Towards a Reconfigurable Platform to Implement Security Architectures of Wireless Communications Standards Based on the AES-CCM Algorithm

Ignacio Algredo-Badillo[1], Claudia Feregrino-Uribe[2], René Cumplido[2], and Miguel Morales-Sandoval[3]

[1] University of Istmo, Campus Tehuantepec,
Computer Engineering
Ciudad Universitaria S/N, Sto. Domingo Tehuantepec, Oax., Mexico. 70760.
algredobadillo@sandunga.unistmo.edu.mx
[2] National Institute for Astrophysics, Optics and Electronics,
Sta. Ma. Tonantzintla, Pue., Mexico,
cferegrino@inaoep.mx, rcumplido@inaoep.mx,
[3] Polytechnic University of Victoria
Information Technology Department
Calzada Luis Caballero No. 1200
Cd. Victoria, Tamps., Mexico. 87070
mmoraless@upv.edu.mx

Abstract. Over decades the design of communication devices has been mainly focused on hardware, where upgrading a design meant to completely abandon it and start a new design. For modern communication networks, the ideal device is the one capable of operating in different networks employing basically the same hardware resources. Recently, software radios offer the capability of being multiband, multimode, software-intensive radios. A key element in software radios is security, this is because these devices are able to access different wireless networks and employ the atmosphere as transmission medium, thus may be vulnerable to malicious attacks when data are transmitted. Several security architectures have been standardized for different networks, such as IEEE 802.11i-2004 for WLANs (Wireless Local Area Networks) and IEEE 802.16e-2005 for WMANs (Wireless Metropolitan Area Networks), operating on the MAC (Medium Access Control) sublayer. This chapter shows how by means of the software radio paradigm, two hardware implementations of these standard security architectures can be implemented in a single and flexible platform.

1 Introduction

In digital communications, mobility is a desirable feature that has motivated the development and the growth of wireless systems. Wireless networks use different set of rules or protocols for governing communication among diverse devices, and each network can support different applications that in turn can use

different protocols. Ideally, a device should operate in diverse applications on different wireless networks. This desired feature motivated the development of the software radio devices, which are radios able to operate with different hardware/software configurations in order to support the functions needed to access different communication networks. Software radios have evolved in response to advances in the technology. Initially, only basic radio architectures were available, these radios then evolved to software capable radios, then into software programmable radios, and finally to software-defined radios (SDR). Future developments will be focused on cognitive radios that will provide new capabilities in order to support more complex functions, such as: awareness, adaptability and the ability to learn, see Fig. 1 [1].

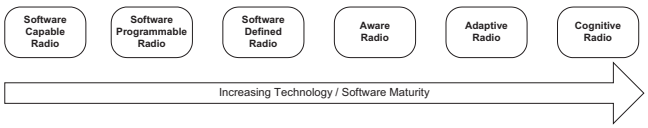

Fig. 1. Evolution of the software radios.

Radio processing platforms usually combine the use of highly efficient Application Specific Integrated Circuits (ASICs) and very flexible programmable General Purpose Processors (GPPs) or Digital Signal Processors (DSPs). ASICs are well suited for performing dedicated functions like A/D converters and are extensively used to build digital receivers that require custom hardware structures to operate in real time. GPPs and DSPs are preferred for performing tasks that carry out some sort of data analysis or decision making which depend on a particular operation mode or application.

After the received signal is digitalized by the A/D converter, all required operations in modern radio systems are executed by digital hardware. This digital signal processing hardware has been traditionally hardwired to achieve the highest possible performance. However, this customization has limited the development of processing platforms with enough flexibility to operate on networks that use different standards.

The development of software radios is currently focused on the lower layers of the OSI model, which are normally implemented in hardware [2]. A key element in software radios is security, this is because these devices are able to access different wireless networks and employ the atmosphere as transmission medium, thus may be vulnerable to malicious attacks when data are transmitted. A number of solutions have been developed to protect these networks. These solutions are based on a variety of techniques and algortihms, examples are: firewalls, cryptography, antivirus, intrusion detectors, secure routing, and security policy management. One of the most important security mechanisms are based on cryptographic algorithms that are used on different operation modes. Security

based in cryptography has become a key element in recent standards of wireless communication networks.

Systems must be able to deal with the extra computations required by the use of cryptographic algorithms, especially in demanding applications that transmit large amounts of data. Cryptographic algorithms are characterized by a large number of complex operations, that may result in system processing bottlenecks. It is important to highlight that hardware cryptographic implementations have shown to have better performance than software only implementations. Hardware architectures are able to better exploit the parallelism of cryptographic algorithms and also, when compared against general purpose processors, are better suited to perform operations directly on bits or values represented by different word sizes.

Reconfigurable logic devices, in particular FPGAs, are becoming an increasingly important part of software radio platforms. Current FPGA devices offer a number of features that make them suitable to efficiently perform a large number of functions and tasks required to implement digital communications systems. Among these features we can find dedicated hardware multipliers, flexible memory structures, plenty of I/O pins, gigabit serial transceivers and other user-configurable system interfaces, and high density of logic slices. All these features combined with the availability of new and powerful design tools allow engineers to deal with very complex design is a relatively short time. In addition, it is now also possible to acquire highly efficient intellectual property (IP) cores from specialized vendors. This plethora of cores that are ready to drop into the FPGA, allows building complex application-specific architectures. Like ASICs, all functions implemented in FPGAs can potentially be executed in parallel. This ability of performing a large number of operations in parallel and the availability of distributing memory along the signal path results in highly efficient architectures. Also, unlike GPPs and DSPs, FPGAs offer the possibility of assigning to each variable exactly the number of bits required. All the advantages offered by configurable logic devices come at the expense of higher power consumption and in some cases higher costs. Thus, for the foreseeable future it is not possible to think that they can fully replace ASICs, GPPs and DSPs. Instead, the combined use of all these type of devices seems to be the best option to implement complex system like those required in software radio applications.

The main idea of the software radio platforms is to provide support for different applications. These platforms must be able to dynamically reconfigure themselves in order to perform the tasks associated to different access technologies and standards. There are several ways to provide flexible platforms [3], being the use of reconfigurable techniques one of the most promising. Different works have explored these ideas for different applications. For example, in [4], a cognitive radio is presented, and in [5], a DSP/FPGA reconfigurable architecture is described. Few works have focused on evaluating implementations of security algorithms on reconfigurable architectures [6]. In this chapter, the aim is to examine two hardware architectures that implement the security architectures of two wireless communication standards as the first step towards developing a sin-

gle processing reconfigurable platform for security. This platform is developed for software-radio applications operating in the MAC sublayer, which executes different configurations, and in this case, for two protocols of two different networks (WMAN and WLAN). To design this platform, characteristics such as hardware resources, throughput, efficiency and reconfigurable modules, are evaluated.

In this work, two hardware architectures that implement the security architectures of two of the most important wireless communications standards are evaluated. The aim is to evaluate the feasibility of implementing a single hardware module that will be able to provide security services for both standards. The selected standards are the IEEE 802.11i-2004 and IEEE 802.16e-2005.

2 Security Protocols

Security protocols for the widely-used wireless communication networks propose the use cryptographic solutions based on diverse cryptographic algorithms. Security is defined in the MAC sublayer, enabling communication networks to provide the security services of privacy, authentication and confidentiality, based on cryptographic algorithms that use several iterative mathematic operations. These algorithms protect data transmissions at the expense of high computational costs that may cause bottlenecks in the data transmissions, thus to cope with the high speeds of future data transmissions, such as in the wireless networks [7] with application to transmit high-quality TV, movies in DVD, and great amount of digital files using personal computers, architectures with high throughput are required, at least performing at 1 Gbps. The IEEE 802.11i-2004 standard is designed to provide enhanced security in the MAC sublayer for 802.11 networks. In this standard, the security architecture is based on AES-CCMP (AES-CCM Protocol) that in turn is based on the Advanced Encryption Standard (AES) in CCM operation mode to provide robust security features for data transfers.

The Mobile WirelessMAN standard defined by the IEEE 802.16e-2005 amendment to the 802.16-2004, includes better support for Quality of Service and the use of Scalable OFDMA, and is sometimes called 'Mobile WiMAX'. This standard, as well as IEEE 802.11i-2004 standard, proposes to implement the CCM operation mode of the AES algorithm. It has specified security mechanisms to provide better security services, although it is required to execute a great number of operations, several iterations, and multiple processes. In this work, proposed hardware architectures are based on the AES-CCM, using parallelization and modular specialization, and reducing critical path without increasing the execution latency.

IEEE802i-2004 Standard. The IEEE 802.11i-2004 or 802.11i is an amendment to the IEEE 802.11 standard that specifies mechanisms for wireless networks. It supersedes the Wired Equivalent Privacy (WEP) security specification which have inherent weaknesses [8] [9] [10]. As an intermediate solution to WEP insecurities, the Wi-Fi Alliance proposed the Wi-Fi Protected Access (WPA).

IEEE 802.11i-2004 makes use of the AES block cipher, whereas WEP and WPA use the RC4 stream cipher [11].

The components of 802.11i architecture are: 802.1X for authentication [12](implicating the use of EAP -Extensible Authentication Protocol- and an authentication server), Robust Security Networks (RSN) for keeping track of associations, and AES-based CCMP (explained in detail later) to provide data confidentiality, integrity, and origin authentication. Another important element of the authentication process is a four-way handshake, a pairwise key management protocol. The IEEE 802.11i amendment introduced the concept of a Robust Security Network (RSN), defined as a wireless security network that only allows the creation of Robust Security Network Associations (RSNA). 802.11i defines two classes of security algorithms: RSNA, for establishing a logical connection between communicating IEEE 802.11 entities established through the IEE 802.11i key management scheme (4-way handshake)[13] and Pre-RSNA. Pre-RSNA security consist of Wired Equivalent Privacy (WEP) and 802.11 entity authentication. RSNA provides two data confidentiality protocols, called the Temporal Key Integrity Protocol (TKIP) and the Counter Mode with Cipher Block Chaining Message Authentication Code (CBC-MAC) Protocol (CCMP). To avoid a range of security problems, the primary recommendation in [14] is the use of CCMP for data confidentiality whenever possible because WEP and TKIP have inherent weaknesses. CCMP uses the CCM (Counter with CBC-MAC) operation mode [15] of the Advanced Encryption Standard (AES) algorithm.

CCMP uses the Advanced Encryption Standard (AES) algorithm, see Fig. 2 (a). Unlike in TKIP, key management and message integrity is handled by a single component built around AES using a 128-bit key and a 128-bit block. AES-CCMP operates on the Medium Access Protocol Data Unit (MPDU) which comprises five sections: 1) MAC header, 2) CCMP header, 3) Data unit, 4) Message Integrity Code (MIC) and 5) Frame Ckeck Sequence (FCS), where only the Data Unit and the MIC are encrypted. In general, the security architecture based on AES-CCMP ciphers data input (plaintext MPDU), using AES-CCM algorithm, and resulting the data output Cipher MPDU. AES-CCMP disassembles each packet in KeyID, packet number (PN) and plaintext MPDU. PN is a 48-bit number stored across 6 octets. The PN never repeats for the same temporal key (TK) since reuse of a PN with the same temporal key voids all security guarantees, so, a fresh TK is required for every ciphering session. MPDU is expanded in several fields, such as payload DataP, Address 2 (A2), a priority octet, and the MAC Header. With these fields, a CCMP Header is constructed as well as a Nonce value for the CCM algorithm (unique for each frame protected by a given TK and PN) and the additional authentication data (AAD). CCMP combines the MPDU Address 2 and priority field, and the PN to create the Nonce value. Then, it feeds the TK, the constructed Nonce, certain header information, and the data unit, to the CCM originator. The CCM origitator returns this encrypted data, and a MIC, which is combined with the unencripted CCMP and MAC headers, and sequence check for transmission.

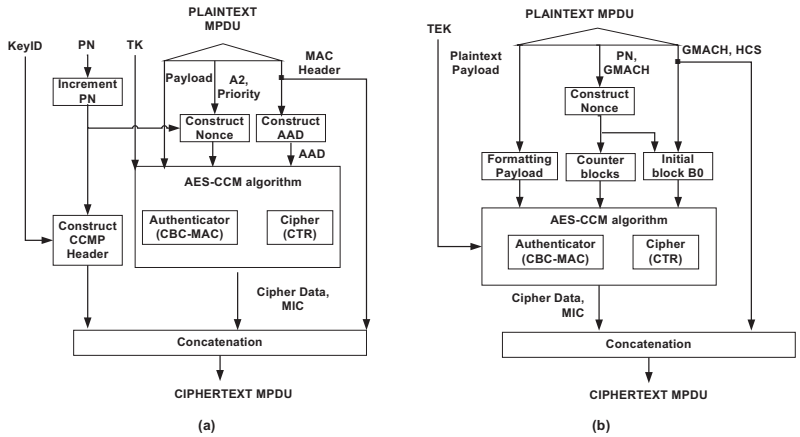

Fig. 2. Security architecture based on the AES-CCM protocol for IEEE 802.11i networks and related processes for ciphering in the IEEE 802.16e-2005 standard.

The payload, TK, Nonce value and ADD are input to the AES-CCM. It outputs the cipher data and MIC that are used together with the CCMP and MAC headers to build the Cipher MPDU. AES-CCM is the main cryptographic algorithm, which executes two related processes: generation-encryption and decryption-verification. CCMP uses CCM with the following parameters: M = 8 - indicating that the MIC is 8 octets and L = 2 - indicating that the Length field is 2 octets. According to an analysis performed to IEEE 802.11i by [14], CCM provides a level of confidentiality and authenticity comparable to other authenticated encryption modes.

For the purposes of this work, which is focused on the reconfiguration of a transmission platform, the generation-encryption process is considered to design the architecture. CBC-MAC process is applied to the payload DataP, the data associated AAD, and the nonce to generate a MIC (Message Integrity Code) whereas CTR mode is applied to the MIC and the payload DataP to obtain the ciphertext (Cipher MPDU).

IEEE802.16e-2005 Standard. The IEEE 802.16e-2005 is the latest standard on broadband wireless metropolitan area networks. It aims at maintaining clients connected to a MAN while moving around and supports enhanced security, mobility management, and improved support for fast handovers while addressing many design and security flaws in original baseline IEEE 802.16-2004 standard [16]. IEEE 802.16e-2005 is also called WiMAX, meaning Worldwide Interoperability for Microwave Access, provides wireless transmission using a variety of transmission modes, from point-to-multipoint links to portable and fully mobile internet access. The WiMAX Fourum has more than 500 members including operators, component and equipment manufacturers, and many others in

the communication ecosystem [17] and was formed to certify and promote the compatibility and interoperability of the standard and describes WiMAX as 'a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL' [18]. To date, commercial WiMAX coverage service has been achieved over 19.8 km. This year, it is expected to see Mobile WiMAX expanding to 20 MHz channel bandwidths with peak download rates exceeding 144 Mbps per sector. In 2010, the WiMAX industry is expected to transition to its next release. Features will include higher channel and VoIP capacity, higher user and data rates and will offer mobility for up to 500 km/hr with a link layer latency less than 10 ms [17].

IEEE 802.16e-2005 security scheme incorporates two component protocols: Privacy and Key Management (PKM) responsible for providing the secure distribution of keying material and the encapsulation [19] protocol for securing packet data. In the general operation of the encapsulation protocol, ciphering is applied to the MAC PDU payload for privacy service, whereas the PKM allows for authentication. In the encapsulation, data are protected by ciphering the information or plaintext payload, and by providing a value for the message integrity. Ciphering payload requires that two values shall be appended: packet number (PN) and message authentication code (MIC), and AES-CCM algorithm shall be applied to the plaintext payload, see Fig. 2 (b). For applying AES-CCM algorithm, other related main functions should be executed, formatting data input such as plaintext payload, counter blocks, initial block, nonce value, packet number (PN), and generic MAC header (GHMAC). These functions are described in the security scheme of the standard. In Section 3, hardware architectures using the AESCCM algorithm are proposed, which combine parallelized structures with low hardware resource requirements.

AES-CCM algorithm. Traditionally, two different cryptographic algorithms are used to provide confidentiality and authentication, but AES-CCM algorithm provides these two security services with the same algorithm, using the AES block cipher and the same key. CCM uses the CTR (Counter) mode and CBC-MAC (Cipher Block Chaining - Message Authentication Code) [20]. The confidentiality is provided by the AES algorithm in CTR mode, requiring a value that ensures uniqueness. The authentication is performed by the AES algorithm in CBC-MAC mode and provides additional capabilities.

AES-CBC-MAC and AES-CTR use AES block cipher as the main module, working in cascade, where the first one generates an intermediate value MIC T for the second one, which then generates the cipherdata and the final value MIC U. On one hand, AES-CBC-MAC, which is an integrity method, works sequentially and it cannot be parallelized, ensuring that every ciphered block depends on every preceding part of the plaintext, where ciphering two identical blocks results in different cipher blocks. AES-CBC-MAC is used when there is an exact number of blocks and hence requires padding. By the other hand, when ciphering two identical input blocks, AES-CTR mode produces different cipher blocks, which is based on a nonce value rather than starting it from a fixed value.

This mode provides authentication by adding extra capabilities. Some properties of AES-CTR is that ciphering can be done in parallel, and the message is not required to break into an exact number of blocks [21].

As it was mentioned, AES-CBC-MAC and AES-CTR modes use the AES block cipher as their main module, which can process data blocks of 128 bits using a 128-bit key [22]. AES executes an initial round followed by ten rounds. These last ten rounds have four transformations: 1) byte-to-byte substitution (SubByte), 2) rotation of rows (ShiftRow), 3) mixing of columns (MixColumn), and 4) addition of round key (AddRoundKey). Other operation is key expansion, which computes a key schedule or a 128-bits key in each round.

3 Hardware Implementation of the Security Architectures

One of the most simple design techniques for hardware implementations is based on modular designs. The next subsections show the modular designs and implementations of the security architectures for the IEEE-802.11i-2004 standard (AESCCMP) and for the IEEE 802.16e-2005 (AESCCM6), they focus on high throughput. This is reached by making an analysis to reduce critical path by developing specialized modules, proposing compact control units, identifying parallelization of the data buses and modules, and balancing paths formed by the combinational and sequential elements. For evaluation purposes and for developing the reconfigurable platform, these architectures are implemented in FPGA devices. The design of the architectures is written in VHDL and simulated using FPGA Advantage 6.3.

The methodology followed for the hardware implementation of the security architectures consisted on firstly modeling the security architectures in software in order to create the test data for validating the corresponding hardware modules. After that, a straightforward initial hardware architecture was designed and implemented with the aim of providing baseline architectures to evaluate improvement strategies. This also allowed identifying processing bottlenecks, critical paths and potential for hardware reutilization. Some techniques, such as loop unrolling, pipelining, and the use of embedded hardware resources [23], allowed reducing the critical path. The focus was on achieving higher throughput and to require lower hardware resources, which results in high througput/area ratio. After simulations, potential modules that could be parallelized were identified as well as a strategy for balancing the processing workload among the more complex modules. The complete functionality of the architecture was tested using the test vectors available in the standards FIPS 190-7 (AES), NIST SP800-38C (AES-CCM), IEEE 802.11i-2004 (AES-CCM Protocol) and IEEE 802.16e-2005 (AESCCM6).

3.1 AESCCM Hardware Architecture.

The general operation of the AESCCM module 3 is divided into these two sub-modules, where the first sub-module is required to calculate the authentication

field value T, and the second sub-module computes the cipher_MPDU and the value MIC U. The plaintext message input is divided into 128-bit data blocks BX, and they are used for processing in the two sub-modules, whereas counter blocks are used only for AESCTR sub-module. These sub-modules have a main component: AES_Cipher [24], which computes AES algorithm with its rounds, transformations and key calculation.

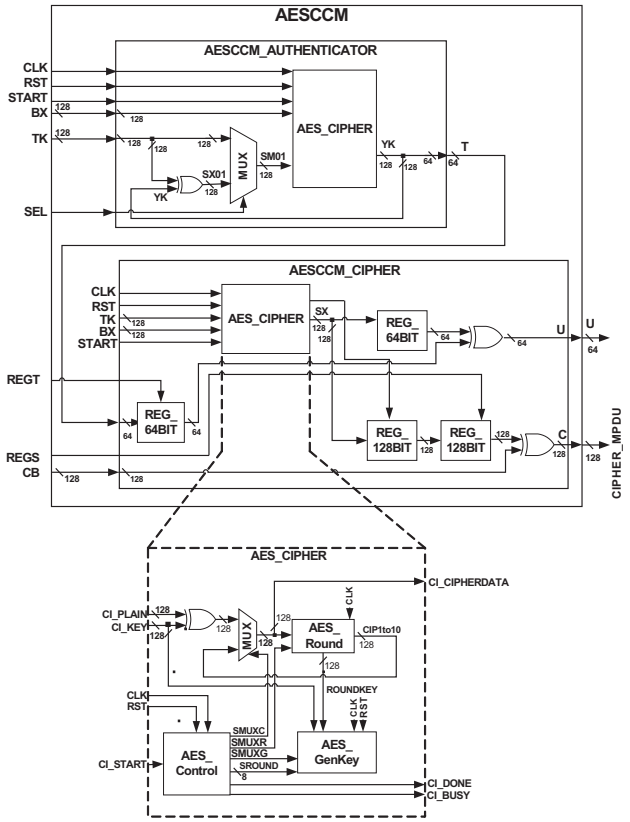

Fig. 3. Block diagram of the AESCCM module.

3.2 AESCCMP Hardware Architecture.

For the IEEE 802.11i-2004 standard, it is proposed the AESCCMP hardware architecture. The AES-CCMP hardware architecture is illustrated in Fig. 4. From Fig. 2, Increment PN and Construct CCMP Header blocks are considered to be executed in an upper layer. The AESCCMP hardware architecture is constituted

by specialized modules to format data (Format N&Q, Format AAD, Format Payload, and Format CB), to compute AES-CCM algorithm (AESCCM) and main control (Control CCMP). Each module to format data has its particular control submodule. The main control module is based on Finite State Machines (FSMs). AESCCM module executes AES-CBC-MAC and AES-CTR submodules in parallel, which compute AES-CBC-MAC and AESCTR algorithm, respectively. The general operation consists on processing two sources of data, parsed in 128-bit data blocks, and the same 128-bit key block through AESCCM module. The first source generates data blocks from three different modules (PAY N&Q, PAY AAD, and PAY PAY) to compute the MIC value in the AES-CBC-MAC submodule, whereas the second source takes data blocks from the same module (Format CB) to compute cipher data in the AES-CTR submodule. After processing all data blocks, AESCCM generates the cipherdata Cipher MPDU and the U value.

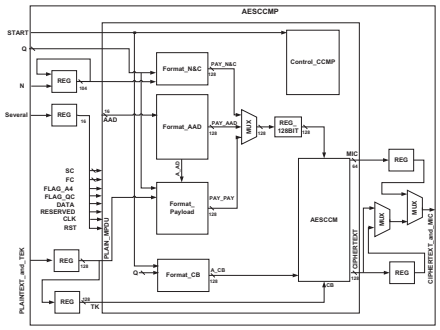

Fig. 4. Block diagram of the AESCCMP.

3.3 AESCCM6 Hardware Architecture.

The security architecture of the IEEE 802.16e-2005 standard is based on the AES-CCM algorithm as illustrated in Fig. 5. For this work, the hardware implementation of this security architecture will be called AESCCM6. The architecture is constituted by specialized modules to format data (Modifying GMACH, Construct Nonce, Format Payload, Format B0, and Format CB), to compute AES-CCM algorithm (AESCCM module), more details are in Section 2. The dataflow is managed by the main control. Format Payload executes a complex process due to the variable length L of the plaintext payload, so, this module has a particular control submodule. Similar to AESCCMP hardware architecture, main control is based on an FSM, generating flag and control signals to the dataflow, whereas AESCCM module computes AES-CBC-MAC and AES-CTR processes in parallel form.

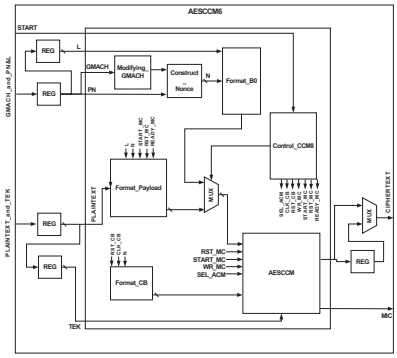

Fig. 5. Block diagram of the AESCCM6.

The general operation consists on processing two sources of data, parsed in 128-bit data blocks, and the same 128-bit key block through AESCCM module. The first data source is taken from two different data blocks (Format Payload and Format B0) to compute the MIC value in the AES-CBCMAC submodule, whereas the second data source is taken from the module Format CB to compute ciphertext in the AES-CTR submodule. After processing all data blocks, AESCCM generates the Ciphertext and MIC value. Computation of the AES algorithm in the AESCCM blocks is executed by an iterative and compact module, which reports high performance based on several studies [24].

4 Implementations

The design and development of the proposed reconfigurable platform is based on trade-off analysis in order to take advantage of parallelism in order to achieve high performance with moderate power consumption. This also allows to reduce hardware resources and to increase the flexibility while maintaining the performance. To reach these objectives, several reconfigurable schemes should be evaluated (see Fig. 6): full reconfiguration to reconfigure the application totally, see Fig. 6 (a) and partial reconfiguration for a partial reconfiguration of the application, see Fig. 6 (b) and Fig. 6 (c). This last type requires a precise analysis of the different functions to be mapped on the same platform in order to find the common components or reconfigurable components. These two reconfigurable schemes have a drawback due to the fact that the device operation is stopped while the reconfiguration is performed, resulting on a timing overhead. This drawback can be solved by implementing other application on the device before switching from one to another.

The synthesis results of the AESCCMP and AESCCM6 hardware architectures are presented in this section. For the purpose of validation and comparison, these architectures were synthesized, mapped, placed and routed for three different FPGA technologies: Virtex-5, Virtex-4 and Spartan-3. The synthesized

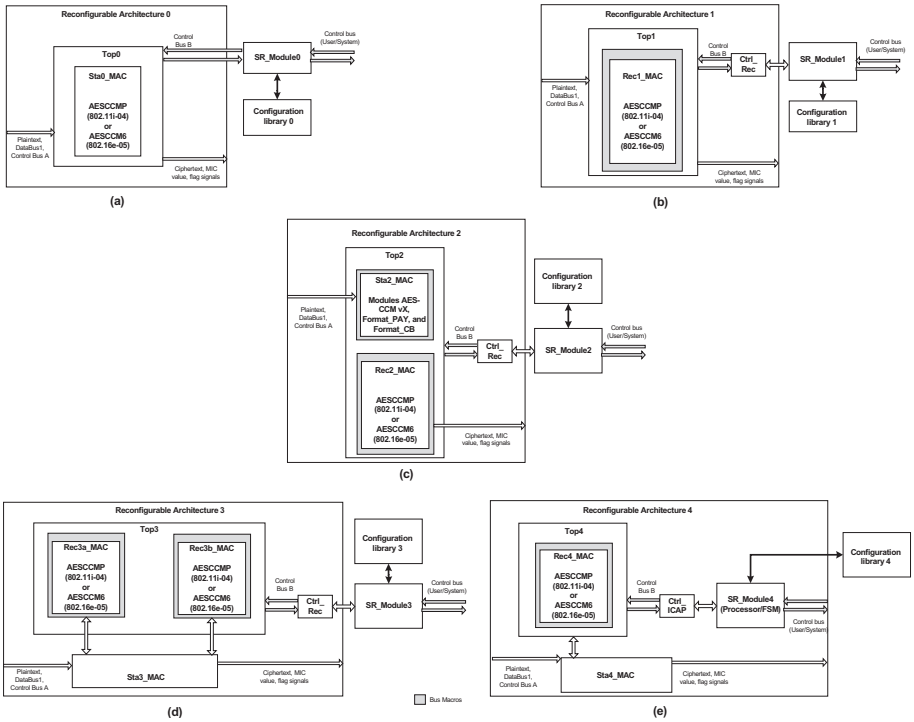

Fig. 6. Reconfigurable schemes for the platform.

architectures were simulated and verified considering real-time operation condition by using the design conformance test data, which are provided by the IEEE 802.11i-2004 and IEEE 802.16e-2005 standards.

The AESCCM6 architecture processes 65 data blocks (64 for the message, and 1 for the initial data block), but the initial data block is considered overhead, so only 64 data blocks have effective bits, i. e., (64) (128 bits) = 8192 bits = Plain_data_block_size. These data blocks for authentication (initial block, and message) and ciphering (CBs and message) are processed in parallel, so, it is necessary to process 65 data blocks, requiring (65) (10 clock cycles) + 10 clock cycles + 3 clock cycles = 663 clock cycles. In the same way, the AESCCMP architecture processes 67 data blocks (64 for the message, one for the initial data block and two for the AAD) in 683 clock cycles. The value of the Plain_data_block_size is (66) (128 bits) = 8448 bits. The throughput of these iterative architectures is given by (1).

$$Throughput = \frac{(Plain\ data\ block\ size)\ (Clock\ period)}{Clock\ cycles} \tag{1}$$

Table 1 shows implementation results of these hardware architectures in three different FPGA devices, Virtex5, Virtex4 and Spartan3, where all but one imple-

mentations support more than 1 Gbps. The designs reported in this work were implemented in FPGA devices for evaluation and validation purposes. These architectures can be also considered in the design of application-specific hardware devices. The implementation efficiency (Gbps/slices) is a measurement of this type of cryptographic hardware implementations and it is defined as the ratio between the reached throughput and the number of slices that each implementation consumes [25].

Table 1. Implementation results of the AESCCMP and AESCCM6 architectures for three technologies

Parameter	CCMP	CCM6	CCMP	CCM6	CCMP	CCM6
Device	Xc5v1x85-1		Xc4vlx60-10		Xc3s4000-4	
Period (ns)	7.064	9.241	7.952	9.091	11.562	15.028
Clock (MHz)	141.56	108.21	125.75	110.00	66.54	66.54
IOBs	269	309	269	309	269	309
Slice-LUT pairs	2920	2761	-	-	-	-
Slices	-	-	2294	1977	2012	1691
BRAMs	10	10	20	20	20	20
Power Cons. (mW)	1425	1396	668	997	576	944
Throughput (Gbps)	1.782	1.321	1.583	1.342	1.089	0.812
Efficiency (Gbps/slice x10-3)	0.610	0.478	0.690	0.679	0.541	0.480
Efficiency (Gbps/MHz)	12.590	12.208	12.590	12.208	12.590	12.208

In this Section, FPGA implementation costs and performance evaluation are discussed for the design and development of a security software-radio platform with reconfigurable architecture. To evaluate implementation costs, some characteristics such as utilized resources, period, clock frequency, and latency have been considered, see Table 1. For performance evaluation, characteristics such as throughput and efficiency have been considered. These studies and performance measurements of the AESCCMP and AESCCM6 implementations are used to design the security software-radio platform with reconfigurable architecture.

Firstly, considering only the AESCCMP or AESCCM6 hardware architecture, different device families (Virtex versus Spartan) will yield different implementation cost and performance, and newer technologies such as Virtex-4 and Virtex-5 present shorter periods or higher operation clock frequencies. When comparing AESCCMP against AESCCM6, it can be noted that the first one uses slightly more hardware resources for the hardware platform. This is due to the use of specific modules, which execute different formatting of data and specifications. This difference in LUTs and slices is not very significant, considering that a predefined part of the FPGA will be selected for the reconfiguration. The two architectures for two different networks can be supported in the same recon-

figurable platform. All implementations use ten BRAMs, situation that enables a consistency in the architectures. These BRAMs are used to implement S-boxes, which are required by the AES cipher. An important detail is the disparity on the use of the IOBs. These pins should be distributed, considering the reconfiguration of the device. The designs of these architectures for the reconfiguration should select tasks to be executed by the input/output data, evaluating reconfigurable/nonreconfigurable modules, which require connections to the exterior. Except for Virtex-4, the AESCCMP implementation reports better performance than compared with AESCCM6 implementation. The minimized area resources of AESCCMP and AESCCM6 do not decrease the system performance, which reach throughput superior to 1 Gbps. These security architectures of the standards are the elements that execute more operations at high computational cost. According to equation (1), *Plain_data_block_size* and *Clock_cycles* have fixed values (8448 bits and 683 clock cycles for AESCCMP, and 8192 bits and 663 clock cycles for AESCCM6), but *Clock_period* is defined by the implementation results, which produces different throughput and efficiency for the implementations in the diverse technologies. If this value is fixed, both AESCCMP and AESCCM6 architectures will report the same throughput on the reconfigurable platform, where hardware resources are just selected for reconfiguration or configuration, where a similar efficiency can be obtained. Comparing against related works, see Table 2, it is important to highlight that these implementations report high throughput and efficiency, characteristics that can be affected by implementing on a reconfigurable platform. There are many works reporting AES-CCM operations, but few works present complete security architectures executing operations based on AES-CCM. The period of each implementation should be analyzed to improve the performance of the platform, which is affected when reconfigurable architectures are mapped and reconfigurable modules are reused. For AESCCM6 architecture, few works have been reported, implemented on FPGAs [26]. For AESCCMP architecture, related works report different AES-CCMP implementations on FPGA [27]-[30], the proposed AESCCMP implementation reports the highest throughput and efficiency, allocating less area than [29] and [30], with higher operation frequency.

Table 2. Related works of 802.11i-2004 and 802.16e-2005 hardware architectures.

Work/ Standard	Slices	BRAM	Clock (MHz)	Throughput (Gbps)
[27]-802.11i	523	-	63.70	0.127
[28]-802.11i	3750	-	50.00	0.243
[29]-802.11i	3474	15	80.30	0.275
[30]-802.11i	5605	-	50.00	0.258
[26]-802.16e	-	-	93.00	-
[26]-802.16e	-	-	197.00	-

[31] presents an analysis, mentioning that CBC-MAC and CTR are the more computationally demanding modules. They propose a minimalist design of AES-CCMP for energy saving. [32] presents a commercial programmable processor with several security functions, including AES-CCMP and reporting a throughput of 1 Mbps at 166 MHz with a maximum-transmission current consumption of 350 mA at 3.3 V. [33] is a commercial processor for different applications and has several security functions as well as AES-CCMP. It consumes 475 mA in the typical transmit mode at 3.3 V, for computations of power consumption. [34] presents a commercial processor with several features for transmission/reception data, considering modulation and security. Elliptic Technology Inc., offers two processors: [35] has the functionality of the standard, supporting AES-CCM and DES-CBC, whereas [36] has a single functionality based on AES-CCM. These two documents do not report implementation results. [37] is a commercial module on ASIC, reporting two architectures implemented on the same technologies. As AESCCM is the main module, there are several special cores for IEEE 802.11i-2004 (such as [38] and [6]) and IEEE 802.16e-2005 security schemes (such as [39] and [6]).

5 Conclusions

Software radio is a hot research topic with focus on designing and developing hardware elements that present capabilities of high flexibility and performance. In these radios, security is a key characteristic to protect the transmissions of data in the wireless networks. The implementation costs and performance evaluation of the proposed security architectures from two different networks, such as WMAN and WLAN, enable to design and propose a reconfigurable platform, which supports these implementations, using similar hardware resource and reporting high efficiency. Due to the latency of ten clock cycles in both implementations, the same throughput is reached when that same clock frequency is applied to the reconfigurable platform. Custom hardware architectures are able to better exploit the parallelism of cryptographic algorithms and also are well suited to perform operations directly on bits or values represented by different word sizes. The results obtained in this work indicate that it is feasible to implement a single hardware module to provide security services for two of the most important wireless communications standards.

References

1. Fette, B. A.: Cognitive Radio Technology: Using TPM in Embedded Systems. Newnes, ISBN 0750679522, Ch. 4, 119–133 (2006)
2. Center for Software Defined Radio, Software Defined Radio: Terms, Trends and Perspectives, White Paper. Available: www.csdr.ck. (2007)
3. Shah A., An Introduction to Software Radio, available at: http://www.vanu.com/resources/intro/SWRprimer.pdf
4. Jrg Lotze, Suhaib A Fahmy, Juanjo Noguera *et al.* (2008) An FPGA-based Cognitive Radio Framework, 138-143. In Irish Signals and Systems Conference (ISSC).

5. J. P. Delahaye, G. Gogniar, C. Roland, P. Bomel, Software Radio and Dynamic Reconfiguration on a DSPFPGA Platform, Journal of Telecommunications, pages 152-159, N58, 5-6/2004.
6. Algredo-Badillo I., Feregrino-Uribe C., Cumplido R., Morales-Sandoval M., FPGA Implementation and Performance Evaluation of AES-CCM Cores for Wireless Networks, 2008 International Conference on ReConFigurable Computing and FPGAs (ReConFig'08), pp. 421-426, ISBN: 978-1-4244-3748-1, 3-5 December, 2008.
7. ICT-Centre, Multi Gigabit Millimeter Wave Wireless, Innovative ICT transforming Australian industries, Available: www.ict.csiro.au/index.php. (2009)
8. W. A. Arbaugh, N. Shankar, and J. Wang. Your 802.11 Network has no Clothes. In Proceedings of the First IEEE International Conference on Wireless LANs and Home Networks, pages 131-144, December, 2001.
9. N. Cam-Winget, R. Housley, D. Wagner, and J. Walker. Security flaws in 802.11 data link protocols. Special Issue: Wireless networking security, Communications of the ACM, Volume 46, Issue 5, pages 35-39, May, 2003.
10. J. S. Park and D. Dicoi. WLAN security: current and future. IEEE Internet Computing, Volume 7, No. 5, pages 60-65. September/October , 2003.
11. LAN/MAN Standards Committee, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11i-2004, IEEE Computer Society, July (2004).
12. IEEE Standard 802.1X-2001. IEEE Standard for Local and Metropolitan Area Networks. June, 2001.
13. Xinyu Xing, Elhadi Shakshuki, Darcy Benoit, Tarek Sheltami, Security Analysis and Authentication Improvement for IEEE 802.11i Specification, Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008, Pp:1 - 5. Nov-Dec. 2008.
14. Changhua He, John C. Mitchell, Security Analysis and Improvements for IEEE 802.11i. The 12th Annual Network and Distributed System Security Symposium (NDSS'05), pages 90-110. Feb. 2005.
15. D. Whiting, R. Housley, and N. Ferguson. Counter with CBC-MAC (CCM). RFC 3610, September, 2003.
16. Sheraz Naseer, Muhammad Younus and Attiq Ahmed, Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, pp. 344-349, 2008.
17. WiMAX Insight, white paper, p. 14, www.wimaxforum.org. Retrieved September 24th, 2009.
18. WiMAX Forum Overview, www.wimaxforum.org. Retrieved September 24th, 2009.
19. LAN/MAN Standards Committee of the IEEE Computer Society and the IEEE Microwave Theory and Techniques Society, "Part 16: Air Interface for Fixed and Mobile BroadbandWireless Access Systems", IEEE Std 802.16e-2005, IEEE Standard for Local and Metropolitan Area Networks,February (2006).
20. M. Dworkin,: NIST Special Publication 800-38C. Recommendation for Block Cipher Operation modes: The CCM Mode for Authentication and Confidentiality, National Instituteof Standards and Technology (NIST), May (2004).
21. Morris Dworkin, NIST Special Publication 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, available at: http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C_updated-July20_2007.pdf.
22. FIPS-197. Announcing the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication, November 2001.

23. R. Chaves, G. K. Kuzmanov, S. Vassiliadis, and L. A. Sousa, Reconfigurable Memory Based AES Co-processor, International Parallel and Distributed Processing Symposium 2006 (IPDPS 2006), IEEE Computer, 446–455, 2006.
24. Algredo-Badillo I., Feregrino-Uribe C., Cumplido-Parra R.,Design and Implementation of an FPGA-Based 1.452-Gbps Non-pipelined AES Architecture, ICCSA 2006, Lecture Notes in Computer Science 3982, 446–455, Springer-Verlag, (2006).
25. N. Sklavos, G. Selimis and O. Koufopavlou, FPGA Implementation Cost and Performance Evaluation of IEEE 802.11 Protocol Encryption Security Schemes, Journal of Physics: Conference Series 10 (2005), 361–364, Second Conference on Microelectronics, Microsystems and Nanotechnology, (2005).
26. Jetstream Media Technologies, JetCCM-6: 802.16e WiMAX AES-CCM Core, Datasheet, (2006). Available: www.security-cores.com.
27. A. Aziz, A. Samiah, and N. Ikram, A Secure Framework for Robust Secure Wireless Network (RSN) using AESCCMP, 4th International Bhurban Conference on Applied Sciences and Technology, June (2005).
28. J. H. Shim, T. W. Kwon, D. W. Kim, J. H. Suk, Y. H. Choi, and J. R. Choi, Compatible Design of CCMP and OCB AES Cipher Using Separated Encryptor and Decryptor for IEEE 802.11i, Proceedings of the International Symposium on Circuits and Systems, 2004. ISCAS'04, pp. III- 645-8 vol. 3, ISBN: 0-7803-8251-X, (2004).
29. N. Smyth, M. McLoone, and J. V. McCanny, WLAN Security Processor, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, Vol. 53, Issue 7, 1506–1520, ISSN: 1057-7122, (2006).
30. D. Bae, G. Kim, J. Kim, S. Park, and O. Song, An Efficient Design of CCMP for Robust Security Network, ICISC 2005, Lecture Notes in Computer Science 3935, 352–361, Springer-Berlin, (2006).
31. M. Razvi Doomun, K.M. Sunjiv Soyjaudah, Resource Saving AES-CCMP Design with Hybrid Counter Mode Block Chaining - MAC, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.10, October 2008.
32. Lantronix , Inc., WiFi Embedded DeviceSserver - Network Processor Module: MatchPort b/g Pro Wireless Device Server, Datasheet, 2008. Available at: www.lantronix.com.
33. Quatech, Inc., Airbone Embedded Radio Modules (802.11b/g): WLRG-RA-DP100 series, Datasheet, 2007. Available at: www.quatech.com
34. ASK Fujitsu Microelectronics Europe, MB86K21 Baseband SoC: The Mobile WiMAX 802.16e-2005 SoC, Factsheet, 2009. Available at: http://emea.fujitsu.com/microelectronics
35. Elliptic Technologies Inc, LLP-02 Product Brief: PDU Processor for 802.16/WiMAX, Datasheet, 2009. Available at: www.elliptictech.com
36. Elliptic Technologies Inc, LLP-03 Product Brief: PDU Processor for WiMAX Mobile Profile, Datasheet, 2009. Available at: www.elliptictech.com
37. IPCores Inc., CCM6 IEEE 802.16e (WiMAX) AES Core, Datasheet, 2008. Available at: www.ipcores.com/wimax_802.16e_aes_ccm_core.htm
38. Helion Technology Limited, AES-CCM Core Family for Xilinx FPGA, Datasheet, 2008. Available at: www.heliontech.com.
39. Elliptic Technologies Inc., CLP-28 AES Core for 802.16/WiMax, Datasheet, 2009. Available at: www.elliptictech.com.