Applied Mathematics and Computation 296 (2017) 153–167

Contents lists available at ScienceDirect

Applied Mathematics and Computation

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

Stackelberg game based relay selection for physical layer security and energy efficiency enhancement in cognitive radio networks

He Fang[a], Li Xu[a,*], Kim-Kwang Raymond Choo[b]

[a] Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou, Fujian 350117, China

[b] Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249-0631, USA

ARTICLE INFO

Keywords:
Cognitive radio networks
Relaying protocol
Channel state information
Physical layer security
Power allocation
Stackelberg game

ABSTRACT

In cognitive radio networks, physical layer security is a promising secure wireless communication solution against eavesdropping attacks. In this paper, we study the problems of physical layer security and energy efficiency through power control and relays' cooperation, where both decode-and-forward and amplify-and-forward protocols are considered. We propose an one-leader one-follower Stackelberg (OLOFS) game model in the presence of multiple eavesdroppers, where optimal power allocation and pricing strategy can be determined to maximize the players' utilities. We also present a best relay selection criterion for OLOFS game model in both perfect channel state information (CSI) and imperfect CSI scenarios, which maximizes the secrecy capacity of the network. A distributed learning algorithm, inspired by the stochastic learning automata, is then proposed to achieve the equilibrium of the proposed games. Finally, we derive closed-form intercept probability expressions of the direct transmission scheme and the proposed game model over Rayleigh fading channels in both decode-and-forward and amplify-and-forward protocols. Our simulations demonstrate that the proposed game model improves network energy efficiency and has an improved performance against eavesdropping attacks, in comparison to Nash equilibrium, rand, and direct transmission schemes. We can also reduce the intercept probability by choosing a different relaying protocol (decode-and-forward or amplify-and-forward), based on the characteristic of channels in the proposed model.

1. Introduction

As higher layers in the open systems interconnection (OSI) model are subject to an increasing range of malicious attacks, implementing security solutions at the physical layer has received renewed attention [8]. For example, in the case of cognitive radio networks (CRNs), due to its broadcast nature, transmissions between primary users (licensed users, PUs) can be readily overheard and intercepted by unauthorized users; thus, vulnerable to potential eavesdropping attacks [23]. While cryptographic techniques [24,26] and authentication methods [30,31] can be deployed to secure the communications, these techniques generally result in increased communication and computational overheads which may be impractical in

* Corresponding author.
E-mail addresses: xuli@fjnu.edu.cn, 529015100@qq.com (L. Xu).

http://dx.doi.org/10.1016/j.amc.2016.10.022
0096-3003/

some real-world situations, especially in distributed systems. Trust management is another effective measure for defending attacks in distributed system, but it may not be a suitable mitigation strategy for eavesdropping attacks. For example, there is no direct communication between legitimate users and eavesdroppers. A number of solutions such as those presented in [21,29,32,33] are not designed to defend against eavesdropping attacks. Therefore, we will not be able to "manage" the trust between legitimate users and eavesdroppers.

Physical layer security (also known as information-theoretic security) was pioneered by Shannon [1] and subsequently extended by Wyner [2]. In [2], it was shown that perfectly secure data transmission can be achieved if the channel capacity of the main link is higher than that of the wiretap link. Physical layer security has also attracted the attention of the wireless security research community, as it allows one to leverage the properties of the wireless channel to secure communications between users [25]. Secrecy capacity, an important concept in physical layer security, is defined as the maximum transmission rate of the source-destination at which the eavesdropper is unable to decode any information [27].

Zou, et al. [23] identified and analyzed the tradeoffs in achieving security and reliability of wireless communications in the presence of eavesdropping attacks. They then proposed an opportunistic relay selection to improve the tradeoffs. A cooperation scheme in CRNs designed for secure communication was proposed in [25]. In another related work [15], distributed beamforming was used as relays to enhance the source's secrecy. Dong et al. [10] sought to address the challenges of achieving secure communications of one source-destination pair using multiple cooperating relays in the presence of one or more eavesdroppers. However, these schemes require prior knowledge of the eavesdropper's channel state information (CSI), which may be unrealistic in practice. Several other anti-eavesdropping techniques (e.g. artificial noise scheme [7], and cooperative beamforming [12]) have also been proposed in the literature. For example, Ding et al. [12] proposed the opportunistic use of relays for secret communications, which did not require the knowledge of the eavesdropper's CSI. However, such techniques consume additional power resources in order to generate artificial noise, and result in an increased computation complexity in the beamforming design.

Cooperative communication can be used to create a "win–win" situation for both PUs and secondary users (unlicensed users, SUs) in CRNs [20]. It can also be used to mitigate signal fading through multipath propagation in a radio environment, by utilizing the special diversity offered by cooperative nodes [16–18]. An appropriate selection of the relays increases the secrecy of the relaying link. Two main relaying protocols are generally used for cooperative diversity networks, namely: decode-and-forward and amplify-and-forward. In decode-and-forward protocol, the received message at the relay is decoded prior to forwarding to the destination. The relay re-encodes the decoded message and forwards it to the destination. In amplify-and-forward protocol, the received noisy message is amplified and forwarded to the destination. The destination then combines the information sent by the source and relay, before making a final decision on the transmitted message [19].

Although the interaction of cooperative diversity concept with secret communication provides opportunity for overcoming this limitation by cooperation (i.e. cooperative relaying and cooperative jamming), the relationships between secrecy capacity enhancement and energy efficiency, and secrecy capacity enhancement and the relaying protocols, have not been thoroughly investigated in the literature. We observe that the Stackelberg game theoretic approach [28] has been applied as a uncooperative game theoretic approach to extensively study cooperative communications [9,13,14]. We also remark that the Stackelberg game theoretic approach is different from the cooperative game theoretic approach [22]. In [13], the authors studied joint pricing and power allocation for dynamic spectrum access networks using Stackelberg game. The authors in [14] studied the relay power allocation and pricing problems, and modeled the interaction between the users and the relay as a two-level Stackelberg game. Thus, we are motivated to study the feasibility of integrating physical layer security and energy efficiency with the cooperative communication and Stackelberg game. We remark that a two-level Stackelberg game had been employed in [9] to jointly consider the benefits of the source node and the relay nodes in which the source node and the relay nodes were respectively modeled as a buyer and sellers.

In this paper, we aim to provide a secure cooperative communication and improve the energy efficiency for CRNs. More specifically, we formulate an one-leader one-follower Stackelberg (OLOFS) game based on the best relay selection model. In our formulation, we seek to maximize the secrecy capacity through cooperative relaying in the presence of multiple eavesdroppers, and improve the energy efficiency of system through power control. Both decode-and-forward and amplify-and-forward protocols are also considered in the cooperative communications. We note that a critical challenge is the imperfect CSI of CRNs, which may result in a poor performance in defending against the eavesdropping attacks and achieving the stability of the proposed game. Therefore, a distributed learning algorithm is proposed to achieve the Stackelberg equilibrium in the proposed game. We regard the contributions of this paper to be three-fold:

1. We propose an one-leader one-follower Stackelberg (OLOFS) game model with the aims of defending against eavesdropping and improving energy efficiency in the presence of multiple eavesdroppers in CRNs;
2. We propose a best relay selection for the OLOFS game model to maximize secrecy capacity in the context of perfect and imperfect CSI;
3. We derive closed-form intercept probability expressions of the proposed schemes and direct transmission scheme over Rayleigh fading channels.

We then evaluate the proposed game using simulations, in terms of its capability to defend against eavesdropping attacks and energy efficiency, against existing schemes namely: Nash equilibrium scheme, rand scheme, and direct transmission scheme. Our empirical findings also demonstrate that by detecting the Gaussian noise of channels, we can reduce