Analyzing the Impact of Security Protocols on Wireless LAN with Multimedia Applications

Thaier Hayajneh, Samer Khasawneh, Bassam Jamil, Awni Itradat
Department of Computer Engineering
Hashemite University
Zarqa, Jordan
{Thaier, Samerkh, Bassam, Itradat}@hu.edu.jo

Abstract—The availability and reasonable cost of broadband Internet made it an attractive and favorable option to billions of users worldwide. Being a fast service also encourages its users to use multimedia applications. The performance of such applications in wireless LAN may be highly affected by security protocols. This paper examines the effect of different security protocols on the performance of wireless LAN with multimedia applications. Experiments were performed on a wireless test-bed and the results were analyzed for throughput, delay and jitter for four security settings: disabled security, WEP, WPA1, and WAP2. The experiments were performed under two different scenarios and using multimedia traffic streams. The results revealed a significant degradation in performance when security protocols were enabled in wireless LAN. Specifically, delay and jitter, were significantly increased, both of which are key metrics for multimedia applications. The increase is clearer when a larger number of hosts exist in the network. We finally propose an outline for a solution to obtain strong security in wireless LAN without significant performance degradation. The solution proposes that the security processing at the hosts be conducted by the powerful host processor rather than by the radio card processor. As for the wireless access point, adding ASIC or FPGA processor is suggested for performing the heavy security processing.

Keywords-WLAN; WEP; WPA1; WPA2; delay; jitter; multimedia traffic.

I. INTRODUCTION

In the last decade, wireless local area networks (WLAN) technology has become more convenient and thus has spread extensively worldwide. The security of this technology, however, is a constant concern to all its users, especially those who use it for online banking, social networking, and monetary transfer. In that regard, determining the relationship between the strength of the used security protocol and the performance of WLAN is of utmost importance. This relationship becomes even more important in applications that require high QoS to operate properly such as video conferencing and live video streaming.

Researchers have extensively investigated the impact of security protocols on the performance of WLAN. The majority focused on the network's throughput while less attention was given to delay. The results were conflicting on the impact of security on the performance of WLAN, with several [1, 2, 3, 6, 7] discussing its tangible negative impact and few concluding its negligible impact on performance of WLAN [5].

The main security protocols in WLAN are wired equivalent privacy (WEP) [8], WiFi protected access (WPA1) [10], and WiFi protected access II (WPA2) [10]. WEP is the simplest and uses computationally light cipher. However, it has been shown to be insecure and should no longer be used. WPA1 is stronger than WEP; but, has few security vulnerabilities and was replaced by WPA2 [11]. WPA2 is known to be secure since it relies on strong cipher as AES. Hence, applying WPA2 is expected to be heavy and requires considerable processing leading to increased delay. Further details will be discussed on each protocol in Section 3.

In this paper, we will examine the impact of security protocols on the performance of WLAN through conducting experiments over a test-bed. The performance of the network was examined under four conditions: disabled security, WEP, WPA1, and WPA2. Given the contemporary trend of using multimedia applications among current Internet users, a special attention was given in this paper to the impact of security protocols on the performance of WLAN in such applications. Since the multimedia applications are most sensitive to delay and jitter, these two performance metrics were the focus in this paper.

Moreover, we have proposed a new solution that will allow us to use a strong security protocol in WLAN while significantly minimizing the degradation in WLAN performance. The solution proposes that the security processing be conducted by the powerful host processors instead of the radio card processors. As for the wireless access point, adding ASIC or FPGA processor is suggested for performing heavy security processing. The need for such a proposition arose from the fact that disabled security WLAN by far outperforms other security settings in all performance aspects. Our work is different from pervious studies in considering different security protocols including WPA2 and different multimedia traffic (video streaming traffic); focusing on delay and jitter; and finally proposing a novel solution to achieve strong security without performance degradation.

The consequent parts of this paper are organized as follows: Section 2 overviews previous related work. Section 3 provides a brief description of the security protocols and their pitfalls in WLAN. Methodology and the hardware/software used in the experiments are discussed in Section 4, and results are described in Section 5. Section 6 illustrates the proposed solution, and the derived conclusion and future work are summarized in Section 7.

 ISBN: 978-1-61208-209-7

II. RELATED WORK

The impact of security protocols on WLAN performance has been studied in the literature from different perspectives. The majority of the researchers considered the impact on throughput and only few considered delay and jitter. Most of the networks were tested with file transfer traffic.

Barka and Boulmalf [1] studied the impact of security protocols on the throughput of WLAN. They considered both TCP and UDP traffic under two scenarios. Only the impact of WEP and WPA1 was considered but not WPA2. The study concluded that adding security will cause a decrease in the average network throughput and increase in the percentage of dropped packets for both TCP and UDP traffic. The authors assume fixed traffic intensity with fixed packet delay. Moreover, Barka and Boulmalf found that WPA1 will have the largest impact on the network performance due to the bigger key sizes and longer processing time.

Kolahi et al. [2] evaluated the impact of different security protocols on network throughput and round trip time (RTT) for both TCP and UDP traffic. They also considered different operating systems (Windows server 2003, XP and Vista). Similar to Barka and Boulmalf [1], the authors did not consider WAP2. The results showed that using security protocols reduces the throughput and increases RTT. The increase in RTT is more noticeable when larger encryption keys are used.

Several experiments have been carried out to explore the impact of security protocols on the performance of voice and data traffic in WLAN [3]. The performance metrics that were tested are: throughput, delay, and jitter. However, delay and jitter were only tested for WEP protocol with 64-bit key size; such a protocol is not secure and could be broken in few seconds [4]. Boulmalf et al. [3] showed that no noticeable throughput degradation is incurred through adding security protocols. However, considerable increase in packets delay and jitter was noticed especially for voice traffic.

Gin and Hunt [5] evaluated the impact of 802.11i security on network throughput performance. Several experimental scenarios were carried out in which the traffic volume and the number of traffic initiators (users) are changed. In their first set of experiments, where only two users coexisted in the network, minor throughput degradation is incurred even if the security level is maximized. In their second set of the experiments, where multiple users are transmitting through the network concurrently, slight throughput degradation resulted when adding security even with larger key length. With their results, Gin and Hunt [5] disagreed with many research papers that confirmed throughput deterioration when implementing increasing security.

In Begh and Mir work [6], IPTraffic was used to generate different rates of TCP and UDP traffic to quantify the impact of adding security on network throughput, transmission delay and packet loss. The results are obtained using five different security setups: no security, WEP-64, WEP-128, WPA-TKIP and WPA-AES. For 1 Mbps and 5 Mbps traffic rates, the results showed no major degradation in network throughput (except for WPA-AES), no significant increase in transmission time, and almost negligible packet loss ratio. However, when the traffic rate is increased to 12 Mbps, noticeable detraction in performance metrics was noticed. Begh and Mir [6] only performed their experiments with a single wireless station and they did not consider WPA2. Furthermore, they did not consider the end-to-end delay, but instead considered the transmission time which may not reflect the impact of using security protocols in WLAN.

In Baghaei and Hunt study [7] the impact of WEP protocol with various settings and key sizes on the performance of WLAN was analyzed. They used a network with three wireless clients and a wired server. Baghaei and Hunt [7] concluded that the stronger the security mechanism implemented the poorer the performance, although the degradation is certainly not linear. Moreover, they found that the response time is increased with stronger security mechanism and also when the network is congested.

As discussed in this section, none of the previous work has studied the impact of WPA1 and WPA2 on multimedia applications where delay and jitter are the key metrics that must be carefully tested. Furthermore, none of the previous work proposed a solution for the performance degradation that is caused by using strong security protocol as WPA2. Therefore, in this paper a special attention will be given to the impact of security protocols on the performance of WLAN in multimedia applications. Moreover, we will propose a new solution that will allow using a strong security protocol in WLAN while significantly minimizing the degradation in WLAN performance.

III. WLAN SECURITY PROTOCOLS

Similar to all wireless technologies, security in WLAN is considered one of its main weaknesses. The wireless medium is shared among the users and open access for any malicious attacker.

In this section, we provide a brief description of the most commonly used security protocols in WLAN.

A. Wired Equivalent Privacy

WEP protocol is the first security protocol for WLAN [8]. It was designed as a part of the original 802.11 standard. Its intended purpose was to provide security to WLAN equivalent to the security existing in the wired network. WEP uses RC4 stream cipher for confidentiality and CRC-32 for integrity. In this paper, we used 128-bit WEP protocol with 104-bit key and 24-bit initialization vector. WEP is known to be insecure since 2001. Tews and Beck [4] surveyed the most common successful attacks against WEP. Although WEP is widely used, it is agreed now that WEP with all its variations and modifications is considered insecure and should not be used. With the available tools such as Aircrack [9] one can break WEP security within minutes.

B. WiFi Protected Access

WPA1 [10] was designed to overcome the limitations and insecurity of WEP protocol. WPA1 implements most of the IEEE 802.11i standard. It uses Temporal Key Integrity Protocol (TKIP) [10] that uses a per-packet key. Hence, unlike WEP, a new 128-bit key is dynamically generated for

 ISBN: 978-1-61208-209-7

each packet. Consequently, this prevents most of the type of attacks that compromised WEP. WPA1 replaced the insecure CRC used in WEP with a stronger message integrity check. Despite the fact that WPA1 addressed most of the problems that exists in WEP, it continues to show some limitations such as relying on stream cipher and cryptographically weak integrity (Michael algorithm). In Moen et al. [11] researchers discovered weaknesses in the temporal key hash of WPA1. Tews and Beck [4] presented the details of a potential attack to break WPA1.

C. WiFi Protected Access II

WPA2 [10] also referred to as IEEE 802.11i replaces WPA1 and implements the mandatory elements of IEEE 802.11i standard. It uses a new AES-based encryption mode CCMP that is highly secure. This resolved the security issue with TKIP in WPA. WPA2 provides Robust Security Network including two new protocols, the 4-way Handshake and the Group Key Handshake. Junaid et al. [12] and Khan et al. [13] showed that the initial counter value used in the CCMP can be predicted and that WPA2 is subject to dictionary attacks.

He and Mitchell [14] concluded that in CCMP, management frames and control frames are neither encrypted nor authenticated by the Link Layer encryption algorithm, and hence, being vulnerable to many threats discussed in their paper. In addition, they expected CCMP to have some impacts on performance because it requires some hardware upgrades.

IV. METHEDOLOGY AND HARDWARE IMPLEMENTATION

In this section, we describe the test bed used to conduct the experiment and the software tools used to collect and analyze the results. We also present the experimental scenarios conducted for studying the impact of security protocols on several network performance metrics such as throughput, delay, and jitter. Clock synchronization as well as a brief description for the performance metrics, especially the end-to-end delay, will be discussed in this section. Finally, traffic streams used in this experiment will be illustrated.

A. Test Bed Description

Two different network setup scenarios were used in this experiment. In the first scenarios, we only used two wireless host (laptops) and one access point as shown in Figure1.

Figure 1. First Scenario

The specification of the devices is as follows:

1) Linksys E2000 Cisco Advanced Wireless-N Router with the following specifications:

- Supports up to 11 channels.
- Supports 802.11n, 802.11a, 802.11g, 802.11b, 802.3, 802.3u, 802.3ab Standards
- Security features : WEP, WPA, WPA2
- Security key bits: up to 128-bit encryption

2) Acer notebooks with the following specifications:

- Model: Acer Intel core i5, 2.24 GHz processor.
- NIC model: Realtek RTL Gigabit Family.
- Operating system: Ubuntu 11.04

The nodes were adjacent (2-3 meters) and other WiFi networks in the area were eliminated to avoid extraneous interference. All the experiments were performed in the same location and within a short period of time. Hence, the impact of multi-fading or coexistence of other WLANs will be the same for all the security protocols and scenarios.

The second scenario is shown in Figure 2 where four laptops existed in the network. All laptops were transmitting at the same time but communication was monitored between two nodes only. The other nodes were added to cause greater interference and congestion in comparison to the first scenario. This is expected to cause more processing, queuing, and backoff delay (possibly caused by collisions). In both scenarios, the streaming bit rate was about 500 kbps. Moreover, beside the video streaming, a large file was transferred between the sender and the receiver.

Figure 2. Second Scenario

B. Clock Synchronization

Accurate synchronization for the Laptops' clocks is crucial to avoid erroneous results on delay and jitter, such as a smaller packet arrival time compared to the packet sending time which may lead to unexplained negative delay. Several techniques can be used to ensure accurate synchronization. One technique is the manual adjustment of the devices' clocks based on a certain reference time. However, this method is prone to human error and therefore may be inaccurate and leading to wrong delay.

Another technique is issuing "net command" between the networked devices. The command guarantees instantaneous and accurate adjustment. However, shortly afterwards, the devices usually skew from the initial adjustment.

A third technique and the one applied in this experiment is the AtomTime Pro software [15], which frequently connects to global servers to adjust the time of the devices used in the experiment. As for the communication with the time server, an out-of-band connection was used to guarantee no interference with our traffic.

C. Software

Wireshark TM packet analyzer was used to capture and analyze network packets. In order to extract the required

 ISBN: 978-1-61208-209-7

data from the large output files, we used AWK scripting language. This tool is used to extract certain packets information being read from Wireshark output files.

Some scripts were written using C# program for packets' matching. Throughput, delay, and jitter were calculated using the list of matched packets obtained from output files.

D. Performance Metrics

1) End-to-End Delay

Delay is one of the most important metrics for multimedia applications. Unlike file transfer, multimedia applications could tolerate packet loss but not a high delay. Delay can be classified into four main types or causes:

a) Transmission delay:

This is the time needed to transmit all the bits of a packet. It is measured by dividing the frame size in bits by the wireless link transmission speed in bits per second. In our case, this time is expected to be in the order of tens of milliseconds.

b) Queuing delay:

This is the time when the packet waits its turn to be transmitted in the queue of a router or host. This delay could be neglected if only few hosts are transmitting in a lightly loaded network. We expect this delay to take place only with the second scenario.

c) Propagation delay:

This is the time needed for one bit to travel from the sending to the receiving host. This delay is measured by dividing the distance between the sender and the receiver by the signal speed (usually equals the speed of light). Usually, this time is small and could be neglected.

d) Processing delay:

This is the time taken to process the packets by the router and hosts. This time is expected to be more significant if security is enabled in the wireless router given that encryption and authentication verification require significant processing and may cause longer delay.

2) Packet Jitter

The packet jitter measures the variation in the end-to-end delay from packet to packet. Multimedia application could tolerate some delay but large jitter could cause a greater damage to the consistency of their operation.

3) Throughput

Throughput is the average number of bits that is sent over the network per second. Usually, it is the most significant metric if the main purpose of the network is to transfer large files.

E. Traffic Streams

In our scenarios, we used video steaming traffic between wireless hosts. Multimedia traffic uses real-time streaming protocol (RTSP) to control the transmission of a media stream. It also relies on real-time protocol (RTP), which runs on the top of UDP or possibly TCP [16]. These multimedia protocols add sequencing and timestamp information to the transferred packets. Hence, their operationability will be significantly affected by the packets delay and jitter. Moreover, a heavily-loaded network will have more collision and backoff time incurring longer delays.

V. RESULTS

In this section, results from both scenarios are discussed in terms of delay, jitter, and throughput. For statistical validation, all the experiments were repeated 10 times and the averages were considered in our results.

A. Delay

Figure 3 shows the total average end-to-end round trip delay in milliseconds for the packets transmitted between two wireless hosts for WEP, WPA1 and WAP2 security protocols. Since our goal was to study the impact of security protocols on the delay, then change in delay is what matters not the value of the delay itself. Hence, we neutralized the results by subtracting the delay with disabled security from the other three cases.

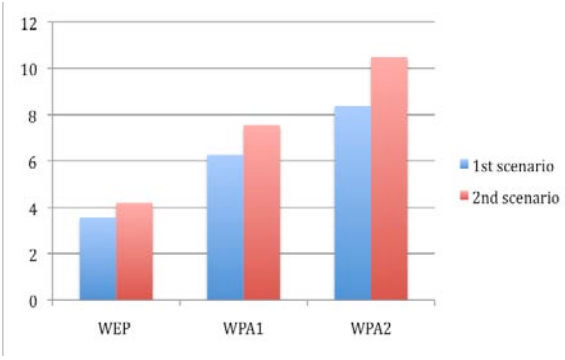

Figure 3. Delay

Figure 3 shows that for both scenarios, delay is increased when security protocols are enabled in WLANs. As expected, WPA2 which is the most complicated security protocol for using the strong AES encryption, showed the highest delay. On the other hand, WEP protocol, which is the lightest protocol for relying on the simple RC4 stream cipher, showed the lowest delay.

For all the security protocols, scenario two has higher delay than scenario one. This is due to the fact that the network traffic in scenario two is much larger than that in scenario one. Larger traffic leads to a larger number of collisions, which in turn results in longer backoff times and longer delay.

Figure 3 also shows that the difference between the delay of WPA1 and WAP2 with scenario two is larger than that with scenario one. This indicates that the processing delay is not the only reason that causes the delay with WPA2. It can also be caused by the overhead in WAP2 protocol handshake messages.

B. Jitter

Figure 4 shows the packet jitter in milliseconds for the packets transmitted between two wireless hosts for WEP, WPA1 and WAP2 security protocols. Since our goal was to study the impact of security protocols on the jitter rather than value of the jitter per se, we neutralized the results by subtracting the jitter with disabled security from the other three cases.

Figure 4 shows that for both scenarios, the jitter is increased when security protocols are enabled in WLANs. As expected, WPA2 showed the highest jitter and WEP showed the lowest.

 ISBN: 978-1-61208-209-7

Similar to Figure 3, for all security protocols, scenario two has higher jitter than scenario one. The same justification also applies here.

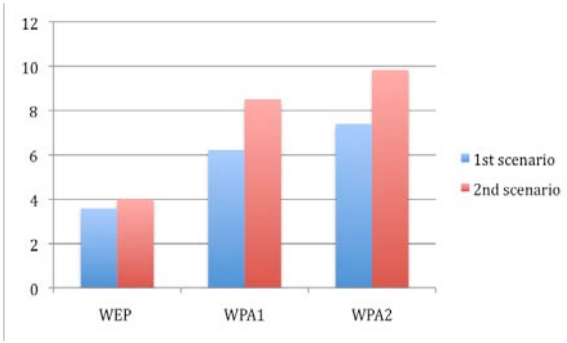

Figure 4. Jitter

Figure 4 also shows that the difference between the jitter of WPA1 and WAP2 with scenario two is even larger compared to scenario one, and for the same reasons that caused the delay to be higher.

C. *Throughput*

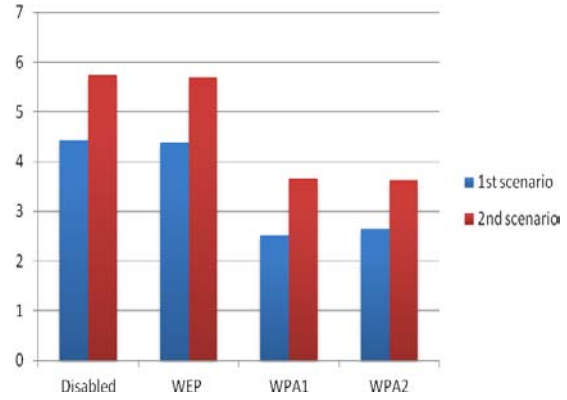

Figure 5. Throughput

Figure 5 shows the throughput in Mbps for the two wireless network scenarios with the four cases: disabled security, WEP, WAP1, and WPA2. The figure shows that WEP has no impact on the throughput. This observation may be explained by the fact that WEP is light and does not cause large overhead. Even for WPA1 and WPA2 protocols, the throughput was slightly affected which may be due to the fact that the multimedia traffic was not heavy on the network. The throughput in the second scenario was higher than the first scenario because of the additional file transfer.

VI. PROPOSED SOLUTION

In this section, we propose an outline for a new approach to achieve security in WLAN while reducing the impact on the network performance. The proposed outline is based on the fact that disabling security in WLAN results in higher throughput and significantly lower delay and jitter. This fact was also agreed upon in other research papers [1, 2, 6, 7].

Potorac and Balan [17] studied the impact of security overheads on 802.11 WLAN throughput. They provided theoretical analysis about the impact of the three security protocols on system's performance. Their findings indicated that theoretically, the impact of WEP, WPA1, and WPA2 security overheads is insignificant for large packets. They concluded that the processing devices and computing resources that are available at the level of the radio station need more processing power for encryption. Thus, according to Potorac and Balan [17] it is possible to observe smaller throughput or larger delay given that the communication processor cannot encrypt or decrypt the data flow at the necessary speed. Lars [18] presented measurements that match the theoretical results presented by Potorac and Balan [17]. Based on our results and the findings we discussed for Potorac and Balan [17] and Lars [18], we propose a solution to overcome the performance degradation caused by using strong security protocols in WLANs. The actual implementation, deep analysis, and performance evaluation of this solution is beyond the scope of this paper and is left for future extension of this work.

The idea of the proposed solution is to move all the security to the end systems and use WLAN with disabled security. Using open access (disabled security) WLAN will give us the following advantages:

- Higher throughput, also shown in [1, 2, 6, 7].
- Lower delay or response time, also shown in [2, 3, 6].
- Less percentage of dropped packets, also shown in [1].

Authentication and encryption will be applied to the data prior to its delivery to the low processor performance wireless card.

At the hosts, the encryption and all other security services, such as authentication and key exchange, will be done before the data is passed to the radio card by the device (possibly laptop) processor. These processors are usually powerful and will process the encryption in much less time compared to the radio card processer. The delay and jitter are both expected to be significantly small and possibly negligible.

At the access point, the increasing complexity of security protocols signifies the need to improve the performance of network processing hardware for real-time cryptographic processing. The cryptographic algorithm throughput and delay can be significantly improved by implementing the algorithm in specialized processors using ASIC solution or FPGA implementation. While ASIC designs are superior in performance, FPGA implementation has the advantages of low cost, reprogramability and short time to market. Numerous ASIC and FPGA designs have been proposed in the literature such as those in Wang et al. [19] and Chang et al. [20]. Wang et al. [19] presented an ASIC implementation with on-the-fly key expansion and reconfigurable core architecture. The design provides a throughput of up to 3.75 Gb/s at 102 MHz. Chang et al. [20] discussed an FPGA implementation of 32-bit AES

 ISBN: 978-1-61208-209-7

algorithm. The design has a low area of 156 slices and a throughput of 876 Mbps.

In terms of hardware implementation of the algorithm, our preliminary analysis indicates that the synthesized HDL design would result in a gate count of 50K gates. An ASIC implementation using 90-nm technology will have an area of 1mm^2 and a power dissipation of 150 mW with a throughput of about 40 Gbps. An FPGA implementation, on the other hand, would require about 10K slices with a throughput of about 15 Gbps.

Figure 6 illustrates the proposed solution. The laptops will use the Fast Security Add-on (FSA), which will be an add-on software to the wireless card driver. FSA will be responsible for all the security algorithms and will be processed by the powerful fast laptop processor (could be dual core, i3, i5, or i7). On the other hand, at the access point the ASIC/FPGA processor will be responsible for all the processing that maybe required by the security protocols.

Figure 6. Proposed Solution

The proposed solution is considered successful only if it causes a negative impact on the performance that is less than the impact caused by WPA2. As for the impact on the throughput, Potorac and Balan [17] analytically proved that the overhead in WPA1 and WPA2 are 20 and 16 bytes per packet, respectively. Thus, it is less likely that the proposed solution will have any impact on the throughput. In our future work, we are planning to implement and test the FSA tool on several laptops platforms to analyze its impact on the delay and jitter. The specialized processors using ASIC solution or FPGA implementation will also be tested for delay and jitter.

VII. Conclusion and Future Work

This paper examined the effect of several security protocols on the performance of a WLAN with multimedia applications. Throughput, delay, and jitter for four security settings: disabled security, WEP, WPA1, and WAP2 were analyzed. The results showed a significant degradation in performance occurring when enabling security protocols in a WLAN. Specifically, delay and jitter, which are key metrics for such applications, were significantly increased. The increase was more noticeable when more wireless hosts exist in the network. Therefore, we proposed a solution outline to achieve strong security in WLAN without noticeable performance degradation. The solution proposes that the security processing be conducted by the powerful host processors rather than by the radio card processors. As for the wireless access point, adding ASIC or FPGA processor is suggested for performing heavy security processing. Our study has shown that in theory, the proposed solution is effective. However, future empirical research is needed to practically prove its effectiveness.

Moreover, in order to better comprehend the possible impact of the increase in delay and jitter with WPA2 one should consider objective and subjective video quality metrics. However, theses quality metrics and the details and prototype of the proposed solution are left for future research.

References

[1] E. Barka and M. Boulmalf, “On The Impact of Security on The performance of WLANS,” Journal of Communications (JCM), Vol. 2, pp. 10-17, June 2007.

[2] S. Kolahi, S. Narayan, Y. Sunarto, D. Nguyen, and P. Mani, "The Impact of Wireless LAN Security on Performance of Different Windows Operating Systems," in Proceedings of the IEEE Symposium of Computers and Communications(ISCC), pp. 260-264, July 2008.

[3] M. Boulmalf, E. Barka, and A. Lakas, “Analysis of the effect of security on data and voice traffic in WLAN,” ACM journal of Computer Communications, vol. 30, pp. 2468-2477, 2007.

[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), pp. 79-86, 2009.

[5] A. Gin and R. Hunt, “Performance Analysis of evolving Wireless IEEE 802.11 Security Architectures,” Proceedings of the 8th International Conference on Mobile Technology, Applications, and Systems, Vol 2, pp. 101-106, 2008.

[6] G.R. Begh and A.H. Mir, "Quantification of the Effect of Security on Performance in Wireless LANs," Proceeding of the 3rd International Conference on Emerging Security Information, Systems and Technologies (SECURWARE '09), pp. 57-62, June 2009.

[7] N. Baghaei and R. Hunt, "Security Performance of Loaded IEEE 802.11b Wireless Networks," Journal of Computer Communications, vol. 27, pp. 1746-1756, 2004.

[8] LAN MAN Standards Committee of the IEEE Computer Society, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std 802.11-1999 edition, IEEE, New York, 1999.

[9] <http://www.aircrack-ng.org> 27.7.2012

[10] ANSI/IEEE standard 802.11i., “Amendment 6 Wireless LAN Medium Access Control (MAC) and Physical Layer (phy) Specifications”, Draft 3. (2003).

[11] V. Moen, H. Raddum, and K. Hole, "Weaknesses in the temporal key hash of WPA," In Proceeding of ACM Mobile Computing and Communications Review (SIGMOBILE 04) , pp. 76-83, 2004.

[12] M. Junaid, Muid Mufti, and M.Umar Ilyas, "Vulnerabilities of IEEE 802.11i Wireless LAN CCMP Protocol," Journal of Transactions on Engineering, Computing and Technology, vol. 11, pp. 228-233, February 2006.

[13] M. Khan, A. Cheema, and A. Hasan, "Improved Nonce Construction Scheme for AES CCMP to Evade Initial Counter Prediction," Proceedings of the 9th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, pp. 307-311, 2008.

[14] C. He and J. Mitchell, "Security Analysis and Improvements for IEEE 802.11i," Proceeding of NDSS, 2005.

[15] < http://www.atomtime.com/> 27.7.2012

 ISBN: 978-1-61208-209-7

[16] J. Kurose and K. Ross, Computer Networking: A Top-Down Approach (5th Edition), Addison-Wesle, 2010.

[17] A. Potorac and D. Balan, "The Impact of Security Overheads on 802.11 WLAN Throughput," Journal of Computer Science and Control Systems, vol. 2, pp. 47-52, 2009.

[18] McCarter Harold Lars, “Analyzing Wireless LAN Security Overhead”, research report at Virginia Tech University, available at http://scholar.lib.vt.edu/theses/ available/etd-04202006-080941/unrestricted, 2006.

[19] M. Wang, C. Su, C. Horng, C. Wu, and C. Huang, "Single- and Multi-core Configurable AES Architectures for Flexible Security," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 18 , pp. 541-552, 2010.

[20] C. Chang, C. Huang, K. Chang, Y. Chen, and C. Hsieh, "High throughput 32-bit AES implementation in FPGA," in Proceeding of IEEE Asia Pacific Conference on Circuits and Systems, 2008.

 ISBN: 978-1-61208-209-7