Design and Implementation of Efficient Reconfigurable Cipher Algorithms for Wireless Sensor Networks

George Krikis[1,2], Christos P. Antonopoulos[2], Nikolaos S. Voros[2]

[1]Noesis Technologies
L.P. Suite B5, Patras Science Park Stadiou Str,
Platani Rion 26504, Greece
gkrikis@noesis-tech.com

[2]Technological Educational Institute of Mesolonghi
Department of Telecommunication Systems and Networks
National Road Antiriou Nafpaktou, Varia, Nafpaktos 30300, Greece
{cantonopoulos,voros}@teimes.gr

Abstract— **Wireless Sensor Networks (WSN) networks are increasingly utilized in highly demanding scenarios such as medical applications. In such cases hardware designs emerge as a prominent approach to address processing demanding tasks offering significant advantages over respective software based solutions. In such cases reconfiguration capabilities enable the achievement of critical trade-off between adequate performance and resource conservation. In this context the main contribution of this paper is the proposal and performance evaluation of a reconfigurable encryption module with respect to the encryption key size aiming towards WSN utilization. Performance will be presented with respect to encryption process delay, reconfiguration delay and power consumption projecting to energy expenditure.**

Keywords: Hardware Encryption Modules, Wireless Sensor Networks, Hardware Design and Implementation, Performance Evaluation, Reconfigurability

I. INTRODUCTION

Over the last few years, Wireless System Networks (WSN) have received increasing interest both from academia and industry targeting at highly demanding applications. The high flexibility, low cost, low complexity platforms in conjunction with increased robustness, reliability and offered performance make such solutions prominent solutions for resource demanding scenarios such as medical applications. One of the most critical requirements posed in medical applications is security level provision [1].

However, respective feature pertains to various aspects of network characteristics such as data privacy, data integrity and authentication of communicating parties governed by strict ethical and legislative regulations. Furthermore, all security related operations correspond to executing complex and intense cipher algorithms, which in the case of WSNs, follow the symmetric encryption approach as more resource conservative yet offering adequate security level.

Even though over the last few years WSN platforms of increased capabilities have been presented, extreme resource limitations remain the Achilles' heel of respective hardware. Such limitations are quite significant in all performance aspects such as processing power, available code and data memory and even more energy availability. At the same time, WSN nodes are expected to operate unattended from many days to months (for communication intensive applications) or even years (for relaxed communication application scenarios). Finally, WSNs are characterized by the bandwidth which poses significant limitations to the amount of data to be transmitted through the wireless medium.

Consequently, any additional software implementation that is required to be executed, pose critical overhead, especially when this appears in the form of computationally intensive cipher algorithms required to operate on all data that is to be transmitted over the air. A prominent way to mitigate this overhead is to design and develop highly efficient and, most importantly, very low power dissipation hardware modules able to offer the required functionality while posing very low power demands [2, 7].

Going one step further, reconfigurable hardware designs can yield even higher efficiency through the same hardware. The need for such capabilities steams from the observation that the same module is required to perform differently depending on specific parameters varying the power consumption with respect to the complexity and computation demands of the functionality. A typical example is a WSN platform able to acquire a wide range of various types of medical information ranging from Electroencephalography (EEG) and