Efficient Hardware Based Security Algorithm Implementation for WSN Medical Applications: The ARMOR Perspective

Christos Antonopoulos[1], George Krikis[2], and Nikolaos Voros[1]

[1] Technological Educational Institute of Mesolonghi, Greece
{cantonopoulos,voros}@teimes.gr
[2] Noesis Technologies, L.P., Patras, Greece
gkrikis@noesis-tech.com

Abstract. Utilization of emerging WSN technologies in the field of demanding medical applications comprise one of the most critical and challenging objectives of the ARMOR project. However, contemporary WSN node implementations are notorious for the resource limitations e.g. in terms of processing and memory capabilities. Therefore, significant effort is devoted in hardware based implementations of critical components with respect to the project objectives that can alleviate respective re-source limitations drawback.

1 Introduction

WSN communication paradigm offers high value features making respective platforms very appealing for a wide range of applications. Additionally, over the last few years platforms and technologies have emerged offering enhanced performance making them adequate candidates for demanding applications [1]. In the ARMOR project such an application is the primary focus in terms of both communication requirements as well as security [2]. The main goal of the ARMOR project is to enable accurate, reliable and non-intrusive monitoring and analysis of epilepsy-relevant multi-parametric data including EEG and ECG signals. Consequently on one hand aiming to study epilepsy requires a high number of sensors being able to acquire and transfer very high amount of data (especially concerning EEG measurements) and one the other hand, it is of paramount importance to offer high security services. The latter aspect requires the efficient execution of state of the art cipher algorithms. Considering the resource limitation exhibited by today's prominent platforms effort has been devoted in designing and implementing an ultra-low power AES hardware based cipher implementation in order to enhance the functionality of existing WSN platforms while not compromising required performance. Furthermore, in the context of the ARMOR project all aspects of an end-to-end EHR system (as depicted in Fig. 1) will be addressed including real time analysis at local site as well as off-line analysis through an EHR system offering advanced services.

P. Brisk, J.G. de Figueiredo Coutinho, P.C. Diniz (Eds.): ARC 2013, LNCS 7806, pp. 233–234, 2013.