Chapter 17
Low Complexity Processor Designs for Energy-Efficient Security and Error Correction in Wireless Sensor Networks

J. H. Kong
The University of Nottingham- Malaysia Campus, Malaysia

J. J. Ong
The University of Nottingham- Malaysia Campus, Malaysia

L.-M. Ang
The University of Nottingham- Malaysia Campus, Malaysia

K. P. Seng
The University of Nottingham- Malaysia Campus, Malaysia

ABSTRACT

This chapter presents low complexity processor designs for energy-efficient security and error correction for implementation on wireless sensor networks (WSN). WSN nodes have limited resources in terms of hardware, memory, and battery life span. Small area hardware designs for encryption and error-correction modules are the most preferred approach to meet the stringent design area requirement. This chapter describes Minimal Instruction Set Computer (MISC) processor designs with a compact architecture and simple hardware components. The MISC is able to make use of a small area of the FPGA and provides a processor platform for security and error correction operations. In this chapter, two example applications, which are the Advance Encryption Standard (AES) and Reed Solomon (RS) algorithms, were implemented onto MISC. The MISC hardware architecture for AES and RS were designed and verified using the Handel-C hardware description language and implemented on a Xilinx Spartan-3 FPGA.

DOI: 10.4018/978-1-4666-0101-7.ch017

INTRODUCTION

Secure data encryption is usually applied for data integrity and protection. Encrypted data transmission requires error correction codes to reliably recover the data during decryption. To implement security and error correction features into an independent system, a processor core has to be pre-established in order to serve as its own instruction execution mechanism. With this base mechanism, functions and programs can be run at this platform with hardware re-configurability features. The original motivation for the One Instruction Set Computer (OISC) processor, sometimes called the URISC (Ultimate Reduced Instruction Set Computer) was meant for educational ideologies of a much simpler version of computer organization to explain the sophisticated Computer Architectures (Gilreath & Laplante, 2003). Concepts of the hardwired or micro-programmed control are to consider the execution sequence of the instruction sets. However, each individual instruction sets of a complex instruction architecture lack of functionality and independency. By breaking down the complex instruction sets, a simplified model of the existing computer organization can be developed. The proposed MISC architecture serves as a new approach, to demonstrate simple arithmetic functions and conditional 'jump' capabilities for the universality of a Computing Device (Gilreath & Laplante, 2003).

The objective to design tiny WSN sensor nodes has always been a challenge. With the nature of the WSN having resource constraint environment and environment adaptation requires on-field restructuring and reprogramming in software and hardware, design approaches often go towards low-area, low-cost and low complexity system designs. Visual data processing and compression modules usually occupy most of the area of the on-board FPGA microcontroller. This leads to a design for low complexity and low area system. In this chapter, the MISC is used to provide data security and error correction, fulfilling both criteria: low-area and low-complexity designs. The Advance Encryption Standard (AES) and Reed Solomon Error Control System (RS) are implemented using the MISC processor to provided security and error correction features to the WSN.

BACKGROUND

Ultimate Reduced Instruction Set Computer (URISC)

The URISC which was first proposed by (Mavaddat & Parhami, 1988) is meant for educational purpose. It has been an inspiration and insight to the CISC (Complex Instruction Set Computer) and RISC (Reduced Instruction Set Computer). This simplified model of computer architecture is flexible with only a single instruction incorporated can be further expanded and implemented on hardware easily. The URISC uses only one instruction called the SBN instruction (Subtract and Branch If Negative). By using only the SBN instruction, the URISC is able to perform data addition and subtraction. Logical operations can be performed to execute data movement from one location to another. The URISC consists of an Adder circuit as its sole ALU. Detailed operation of the URISC can be found in (Mavaddat & Parhami, 1988). Figure 1 shows the schematic of the URISC architecture.

The 'Subtract and Branch if Negative' (SBN) processor was first proposed by Van der Poel (Gilreath & Laplante, 2003). With this primitive SBN instruction, the URISC is built from its basic processor. The basic operations of URISC are moving operands to and from the memory, with addresses corresponding to the registers. The arithmetic computation can be performed and the results are stored in the 2nd operand's memory location. Similarly, to execute URISC instructions, the Core subtracts the 1st operand from the 2nd operand, storing the results in the 2nd operand's memory location. If the subtraction results a