Proceedings of 2015 3rd International Conference on Advances in Electrical Engineering
17-19 December, 2015, Dhaka, Bangladesh

# A comparative study of WLAN security protocols: WPA, WPA2

Abdillahi Hassan Adnan[1], Mohamed Abdirazak, A.B.M Shamsuzzaman Sadi, Towfique Anam, Sazid Zaman Khan, Mohammed Mahmudur Rahman
Department of Computer Science and Engineering
International Islamic University Chittagong
Chittagong, Bangladesh
[1]abdilaahi01@gmail.com

Mohamed Musse Omar
Department of Computer Science and Engineering
Independent University Bangladesh
Dhaka, Bangladesh
mgalde992@gmail.com

***Abstract*—in this paper, we have made a comparison between different WLAN security protocols, WPA and WPA2, and we correlated the two with respect to performance. We have emphasized on IEEE 802.11n amendment. We performed an experiment to measure the maximum throughput achieved by different encryption protocols. We concluded that WPA2 has less reduction on network throughput than WPA due to its encryption algorithm, CCMP, which is highly improved compared to TKIP, which is adopted by WPA.**

***Keywords—WLAN Security Protocols, WPA, WPA2, WiFi, IEEE 802.11, IEEE 802.11i, TKIP, CCMP.***

## I. INTRODUCTION

The 802.11i, an amendment ratified on June 24, 2004, specifies security mechanisms for WLANs. IEEE 802.11 originally specifies the equivalent of wired LAN security algorithm Wired Equivalent Privacy (WEP). However, it's shown in many researches that WEP cannot achieve the required data confidentiality, integrity, and authentication. WEP had many design flaws and is considered completely broken. As a result, the use of WEP for confidentiality, authentication, or access control is deprecated on later revision of the standard in 2012 [1].

Although WEP fails to satisfy the security requirements of the standard, a new standard will require a new hardware. It is not practical to easily discard the users with legacy devices supporting only WEP. Hence, WEP has been succeeded by Wi-Fi Protected Access (WPA) which uses the legacy hardware. WPA was just an intermediate solution to cover the weaknesses of WEP and was later superseded by WPA2.

WPA adopts Temporal Key Integrity Protocol (TKIP) for confidentiality and Integrity, which still uses Rivest Cipher 4 (RC4) for data encryption. A key mixing function is included in TKIP as well as an extended IV space to construct unrelated and fresh per-packet keys. WPA introduced Michael algorithm [2] for improving data integrity. Furthermore, WPA implements a packet-sequencing mechanism by binding a monotonically increasing sequence number to each packet. This helps in replay packets detection.

Although TKIP addresses all known vulnerabilities, yet it had some limitations due to the use of legacy hardware. TKIP relies on Message Integrity Check (MIC) algorithm called Michael, which provided inadequate security [3, 4]. As a result, it has been replaced by the more secure algorithm CCMP (Counter Mode/CBC-MAC Protocol). However, TKIP is still supported by many people [5] and should be discouraged.

Considering the use of new hardware, a new long-term solution is proposed for enhancing the security in the MAC layer. IEEE 802.11i uses CCMP to provide confidentiality, integrity, and replay protection. Moreover, it uses 802.1X authentication and key management in order to provide mutual authentication and generate fresh session key for data transmission. IEEE 802.11i improves the security in terms of data confidentiality, integrity and authentication.

Several works discussed the effect of TKIP, CCMP security algorithms on network throughput for IEEE 802.11 networks. However, most of the works done were based on older versions of the standard.

In this paper, we provide a theoretical comparison on different security protocols, WPA and WPA2, and evaluate the effect of these protocols on network performance using IEEE 802.11n amendment. To the best of our knowledge, there are very few works that have been carried under 802.11n.

## II. SECURITY METHODS

In a wireless network, security mechanics involve the capability of access control, authentication, authorization, confidentiality, integrity and availability. Some important security mechanisms used include encryption protocols and key management.

IEEE 802.11i specification is of two classes: Robust Security Network Association (RSNA), and the earlier version Pre-RSNA. RSNA provides TKIP and CCMP as data confidentiality standards, and RSNA establishment procedure. Pre-RSNA security consists of WEP and 802.11 entity authentication. Figure 1 provides a summary of different classes in IEEE 802.11i security.

WEP uses RC4 stream cipher for providing confidentiality, and cyclic redundancy check (CRC) for data integrity. There are two methods for pre-RSNA authentication; open system and shared key authentication. All pre-RSN security algorithms have been deprecated except for open system authentication.

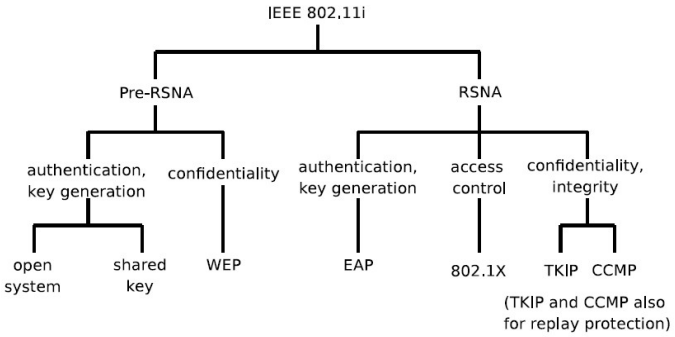


Fig. 1. Summary of 802.11i security [6]

## III. WPA AND WPA2

WPA was an intermediate solution for enhancing the previous security standard. However, WPA has shown significant vulnerabilities and was later superseded by WPA2 which is based on IEEE 802.11i standard ratified in June 2004.

Both of WPA and WPA2 use the same authentication system. Enterprise networks use 802.1 X/EAP frameworks for centralized mutual authentication system. For home and small office environments Pre-Shared Key (PSK) is used.

On the other hand, differences between these two security methods include; WPA2 is backward compatible with WPA. It uses a mixed mode that supports both WPA and WPA2 enabled devices on the same wireless network. Another difference is that; WPA uses TKIP encryption as a Security Protocol which in turn uses RC4 cipher, while as WPA2 uses CCMP-AES as a Security Protocol. WPA uses Michael algorithm for data integrity but WPA2 uses more robust, efficient and stronger algorithm, CBC-MAC. A comparison of WPA and WPA2 is shown in Table 1.

TABLE I. SUMMARY OF 802.11 SECURITY METHODS [7]

| | WEP | 802.11i Methods | |
|---|---|---|---|
| | | WPA | WPA2 |
| Security Protocols | RC4 | TKIP | CCMP |
| Cipher | RC4 | RC4 | AES |
| Key Length | 40 or 104 bits | 128 bits encryption 64 bits authentication | 128 bits |
| Key Life | 24 bit IV | 48 bit IV | |
| Key Generation | Concatenation | Two phase mixing function | Not needed |
| Data Integrity | CRC-32 | Michael | CBC-MAC |
| Header Integrity | None | Michael | CBC-MAC |
| Replay Protection | None | Packet Number | |
| Key Management | None | EAS-based | |
| Authentication | Open or Shared key | 802.11x or Pre-Shared Key (PSK) | |

### A. *Confidentiality and Integrity*

Since both WPA and WPA2 use the same authentication system, we will consider only Confidentiality and Integrity in our comparison of the two protocols.

"Confidentiality is the non-occurrence of the unauthorized disclosure of information, whereas Integrity is the non-occurrence of the unauthorized manipulation of information" [8]. To ensure security, confidentiality and integrity must be provided by the security standard. Data confidentiality and integrity are provided by; WEP, TKIP and CCMP. WEP and TKIP are deprecated and no longer in use, leaving CCMP as the ruling standard in 802.11i confidentiality since 2004. CCMP provides stronger encryption than TKIP and it incorporates replay protection. In this section we will focus on TKIP and CCMP as WEP is obsolete and no longer in use. The standard also defines one integrity protocol for management frames: BIP (Broadcast Integrity Protocol).

The aim for TKIP was to provide an intermediate solution for devices supporting only WEP. Thus, it's optional for an RSNA and it's used for the protection of data frames. BIP is used for management frame protection. It protects management frames within the Basic Service Set (BSS) [1].

## IV. EFFECT ON THROUGHPUT

### A. *Main goals*

In this section, we analyze the impact of different security protocols on WLAN performance. We performed practical experiments on IEEE 802.11 wireless network. In the experiment we enabled and disabled WPA and WPA2 on different cases and scenarios and then analyzed the throughput variation of different TCP traffic over the network. We analyzed the initial results when no security protocol was used and then compared the results obtained for different security protocols.

Transmission Control Protocol (TCP)/ Internet Protocol (IP) are the internet's core protocols. TCP provides a reliable connection-oriented service, for applications that require a reliable data stream, such as file transfer and email. Applications that do not require reliable service may use User Datagram Protocol (UDP) on top of IP. UDP provides a connectionless datagram service that emphasizes less on reliability [9]. We used TCP to measure the throughput of the network.

In order to measure the throughput, we transfer a large file over a network and measure the time it takes to transfer from one system to another system. The throughput is calculated by dividing the file size by the time. It's measured in bits per second (bit/s).

The Maximum bandwidth is calculated as follows:

$$Throughput \leq TCP\ Receive\ Window/Round\text{-}Trip\ Time$$

The Max TCP Window size in Windows Operating System is 65,535bytes. For this RWIN, the bandwidth will be limited to 2.62 Mbits/s for a single TCP connection.

The main objective of this paper is to discover the compared effect of WPA and WPA2 on network performance. To realize this, we measure the throughput of the network by sending a synthetic data, generated by IPTraffic, over the network. We then examine different security arrangements when we are not using any security protocol, in the contrary when we are using advanced security protocols WPA and WPA2.

### B. *Network design*

#### *1) Network setup*

A Prolink-PRN2001 access point (AP) is used in the test The AP was functioning in the 802.11n 2.4GHz 54Mbps mode.

A small difference is present between 5GHz and 2.4GHz concerning propagation in an indoor office setting. For this reason, we have used 2.4GHz in our setup. Client isolation was disabled and re-authentication level in the router was defined in terms of seconds passed.

Two clients were used to send generated packets from ClientA to ClientB.

ClientA was an Intel® Core™ i5-2410M CPU @2.30GHz with 4GB RAM, running Windows Technical Preview 64-bit (6.4, Build 9841) with wireless adapter Qualcomm Atheros AR9285 802.11 b|g|n Wi-Fi Adapter.

ClientB was an Intel® Core™ i3-3120M CPU @2.50GHz with 4GB RAM, running Windows Technical Preview 64-bit (6.4, Build 9841) with wireless adapter Realtek RTL8188CE Wireless LAN 802.11n PCI-E NIC.

All clients avoided to use any programs which might affect the processor or network utilization. Table II shows a summary of the clients used in the test.

TABLE II. SUMMARY OF THE SYSTEMS USED IN THE EXPERIMENT

| System | Processor | RAM | Interface |
|---|---|---|---|
| ClientA | Intel® Core™ i5-2410M CPU @2.30GHz | 4GB | Qualcomm Atheros AR9285 |
| ClientB | Intel® Core™ i3-3120M CPU @2.50GHz | 4GB | Realtek RTL8188CE Wireless LAN 802.11n PCI-E NIC |

Most of the hardware used in this investigation were located in the same hall and roaming was avoided. This was done to guarantee that the walls and other obstacles would not be a factor affecting the measurement. Wireless devices restrict signals that are too strong [10]. Thus, we situated the antennas not less than 1.5m (5 feet) apart. Figure 2 shows the network setup.

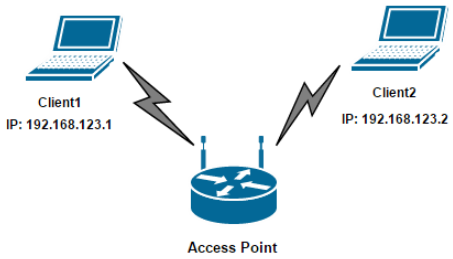


Fig. 2. Network Setup

#### *2) Security Levels*

Three different security configurations were used in our test:

*a) No Security:* This is often default configuration of most wireless devices. The main reason for using this level is to insure the minimum effect on throughput. It is used as a reference for other security standards.

*b) WPA with PSK authentication and RC4 encryption:* This uses WPA configuration, Pre-Shared Key is used for authentication.

*c) WPA2 with PSK authentication and AES encryption:* This uses WPA2 configuration, Pre-Shared Key method of authentication is used.

#### *3) The Network Measurement Methodology*

As mentioned earlier, the main goal of this paper is to compare to what degree the used security mechanisms decrease the throughput in Wireless LAN. Hence, to perform this analysis we need to generate traffic and send it through the Wireless channel and measure it from both the Sender (Tx) side and the Receiver (Rx) side and compare these results. We used a traffic generator on ClientB to send to ClientA. Since there are numerous traffic generators like NetPerf and IPTraffic. Using Ethereal for the comparison of these generators and to analyze whether the tool used generates the traffic according to the parameters specified. Andrew Gin [11] suggested on his evaluations that IPTraffic was the only reliable tool which can generate traffic based on the given parameters. LANTraffic was the other software we used to measure the total send/receive throughput of the network. IPTraffic and LanTraffic were both used to increase the accuracy of the measurement taken.

#### *4) Configuration of Traffic Generator*

In this study we used IPTraffic and LANTraffic, which are network testing tools that can create data streams such as transmission control protocol (TCP) and user datagram protocol (UDP), and measure the throughput of the network that is carrying those protocols. The tools are used for networking performance measurement and packet control.

*IPTraffic and LanTraffic were configured as follows:*

*The Total Number of Packets:* The amount of packets used has no effect in the network throughput. The experiment was

conducted with ClientA getting a minimum of 20,000 packets. We have observed the throughput for an average of 5min and 30seconds. And during this time the range was minimal, showing that the number of packets has no effect on the throughput.

*Outgoing Bandwidth:* We did not use any bandwidth limiting software and there was no any other running process which used the network. We configured the tool to propel more traffic through the interface.

*TCP Windows:* the experiment is Windows configuration dependent. TCP uses a receive window that is four times the size of the maximum TCP segment size negotiated during connection setup, it uses up to a maximum size of 64 KB (65535 bytes).

*Traffic Protocol:* The main protocol we used in the IP Traffic Generator is the TCP protocol. Since UDP is used for time sensitive applications, such as VOIP. UDP is slightly used in the Traffic generator, only in certain scenarios.

*Traffic Type:* The traffic type was not important for the test. So we depended on automatically generated traffic by the LanTraffic and/or IPTraffic.

## V. Results and Discussion

### A. Effect on Throughput:

In this experiment, ClientB was configured to send the generated traffic data to ClientA. We measured the respective Throughputs of TCP packets based on different security configurations (No Security, WPA and WPA2 respectively). We used LanTraffic in the measurement as a Traffic generator and receiver on ClientB and ClientA respectively.

All the statistics in this section, tables and graphs, were taken from the Receiver's side (ClientA).

We used LanTraffic to measure the received throughput and put the values in graph. First off, the average throughput was measured disabling the security protocols as a reference; this helps us identify any reduction in throughput when security protocols are used in WLANs. A total of 16 connections were allowed to send TCP packets from ClientB to ClientA. The Total Received Throughput was approximately 35Mb/s, Figure 3. But, when WPA is allowed there was a significant reduction in the throughput of the network and the Total Received Throughput after summing the 16 connections from ClientB to ClientA became 13Mb/s as in Figure 4. Finally, WPA2 has shown an improved throughput over WPA. Figure 4 shows the total received throughput for WPA2 configuration became 30Mb/s with only 5Mb/s reductions from the No Security configuration.

Wherever the levels of security are different, the WPA2 throughputs are more than the respective WPA2 throughputs. This shows that WLAN has less support for RC4/TKIP than it has for AES/CCMP which is obvious in the one to one 1460 byte TCP transfer. Transfers with two senders also support this; in the 6 byte TCP and UDP transfer, the WPA2 throughputs are slightly higher than the throughputs of WPA.

Comparing the above values, it is clear that the throughput of WLAN decreases with the use of complex security mechanisms. However, Figure 3 shows that WPA2 have improved performance compared to WPA which uses TKIP. Although several factors affect the performance, for example the chipset of the access point may have enhanced performance on AES over TKIP. For now, we can conclude that WPA2 has enhanced throughput and thus better performance than WPA [11]. The network throughput is largely unaffected when we apply the various security levels. But from our analysis it is clear that throughput is affected by the use of security protocols though the effect might be negligible, considering one-to-one transmission. This is similar to findings in [12] and [13], as the throughputs were decreased with the use of more complex security protocol.

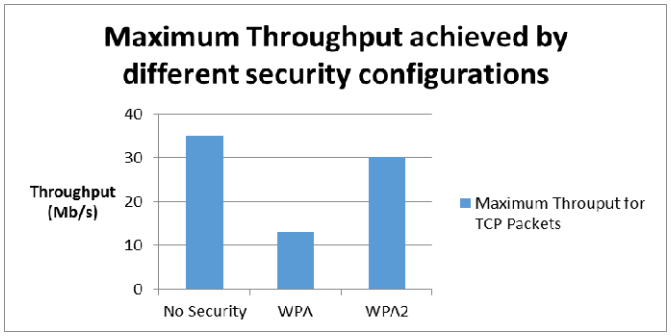


Fig. 3. Comparison of Maximum Throughput achieved by the three security levels.

Even though CCMP is largely improved compared to TKIP, yet there is a significant reduction in throughput. A possible explanation of this might be the cost of combining the encryption and integrity protocols in CCMP.

"First, the encryption of the various message blocks can no longer be carried out in parallel since CBC-MAC requires the output of the previous block to calculate the MAC for the current block. This slows down the protocol. Second, CBC-MAC requires the message to be broken into an exact number of blocks. This means that if the message cannot be broken into an exact number of blocks, we need to add padding bytes to it to do so. The padding technique has raised some security concerns among some cryptographers but no concrete deficiencies attacks have been found against this protocol." [8]

Previous works have been carried on IEEE 802.11a/b/g wireless amendments. But, in this paper we used IEEE 802.11n amendment. We were unable to find the necessary hardware for testing the effect on throughput for the new IEEE 802.11ac since all the devices we use today are capable only on IEEE 802.11n and require hardware upgrade for the new amendment.

We did not consider the case for multiple clients since almost all other researches, [11] and [12], showed the same effect for multiple clients.

## VI. Conclusion

A lot works has been done in the area of analyzing the security protocols of WLAN. However, much of these researches remain focused on the old protocol, wired

equivalent protocol (WEP), rather than on the upgraded new encryption techniques existing in our day, Wi-Fi Protected Access WPA and WPA2. Even the academic works on these advanced encryption protocols did not associate the two protocols with respect to performance, but most of the works are on other aspects other than the performance. Moreover, over study aims to bind together the previous works and scrutinize difference and similarities amid those works.

Our method relied on investigating the basic security mechanisms employed in 802.11n, since older works were done regarding the 802.11a/b/g mechanisms.

The 802.11n amendment is hardly mentioned in any research. 802.11n provides best security mechanism in comparison together with 802. 11g [14] and it utilizes the CCMP encryption algorithm much better than 802.11g. In our study we have emphasized on IEEE 802.11n amendment and we proved that it provides similar outcome and effect on the wireless network.

## ACKNOWLEDGMENT

We are very much thankful to Monirul Islam and Abdullahil Kafi for their guidance and recommendations.

## REFERENCES

[1] Nikita Borisov, Ian Goldberg, David Wagner. "Intercepting Mobile Communications: the insecurity of 802.11." Proceedings of the 7th annual international conference on Mobile computing and networking. ACM. 2001. 180-189.

[2] IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications". (2012 revision). IEEE-SA. 5 April 2012. doi:10.1109/IEEESTD.2012.6178212

[3] N.Ferguson. Michael: an improved MIC for 802.11 WEP. IEEE doc. 802.11-2/020r0, Jan. 2002.

[4] E. Tews and M. Beck. Practical attacks against WEP and WPA. In Proceedings of the second ACM conference on Wireless network security, WiSec '09, 2009.

[5] A. Wool. A note on the fragility of the Michael message integrity code. IEEE Transactions on Wireless Communications, 3(5):1459{1462, 2004

[6] Fleming, K. "Wireless Security Initiatives." (2005).

[7] McCarter, Harold Lars. "Analyzing Wireless LAN Security Overhead." (2006).

[8] Chandra, Praphul. Bulletproof Wireless Security: GSM, UMTS, 802.11, and Ad Hoc Security. Elsevier, 2011.

[9] Stallings, William. “Cryptography and network security, principles and practices, 2003." Practice Hall.P-4

[10] D. Dobkin, “Indoor propagation and wavelength,” tech. rep., WJ Communications, September 2002.

[11] Gin, Andrew. "The Performance of the IEEE 802.11 i Security Specification on Wireless LANs." (2005)

[12] R. Hunt, J. Vargo, and J. Wong, “Impact of security architectures on wireless network performance,” in 5th IEEE International Conference on Mobile and Wireless Communications Networks (MWCN 2003), October 2003.

[13] N. Baghaei and R. Hunt, “Security performance of loaded IEEE 802.11b wireless networks,” Computer Communications, Elsevier, U.K., vol. 27, no. 17, pp. 1746–1756, 2004.

[14] Awan, Salman Afsar, and Amer Sohail. " Experimental Performance Analysis of Wireless LAN IEEE 802.11 N Secuirty Mechanisms." (2014)