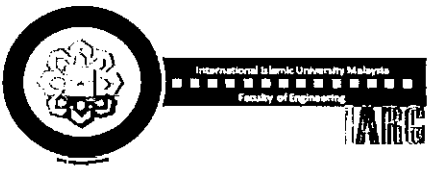
Topics in Coding, Cryptography and Information Security

Editors:

Mohammad Umar Siddiqi
Sigit Puspito Wigati Jarot
Othman Omran Khalifa

IIUM PRESS
2011



Topics in Coding, Cryptography and Information Security

Editors:

Mohammad Umar Siddiqi
Sigit Puspito Wigati Jarot
Othman Omran Khalifa

IIUM Press
2011

Published by:
IIUM Press
International Islamic University Malaysia

First Edition, 2011

Perpustakaan Negara Malaysia Cataloguing-in-Publication Data

Mohammad Umar Siddiqi, Sigit Puspito Wigati Jarot and Othman Omran Khalifa: Topics in Coding, Cryptography and Information Security

ISBN: 978-967-418-169-7

Member of Majlis Penerbitan Ilmiah Malaysia – MAPIM
(Malaysian Scholarly Publishing Council)

Printed by :
IIUM PRINTING SDN. BHD.
No. 1, Jalan Industri Batu Caves 1/3
Taman Perindustrian Batu Caves
Batu Caves Centre Point
68100 Batu Caves
Selangor Darul Ehsan

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 2
   Othman O. Khalifa, Emir Tabakovic, Zlatko Memisevic and Aisha-Hassan Abdullah

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

PART II: CHANNEL CODING

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

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

5. Viterbi Decoder: A Review and Implementation 42
   Noorainani Ainina Bt. Md Noor Albakri and Othman O. Khalifa

6. Zigzag Codes: High Rate Low Complexity Iterative Codes 53
Sigit P.W. Jarot

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

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

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

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

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

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

PART III: CRYPTOGRAPHY AND INFORMATION SECURITY

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

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

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

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

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

18. Simulation of Artificial Noise based Physical Layer Security 174
Muhammad Izzat bin Zurkiple and Sigit Puspito Wigati Jarot

19. Secure IPv6 Address Generation 183
Nashrul Hakiem, Mohammad Umar Siddiqi, and Sigit Puspito Wigati Jarot

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

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

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

Index

Chapter 18

Simulation of Artificial Noise based Physical Layer Security

Muhammad Izzat bin Zurkiple and Sigit Puspito Wigati Jarot

18.1. Introduction

Security enhancement in wireless communication usually considers, at least, three nodes: transmitter, receiver and an eavesdropper. The transmitter's concern is to send a message over the wireless channel such that the eavesdropper unable to decode it. Usually, the eavesdropper is assumed to be passive which means that the location and presence will be unknown to the transmitter. Many techniques have been proposed to use the characteristic of the radio channel itself in order to provide a secret communication in a mobile radio environment. However, the perfect secrecy of encryption cannot be guaranteed if the eavesdropper has infinite computational power [6]. However, according to recent information-theoretic studies it has been found some conditions that may provide a reliable and secure communication. The first study and work of information-theoretic security was introduced by Wyner [1]. He introduced a wiretap channel for point-to-point communication. Later, it was improved by Csiszar and Korner [2] by extending the concept of wiretap into broadcast channels. In the early days of these works, it showed that a positive secrecy capacity can be achieved if the receiver has a better channel than the eavesdropper. One of the implementation methods is by generating an artificial noise at the transmitter as proposed [4]. In this method, the noise is generated by the transmitter in which it is design such that the eavesdropper channel is degraded by the additional artificial noise. Thus, by selectively degrading the eavesdropper's channel. One of the scheme for generating the artificial noise is by using multiple transmit antenna to generate 'artificial' noise.

In this chapter, we provide a simulation of physical layer security based on the artificial noise. The chapter is organized as follows. In the Section 18.2, the system model for the simulation is described. In Section 18.3, we explain about how to generate the orthogonal signal using QR decomposition. The simulation results are provided in Section 18.4. And, the conclusion is presented in Section 18.5.

18.2. System Model

We now describe the approach that has been discussed before which is transmitting the artificially generated noise along with the information signal. The trans-