Topics in Coding, Cryptography
and Information Security

Editors:
Mohammad Umar Siddiqi
Sigit Puspito Wigati Jarot
Othman Omran Khalifa

IIUM Press
2011
Topics in Coding, Cryptography and Information Security

Contents

List of Contributors ii

Editorial Introduction vi

PART I: SOURCE CODING

1. Performance Analysis of Image Data Compression using Zero-Tree Wavelet Transform
   Othman O. Khalifa, Emir Tabakovic, Zlatko Memisevic and Aisha-Hassan Abdullah 2

2. Scalable and Robust Streaming Video System Challenges
   Othman O. Khalifa, Sinzobakwira Issa and Mohammad Umar Siddiqi 12

PART II: CHANNEL CODING

3. Golay Codec: An Overview
   Othman O. Khalifa 23

4. Reed-Muller Codes: An Overview
   Othman O. Khalifa 35

5. Viterbi Decoder: A Review and Implementation
   Noorainam Ainina Bt. Md Noor Albakri and Othman O. Khalifa 42
6. Zigzag Codes: High Rate Low Complexity Iterative Codes  
   *Sigit P.W. Jarot*  
   53

7. Convolutional Coded OFDM in Broadband Mobile Communication  
   *Sigit P.W. Jarot*  
   66

8. Channel Coding Techniques in Mobile Communication Systems  
   *Othman O. Khalifa and Rashid A. Saeed*  
   77

9. Channel Coding in CDMA 2000  
   *Othman O. Khalifa*  
   85

10. Channel Coding in Mobile WiMAX  
    *Rashid A. Saeed and Othman O. Khalifa*  
    91

11. Turbo Codes: An Error Correction Technique for 4G  
    *Mosharrof Hussain Masud and Mohammad Umar Siddiqi*  
    99

12. Combined Source Channel Decoding for Image Transmission over Noisy Channels  
    *Jalal Chebil*  
    108

**PART III: CRYPTOGRAPHY AND INFORMATION SECURITY**

13. Cryptographic Boolean Functions: Transform Domain Perspective  
    *Hashum Mohamed Rafiq and Mohammad Umar Siddiqi*  
    120

14. Implementation of RSA Algorithm  
    *Hafizul Azizi Rasid, Mohd Azmi Jabar and Othman O. Khalifa*  
    141

15. GSM Security: Problems and Solutions  
    *Rashid A. Saeed and Othman O. Khalifa*  
    152

16. Recent Approaches to Wireless Physical Layer Security  
    *M. Tahir, Sigit P.W. Jarot and M.U. Siddiqi*  
    161

17. Securing OFDM-based Systems from the Physical Layer  
    *Sigit P.W. Jarot*  
    169

18. Simulation of Artificial Noise based Physical Layer Security  
    *Muhammad Izzat bin Zuirkiple and Sigit Puspito Wigati Jarot*  
    174
19. Secure IPv6 Address Generation
   Nashrul Hakiem, Mohammad Umar Siddiqi, and Sigit Puspito Wigati Jarot
   183

20. Video Streaming and Encrypting Algorithms
   Mohammed Abumual, Othman O. Khalifa, and Aisha-Hassan A. Hashim
   190

21. Wireless IP Camera based on Motion Detection Surveillance System
   Zeeshan Shahid and Khaizuran Abdullah
   217

22. Design of Mobile Phone Jammer
   Fauzun Abdullah Asuhaimi, Nur Fatin Mohd Zakki, and Khaizuran Abdullah
   223

Index
Chapter 17

Securing OFDM-based Systems from the Physical Layer

Sigit P.W. Jarot

17.1. Introduction

Mobile communication industry has been growing at an unexpectedly rapid pace in the last decade, much faster than all predictions, and it is expected that the growth will continue and accelerate at least over this decade. Orthogonal Frequency Division Multiplexing (OFDM) is one of the most promising choices for air interfaces. Many standards have been official selected OFDM for the physical layer solution such as LTE, 802.11, WiMax, etc. The widespread use of OFDM in these standards will survive at least in the coming decades of evolution of all that standards.

On the other hands, in recent years, there is increasing attention to an emerging research area that explores the possibility of achieving perfect-secrecy for data transmission among intended network, known as physical layer security. In the beginning, research on physical layer security is more on the information theoretical aspects such as: secrecy capacity in wiretap channel models, wireless secret key agreement, and wireless secret codes. However, some recent approaches have been shifting toward more practical physical layer security, such as the possibility of implementations in OFDM systems, the anechoic-chamber experimentations, and so on. In this chapter, we will be discussing about several approaches of securing physical layer in OFDM-based systems.

17.2. Typical OFDM System Model

A system model of Convolutional Coded OFDM considered is depicted in Figure 17.1. At the transmitter, the binary information data symbols are encoded using channel code. The encoded sequence is serial-to-parallel (S/P) converted into a number of parallel sequences, which equals to the number of subcarriers. In each parallel stream, the data symbols are. Pilot symbols are time-multiplexed to the data sequence to form a packet. Frequency interleaving is applied to the parallel sequences, in order to decrease fading correlation between adjacent parallel sequences, namely between successive symbols. The interleaved sequence is applied to Inverse Fast Fourier Transform (IFFT), to generate OFDM symbol. Guard interval is inserted between successive OFDM symbols to avoid inter-symbol interference. Then, the signals are transmitted over multipath fading channel.