Ad Hoc Networks 25 (2015) 237–250

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Turning foes to allies in cognitive radio networks

Karim Khalil *, Eylem Ekici

Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH 43210, USA

ARTICLE INFO

Article history:
Received 7 May 2014
Received in revised form 9 September 2014
Accepted 23 October 2014
Available online 4 November 2014

Keywords:
Secrecy
Threats
Spectrum access
Stackelberg games

ABSTRACT

We study a class of problems in Cognitive Radio Networks where multiple half-duplex unlicensed (secondary) users can eavesdrop and jam the communications of licensed (primary) users unless granted access to communicate over the same spectrum band. The problem is to characterize the optimal rule for the primary system that grants spectrum access to selected secondary users and the optimal resource allocation for the secondary users. We model the problem as a Stackelberg game with the primary system as the leader. The equilibrium analysis shows that it is not always optimal to grant access to the strongest eavesdroppers. In addition, it is shown that transmitting secondary users can limit the eavesdropping capabilities of other secondary users, possibly leading to improved primary secure transmission data rate. Thus, interestingly, the outcome reveals a recruiting process that turns selected eavesdroppers into helping jammers under certain conditions. Finally, we propose a low complexity algorithm to select a subset of secondary users for transmission and evaluate the performance of the primary system when different number of secondary users are granted access through simulations.

1. Introduction

In this paper, we study a kind of unregulated cognitive radio networks in which unlicensed (secondary) users can possibly compromise confidentiality or disrupt the transmission of licensed primary users (PUs) by eavesdropping or jamming. Specifically, the eavesdropping secondary users (ESUs) may threaten the primary system by either eavesdropping primary traffic or jamming the primary receiver when they cannot transmit their own information. Since ESUs have half-duplex transceivers, they can either transmit or eavesdrop at any given time. Thus, granting spectrum access to selected ESUs to transmit their own information on the same spectrum band will neutralize their eavesdropping threat and may improve the secrecy of the transmission of PUs.

The novel idea of "threaten-to-access" in Cognitive Radio Networks (CRNs) was recently introduced in [1,2]. In this work, ESUs that wish to transmit their own information to a base station owned by the primary system and primarily serving PUs (e.g., a mobile network operator), may pose secrecy threats to PUs by eavesdropping the primary transmitted signals and hence decreasing primary secure transmission data rates.[1] The main goal, however, for ESUs is *communicating their own information* to the primary base station, which then serves as the common destination for both the primary and secondary users in this model. This is in contrast to most of the works in the literature on security [3], where the only objective of attackers is to minimize the achievable confidential rates of PUs. The scenario studied in this paper can model cases when sensitive PU traffic is to be transmitted (e.g., banking information) in the presence of untrusted nodes willing to access

* Corresponding author.
E-mail addresses: khalilk@ece.osu.edu (K. Khalil), ekici@ece.osu.edu (E. Ekici).

[1] For simplicity, we use the terms *secure rates* and *confidential rates* in the rest of the paper. This quantity is defined precisely in Section 2.

http://dx.doi.org/10.1016/j.adhoc.2014.10.015
1570-8705/© 2014 Elsevier B.V. All rights reserved.

spectrum. Our goal is to study fundamental performance and thus physical layer secrecy is considered as a measure of transmission privacy.

Physical layer secrecy is a notion introduced in information theory to measure confidentiality of data transmission with respect to unauthorized eavesdroppers. As defined originally by Shannon [4], perfect secrecy is achieved when the received signals at the eavesdropper are independent from the transmitted signals. The research in physical layer secrecy is largely motivated by Wyner's seminal work [5]. The main idea is to exploit the physical characteristics of the wireless channel (such as noise or fading) to confuse the eavesdroppers, in contrast to classical cryptographic techniques relying on secret keys [6,7]. Through means of artificial noise forwarding (also called cooperative jamming), achievable secrecy rates of legitimate transmitters can be improved [8,9]. In our work, transmitting ESUs can cause interference on the receivers at eavesdropping ESUs and thus can improve the secure rate of PUs.

In this paper, we seek to answer the following questions:

1. When is it optimal for the primary system to grant an eavesdropping secondary user (ESU) access to licensed spectrum?
2. When multiple ESUs exist, which subset of ESUs does the primary system select to grant spectrum access so that the primary secrecy rate is improved?
3. For each ESU, what is the optimal resource allocation?

To this end, we develop static non-cooperative games [10] that model interactions between half-duplex ESUs wishing to transmit their own information to a common destination (e.g., base station in a cellular system or access point in WiFi network) and a PU, which is interested in maximizing its secure rate. We adopt the information theoretic secrecy notion [11,12] as a measure of the confidentiality of the transmission of PU. In information theoretic secrecy schemes, security can be proven mathematically without imposing any restriction on the computational ability of the eavesdroppers, which is not possible in conventional cryptography. Its results are thus fundamental and independent on the state of technology. When an ESU is granted spectrum access and starts transmitting its own information, it is no longer an eavesdropper. In addition, when multiple ESUs exist, the transmission of a selected ESU causes interference on other receiving ESUs and therefore may limit their eavesdropping capabilities. Thus, selected ESUs may be considered as allies in this case. In this paper, we analyze equilibria of the strategic games and discuss their uniqueness properties. Moreover, we present interesting observations about some special cases and then provide a discussion on how our model can be implemented in cellular networks.

In [1,2], transmission coordination is employed between PU and ESUs (during transmission of ESU) where an optimal multiple access coding scheme [13] is used. In this paper, we consider more practical level of coordination between PUs and ESUs, where the decoder treats signals other than the intended ones as noise. Moreover, we consider the case when multiple ESUs exist in the cognitive radio network and characterize the optimal ESU spectrum access rule the primary system should employ to improve secure rate of the PU. We also show that this model bridges the gap between coordination models considered in [2] and conventional CRN models [14], where there is minimal interaction between PUs and SUs. Specifically, the scheme developed in this paper only requires changes to the admission control algorithms at the base station and the channel state feedback algorithm at PUs.

The rest of this paper is organized as follows. Section 2 presents our system model and our assumptions. In Section 3, we formulate a 2-player game, characterize equilibria in different cases of channel conditions and study their uniqueness. In Section 4, we extend the game to multiple ESUs. In Section 5, we discuss interesting observations on the outcome of the games considered. Finally, we evaluate the performance of the primary system through simulations in Section 6 and conclude the paper in Section 7.

2. Preliminaries and network model

In this section, we review results and definitions from information theory and game theory that are essential to our analysis. Then, we introduce our network model and the assumptions we make in the paper.

2.1. Wire-tap channel

In the presence of an eavesdropper, the achievable secrecy rate of a transmitter is defined as the rate at which the message of the sender is almost independent from the received signals at the eavesdropper. Achievability schemes (i.e., channel coding schemes) are designed to maximize the confusion at the eavesdropper while maximizing the achievable rate at the legitimate receiver by exploiting the wireless channel characteristics such as noise and fading. A Gaussian wiretap channel model consists of a transmitter, a legitimate (intended) receiver and an eavesdropper, where the signals received at both the legitimate receiver and the eavesdropper are corrupted by additive white Gaussian noise (AWGN). The secrecy capacity of this channel, when noise variances are unity, is given by [15]

$$R_s(P) = \log_2(1 + aP) - \log_2(1 + bP), \tag{1}$$

for $a \geqslant b$ and $R_s(P) = 0$ otherwise, where $a, b > 0$ are the channel power gains of the legitimate receiver's channel and the eavesdropper channel, respectively, and P is the transmission power.

In our game, we assume that an ESU is equipped with a half duplex transceiver and can either transmit to the common destination D or eavesdrop the transmission of PU at any given time. Thus, the channel model during ESU's eavesdropping is a wiretap channel. Throughout the paper, we refer to the channel between PU and D as the primary channel, the channel between ESU and D as the secondary channel, and the channel between PU and ESU as the eavesdropper channel.

We note that information theoretical notion of secrecy assumes no limitations on the computational power at