Chapter 10
Development of an Efficient and Secure Mobile Communication System with New Future Directions

Abid Yahya
Universiti Malaysia Perlis, Malaysia

Aini Syuhada
Universiti Malaysia Perlis, Malaysia

Farid Ghani
Universiti Malaysia Perlis, Malaysia

Othman Sidek
Collaborative Microelectronic Design Excellence Center, Malaysia

R. Badlishah Ahmad
Universiti Malaysia Perlis, Malaysia

M. F. M. Salleh
Universiti Sains Malaysia, Malaysia

Mostafijur Rahman
Universiti Malaysia Perlis, Malaysia

ABSTRACT

This chapter presents performance of a new technique for constructing Quasi-Cyclic Low-Density Parity-Check (QC-LDPC) encrypted codes based on a row division method. The new QC-LDPC encrypted codes are flexible in terms of large girth, multiple code rates, and large block lengths. In the proposed algorithm, the restructuring of the interconnections is developed by splitting the rows into subrows. This row division reduces the load on the processing node and ultimately reduces the hardware complexity. In this method of encrypted code construction, rows are used to form a distance graph. They are then transformed to a parity-check matrix in order to acquire the desired girth. In this work, matrices are divided into small sub-matrices, which result in improved decoding performance and reduce waiting time of the messages to be updated. Matrix sub-division increases the number of sub-matrices to be managed and memory requirement. Moreover, Prototype architecture of the LDPC codes has been implemented by writing Hardware Description Language (VHDL) code and targeted to a Xilinx Spartan-3E XC3S500E FPGA chip.

DOI: 10.4018/978-1-61350-116-0.ch010

INTRODUCTION

The means by which people correspond has radically changed since the early days of communication. At the moment, wireless networks and devices communicate far more than conventional verbal conversations. It has been noted that the cellular phone industry is facing revenue losses every year due to illegal handling of their services. As the cellular systems are developed, newly employed security features cut down the possibility of technical hoaxs. Nevertheless, as third generation (3G) cellular systems become the main part of omnipresent wireless communication, the security of cellular systems confronts new challenges. Integration and interfacing of these systems into packet switching networks will expose them to all kinds of intentional and unintentional attacks, and will require an advanced level of security. Security and encryption are necessary concerns in this computer age.

This chapter explores the research and development of new encryption codes and systems. The term code has a number of different meanings and in this chapter where it is used to refer to a computer program or software those terms will be used everywhere else the term code or coding will be used to refer to encryption and digital security systems. A secure system constrains from doing anything that it is not supposed to do. The key prospects of security are Confidentiality, Integrity and Availability. These three views also are named as Computational Intelligence (CI). Confidentiality is all about asserting privacy and Integrity is about ascertaining the precision and completeness of information while Availability is about guaranteeing the availability of information to authorized hands.

This chapter presents a new technique for designing and implementing QC-LDPC encrypted codes based on a row division method. The new encrypted codes offer more flexibility in terms of large girth, multiple code rates and large lengths. In this method of encrypted code construction, the rows are used to form the distance graph. In the proposed algorithm, the restructuring of the interconnections is developed by splitting the rows into subrows. This row division reduces the load on processing nodes and ultimately reduces the hardware complexity.

Channel coding is a broadly used term mostly referring to the forward error correction code and bit interleaving in communication and storage where the communication media or storage media is viewed as a channel and plays a key role in providing a reliable communication method that can overcome signal degradation in practical channels. The breakthrough of convolutional codes (Charles, 1997) led a new field of study into non-algebraic codes based on linear transformations using generator and parity-check matrices. These use error-correcting that firstly transforms each m-bit information symbol (each m-bit string) into an n-bit symbol, where m/n is the code rate ($n \geq m$) and secondly the transformation is a function of the last k information symbols, where k is the constraint length of the code. Convolutional codes are encoded using a finite-state process, which generates a linear order encoding scheme. Since then convolutional codes have led to the discovery of a new class of codes called Turbo codes (Berrou et al., 1993), which are a class of concatenated convolutional codes that randomize the order of some of the bits by using an interleaver.

Turbo codes are the first to approach error correction, providing a powerful error correction capability when decoded by an iterative decoding algorithm (Berrou et al., 1993). The rediscovery of Low Density Parity Check (LDPC) code, which was originally proposed by Gallager (1963) and was later generalized as MacKay-Neal code (Mackay and Neal, 1996) making Turbo codes the Forward Error Correction (FEC) technique. LDPC codes were neglected for a long time as their computational complexity was too high for the hardware technology available. LDPC codes have acquired considerable attention due to their near-capacity error execution and powerful chan-