac.nz/research/reports/HonsReps/hons-0304.pdf.

Shaneel, N., T. Feng, X. Xu and S. Ardham, 2009. Impact of wireless IEEE802.1 in encryption methods on network performance of operating systems. ICETET, Second International Conference on Emerging Trends in Engineering Technology, pp: 1178-1183.

Wong Stanley, 2003. 1 GSEC The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards. Practical v1.4b, SANS Institute, May 20.