JOURNAL OF INFORMATION SECURITY AND APPLICATIONS 29 (2016) 65–79

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/jisa

Design and implementation of hardware-efficient modified Rao–Nam scheme with high security for wireless sensor networks

Celine Mary Stuart *, *Spandana K.*, *Dhanaraj K.J.*, *Deepthi P. Pattathil*

Department of Electronics and Communication Engineering, National Institute of Technology Calicut, PIN-673601 Kerala, India

ARTICLE INFO

Article history:
Available online 31 March 2016

Keywords:
QC-LDPC code
LFSR
Cryptosystem
RN scheme

ABSTRACT

This paper presents the design and implementation of a crypto channel coder with very low hardware complexity and high security for securing communication in resource-constrained applications such as Wireless Sensor Networks (WSNs). The integrated secure channel coder system is proposed as a modification of the Rao–Nam (RN) scheme by embedding security in a structured Low-Density Parity-Check (LDPC) code. A novel stream ciphering method based on the Linear Feedback Shift Register (LFSR) with high throughput is incorporated to generate random error vectors, so that a large number of vectors with very good cryptographic properties can be made available with simple hardware. An efficient design method to vary the encryption matrix and the intentional error vector with each message block provides high degrees of freedom for an intended receiver without compromising hardware simplicity. Prototypes of the proposed encoder architecture with both (28, 14) and (248, 124) Quasi-Cyclic (QC) LDPC codes have been implemented on Xilinx Field Programmable Gate Array (FPGA) Spartan 3E kit using Very High Speed Integrated Circuit Description Language (VHDL). Analytical and synthesis results show that this scheme is highly suitable for resource-constrained applications such as wireless sensor networks due to its low hardware complexity and high security.

1. Introduction

A wireless sensor network consists of a group of sensor nodes that perform collaborative sensing and data processing tasks in a self-organized manner using a wireless medium. Since they are deployed in large quantities without any human attention, they are prone to attacks. However, complex security measures (Pathan et al., 2006) cannot be effectively implemented in them due to resource-constraints. To save power, they may use weaker cryptographic methods, thereby making them easy targets to the attacker. Therefore, it is crucial to develop a light weight highly secure cryptosystem to protect the data from the attacker in the resource-constrained environment. Recently, research ideas have been highly developed to merge the two processes (encryption and error control) to achieve efficient implementation and to provide an optimized cost without any trade-off between security and reliability. Security of such schemes is based on the difficulty of decoding a typical linear block code with unknown structure (Berlekamp et al., 1978). This paper aims to develop and implement efficient techniques for providing high level of

* *Corresponding author.* Department of Electronics and Communication Engineering, National Institute of Technology Calicut, PIN-673601 Kerala, India. Mobile: +91 9446126125; fax: 91 495 2287250.
E-mail address: celinemarystuart@gmail.com (C.M. Stuart).
http://dx.doi.org/10.1016/j.jisa.2016.03.004

security for the message to be transmitted with minimum complexity of operations.

The first symmetric key cryptosystem based on linear block code was introduced by Rao (1984), keeping the encryption matrix secret. However, it was revealed by Rao and Nam that this cryptosystem is vulnerable to a chosen-plaintext attack (Rao and Nam, 1989). They introduced another symmetric key cryptosystem with smaller block length, but channel error could not be decoded effectively (Cheng et al., 1998). The security of RN cryptosystem (Rao and Nam, 1989) depends heavily on the Hamming weight and other properties of the deliberate error vector added to the encoded message. Cryptanalysis of RN scheme clearly imposes that the deliberate random error vector should have a high Hamming weight, approximately half the length of the codeword for a high level of security. Later, a few variants (Hooshmand et al., 2012; Sobhi Afshar et al., 2009) of the RN scheme have been developed in the literature using various types of codes and different sets of error models. In most of these schemes, the random vector generation employed by multiplying the syndrome with a right inverse matrix results in an added encoding complexity. The random vector generated in this manner causes information leakage due to the fixed zero coordinates present in them. Additional randomization is required to remove the effect of fixed zeroes, which further increases computational complexity. All variants of RN cryptosystems available in the literature use a fixed random scrambler matrix and a fixed permutation matrix with every message.

Considering the drawbacks of the above mentioned systems, we have proposed a low-complex symmetric key cryptosystem (Stuart and Pattathil, 2015) using secure concatenated code with a nonlinear filter generator (NLFG) based stream cipher for error vector generation. The method of error vector generation proposed there was thoroughly analyzed and proved to have high security against possible attacks available in the literature. In that work, security is embedded in QC-LDPC code and interleaver in addition to the intentional random error vector. Using the method of Tanner et al. (2004), QC-LDPC code was constructed and a method of embedding security in that code has been investigated in that work (see Stuart and Pattathil, 2015). The number of equivalent matrices can be made high in that construction method, only if the cardinality of field of operation selected is high, which in turn results in a large code length. In wireless sensor networks, single stage short length block codes are used because of severe energy constraints. Hence attempts are done in the present work to embed high level of security in a single stage QC-LDPC based channel code, which eliminates the stages of RS encoding and interleaving in the previous work. QC-LDPC code constructed from the Extended Difference family (EDF) (Xia and Xia, 2005) is chosen in the present work since it offers a large number of equivalent matrices even for smaller dimension.

The major contributions of this work are as follows: (i) developed a mathematical model for a secure channel coding scheme that can ensure high security even for channel codes of low block length and high code rate, (ii) implemented the hardware for generating large number of random error vectors with good cryptographic properties using a hardware-efficient LFSR based structure (Deepthi and Sathidevi, 2008), (iii) implemented the hardware architecture for embedding security into the structure of EDF-QC-LDPC code, (iv) developed design methods for varying encryption matrix, permutation matrix and error vectors for different messages with minimum hardware redundancy, (v) implemented the prototype of the proposed hardware efficient modified RN scheme on FPGA platform based on both (28, 14) and (248, 124) EDF-QC-LDPC codes, and (vi) verified the enhanced security, low hardware complexity and good error performance of the proposed system with varying encoding matrices through analysis and experimental results.

This paper is organized as follows: Section 2 describes the basic RN cryptosystem and its disadvantages. In Section 3, mathematical and structural models of the proposed RN cryptosystem are explained. In Section 4, security analysis is done and in Section 5, FPGA implementation of the proposed cryptosystem is discussed. The implementation results of the proposed scheme using both (28, 14) and (248, 124) EDF-QC-LDPC codes are also given. Typical application of the proposed scheme in WSN is discussed in Section 6 and conclusions are drawn in Section 7.

2. Rao–Nam (RN) cryptosystem

The private key algebraic-code cryptosystem proposed by Rao and Nam encrypts the plaintext as follows:

$$\mathbf{c} = (\mathbf{m}SG + \mathbf{z})P = \mathbf{m}SGP + \mathbf{z}P = \mathbf{m}G' + \mathbf{z}P \tag{1}$$

where $\mathbf{c}$ is ciphertext of length n; $\mathbf{m}$ is plaintext of length k; S is a random non-singular invertible matrix; G is generator matrix of an (n, k) block code; $\mathbf{z}$ is an error vector of length n, whose average Hamming weight $\approx n/2$ selected randomly from a syndrome error table; and P is permutation matrix. Here the final encryption matrix $G' = SGP$ is fixed for all messages and is kept secret.

Let $\mathbf{r}$ be the erroneous ciphertext received when a plaintext $\mathbf{m}$ has been encrypted and transmitted through a noisy channel; then $\mathbf{r} = \mathbf{c} + \mathbf{e}$, where $\mathbf{e}$ is the channel noise. The intended user knows the predetermined set of vectors (syndrome error table) used as $\mathbf{z}$. Then the syndrome for the received $\mathbf{r}$ is computed as

$$\mathbf{s} = \mathbf{r}P^{\mathrm{T}}H^{\mathrm{T}} = (\mathbf{m}SG + \mathbf{z})PP^{\mathrm{T}}H^{\mathrm{T}} + \mathbf{e}P^{\mathrm{T}}H^{\mathrm{T}} = (\mathbf{z} + \mathbf{e}P^{\mathrm{T}})H^{\mathrm{T}} \tag{2}$$

where H is parity check matrix. If $\mathbf{e}$ is a non-zero vector, the error vector cannot be correctly found from the syndrome table using the computed syndrome $\mathbf{s}$ since the computed syndrome may be changed due to channel noise. Therefore, the scheme cannot tolerate transmission error due to channel noise. Assuming the channel is error-free, decryption can be done by applying inverse permutation and then subtracting the error vector obtained from the syndrome error table using the computed syndrome.

Due to the restricted set of error patterns, the system is not optimally secured against chosen plaintext attack based on majority voting. The security of RN scheme depends on Hamming weight and number of perturbation vectors, which demands