DESIGN AND ANALYSIS OF NEW COOPERATIVE RELAYING NETWORKS FOR ENHANCING PHYSICAL LAYER SECURITY

BY

AHMED HASSAN ABD EL-MALEK

A Dissertation Presented to the

DEANSHIP OF GRADUATE STUDIES

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the

Requirements for the Degree of

DOCTOR OF PHILOSOPHY

In

ELECTRICAL ENGINEERING

DECEMBER 2015

THESIS ABSTRACT

NAME:	Ahmed Hassan Abd El-Malek
TITLE OF STUDY:	Design and Analysis of New Cooperative Relaying Networks for Enhancing Physical Layer Security
MAJOR FIELD:	Electrical Engineering
DATE OF DEGREE:	December 2015

The advantages of wireless communication networks such as mobility, flexibility and installation simplicity nominated these networks to be a backbone of most of the people business and social activities. Despite these advantages and due to the nature of the wireless medium, one of the major problems in wireless networks is the security of the shared information over the network. As wireless communication networks are rapidly included in many daily activities resulting in a growing security concern, this security interest inspired researchers in the area of wireless network security to proposed new communication models with high data transmission security and to present a recent new security approach known as physical layer security approach.

Therefore, free space optical communications are presented as an effective se-

cure means of transferring data at high rates over short distances. Free space optical communication offers the potential of broadband communication capacity, as they operate on unlicensed optical beams, and therefore represent a cost-effective alternative and/or complement to their radio frequency counterparts.

Moreover, physical layer security is increasingly recognized as a potentially powerful means of ensuring secure communication over publicly accessible wireless networks. The main concept of physical layer security is to ensure that the wiretap channel of an eavesdropper is a degraded version of the main authorised channel. This increases the security of the wireless networks and that is highly applicable to emerging wireless systems.

In the area of cooperative cognitive radio, we propose two new bandwidth efficient cooperative cognitive radio systems which enable cooperation between the primary user system and the secondary user system. The goals of these newly proposed systems are to enhance the wireless network bandwidth efficiency, minimize the total error probability, and maximize the total sum-rate of the system. Then, we propose new cooperative scenarios to enhance the physical layer security performance against eavesdropping attacks. The results show that the proposed models enhance the spectral efficiency, improve the system error performance and increase the total achievable sum rate. In addition, the proposed models enhance the secrecy performance of primary networks against eavesdropping attacks.

In the area of mixed RF/FSO networks, we investigate performance of multiuser single-input-multiple-output mixed RF/FSO systems for different diversity

combining techniques employed by a multi-antenna relay node. Then, we propose power allocation model with the help cooperative jamming technique to enhance the physical layer security of the considered systems by utilizing the selected worst user based on the authorized relay selection. Finally, we study the impact of non-identical co-channel interference signals on the security reliability trade-off analysis of multiuser mixed RF/FSO networks. Then, we employ the cooperative jamming technique to enhance the system secrecy performance against eavesdropping attack. The results show that the proposed mixed RF/FSO networks increase the ergodic capacity and enhances the secrecy performance against eavesdropping attacks.