FPGA implementation cost and performance evaluation of IEEE 802.11 protocol encryption security schemes

To cite this article: N Sklavos et al 2005 J. Phys.: Conf. Ser. 10 361

You may also like

- Study of Adjustment Delay Scheme on IEEE 802.15.4 Networks at Beacon Enabled Mode
  E Yundra

- A Study of Wi-Fi Security in City Environment
  H Valchanov, J Edikyan and V Aleksieva

- The Throughput of TCP Over Wireless Local Area Networks
  J Liu, J Lu, J Wang et al.

View the article online for updates and enhancements.
FPGA implementation cost and performance evaluation of IEEE 802.11 protocol encryption security schemes

N Sklavos, G Selimis and O Koufopavlou
Electrical and Computer Engineering Department, University of Patras, Patras, Greece
E-mail: nsklavos@ee.upatras.gr

Abstract. The explosive growth of internet and consumer demand for mobility has fuelled the exponential growth of wireless communications and networks. Mobile users want access to services and information, from both internet and personal devices, from a range of locations without the use of a cable medium. IEEE 802.11 is one of the most widely used wireless standards of our days. The amount of access and mobility into wireless networks requires a security infrastructure that protects communication within that network. The security of this protocol is based on the Wired Equivalent Privacy (WEP) scheme. Currently, all the IEEE 802.11 market products support WEP. But recently, the 802.11i working group introduced the Advanced Encryption Standard (AES), as the security scheme for the future IEEE 802.11 applications. In this paper, the hardware integrations of WEP and AES are studied. A Field Programmable Gate Array (FPGA) device has been used as the hardware implementation platform, for a fair comparison between the two security schemes. Measurements for the FPGA implementation cost, operating frequency, power consumption and performance are given.

1. Introduction
IEEE 802 standards committee formed the 802.11 Wireless Local Area Networks (WLAN) Standards Working Group in 1990 [1]. IEEE 802.11 standard does not provide technology or implementation, but introduces the specifications for the physical and the Media Access Control (MAC) layers. 802.11 is the wireless protocol for both ad-hoc and client/server networks. The users’ acceptance of this protocol is high. Although, the security of the transmission channel is a matter of special attention that always has to be considered [2].

The Wired Equivalent Privacy (WEP) scheme has been adopted by IEEE 802.11 standard to ensure security for the transmitted information [1-2]. The basic two components of WEP are: the Pseudorandom Number Generator (PRNG) and the Integrity Algorithm. The PRNG is the most valuable component because it actually is the original encryption core. WEP adopts RC4 cipher as the PRNG unit and Cyclic Redundancy Check (CRC-32) as the Integrity Algorithm. Although WEP is a good security scheme, the offered security in some cases can not satisfy the user demands [3]. In order a higher security level to be ensured [4], 802.11i working group introduced, as protocol’s security scheme, the Advanced Encryption Standard (AES) [5].

This paper presents the hardware implementation cost of both WEP and AES schemes. In order to have a fair and detailed comparison between the two schemes, the same implementation platform has been used (i.e.
the same Field Programmable Gate Array (FPGA) device).

For the AES scheme, a compact VLSI architecture is presented. The implementation of this architecture minimizes the allocated area resources. The area-optimized design does not sacrifice the system performance in a restricted way. The throughput of the design is much higher than the required by the IEEE 802.11 standard [6]. Both WEP and AES schemes are compared in terms of implementation performance: allocated area resources, operating frequency, throughput and power consumption. Aspects of the supported security of these encryption schemes are discussed and security level strength comparisons are given.

2. IEEE 802.11 & Wired Equivalent Privacy (WEP)
The proposed architecture for the implementation of the Wired Equivalent Privacy (WEP) scheme, is illustrated in Figure 1.

![WEP Scheme Architecture](image)

**Figure 1. Wired Equivalent Privacy (WEP) Scheme Architecture**

In order to implement in hardware the Cyclic Redundancy Check (CRC-32), a shift register of 32 Flip-Flops (F/Fs) and a number of XOR gates are used. So, a Linear Feedback Shift Register (LFSR) design is produced by using the F/Fs chain with the XOR gates. The characteristic polynomial of this LFSR is:

\[
(X) = X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1
\]

The presence/absence of an XOR gate in CRC-32 architecture corresponds to the presence/absence of a term in G(X) polynomial. The required output message is the content of the LFSR after the input message last bit is sampled.

RC4 is a variable key-size stream cipher and operates on one plaintext block at a time. RC4 architecture consists of the Key Expansion Unit and the Transformation Round. The Key Expansion Unit is mainly a S-Box component. For the S-BOX implementation a 256-byte RAM memory block is used and another similar memory block is needed for the key array. The Transformation Round is a simple bit-by-bit XOR between the plaintext and the key.
3. IEEE 802.11i & Advanced Encryption Standard (AES)

AES proposed architecture operates in Counter Mode with Cipher Block Chaining–Message Authentication Code (CCMP) [5]. According to IEEE 802.11i working group, this operation mode is used to ensure, at the same time, integrity and privacy. The proposed AES architecture is shown in Figure 2:

![AES Architecture Diagram](image)

The AES scheme architecture operates each time on a column of 32-bit data. It needs 41 clock cycles to complete the transformation of a 128-bit plaintext block. The column subunit is composed of 4 basic building blocks: S-Box, DataShift, MixColumn and KeyAddition. The RAM based design for the S-BOXes ([256x8]-bit) guarantees high performance. This "column" based architecture, minimizes the area resources compared with "State" based architectures [7, 8].

4. Implementation Cost and Performance Evaluation

In Figure 4, the synthesis results for both WEP and AES implementations are illustrated. For the hardware integration the FPGA device Xilinx Virtex (2V250fg256) has been used. For power consumption estimation, the Xilinx tool provided in [9] was used. Energy optimized methods could be applied to the above described architectures, similar to those used in WTLS security [10] of WAP [11].

![Implementations Comparisons](image)
Based on the synthesis results regarding the area resources the utilization of both implementations are: AES, 323 CLBs (allocated) + 1213 CLBs (unused) = 1526 CLBs (available in the FPGA device), and for WEP, 750 CLBs (allocated) + 776 CLBs (unused) = 1526 CLBs (available in the FPGA device). The AES implementation performs better compared with WEP implementation. The minimized area resources of AES, do not sacrifice the system performance, which reaches throughput value 177 Mbps. This data rate is much higher compared with the highest specified by IEEE 802.11 [6] throughput of 11 Mbps. On the other hand, RC4 is a more "heavy" design for mobile devices hardware implementation. This is due to the specified S-Boxes and the Key Expansion Unit specifications. RC4 performance is the bottleneck for WEP throughput which reaches the value of 2.22 Mbps. The main RC4 implementation disadvantages, compared with AES are: 1) more required silicon area resources 2) higher power consumption and 3) lower operating frequency. Compared with [7] and [8] proposed AES implementation allocates less area than [7], [8], with higher operation frequency than [8]. The reached throughput values of [7] and [8] are better compared with the proposed implementation. Since the works of [7] and [8] do not present any power consumption results such a comparison with the presented work is not efficient. Concluding and based on the above comparison results, the proposed AES implementation is proposed for applications with special needs in both area resources and operation frequency.

Concerning security aspects AES offers, at the same time, privacy and integrity. On the contrary, WEP scheme needs two different algorithms, in order to support bulk encryption and data integrity. In some cases, where AES security is unbreakable, WEP security could be broken. These comparisons give AES advantages and make it an efficient and trustworthy solution for the next years IEEE 802.11 networks.

5. References
[1] IEEE Standards Board 2003 802 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
[2] Sklavos N, and Koufopavlou O 2003 Mobile Communications World: Security Implementations Aspects: A State of the Art CSJM Journal, Institute of Mathematics and Computer Science 11 N° 2
[3] Borisov N, Goldberg I and Wagner D 2001 Intercepting Mobile Communications: The Insecurity of 802.11 Proc. of 7th Annual International Conference on Mobile Computing and Networking (July 16-21)
[4] Undercoffer J, Perich F, Cedilnik A., Kagal L and Joshi A 2003 A Secure Infrastructure for Service Discovery and Access in Pervasive Computing Journal of Mobile Networks and Applications 8 113-125 Kluwer Academic Publishers
[5] Advanced Encryption Standard, (AES) 2003 http://www.nist.gov/aes
[6] Xiao Y and Rosdahl J 2002 Throughput and Delay Limits of IEEE 802.11 IEEE Communications Letters 6 N° 8
[7] Zhang X and Parhi K 2002 Implementation Approaches for the Advanced Encryption Standard Algorithm IEEE CAS 2 N° 4
[8] Sklavos N and Koufopavlou O 2002 Architectures and VLSI Implementations of the AES-Proposal Rijndael", IEEE Transactions on Computers 51 Issue 12 pp 1454-1459
[9] Xilinx Inc., San Jose, California 2003 Virtex, 2.5 V Field Programmable Gate Arrays, & A simple method of estimating power in XC40000XI/XE/E FPGAs Application Brief XBRF 014 v1.0, www.xilinx.com
[10] Karri R and Mishra P 2003, Optimizing the Energy Consumed by Secure Wireless Sessions-Wireless Transport Layer Security, Journal of Mobile Networks and Applications 8, 177-185, Kluwer Academic Publishers
[11] Hwang G J, Tseng J C R, and Huang Y S 2002 I-WAP: An Intelligent WAP Site Management System, IEEE Transactions On Mobile Computing 1 N° 2