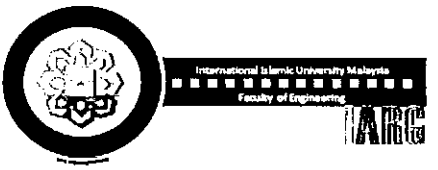
Topics in Coding, Cryptography and Information Security

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

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 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 those 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.