An Enhanced WLAN Security System with FPGA Implementation for Multimedia Applications

Thaier Hayajneh

Sana Ullah*

Bassam Jamil Mohd

Kiran Balagani

*CISTER Research Center

CISTER-TR-150601

2015

An Enhanced WLAN Security System With FPGA Implementation for Multimedia Applications

Thaier Hayajneh, Sana Ullah*, Bassam Jamil Mohd, Kiran Balagani

*CISTER Research Center
Polytechnic Institute of Porto (ISEP-IPP)
Rua Dr. António Bernardino de Almeida, 431
4200-072 Porto
Portugal
Tel.: +351.22.8340509, Fax: +351.22.8321159
E-mail: sauah@isep.ipp.pt
http://www.cister.isep.ipp.pt

Abstract

Maintaining a high level of data security with a lowimpact on system performance is more challenging in wirelessmultimedia applications. Protocols that are used for wireless localarea network (WLAN) security are known to significantly degradeperformance. In this paper, we propose an enhanced security system for a WLAN. Our new design aims to decrease the processingdelay and increase both the speed and throughput of the system,thereby making it more efficient for multimedia applications. Ourdesign is based on the idea of offloading computationally intensiveencryption and authentication services to the end systems' CPUs.The security operations are performed by the hosts' central processor (which is usually a powerful processor) before deliveringthe data to a wireless card (which usually has a low-performanceprocessor). By adopting this design, we show that both the delayand the jitter are significantly reduced. At the access point, weimprove the performance of network processing hardware forreal-time cryptographic processing by using a specialized processor implemented with field-programmable gate array technology.Furthermore, we use enhanced techniques to implement theCounter (CTR) Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) and the CTR protocol. Ourexperiments show that it requires timing in the range of 20–40 &#956;sto perform data encryption and authentication on differentend-host CPUs (e.g., Intel Core i5, i7, and AMD 6-Core) as compared with 10–50 ms when performed using the wireless card.Furthermore, when compared with the standard WiFi protectedaccess II (WPA2), results show that our proposed security systemimproved the speed to up to 3.7 times.

An Enhanced WLAN Security System With FPGA Implementation for Multimedia Applications

Thaier Hayajneh, *Member, IEEE*, Sana Ullah, Bassam J. Mohd, and Kiran S. Balagani, *Member, IEEE*

***Abstract*—Maintaining a high level of data security with a low impact on system performance is more challenging in wireless multimedia applications. Protocols that are used for wireless local area network (WLAN) security are known to significantly degrade performance. In this paper, we propose an enhanced security system for a WLAN. Our new design aims to decrease the processing delay and increase both the speed and throughput of the system, thereby making it more efficient for multimedia applications. Our design is based on the idea of offloading computationally intensive encryption and authentication services to the end systems' CPUs. The security operations are performed by the hosts' central processor (which is usually a powerful processor) before delivering the data to a wireless card (which usually has a low-performance processor). By adopting this design, we show that both the delay and the jitter are significantly reduced. At the access point, we improve the performance of network processing hardware for real-time cryptographic processing by using a specialized processor implemented with field-programmable gate array technology. Furthermore, we use enhanced techniques to implement the Counter (CTR) Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) and the CTR protocol. Our experiments show that it requires timing in the range of 20–40 μs to perform data encryption and authentication on different end-host CPUs (e.g., Intel Core i5, i7, and AMD 6-Core) as compared with 10–50 ms when performed using the wireless card. Furthermore, when compared with the standard WiFi protected access II (WPA2), results show that our proposed security system improved the speed to up to 3.7 times.**

***Index Terms*—Field-programmable gate array (FPGA), IEEE 802.11i, multimedia security, wireless local area network (WLAN), WiFi protected access II (WPA2).**

I. Introduction

THE IEEE 802.11 standard is widely used to provide solutions for wireless local area networks (WLANs). The ubiquitousness of mobile devices and the availability of high-speed broadband internet connections have exponentially increased the use of multimedia applications supported by the IEEE 802.11 standard [1]. The security of this technology, however, is a constant concern to all its users. In this regard, determining the relationship between the strength of the adopted security protocol and the performance of a WLAN is of utmost importance [2]. This relationship becomes even more important in applications that require a high quality of service to operate properly, such as video conferencing and live multimedia streaming [3], [4].

In general, the security in the IEEE 802.11 standard is classified into two main classes, i.e., prerobust security networks (pre-RSNs) and RSNs [5]. The pre-RSN wired equivalent privacy (WEP) [6] was used to provide confidentiality, whereas authentication is optional and can be offered using a shared key. However, WEP was shown to be insecure [7]. On the other hand, an RSN provides solutions to the security issues that exist in WEP. Nowadays, WiFi Alliance must follow the IEEE 802.11i standard identified by WiFi protected access (WPA1) [8] and WiFi protected access II (WPA2) [8] network security certifications. WPA1 is stronger than WEP; however, it has few security vulnerabilities and was replaced by WPA2 [9]. WPA2 is known to be secure as it relies on strong ciphers such as the Advanced Encryption Standard (AES) . As a result, adopting WPA2 security is expected to be computationally overloading and requires considerable processing.

The WLAN authentication and privacy infrastructure is another security standard that was developed and adopted in China [10]. The protocol consists of two main security schemes, i.e., the WLAN authentication infrastructure that authenticates user identities and manages keys, and the WLAN privacy infrastructure that protects the data transmitted on WLANs and provides the encryption, data verification, and antireplay functions.

The impact of security protocols on the performance of a WLAN was investigated by researchers in literature. The majority focused on the network throughput, whereas less attention was given to the delay and the jitter. The studies on the impact of security protocols on the performance of a WLAN reported tangible degradation in performance when the WLAN applies strong security protocols [11]–[15].

Potorac and Balan [16] studied the impact of security overheads on the IEEE 802.11 WLAN throughput. They provided theoretical analysis about the impact of three security protocols on system 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 the work in [16], it is possible to observe a smaller throughput or a larger delay, given

Manuscript received November 15, 2014; revised February 28, 2015; accepted April 2, 2015.

T. Hayajneh and K. S. Balagani are with the Department of Computer Science, School of Engineering and Computing Sciences, New York Institute of Technology, New York, NY 10023 USA (e-mail: thayajne@nyit.edu; kbalagan@nyit.edu).

S. Ullah is with the Research Centre in Real-Time and Embedded Computing Systems (CISTER) Research Unit, School of Engineering (ISEP), Polytechnic Institute of Porto (IPP), 4200-135Porto, Portugal (e-mail: sauah@isep.ipp.pt).

B. Mohd is with the Department of Computer Engineering, Faculty of Engineering, Hashemite University, Zarqa 13133, Jordan (e-mail: bassam@hu.edu.jo).

Digital Object Identifier 10.1109/JSYST.2015.2424702

that the communication processor cannot encrypt or decrypt the data flow at the necessary speed. McCarter [17] presented measurements that match the theoretical results presented by Potorac and Balan [16].

It is imperative to provide adequate security and authentication services to wireless networks due to the sensitivity of the applications they carry [18]. However, providing these services, as well as getting a minimum processing delay, is challenging; on one hand, encryption is a heavy process that needs many transformations and calculations, and authentication needs to verify each bit in the message, which consumes time. On the other hand, wireless cards have limited resources, such as low processor speed and limited memory capacity.

In this paper, we propose an enhanced security system for WLANs. Our new design mainly decreases the processing delay and increases both the speed and the throughput, thereby making it particularly suitable for multimedia applications. Our idea is to move the computationally intensive security part to the end systems' CPUs and use a WLAN with disabled security. In fact, with disabled security (open access), a WLAN was shown to have a lower delay or response time, a lower jitter, a higher throughput, and less percentage of dropped packets [3], [6], [8], [9], [13], [19].

At the end hosts, the encryption and authentication services are performed before the data are passed to a radio card. Thus, the expensive security part is applied to the data prior to its delivery to a low-performance processor at the wireless card and computed with the host central processor that is usually powerful. Hence, the delay and the jitter are both expected to be significantly small and negligible.

At the access point (AP), the increasing complexity of security protocols signifies the need to improve the performance of network processing hardware for real-time cryptographic processing. The cryptographic algorithms' throughput and delay can be improved by implementing the algorithms in specialized processors using an application-specified integrated circuit (ASIC) solution or a field-programmable gate array (FPGA) implementation. Although ASIC designs are superior in performance, the FPGA implementation has the advantages of a low cost, reprogrammability, and a short time to market.

Several hardware implementations to enhance the performance of cryptographic algorithms have been proposed in literature. Examples are included in [20] and [21]. Wang *et al.* [20] presented an ASIC implementation with on-the-fly key expansion and a reconfigurable core architecture. The design provides a throughput of up to 3.75 Gb/s at 102 MHz. Chang *et al.* [21] discussed the FPGA implementation of a 32-bit AES algorithm. The design has a low area of 156 slices and a throughput of 876 Mb/s.

Moreover, in this paper, we applied enhanced techniques to implement both the Counter (CTR) Mode with Cipher Block Chaining (CBC) Message Authentication Code Protocol (CCMP) and the CTR protocol. The aim is to have the protocols run with some parallel settings to improve their speeds. The improvement is helpful in achieving a higher speed to process high-data-rate multimedia applications. The proposed enhanced system and the adapted techniques are implemented and tested experimentally. As for the specialized hardware, cryptographic techniques were designed and tested with the FPGA technology.

The rest of this paper is structured as follows. Section II briefs the related research in the field. Section III highlights the main features and issues with WLAN security protocols. Our proposed enhanced system is presented and discussed in Section IV. Section V presents the system implementation and evaluation results. Finally, Section VI concludes this paper.

II. Related Work

The impact of security protocols on the WLAN performance has been studied in literature from different perspectives. In this section, we will highlight some of these studies. Barka and Boulmalf [11] studied the impact of security protocols on the throughput of a WLAN. They considered the impact of WEP and WPA1, and they concluded that adding security causes a decrease in the average network throughput and an increase in the percentage of dropped packets for both Transmission Control Protocol (TCP) traffic and User Datagram Protocol (UDP) traffic. Moreover, they found that WPA1 has the largest impact on the network performance due to the bigger key sizes and the longer processing time.

Kolahi *et al.* [12] evaluated the impact of different security protocols on the network throughput and the round-trip time (RTT) for both the TCP traffic and the UDP traffic. In their study, they considered different operating systems (Windows server 2003, XP, and Vista). Similar to the work in [11], the results showed that using security protocols reduces the throughput and increases the RTT. The increase in the RTT was more noticeable when larger encryption keys are used.

In [13], several experiments were carried out to explore the impact of security protocols on the performance of voice traffic and data traffic in a WLAN. In this study, the delay and the jitter were only tested for the WEP protocol with a 64-bit key size, which is not secure and can be broken in few seconds [7]. The results showed a significant increase in the packet delay and the jitter for the voice traffic.

Gin and Hunt [22] evaluated the impact of the IEEE 802.11i standard security on the network throughput performance with several experimental scenarios. The results showed slight throughput degradation when adding security even with a larger key length.

Begh and Mir [14] used IPTraffic to generate different rates of the TCP and the UDP to quantify the impact of adding security on the network throughput, the transmission delay, and the packet loss. Results were obtained using five different security settings, i.e., no security, WEP-64, WEP-128, WPA-Temporal Key Integrity Protocol (TKIP), and WPA-AES. For traffic rates of 1 and 5 Mb/s, the results showed no major degradation in the network throughput (except for WPA-AES), no significant increase in the transmission time, and an almost negligible packet loss ratio. However, when the traffic rate was increased to 12 Mb/s, noticeable detraction in the performance metrics was noticed. Begh and Mir only performed their experiments with a single wireless station and did not consider WPA2.

Baghaei and Hunt [15] investigated the impact of the WEP protocol on the performance of a WLAN with various settings and key sizes. They concluded that the stronger the security mechanism, the poorer the performance, although the degradation is certainly not linear. Moreover, they found that the response time increased with a stronger security mechanism and when the network is congested. Hayajneh *et al.* [3] studied the impact of security protocols on a WLAN with different security settings. They mainly focused on multimedia applications, and their results showed tangible degradation in the network performance with increased security.

Zhou *et al.* [23] proposed a joint physical–application layer security architecture of wireless multimedia communication. Their idea was to efficiently utilize the available network resources by exploiting the security capacity and signal processing technologies at the physical layer with the authentication and watermarking strategies at the application layer. Moreover, they incorporated the security capacity into security levels and managed to have a tradeoff between the security level and the communication overhead. Finally, they studied the impact of the quality of the security service on wireless multimedia networks.

Zhou and Chao [24] proposed a new media-aware security framework for facilitating various multimedia applications in the Internet of Things. At first, the heterogeneity of the diverse applications was handled by creating methods for multimedia traffic classification and analysis. Based on the classification, they proposed a new media-aware traffic security architecture and management scheme.

III. WLAN Security

As with most wireless technologies, the security in a WLAN is one of its main weaknesses. The communication medium, where any malicious attacker can inject bogus messages, is open and shared among the users. In this section, we provide a brief description of the IEEE 802.11 security protocols (WEP, WPA1, and WPA2) and highlight their main features and issues.

A. WEP

The WEP protocol is the first security protocol for WLANs [6] that was designed as a part of the original IEEE 802.11 standard. Its intended purpose was to provide security to a WLAN that is equivalent to the security of wired networks. WEP uses the Rivest Cipher 4 (RC4) stream cipher for confidentiality and the 32-bit cyclic redundancy check (CRC-32) for integrity. WEP has been known to be insecure since 2001, and Tews and Beck [7] 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, one can break the WEP security within minutes.

B. WPA1

WPA1 [8] was designed to overcome the security limitations of the WEP protocol. WPA1 implements most of the IEEE 802.11i standard. It uses the TKIP [8] that uses a per-packet key. Hence, unlike WEP, a new 128-bit key is dynamically generated for each packet. Consequently, most of the attacks that compromised WEP were prevented. WPA1 replaced the insecure CRC that was used in WEP with a stronger message integrity check. Although WPA1 addressed most of the problems that existed in WEP, it continues to show some security limitations such as relying on the stream cipher and having cryptographically weak integrity (the Michael algorithm). Moen *et al.* [9] discovered weaknesses in the temporal key hash of WPA1. Moreover, Tews and Beck [7] presented the details of a potential attack to break WPA1.

C. WPA2

WPA2 [8], which is also referred to as IEEE 802.11i, replaces WPA1 and implements the mandatory elements of the IEEE 802.11i standard. It uses a new AES-based encryption mode CCMP that is highly secure. This resolved the security issue with the TKIP in WPA1. WPA2 provides an RSN including two new protocols, i.e., the four-way handshake and the group key handshake. As elaborated earlier, Tews and Beck [7] and Vanhoef and Piessens [25] showed that WPA and WEP have major security flaws; hence, ZDNet reported that WEP and the TKIP should be disallowed on WiFi. This leaves WPA2 as the only security option without known or exploited security flaws.

Despite the fact that WPA2 provided a strong security solution to WLANs, potential flaws in the algorithms that were adopted by WPA2 remain questionable. For example, Junaid *et al.* [19] and Khan *et al.* [26] showed that the initial counter value used in the CCMP can be predicted and that WPA2 is subject to dictionary attacks. Moreover, Mitchell and He [27] concluded that, in the CCMP, management frames and control frames are neither encrypted nor authenticated by the link-layer encryption algorithm and are therefore vulnerable to several threats, which were discussed in their paper. In addition, they expected the CCMP to have some impact on the system's performance as it requires some hardware upgrades.

IV. Proposed Enhanced System

A. Main Idea

In this section, we present the main idea of our new approach to provide security in a WLAN while reducing the impact on the performance of the network. As we elaborated earlier, the proposed approach is based on the fact that disabling the security in a WLAN results in a higher throughput and significantly lower delay and jitter. This fact was also agreed upon in other research papers [3], [11], [12], [14], [15].

In this paper, we propose a solution to overcome the performance degradation caused by using strong security protocols in WLANs. The idea is to move the heavy security part to the end systems' CPUs and use a WLAN with a setting similar to disabled security. With open access (disabled security), a WLAN has the following advantages:

a) a higher throughput, which is also shown in [11], [12], [14], and [15];
b) a lower delay or response time, which is also shown in [12]–[14];
c) Less percentage of dropped packets, which is also shown in [11].

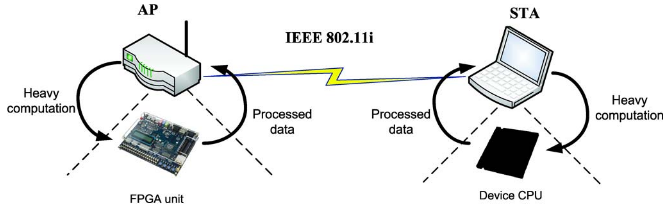


Fig. 1. Idea of the enhanced security system.

The heavy security part, i.e., authentication and encryption, is to be applied to the data prior to its delivery to the processor at the wireless card that typically has low performance. At the end hosts, the encryption and authentication services are performed before the data are passed to the radio card. Hence, the computationally expensive cryptographic components are computed with the host CPU that is usually powerful and can process the encryption in much less time compared with the radio card processor. Hence, with the proposed system, the delay and the jitter are both expected to be significantly small and negligible, thereby making the proposed system highly efficient for multimedia applications.

At the AP, the cryptographic algorithms' throughput and delay can be significantly improved by implementing the algorithms in specialized processors using the ASIC solution or the FPGA implementation. Although ASIC designs are superior in performance, the FPGA implementation has the advantages of a low cost, reprogrammability, and a short time to market.

The decomposition of an algorithm (e.g., the security protocol) into two software and hardware components is the essence of the partitioning problem in system design [28]. Partitioning primarily groups the algorithm instructions (e.g., steps) into blocks/functions and maps them to either a software implementation or a hardware implementation. To strive for optimum partitioning, a designer must carefully balance the desired performance gains, the increased resources/complexity (of area/power/energy), and the communication overhead amongst the implementations. In this paper, we decided to move the computation-intensive security part to the end systems' CPUs (which typically employ a power processor), as well as map the AP network processing to the FPGA design. This partitioning relieves the resource-constrained AP from intensive computations and improves its network performance.

Fig. 1 illustrates the idea of the proposed solution. The laptops (or hosts) move the expensive cryptographic operations to the main CPU (which is usually powerful). On the other hand, at the AP, the FPGA processor performs for all the encryption and authentication processing that are required by the security protocols.

The proposed solution is only considered successful if it causes a negative impact on the performance that is less than the impact caused by the standard WPA2. As for the impact on the throughput, Potorac and Balan [17] analytically proved that the overheads 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 what follows, we implement and test the proposed system to analyze its impact on the delay and the jitter, which are the key metrics for multimedia applications. Furthermore, we will also present the details of implementing the design of our proposed system in the FPGA technology and evaluate its performance.

B. Our WPA2 Modifications

The structure of the IEEE 802.11i RSN consists of five distinct phases of operation. The main components are the authentication server (AS), the AP, the mobile station (STA), and the end station. The five phases are as follows [5].

a) Discovery: The AP advertises its security policy using messages called beacons and probe responses that are used by the STA to identify an AP for a WLAN with which it wishes to communicate. Then, the STA associates with the AP based on the choices presented by the beacons and probe responses. The STA picks the cipher suite and the authentication mechanism.
b) Authentication: In this phase, the STA and the AS prove their identities to each other. The role of the AP is to only forward traffic between the STA and the AS, and to block nonauthenticated traffic until the authentication transaction is successful.
c) Key generation and distribution: The AP and the STA exchange few challenge–response messages that create shared cryptographic keys between them. Two key hierarchies are defined by the IEEE 802.11i standard to specify the interrelations of the keys [5]. The two key hierarchies are the pairwise key hierarchy, which is designed for unicast traffic protection, and the group key hierarchy, which is intended for multicast/broadcast traffic protection.
d) Protected data transfer: Through the AP, frames are exchanged between the STA and the end station. However, security is not provided end-to-end, and secure data transfer only occurs between the STA and the AP.
e) Connection termination: In this phase, the secure connection is torn down, and the connection is restored to the original state.

As observed from the phases of operation of the IEEE 802.11 RNS, during the first three phases, the STA and the AP exchange the security policy and securely establish the cryptographic keys. Afterward, the data are only securely transferred between the AP and the STA, whereas it is the organizations' responsibility to provide security for the data transfer between the AP and the rest of the system.

In this paper, our proposed system modifies the phases of operation of the IEEE 802.11i standard, as illustrated in Fig. 2. In particular, after the third phase when the cryptographic keys are ready and securely shared between the AP and the STA, these keys are transferred to the operating system at the STA so that the CPU performs data encryption and authentication. Since the IEEE 802.11i standard allows the STA and the AP to select and use several cryptographic algorithms, the operating system is also informed about the chosen algorithms. Accordingly, in phase four, the wireless card directly transfers the received data to the AP without performing any encryption or authentication. Similarly, at the AP, the cryptographic operations (encryption

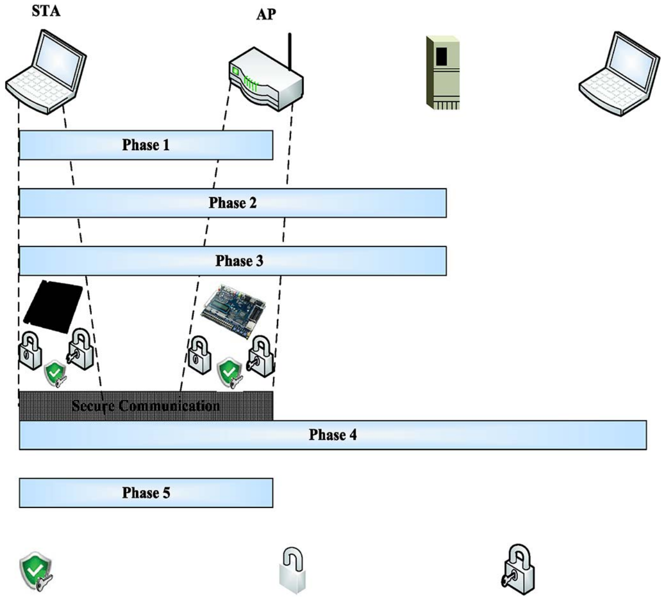


Fig. 2. IEEE 802.11i modified phases of operation.

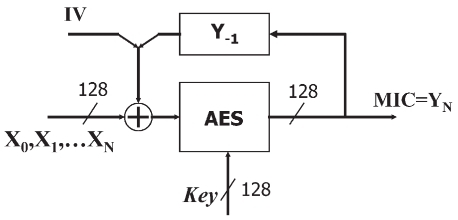


Fig. 3. Standard CBC diagram.

and authentication) are carried by the specialized hardware (the FPGA in our implementation).

The TKIP uses RC4 and the Michael message integrity code (MIC), and they were broken with the practical attack presented by Tews and Beck [7]; hence, the TKIP is not suitable for high-assurance environments. In our implementation, we used the CCMP, which is based on the CCM, which is a generic authenticated encryption block cipher mode of the AES. According to the IEEE 802.11i standard, the CCMP is mandatory for all RSN compliance and is known to be secure.

C. *Improvements on CCMP and CTR*

The main issue with the encryption and authentication techniques used in the CCMP is that it could be slow on both the AP and the network interface controller (NIC) card. The MIC computation with the CBC mode is a recursive process as each step depends on the encrypted output of the previous step, and so on. Thus, we have to wait all the way to the last block to get the MIC as it is a series of operations, as shown in Fig. 3. This process limits the maximum throughput of the algorithm and increases the time to compute the MIC.

One approach to improve the performance is to break the chain into two or more subchains, where the final output is the XOR of the output of all the subchains. In our implementation, we considered breaking the CBC chain to two parts, as shown in Fig. 4. Thus, theoretically, it is expected to reduce the time by half. We will also present testing results in which this process is broken into two, four, and eight chains.

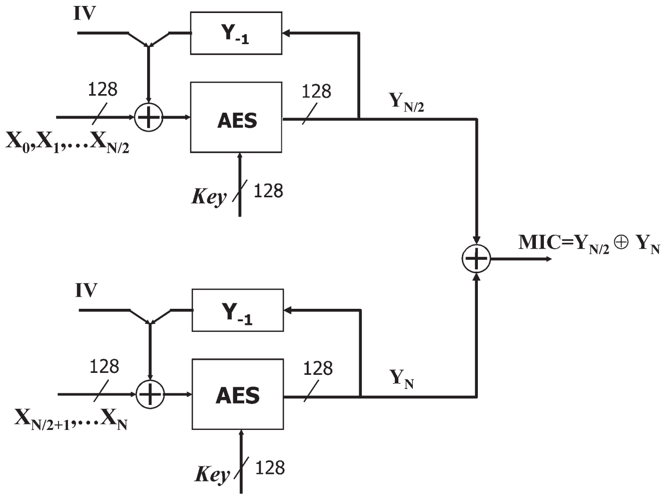


Fig. 4. Parallel CBC diagram.

As for the CTR mode, it can be also done in parallel over multiple blocks of plaintext or ciphertext. Researchers agreed that the CTR throughput is related to the amount of parallelism that is achieved [29]. Thus, in our implementation, we have used two parallel AESs in the CTR mode to improve the throughput and the speed. Furthermore, we present testing results for two, four, and eight parallel settings.

V. System Implementation and Results

A. *Experimental Testing*

We first examine the impact of the security protocols on the performance of a WLAN by conducting experiments over a simple test bed. The performance of the network is examined under four conditions, i.e., disabled security, WEP, WPA1, and WPA2. Special attention is given to the impact of the security protocols on the performance of the WLAN in high-data-rate multimedia applications. These applications are most sensitive to metrics such as the delay and the jitter; hence, these two performance metrics were the focus in our experiments.

The test-bed scenario consists of four laptops and one AP. The specification of the devices is as follows:

1) Linksys E2000 Cisco Advanced Wireless-N Router with the following specifications:
   a) supports up to 11 channels;
   b) supports 802.11n, 802.11a, 802.11g, 802.11b, 802.3, 802.3u, and 802.3ab standards;
   c) security features: WEP, WPA, and WPA2;
   d) security key bits: up to 128-bit encryption;

2) Acer notebooks with the following specifications:
   a) model: Acer Intel core i5, with a 2.24-GHz processor;
   b) NIC model: Realtek register-transfer level (RTL) Gigabit Family;
   c) Operating system: Ubuntu 11.04.

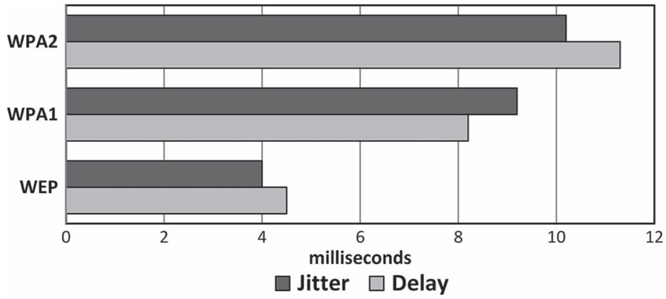


Fig. 5. Delay and jitter with security settings.

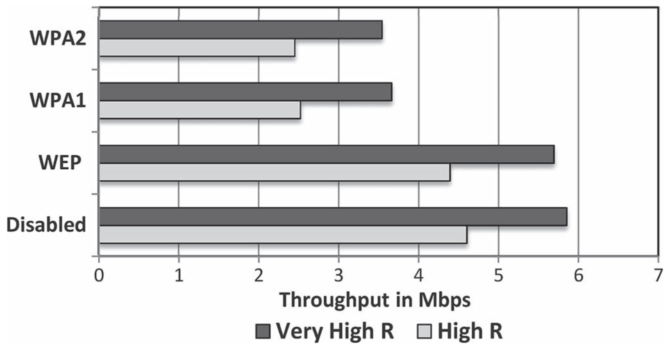


Fig. 6. Throughput with security settings.

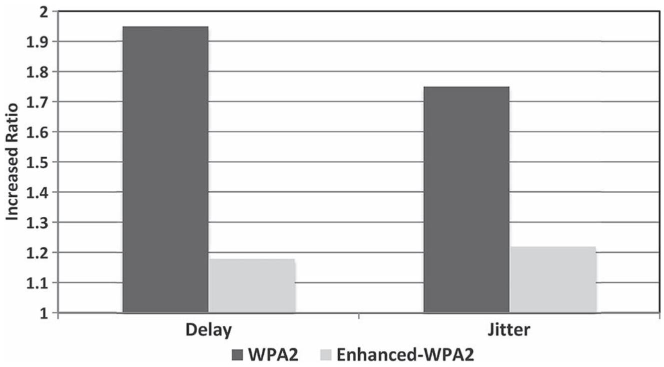


Fig. 7. WPA2 and Enhanced-WPA2 comparison.

TABLE I
MIC With the CCMP Timing Results in Microseconds

Processor	Std.	Parallel settings		
		2	4	8
i5	40	29	24	22
i7	38	28	24	19
AMD 6-Core	34	25	20	18

TABLE II
AES CTR-Mode Timing Results in Microseconds

Processor	Std.	Parallel settings		
		2	4	8
Intel Core i5	47	35	28	25
Intel Core i7	44	35	22	20
AMD 6-Core	38	27	21	19

While conducting our experiments, the devices were adjacent (2–3 m) and isolated from other WiFi networks in the area to avoid potential interference and coexistence issues [30]. The experiments were all performed in the same location and within a short period of time. This makes it likely that the potential impact of multifading or the coexistence of other WLANs would be similar for all the experimental scenarios.

We examined the effect of several security protocols on the performance of a WLAN with multimedia applications. In our scenarios, we transmitted high-definition video steaming traffic between the wireless hosts. The throughput, the delay, and the jitter for the four security settings, i.e., disabled security, WEP, WPA1, and WAP2, were analyzed.

Fig. 5 shows the total average end-to-end round-trip delay and jitter in milliseconds for the packets transmitted between the two wireless hosts for the WEP, WPA1, and WAP2 security protocols. The values in Fig. 5 were neutralized by subtracting the delay and jitter values for the disabled-security case from the WEP, WPA1, and WAP2 security protocol cases. The results in Fig. 5 show that noticeable degradation in the performance occurred when enabling security protocols in the WLAN. Specifically, the delay and the jitter, which are the key metrics for multimedia applications, were significantly increased.

Similarly, Fig. 6 shows the throughput in megabits per second for two data rate scenarios (high-data-rate and very-high-data-rate scenarios) with the four security setting cases, i.e., disabled security, WEP, WAP1, and WPA2. This figure shows that WEP has no tangible impact on the throughput. This is because WEP is known to be light and does not cause a large overhead. However, as for the WPA1 and WPA2 protocols, the throughput was affected with the very-high-data-rate case. This indicates that the multimedia traffic overwhelmed the network capacity. The throughput in the high-rate scenario was higher compared with that in the very-high-rate scenario.

The proposed system, which is referred to as Enhanced-WPA2, is also implemented and tested using the same test-bed settings. Fig. 7 shows the increased ratio (as compared with the disabled-security case) in the delay and the jitter for the WPA2 security and the proposed Enhanced-WPA2 system. The results in Fig. 7 show that our Enhanced-WPA2 system only increased the delay and jitter values by approximately 20% compared with the disabled-security case. On the other hand, WPA2 has almost doubled the values of the delay and the jitter. These results were obtained for the Enhanced-WPA2 system without the parallel setting suggested in the previous section. With the parallel CBC and CTR settings, we obtained a speed of up to 3.85. These results vary depending on the type of traffic that run on the network; however, the improvement was more significant with the high-rate multimedia traffic.

We have further tested our proposed security system by running the encryption and authentication services on the end hosts' CPU. Table I shows the timing results for running the MIC with the CCMP on an Intel Core i5, Intel Core i7, and AMD 6-Core processors with standard and several parallel settings of two, four, and eight. Similarly, Table II shows the timing results for running the AES in the CTR encryption mode using the same CPUs and settings. The results confirm our

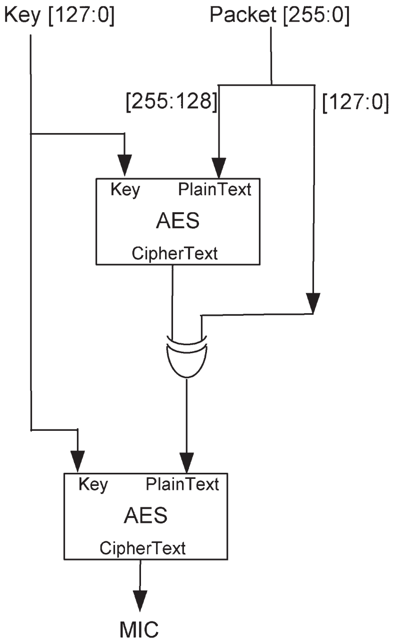


Fig. 8. CBC hardware design.

thesis that running the authentication and encryption services with the powerful CPU at the end hosts results in small or negligible delays (20–40 μs) compared with the delay that occurred at the NIC card (10–50 ms).

B. Hardware Design

Numerous technology options could be used to realize the encryption algorithms in the hardware. In this paper, we implemented the design in the FPGA technology for the following reasons. In general, the FPGA solution provides a reduced development cost, a shorter time to market, and a flexible and configurable design. Additionally, the embedded resources in the processors and random access memory devices enhance the speed of the arithmetic operations, such as the Galois field operations [31]. Understandably, the price of the flexibility is lower performance [32].

The flexibility provided by reconfiguring and reprogramming the hardware design is a great feature of the FPGA technology. It facilitates algorithm agility (i.e., the switching of algorithms during operation), algorithm upload (i.e., upgrading the device with a new algorithm), and algorithm modification [33]. For instance, it is desirable in some cases to upload proprietary S-boxes instead of the standard S-boxes. The FPGA design allows the replacement of S-boxes. Another example is updating the elliptic curve cryptography implementation by modifying the curve parameters' hardware implementations [31]. In [34], it was noted that a reconfigurable hardware design is capable of evolving with algorithms and resisting new strains of attacks.

Realizing the encryption algorithm on an FPGA board consists of several steps. First, the algorithm is implemented in a hardware description language (HDL), e.g., Verilog$_{\mathrm{TM}}$. The implementation is performed at the RTL. Figs. 8 and 9 show the block diagrams of the implemented CBC and CTR designs, respectively. The HDL design is then verified by dynamic simulations. Dynamic simulations are performed using the Modelsim software tool. Fig. 10 shows the waveform for the input and output signals generated by the AP for the CTR AES encryption. Clearly, Fig. 10 illustrates the correct behavior of the implementation.

After the verification of the HDL code, the code is compiled with the Altera software before it is downloaded on the FPGA board. Initially, the HDL code is compiled using Altera Quartus-II [35], with Cyclone II as the target device [36]. The next step is to analyze the generated results by Quartus-II, including resources, timing, and power reports. In what follows, we discuss the FPGA design results.

Table III highlights the resource utilization results expressed in logical elements (LEs). The number of LEs indicates the area of the synthesized design. LEs are the smallest unit used in the logic circuits implemented in the Altera FPGA. These elements are configured as a combinational circuit, registers, and both. The parallel design understandably requires 2.4, i.e., the number of the standard design LEs, because of the added parallelism.

The timing results for the different implemented designs are summarized in Table IV. The exhibited results include the following categories: the propagation delays from the primary inputs to the register (Tsu), from the register to the primary outputs (Tco), and from register to register (Clk-Clk). As shown in Table IV, the parallel design has slightly shorter timing delays compared with the standard design due to lesser levels of logic. Based on the Modelsim simulations, the total time for the parallel design is 770 ns, whereas the total time for the standard design is 2830 ns. This implies that the speedup ratio is 3.7, which is an outstanding result.

In the power analysis, the signal activities (generated from the Modelsim simulations) are annotated to the synthesized HDL design. The reported power is the core dynamic power that consists of the combinational logic power, the register power, and the clock circuitry power. Table V shows the power dissipation of the standard and parallel designs. Justifiably, the parallel setting consumes more power due to the extra employed resources. Next, the energy consumption is computed by multiplying the design time (see Table IV) by the power dissipation (see Table V). The computed energy numbers, which are listed in Table V, show that the parallel design dissipates less energy.

VI. Conclusion

The security protocols used in WLANs are known to degrade the system performance, which is critical for video streaming and multimedia applications. In this paper, we have proposed an enhanced security system for a WLAN with the objective of decreasing the processing delay and increasing both the speed and the throughput. The proposed system moves the computationally intensive security components to the end systems' CPUs and uses the WLAN with a disabled-security setting. The encryption and authentication services are performed by the end hosts' powerful CPUs before the data are passed to a radio card (which has a relatively less powerful processor). As demonstrated by the results of our experiments, offloading

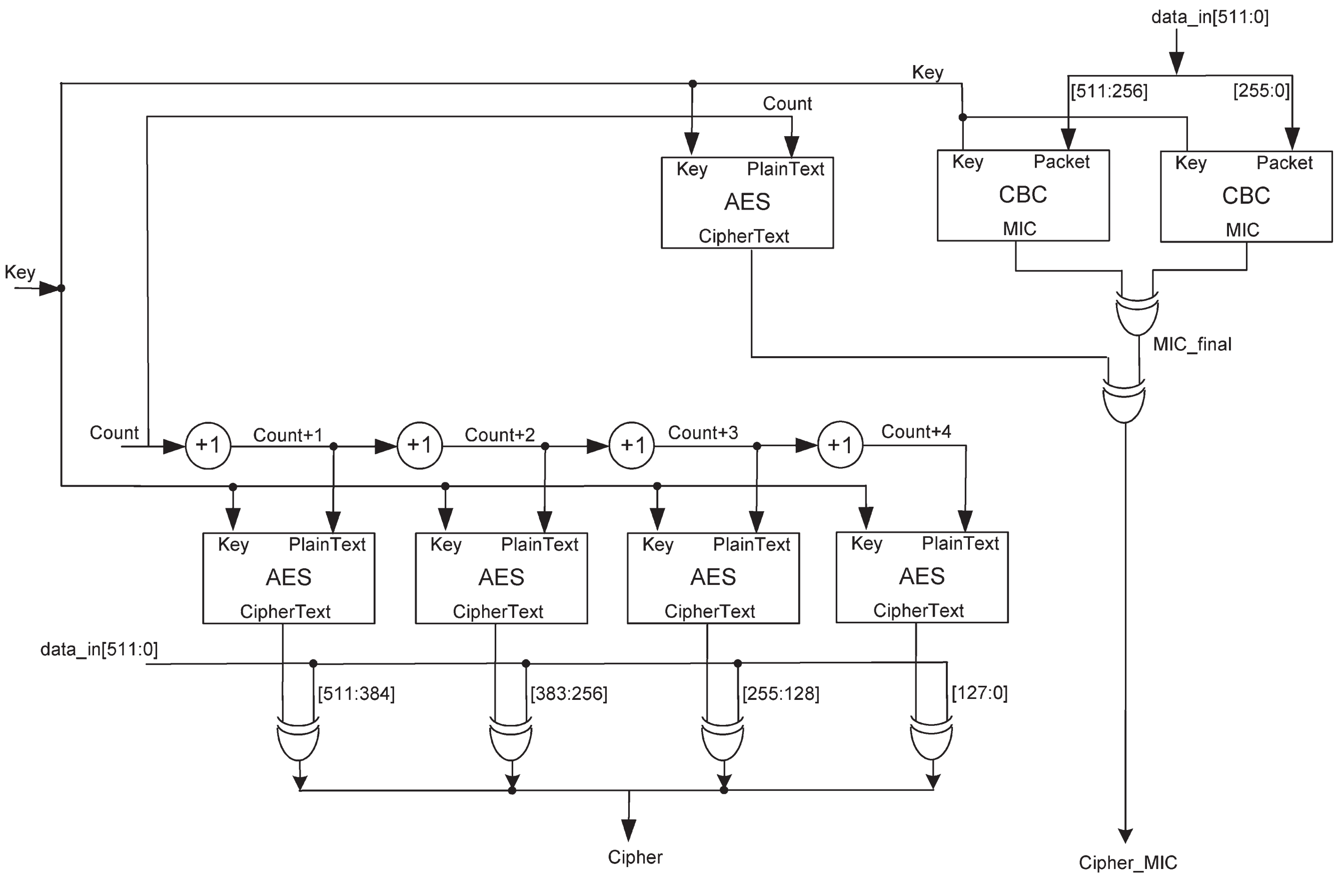
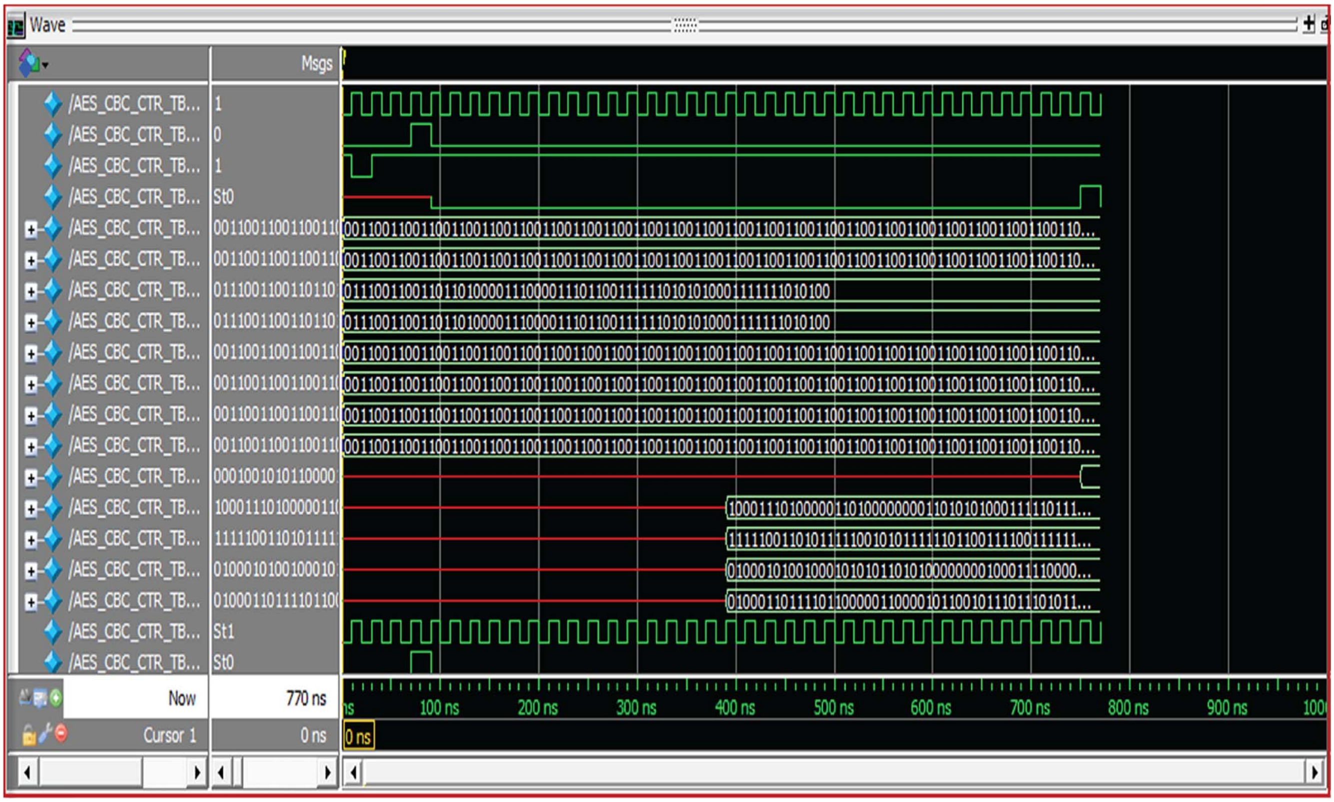


Fig. 9. CTR hardware design.



```
/AES_CBC_CTR_TB... 1
/AES_CBC_CTR_TB... 0
/AES_CBC_CTR_TB... 1
/AES_CBC_CTR_TB... St0
/AES_CBC_CTR_TB... 0011001100110011( 0011001100110011001100110011001100110011001100110011001100110011001100110011001100110011001100110...
/AES_CBC_CTR_TB... 0011001100110011( 0011001100110011001100110011001100110011001100110011001100110011001100110011001100110011001100110...
/AES_CBC_CTR_TB... 011100110011011( 0111001100110110100001110000111011001111110101010001111111010100
/AES_CBC_CTR_TB... 011100110011011( 0111001100110110100001110000111011001111110101010001111111010100
/AES_CBC_CTR_TB... 0011001100110011( 0011001100110011001100110011001100110011001100110011001100110011001100110011001100110011001100110...
/AES_CBC_CTR_TB... 0011001100110011( 0011001100110011001100110011001100110011001100110011001100110011001100110011001100110011001100110...
/AES_CBC_CTR_TB... 0011001100110011( 0011001100110011001100110011001100110011001100110011001100110011001100110011001100110011001100110...
/AES_CBC_CTR_TB... 0011001100110011( 0011001100110011001100110011001100110011001100110011001100110011001100110011001100110011001100110...
/AES_CBC_CTR_TB... 0001001010110000
/AES_CBC_CTR_TB... 100011101000001 10001110100000110100000000110101010001111110111...
/AES_CBC_CTR_TB... 1111100110101111 11111001101011111001010111111011001110011111 1...
/AES_CBC_CTR_TB... 0100010100100010 0100010100100010101011010100000000100011110000...
/AES_CBC_CTR_TB... 0100011011110110( 0100011011110110000011000010110010111011101011...
/AES_CBC_CTR_TB... St1
/AES_CBC_CTR_TB... St0
```

Fig. 10. Modelsim wave diagram at the AP.

TABLE III
RESOURCE UTILIZATION

Algorithm	LEs	LE type		
		Combinational	Register	Both
Standard	13307	9704	2244	1359
Parallel	31314	26510	1664	3140

TABLE IV
TIMING ANALYSIS (IN NANOSECONDS)

Algorithm	Tsu	Tco	Clk-Clk
Standard CBC	3.3	13.7	12.4
Parallel CBC	7.4	14.7	11.4

TABLE V
POWER AND ENERGY RESULTS

Algorithm	Power (mW)	Energy (nJ)
Standard CBC	82.4	233
Parallel CBC	124.7	96

security-related computations to the end hosts significantly decreased the delay and the jitter. At the AP, the data were encrypted and authenticated using a specialized processor. Our experiments showed that the time to perform data encryption and authentication at the end hosts' CPUs (e.g. Intel Core i5, i7, and AMD 6-Core) is orders of magnitude lower than when performed using the wireless card. Moreover, our proposed security system achieved improvement in the speed of up to 3.7 compared with the standard WPA2. Finally, we implemented our proposed system in the FPGA technology. Quartus-II was used to analyze the design in terms of resources, timing, and power.

REFERENCES

[1] T. Hayajneh and G. Al-Mashaqbeh, "Multimedia traffic over WLANs: QoS support and performance evaluation," in *Proc. 5th ICICS*, 2014, pp. 1–6.

[2] T. Hayajneh, B. J. Mohd, A. Itradat, and A. N. Quttoum, "Performance and information security evaluation with firewalls." *Int. J. Security Appl.*, vol. 7, no. 6, pp. 355–372, 2013.

[3] T. Hayajneh, B. J. Mohd, A. Itradat, and A. N. Quttoum, "Analyzing the impact of security protocols on wireless LAN with multimedia applications," in *Proc. 6th Int. Conf. SECURWARE*, pp. 169–175, 2012.

[4] N. Tadayon, E. Askari, S. Aissa, and M. Khabazian, "A novel analytical model for service delay in IEEE 802.11 networks," *IEEE Syst. J.*, vol. 6, no. 4, pp. 627–634, Dec. 2012.

[5] S. Frankel, B. Eydt, L. Owens, and K. Scarfone, "Establishing wireless robust security networks: A guide to IEEE 802.11 i," Nat. Inst. Std. Technol., Gaithersburg, MD, USA, 2007.

[6] *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, NY, USA, 1999.

[7] E. Tews and M. Beck, "Practical attacks against WEP and WPA," in *Proc. 2nd ACM Conf. Wireless Netw. Security*, 2009, pp. 79–86.

[8] *Amendment 6 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Draft 3*, ANSI/IEEE Std. 802.11i, 2003.

[9] V. Moen, H. Raddum, and K. J. Hole, "Weaknesses in the temporal key hash of WPA," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 8, no. 2, pp. 76–83, Apr. 2004.

[10] *Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Network-Specific Requirements-Parts 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1*, Gb 15629.11-2003-xg1-2006, 2006.

[11] E. Barka and M. Boulmalf, "On the impact of security on the performance of WLANs," *J. Commun.*, vol. 2, no. 4, pp. 10–17, Jun. 2007.

[12] S. S. Kolahi, S. Narayan, D. D. Nguyen, Y. Sunarto, and P. Mani, "The impact of wireless LAN security on performance of different windows operating systems," in *Proc. IEEE ISCC*, 2008, pp. 260–264.

[13] M. Boulmalf, E. Barka, and A. Lakas, "Analysis of the effect of security on data and voice traffic in WLAN," *Comput. Commun.*, vol. 30, no. 11, pp. 2468–2477, Sep. 2007.

[14] G. R. Begh and A. H. Mir, "Quantification of the effect of security on performance in wireless LANs," in *Proc. 3rd Int. Conf. SECURWARE*, 2009, pp. 57–62.

[15] N. Baghaei and R. Hunt, "Security performance of loaded IEEE 802.11 b wireless networks," *Comput. commun.*, vol. 27, no. 17, pp. 1746–1756, Nov. 2004.

[16] A. D. Potorac and D. Balan, "The impact of security overheads on 802.11 WLAN throughput," *J. Comput. Sci. Control Syst.*, vol. 2, no. 1, pp. 47–52, 2009.

[17] H. L. McCarter, "analyzing wireless LAN security overhead," Ph.D. dissertation, Virginia Polytechnic Inst. State Univ., Blacksburg, VA, USA, 2006.

[18] V. Namboodiri, V. Aravinthan, S. N. Mohapatra, B. Karimi, and W. Jewell, "Toward a secure wireless-based home area network for metering in smart grids," *IEEE Syst. J.*, vol. 8, no. 2, pp. 509–520, Jun. 2014.

[19] M. Junaid, M. Mufti, and M. U. Ilyas, "Vulnerabilities of IEEE 802.11 i wireless LAN CCMP protocol," *Trans. Eng., Comput. Technol.*, vol. 11, pp. 228–233, Feb. 2006.

[20] M.-Y. Wang, C.-P. Su, C.-L. Horng, C.-W. Wu, and C.-T. Huang, "Single- and multi-core configurable AES architectures for flexible security," *IEEE Trans. VLSI*, vol. 18, no. 4, pp. 541–552, Apr. 2010.

[21] C.-J. Chang, C.-W. Huang, K.-H. Chang, Y.-C. Chen, and C.-C. Hsieh, "High throughput 32-bit AES implementation in FPGA," in *Proc. IEEE APCCAS*, 2008, pp. 1806–1809.

[22] A. Gin and R. Hunt, "Performance analysis of evolving wireless IEEE 802.11 security architectures," in *Proc. Int. Conf. Mobile Technol., Appl., Syst.*, 2008, pp. 101–106.

[23] L. Zhou, D. Wu, B. Zheng, and M. Guizani, "Joint physical-application layer security for wireless multimedia delivery," *IEEE Commun. Mag.*, vol. 52, no. 3, pp. 66–72, Mar. 2014.

[24] L. Zhou and H.-C. Chao, "Multimedia traffic security architecture for the internet of things," *IEEE Netw.*, vol. 25, no. 3, pp. 35–40, May/Jun. 2011.

[25] M. Vanhoef and F. Piessens, "Practical verification of WPA-TKIP vulnerabilities," in *Proc. 8th ACM SIGSAC Symp. Inf., Comput. Commun. Security*, 2013, pp. 427–436.

[26] M. A. Khan, A. R. Cheema, and A. Hasan, "Improved nonce construction scheme for AES CCMP to evade initial counter prediction," in *Proc. 9th ACIS Int. Conf. SNPD*, 2008, pp. 307–311.

[27] J. C. Mitchell and C. He, "Security analysis and improvements for IEEE 802.11 i," in *Proc. 12th Annu. NDSS*, 2005, pp. 90–110.

[28] R. Sass and A. G. Schmidt, *Embedded Systems Design With Platform FPGAs: Principles and Practices*. San Mateo, CA, USA: Morgan Kaufmann, 2010.

[29] W. Stallings, *Cryptography and Network Security, 6/E*, New York, NY, USA: Pearson Education, 2014.

[30] T. Hayajneh, G. Almashaqbeh, S. Ullah, and A. V. Vasilakos, "A survey of wireless technologies coexistence in WBAN: Analysis and open research issues," *Wireless Netw.*, vol. 20, no. 8, pp. 2165–2199, Nov. 2014.

[31] A. De la Piedra, A. Braeken, and A. Touhafi, "Sensor systems based on FPGAs and their applications: A survey," *Sensors*, vol. 12, no. 9, pp. 12 235–12 264, 2012.

[32] I. Kuon and J. Rose, "Measuring the gap between FPGAs and ASICs," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 26, no. 2, no. 2, pp. 203–215, Feb. 2007.

[33] T. Wollinger, J. Guajardo, and C. Paar, "Security on FPGAs: State-of-the-art implementations and attacks," *ACM TECS*, vol. 3, no. 3, pp. 534–574, Aug. 2004.

[34] L. Bossuet, M. Grand, L. Gaspar, V. Fischer, and G. Gogniat, "Architectures of flexible symmetric key crypto engines a survey: From hardware coprocessor to multi-crypto-processor system on chip," *ACM CSUR*, vol. 45, no. 4, p. 41, Aug. 2013.

[35] "Quartus ii Introduction Using Verilog Designs," Altera Inc., San Jose, CA, USA. [Online]. Available: ftp://ftp.altera.com/up/pub/Altera-Material/9.1/Tutorials/Verilog/Quartus-II-Introduction.pdf

[36] "Cyclone ii Architecture." [Online]. Available: http://www.altera.com/literature/hb/cyc2/cyc2_cii51002.pdf

Thaier Hayajneh (M'15) received the B.S. and M.S. degrees in electrical and computer engineering from Jordan University of Science and Technology, Irbid, Jordan, in 1997 and 1999, respectively, and the M.S. and Ph.D. degrees in computer and network security from the University of Pittsburgh, Pittsburgh, PA, USA, in 2005 and 2009, respectively.

He is currently an Assistant Professor with the Department of Computer Science, School of Engineering and Computing Sciences, New York Institute of Technology, New York, NY, USA. From 2009 to 2014, he worked as the Chair of and an Associate Professor with the Department of Computer Engineering, Hashemite University, Zarqa, Jordan. He is the author or coauthor of over 30 papers in peer-reviewed journals and international conferences. His current research interests include information assurance and security, network security and privacy, wireless security, cryptography, steganography, wireless body area networks and medical health monitoring systems, mobile wireless ad hoc and sensor networks, and mobile cloud computing, i.e., the quality of service and security.

Dr. Hayajneh has served as a Reviewer for several prestigious journals, such as the IEEE Transactions on Parallel and Distributed Systems, the IEEE Transactions on Information Forensics and Security, the *IEEE Systems Journal*, *Association for Computing Machinery/Springer Wireless Network (WINET)*, *Springer Wireless Personal Communications*, etc. He has also served on the Technical Program Committees of numerous international conferences, including the IEEE Global Communications Conference (GLOBECOM), the IEEE International Conference on Communications, the IEEE Nuclear Science Symposium, the IEEE International Conference of Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), etc.

Sana Ullah received the Ph.D. degree in information and communication engineering from Inha University, Incheon, Korea, in 2011.

He is currently working as a Research Scientist with the Research Centre in Real-Time and Embedded Computing Systems (CISTER) Research Unit, School of Engineering (ISEP), Polytechnic Institute of Porto (IPP), Porto, Portugal. From 2011 to 2014, he worked as an Assistant Professor with the College of Computer and Information Science, King Saud University, Riyadh, Saudi Arabia.

Dr. Ullah is currently serving as an Editor for the *Springer Journal of Medical Systems*, the *Korean Society for Internet Information Transaction of Internet and Information Systems*, *Wiley Security and Communication Network*, the *Journal of Internet Technology*, and the *International Journal of Autonomous and Adaptive Communications Systems*. He served as a Guest Editor for many top journals, including the *Elsevier Journal of Information Science*, the *Springer Journal of Medical System*, and the *Springer Journal of Telecommunication Systems*. He also served as a Cochair/Technical Program Committee Member for a number of international conferences, including the International Conference on Body Area Networks (BodyNets); the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC); the IEEE International Conference on E-health Networking, Application and Services (Healthcom); the IEEE Global Communications Conference (GLOBECOM); and the IEEE Wireless Communications and Networking Conference.

Bassam J. Mohd received the B.S. degree in computer engineering from the King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia, in 1990; the M.S. degree in computer engineering from the University of Louisiana, Lafayette, LA, USA, in 1992; and the Ph.D. degree from the University of Texas at Austin, Austin, TX, USA, in 2008.

He has worked for several semiconductor companies, including Intel, SUN, Synopsys, and Qualcomm. He is currently an Assistant Professor with the Department of Computer Engineering, Faculty of Engineering, Hashemite University, Zarqa, Jordan. His research interests include digital signal processor designs, steganographic processors, encryption processors, and power reduction/estimation techniques.

Kiran S. Balagani (M'09) received the B.S. degree from Bangalore University, Bengaluru, India, and two M.S. degrees and the Ph.D. degree from Louisiana Tech University, Ruston, LA, USA.

He is currently an Assistant Professor of computer science with the Department of Computer Science, School of Engineering and Computing Sciences, New York Institute of Technology, New York, NY, USA. He is the author or coauthor of works published in several peer-reviewed journals, including the IEEE Transactions on Pattern Analysis and Machine Intelligence, the IEEE Transactions on Information Forensics and Security, the IEEE Transactions on Knowledge and Data Engineering, the IEEE Transactions on Systems, Man, and Cybernetics, and *Pattern Recognition Letters*. He is the holder of three U.S. patents in network-centric attack detection. His teaching interests include the development of graduate and undergraduate courses in network security and biometrics. His research interests include cyberbehavioral anomaly detection (e.g., unauthorized user-access behaviors), behavioral biometrics, and privacy-preserving biometrics.