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/

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]

$$R_s(P) = \log_2(1 + aP) - \log_2(1 + bP), \quad (1)$$

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

the eavesdropper, in contrast to conventional cryptography. Thus, this paper presents fundamental limits where the results developed serve as bounds on the expected performance in practical systems in which eavesdroppers may not be able to fully decode secured information.

2.2. Game theory basics

Game theory provides an analytical framework to analyze situations of conflict between multiple decision makers that are ***rational, intelligent and selfish***. These attributes accurately characterize wireless devices designed to optimize their own performance. Here, we borrow definitions from [10] that are needed for the equilibrium analysis in the following sections.

A strategic game is any $\mathcal{G}$ of the form $\mathcal{G} = (\mathcal{N}, (\mathcal{S}_i)_{i\in\mathcal{N}}, (u_i)_{i\in\mathcal{N}})$, where $\mathcal{N}$ is the set of players in the game, and the utility of player i is given by $u_i(s_i, s_{-i})$, where $s_i \in \mathcal{S}_i$ is the strategy (or action) of player i chosen from the set of available strategies $\mathcal{S}_i$ and $\mathbf{s}_{-i}$ is the strategy profile of all other players except for player i chosen from $\times_{j\in\mathcal{N}-\{i\}}\mathcal{S}_j$. If the strategy sets of all players in $\mathcal{G}$ are finite sets, the game is said to be a finite game. A best response strategy s_i^* for player i is a strategy that maximizes $u_i(s_i, s_{-i})$ over $s_i \in \mathcal{S}_i$ given s_{-i}. In the following definitions, we focus on two-player games, i.e., $\mathcal{N} = \{1, 2\}$.

A Nash Equilibrium (NE) is a strategy profile at which no user has incentive to unilaterally deviate to other operating points.

Definition 1. An NE point is a strategy pair (s_1^*, s_2^*) such that

$$\begin{aligned} &u_1(s_1^*, s_2^*) \geqslant u_1(s_1, s_2^*), \quad \forall s_1 \in \mathcal{S}_1, \\ &u_2(s_1^*, s_2^*) \geqslant u_2(s_1^*, s_2), \quad \forall s_2 \in \mathcal{S}_2. \end{aligned} \tag{2}$$

Assume there exist two well defined unique mappings $T_1 : \mathcal{S}_2 \to \mathcal{S}_1$ and $T_2 : \mathcal{S}_1 \to \mathcal{S}_2$ such that for any fixed $s_2 \in \mathcal{S}_2, u_1(T_1(s_2), s_2) \geqslant u_1(s_1, s_2), \forall s_1 \in \mathcal{S}_1$ and for any fixed $s_1 \in \mathcal{S}_1, u_2(s_1, T_2(s_1)) \geqslant u_2(s_1, s_2), \forall s_2 \in \mathcal{S}_2$, i.e., T_i defines strategies that are best response to each strategy chosen by the other player. Let the set $D_i = \{(s_1, s_2) \in \mathcal{S}_1 \times \mathcal{S}_2 : s_i = T_i(s_j)\}$ for $i = 1, j = 2$ and $i = 2, j = 1$ be called the rational reaction set of player i and let $D_i(s_j) = \{s_i \in \mathcal{S}_i : (s_i, s_j) \in D_i\}$. Note that any pair in the set $D_1 \cap D_2$ is an NE according to Definition 1. Hence, a strategy profile $\mathbf{s}$ is an NE if and only if the strategy of every player in $\mathbf{s}$ is a best response to the other player's strategy.

The other type of game formulations we employ is Stackelberg games. In a Stackelberg game, a leader makes a decision about its own strategy and followers then choose their strategies accordingly. In the following definitions, we fix player 1 as the leader and player 2 as the follower. The leader chooses the strategy that maximizes its utility from the rational reaction set of the follower.[2]

[2] In games with more than two players and with one leader, the followers choose their strategies simultaneously after the leader has chosen its strategy.

Definition 2. A strategy $\tilde{s}_1 \in \mathcal{S}_1$ is a Stackelberg equilibrium strategy for the leader if

$$\inf_{s_2\in D_2(\tilde{s}_1)} u_1(\tilde{s}_1, s_2) \geqslant \inf_{s_2\in D_2(s_1)} u_1(s_1, s_2), \quad \forall s_1 \in \mathcal{S}_1. \tag{3}$$

The utility of the leader is a well defined quantity [10] and is given by

$$\tilde{u}_1 = \sup_{s_1\in\mathcal{S}_1} \inf_{s_2\in D_2(s_1)} u_1(s_1, s_2). \tag{4}$$

One important result about Stackelberg games is that every finite Stackelberg game admits a Stackelberg equilibrium strategy for the leader [10].

2.3. Network model

We consider an infrastructure-based wireless network where both primary users and secondary users are interested in communicating to a common destination (e.g., a base station) subject to average power constraints. In this paper, we consider a system comprised of one PU and N ESUs, all assumed to be in the same range. Our model is not restrictive in the sense that practical networks utilize orthogonal resources for different users (e.g., different time frequency resource blocks for different UEs in LTE networks). We denote PU as node 0 and ESUs as $\{1, 2, \ldots, N\}$. The average power constraint is denoted by $P_i, i \in \{0, 1, \ldots, N\}$.

We consider a time slotted system where channel gains are fixed during a time slot, and formulate one-shot games for each individual time slot. We also assume that channel gains are independent across users and reciprocal, i.e., the channel gain from node 1 to node 2 is identical to the channel gain from node 2 to node 1. Fig. 1 shows an example of the considered network when $N = 2$ with different channel gains labeled.

In this paper, we employ an interference model in which the receiver D treats signals from unintended transmitters (i.e., interference signals) as noise. We assume half-duplex ESUs. Each ESU can either transmit its own information or receive signals. In the receive mode, ESUs may decode the messages of PU and hence compromise its confidentiality. In our model, we do not consider collusion; we assume that each ESU acts independent of other ESUs.

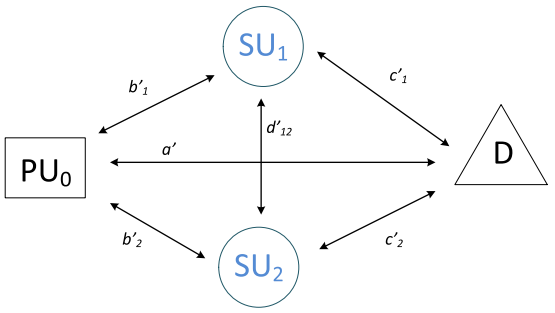

Fig. 1. Network Model with $N = 2$ ESUs. Primary system is composed of one PU (node 0) and the base station D. Different channel gains are marked on each link.

We model our problem as a non-cooperative game where the players are the base station D (representing the primary system) and the ESUs. Let $\mathcal{N} = \{1, \ldots, N\}$. The strategy of the primary system is to *select a subset of ESUs* $s_P = \mathcal{A} \subset \mathcal{N}$ for which the transmission is decoded in addition to transmission of PU, where $\mathcal{A} = \phi$ means no ESU is selected. The strategy of an ESU i is to select a time fraction $s_i \in [0,1], i \in \{0,1,\ldots,N\}$ such that if $s_i > 0$ it transmits with a power level $\frac{P_i}{s_i}$ for an s_i fraction of the time slot and eavesdrops the transmission of PU for the remaining fraction. If $s_i = 0$, then ESU i will eavesdrop for the entire time slot. We call ESU's strategy the compound jamming and eavesdropping threat strategy. Note that if an ESU is not selected by the base station, its transmission will not be decoded even if it chooses to transmit for a nonzero fraction of the time.

In this game, the primary system is interested in maximizing the PU's achievable secure rate while each ESU is interested in maximizing achievable rate minus the transmission cost. In this model, we assume that the energy spent by ESUs during reception can be ignored. In addition, since ESUs are interested in sending information to the base station, the base station can enforce its strategy s_P by decoding or ignoring transmission from certain ESUs. This fact motivates the Stackelberg equilibrium formulation in the next section.

3. Single ESU game

In this section, we analyze the scenario when only one ESU is present in the network. We characterize the cases when it is beneficial for the primary system to allow the ESU to transmit its own information. The results in this section are then used in the more interesting scenario with multiple ESUs, which is discussed in Section 4.

Here, the strategy of the base station is either to allow the ESU to transmit its own information, by choosing $s_P = 1$, or block ESU traffic by choosing $s_P = 0$. When $s_P = 1$, the base station decodes PU's and ESU's signals, treating signals other than the intended one as noise. When $s_P = 0$, the base station just ignores ESU's transmission (if any), treating it as noise.[3] Let $a = a'P_0, b_1 = b_1'P_0$ and $c_1 = c_1'P_1$. The utility functions of players in this game are given by:

$$u_P(s_P, s_1) = s_1 \log_2\left(1 + \frac{a}{1 + c_1/s_1}\right) + (1 - s_1)\left[\log_2\left(\frac{1+a}{1+b_1}\right)\right]^+, \quad (5)$$

$$u_1(s_P, s_1) = s_1 \log_2\left(1 + \frac{c_1/s_1}{1+a}\right)\mathbb{1}_{s_P=1} - s_1 \log_2(1 + \gamma_1 P_1/s_1), \quad (6)$$

where $\mathbb{1}_x = 1$ when statement x is true and $\mathbb{1}_x = 0$ otherwise, $[\cdot]^+ = \max\{\cdot, 0\}$ and γ_1 is ESU's transmission cost parameter. Note that s_P affects the primary utility u_P only indirectly, where s_1^* is function of s_P. Also since we consider a model in which PU always transmits at a fixed power level P_0, we ignore the constant power cost term in u_P as it will not affect the equilibrium analysis.

Let $s_1^*(s_P) = \arg\max_{s_1 \in [0,1]} u_1(s_P, s_1)$. We have the following property.

Lemma 1. *Jamming is a credible threat only if* $\gamma_1 = 0$.

Proof. ESU threatens the primary system by choosing s_1 such that $u_P(\cdot)$ is minimized if it is not granted access, i.e., if $s_P = 0$. Suppose $s_P = 0$, then, $u_1(0, s_1) = -s_1 \log_2\left(1 + \frac{\gamma_1 P_1}{s_1}\right)$. Since ESU is rational, it is easy to see that $s_1^*(0) > 0$ only if $\gamma_1 = 0$. □

Lemma 1 suggests the separation of the analysis into two cases according to the value of γ_1. Thus, in the following, we characterize the equilibrium for the single ESU Stackelberg game for each case separately.

3.1. Zero transmission cost for ESU

In this subsection, we focus on the analysis for the case where $\gamma_1 = 0$. First, we study the response of the follower in the game, i.e., ESU.

First, using the second derivative test, it can be shown that the first term in (6) is concave in s_1 for any non-negative value of s_1, when $s_P = 1$. Moreover, this term is monotonically increasing in s_1. Thus, $s_1^*(1) = 1$. It remains to find the response of ESU when primary system chooses not to grant it access, i.e., $s_1^*(0)$. In this case, ESU will try to minimize the utility of the primary system so that the threat may discourage the primary system from choosing $s_P = 0$ at the first stage of the game. Thus, ESU will solve the following optimization problem.

$$s_1^*(0) = \arg\min_{s_1 \in [0,1]} s_1 \log_2\left(1 + \frac{a}{1 + c_1/s_1}\right) + (1 - s_1)R_s, \quad (7)$$

where we used $R_s = \left[\log_2\left(\frac{1+a}{1+b_1}\right)\right]^+$. It can be seen that $u_P(s_1)$ is convex in s_1. Thus, the solution to (7) can be obtained by solving the following non-linear equation in s_1 (obtained by differentiating and equating to zero):

$$\frac{s_1 a c_1}{\ln 2 (s_1 + c_1)(s_1 + c_1 + a s_1)} + \log_2\left(1 + \frac{a s_1}{s_1 + c_1}\right) = R_s. \quad (8)$$

Now, the primary system knows exactly what will be the response of the ESU for each choice of the strategy s_P and can take an informed decision whether to grant the ESU spectrum access or not. Specifically, given the solution of (8), the base station will solve the following:

$$s_P^* = \arg\max_{s_P \in \{0,1\}} u_P(s_1^*(s_P)). \quad (9)$$

Remark 1. It is worth noting the significance of the compound jamming and eavesdropping threat in the Stackelberg game considered in the cases when jamming is a credible threat (i.e., $\gamma_1 = 0$). In this case, ESU can leverage its transmission to have a better position in the game, possibly forcing the primary system to grant it access to spectrum in cases where it was not possible without using jamming threat. Consider for example the

[3] It is worth noting that a related strategy set for ESUs was considered in [2] Specifically, a constant power time fraction strategy was considered where $s_1 = P_1$ for a time fraction α and $s_1 = 0$ for a fraction $1 - \alpha$. In this paper, however, we employ variable power level that scales with the fraction of time the ESU is transmitting, while the average power is fixed.

case shown in Fig. 2 where $a = 0.5, b_1 = 0.1, c_1 = 0.5$. If the ESU employs a purely eavesdropping threat ($s_1 = 0$ if $s_P = 0$), then the primary system equilibrium strategy is $s_P = 0$ since it maximizes the utility function u_P. However, if ESU employs a compound jamming and eavesdropping threat, then the primary system would achieve the lower utility value marked on the figure if $s_P = 0$ is selected. Thus, the primary system will select $s_P = 1$ and achieve $u_P(1,1)$.

3.2. Non-zero transmission cost for ESU

Here, we consider the case when $\gamma_1 > 0$. We study the properties of $u_1(s_P, s_1)$. First, from Lemma 1, we know that $s_1^*(0) = 0$. We now study the best response for the ESU when $s_P = 1$.

Lemma 2. *Let $\gamma_1 > 0$. Then, for the ESU utility in (6), we have*

$$s_1^*(1) = \begin{cases} 1; & \text{if } \frac{c_1}{1+a} > \gamma_1, \\ 0; & \text{otherwise.} \end{cases} \quad (10)$$

Proof. Given $s_P = 1$, it can be seen that the function $u_1(s_P, s_1)$ is monotonic in s_1. Specifically, when $\frac{c_1}{1+a} > \gamma_1$, it is an increasing function in s_1 while it is decreasing otherwise, concluding the proof. □

The following result follows immediately from Lemmas 2 and 1.

Proposition 1. *Let $\gamma_1 > 0$. Then, it is not restrictive for the ESU to only consider the discrete strategy space $s_1 \in \{0, 1\}$.*

Using the result in Proposition 1, the utility functions in (5) and (6) can alternatively be rewritten as:

$$u_P(s_P, s_1) = \left[\log_2\left(1 + \frac{a}{1 + c_1 s_1}\right) - \log_2(1 + b_1 \bar{s}_1)\right]^+, \quad (11)$$

$$u_1(s_P, s_1) = s_1\left(\log_2\left(1 + \frac{c_1}{1+a}\right)s_P - R_1^{\min}\right), \quad (12)$$

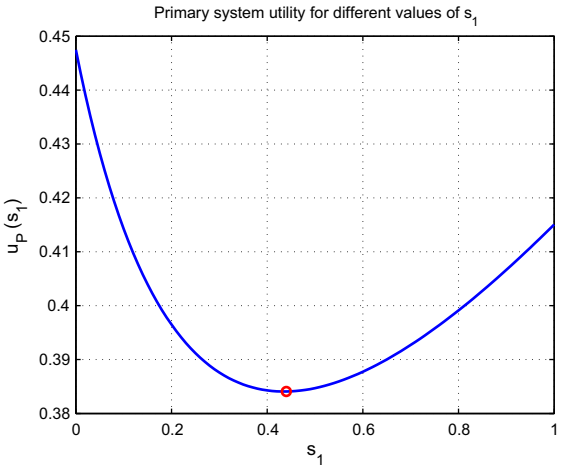

Fig. 2. Example showing the leverage of the compound jamming and eavesdropping threat of ESU.

where $\bar{s}_1 = 1 - s_1$, and $R_1^{\min} = \log_2(1 + \gamma_1 P_1)$. In the following, we will use the $\tilde{s}$ notation to denote the Stackelberg equilibrium strategy.

It can be seen that ESU only transmits when it is granted access (i.e., when $s_P = 1$) and when the achievable rate is above certain threshold $R_1^{\min}$. When ESU's transmission is not decoded (i.e., $s_P = 0$), however, ESU is better off not transmitting (i.e., chooses $s_1 = 0$) to avoid negative utility. The base station decides whether it would tolerate interference if it allowed the ESU to transmit. If the effect of interference on PU's utility is less than the effect of eavesdropping, then the primary system may choose $s_P = 1$ at the equilibrium.

As will be illustrated in Proposition 2, since the base station can enforce its strategy s_P, Stackelberg equilibrium will be the outcome of the game, with the base station as the leader. The outcome of the game has phase transition nature as follows.

Proposition 2. *Suppose $\gamma_1 > 0$. Then, ESU is granted spectrum access and transmits its own information if and only if*

$$\log_2\left(1 + \frac{c_1}{1+a}\right) > R_1^{\min}, \quad (13)$$

and

$$\frac{ac_1}{1 + a + c_1} < b_1. \quad (14)$$

Proof. To prove the proposition, we will characterize the Stackelberg equilibrium of the game, with the base station as the leader and ESU as follower, for all ranges of the parameters $a, b_1, c_1, R_1^{\min} > 0$ and show that the profile $(s_P, s_1) = (1, 1)$ is the only equilibrium if and only if (13) and (14) are true.

First, we find the best response of the ESU. The condition $\log_2(1 + c_1/(1+a)) > R_1^{\min}$ is equivalent to the first case of (10). In this case, the ESU is willing to switch from eavesdropping to transmission if it is granted spectrum access by the base station. Thus, the solution of the game in pure Stackelberg equilibrium strategy depends on the relative advantage the PU will gain, in terms of secure rate, if the ESU is granted spectrum access. Specifically, if $b_1 > ac_1/(1 + a + c_1)$, then $\tilde{s}_P = 1$ and the solution of the game is $(\tilde{s}_P, \tilde{s}_1) = (1, 1)$. However, if $b_1 \leqslant ac_1/(1 + a + c_1)$, then the solution is $(0, 0)$.

On the other hand, when $\log_2(1 + c_1/(1+a)) \leqslant R_1^{\min}, s_1 = 1$ is a strictly dominated strategy for the ESU and $\tilde{s}_1 = 0$, independent of s_P. Thus, both the strategy profiles $(0, 0)$ and $(1, 0)$ are pure strategy Stackelberg equilibria in this case. The non-uniqueness here does not create a problem since the utility of the primary system (leader) is unique. This concludes the proof. □

The equilibrium analysis of the discrete game considered in this section suggests that ESU is willing to switch from eavesdropping to transmission only if the PU channel (i.e., a) is weak enough with respect to its rate requirement $R_1^{\min}$. In this case, the primary system will grant ESU spectrum access if the effect of ESU's eavesdropping threat is worse than its interference effect on the transmission of PU. Otherwise, ESU will only eavesdrop PU traffic.

The analysis also reveals the fact that sometimes the primary system prefers to tolerate noise from ESU than to tolerate eavesdropping. In the following section, we study the multiple-ESU scenario and investigate how noise from one ESU can even improve the secure rate of the PU by interfering with PU's signals at other eavesdroppers.

4. The multiple-ESU game

In this section, we extend the game in Section 3.1 to multiple ESUs. Here, we consider the case when only one ESU can be granted spectrum access. We study a 3-player static game with the base station and two ESUs (nodes 1 and 2) as shown in Fig. 1. It can be seen that the extension to the game with larger number of ESUs is straightforward. We also discuss the extension to grant spectrum to multiple ESUs in Sections 5 and 6. In addition, in the remaining parts of the paper, we focus on the scenario with $\gamma_i > 0, \forall i$ for analytical tractability of the analysis.

In this game, the strategy set of the base station is $s_P \in \{0,1,2\}$ while the strategy set of each ESU is $s_i \in \{0,1\}, i \in \{1,2\}$, as in the previous section. Utility functions are given as follows.

$$u_P = \left[\log_2\left(1+\frac{a}{1+c_1 s_1 + c_2 s_2}\right) - \log_2\left(1+\max\left\{\frac{b_1\bar{s}_1}{1+d_{12}s_2}, \frac{b_2\bar{s}_2}{1+d_{21}s_1}\right\}\right)\right]^+, \quad (15)$$

$$u_i = s_i\left(\log_2\left(1+\frac{c_i}{1+a+c_{3-i}s_{3-i}}\right)\mathbb{1}_{s_P=i} - R_i^{\min}\right), \quad i \in \{1,2\}, \quad (16)$$

where $d_{ij} = d'_{ij}P_j, d'_{ij}$ is the channel gain between ESUs i and j, and $R_i^{\min} = \log_2(1+\gamma_i P_i)$.

From (15), it can be seen that only those ESUs that are not transmitting (i.e. with $s_i = 0$) can eavesdrop PU's transmission. Also the capability of reducing the confidential rate of PU is reduced by interference from other transmitting ESUs as shown by the denominator of the second term in (15).

Now, we define multiple quantities that will help us characterize equilibrium points for the game. Let

$$R_0^0 = [\log_2(1+a) - \log_2(1+\max\{b_1,b_2\})]^+, \quad (17)$$

$$R_0^1 = \left[\log_2\left(1+\frac{a}{1+c_1}\right) - \log_2\left(1+\frac{b_2}{1+d_{21}}\right)\right]^+, \quad (18)$$

$$R_0^2 = \left[\log_2\left(1+\frac{a}{1+c_2}\right) - \log_2\left(1+\frac{b_1}{1+d_{12}}\right)\right]^+, \quad (19)$$

$$\Delta R_i = \log_2\left(1+\frac{c_i}{1+a}\right) - R_i^{\min}. \quad (20)$$

where R_0^0 is PU's achieved utility when both ESUs are eavesdropping, $R_0^1(R_0^2)$ is PU's achieved utility when ESU 1 (ESU 2) is transmitting and ESU 2 (ESU 1) is eavesdropping, and ΔR_i is the slope of the utility function of ESU i when it is the only transmitting ESU. The primary system offers spectrum access to an ESU i only if $R_0^i > R_0^0$. In addition, an ESU i accepts spectrum access offer and switch from $s_i = 0$ to $s_i = 1$ only if $\Delta R_i > 0$.

We now characterize equilibrium points for the multiple-ESU game. In this game, the base station is the leader who chooses its strategy first then announces it to the followers. ESUs then play a Nash game by taking simultaneous decisions, given the strategy announced by the base station. The following results are derived based on the equilibrium analysis in Section 3.

First, the best response of ESU $i, i \in \{1,2\}$, is given by:

$$T_i(s_P) = \begin{cases} 1; & \text{if } \Delta R_i > 0,\ s_P = i \\ 0; & \text{otherwise.} \end{cases} \quad (21)$$

Given the knowledge of the best response of ESUs, the base station now decides its strategy then announces it. Given the strategy of the leader in the Stackelberg game, both ESUs then react by playing a 2-player Nash game. We now check the outcome of the 3-player non-cooperative game, depending on the network model parameters:

1. When $\Delta R_1, \Delta R_2 > 0$ (all ESUs are motivated to transmit), then:
   (a) If $R_0^0 > R_0^1, R_0^2$ (if spectrum cannot be granted to either ESU), then $\tilde{s}_P = 0$ and the solution of the game is $(0,0,0)$.
   (b) If $R_0^0 \not> R_0^1, R_0^2$ and $R_0^1 < R_0^2$ (if spectrum can be granted to ESU 2), then the solution is $(2,0,1)$. The solution is $(1,1,0)$ otherwise.
2. When $\Delta R_1 < 0 < \Delta R_2$ (if only ESU 2 is motivated to transmit), then the solution depends on the value of R_0^2. If $R_0^0 < R_0^2$ (if spectrum can be granted to ESU 2), the solution is $(2,0,1)$. Otherwise, it is $(0,0,0)$. A similar result holds when only ESU 1 is motivated to transmit.
3. When $\Delta R_1, \Delta R_2 < 0$ (no ESU is motivated to transmit), the points $(0,0,0), (1,0,0)$ and $(2,0,0)$ all represent the solutions to the non-cooperative game. However, at each of the three points, the utility of all players is the same.

4.1. ESU selection algorithm

The equilibrium analysis shown above suggests the following ESU selection algorithm, to be implemented at the base station. Let $\mathcal{W}$ be the set of ESUs such that for all $i \in \mathcal{N}, i \in \mathcal{W}$ if $\Delta R_i > 0$. Also let $\mathcal{F}$ be the set such that for all $i \in \mathcal{N}, i \in \mathcal{F}$ if $R_0^i > R_0^0$. $\mathcal{W}$ represents the set of ESUs in $\mathcal{N}$ that can tolerate noise from PU's transmission and are willing to switch from eavesdropping mode to transmission mode, while $\mathcal{F}$ represents the set of ESUs that can improve the secure rate of PU if granted spectrum access. It is then the duty of the base station to select an ESU from $\mathcal{W} \cap \mathcal{F}$ such that the utility u_P is maximized. If the intersection of $\mathcal{W}$ and $\mathcal{F}$ is empty in a certain time slot, then no ESU is granted spectrum access in that time slot.

5. Discussion

In this section, we present some interesting observations on the outcome of the multiple-ESU game and also discuss extensions to the model considered.

5.1. Interference vs. eavesdropping

When an ESU is selected to transmit and d_{12} is large, the negative term in the achievable PU secrecy rate expression becomes small. The decision is then based mainly on how interference affects the achievable PU rate at D. This models, for example, the case when ESUs are very near to each other geographically. When d_{12} is small (e.g., far apart ESUs), both interference effect at D and eavesdropping effect are significant in the decision of PU. In this case, our model complements the model in [2] which focused only on the eavesdropping effect.

Now, consider the scenario where $b_1 > b_2$ and $R_1^{\min}$ is large. This implies that $\Delta R_1, \Delta R_2 > 0$ and $R_0^2 > R_0^1 > R_0^0$ implying the solution $(2,0,1)$. So even though ESU 1 has better eavesdropping capabilities than ESU 2, ESU 2 is granted access since the relative advantage gained by PU from interference on ESU 1 (specified by d_{12}) is larger than the relative disadvantage of interference on D (specified by c_2). In addition, it shows that its not always optimal to select the ESU with the largest eavesdropping capabilities.

5.2. Distributed property

The strategies developed in this paper are distributed in nature since they are based on equilibrium concepts of game theory. However, knowledge of different channel parameters is assumed at each node, which limits the distributed decision making process. Nevertheless, this complete information assumption can be justified in a practical scenario that guarantees knowledge of different channel parameters at different nodes as follows.

For a wireless cellular network, PU transmits to the base station. Each ESU that wishes to transmit its own information to the base station announces its presence by sending its minimum rate requirement to transmit. After an announcement by ESU i, all other nodes in the network can measure their channel gain from node i. Recall that we assume reciprocal channels. Then, PU reports the values of eavesdropper channel gain $b_i, \forall i$, to the base station, since it is the actual decision maker in the game on behalf of PU. Since each ESU is actually interested to access the channel, each ESU sends channel gain with other ESUs to the base station to show its jamming capabilities. Note that cheating in reporting jamming capabilities can be detected at the base station by comparing channel gains reported from different ESUs. The base station then will have all the necessary information to decide whether it will grant access to an ESU and the index of that ESU.

5.3. A comment on implementation

The parameter s_P in the games we developed is decided by the base station. Consequently, when P_0 is fixed in the discrete game, there will be no involvement of PUs in the selection algorithm other than reporting eavesdropper channel gain, which make this scheme suitable for practical applications with simple modifications to current cellular networks that assign one PU per resource (time or frequency slot). Research in CRNs is usually classified either in commons model, where the primary system is oblivious to secondary users activity, or property rights model where primary users get paid by secondary users (e.g., using cooperative communications techniques) to be granted spectrum access [16,17]. Consequently, this can be considered as an intermediate case between commons model cognitive radio networks with no interaction between the two systems and property rights model where there is more interaction.

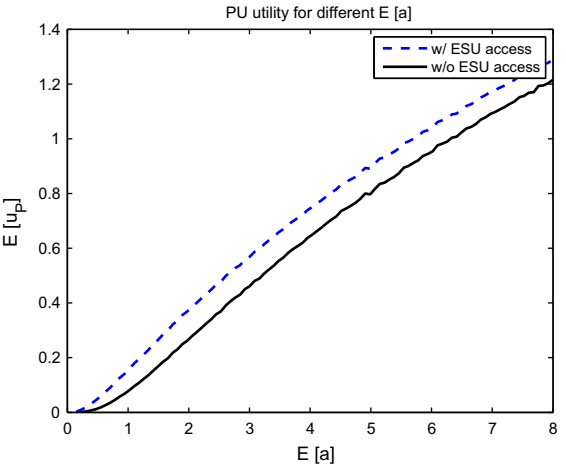

Fig. 3. PU utility vs. average channel gain.

5.4. Multiple-ESU transmission

In this section, we discuss the extension where the primary system is willing to decode messages of $M \leqslant N$ ESUs simultaneously. We denote the subsets of ESUs that are granted and denied spectrum access as $\mathcal{A}$ and $\mathcal{A}^c$, respectively, where $|\mathcal{A}| \leqslant M$ and $\mathcal{A}^c = \mathcal{N} - \mathcal{A}$. Let the strategy profile of the players in the game be defined as $\mathbf{s} = (\mathcal{A}, s_1, s_2, \cdots s_N)$.

In this case, the utility functions of the primary system and ESUs, respectively, are given by:

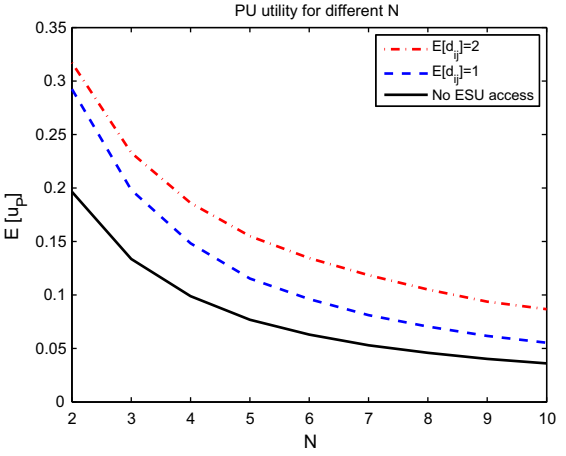

Fig. 4. PU utility vs. number of ESUs.

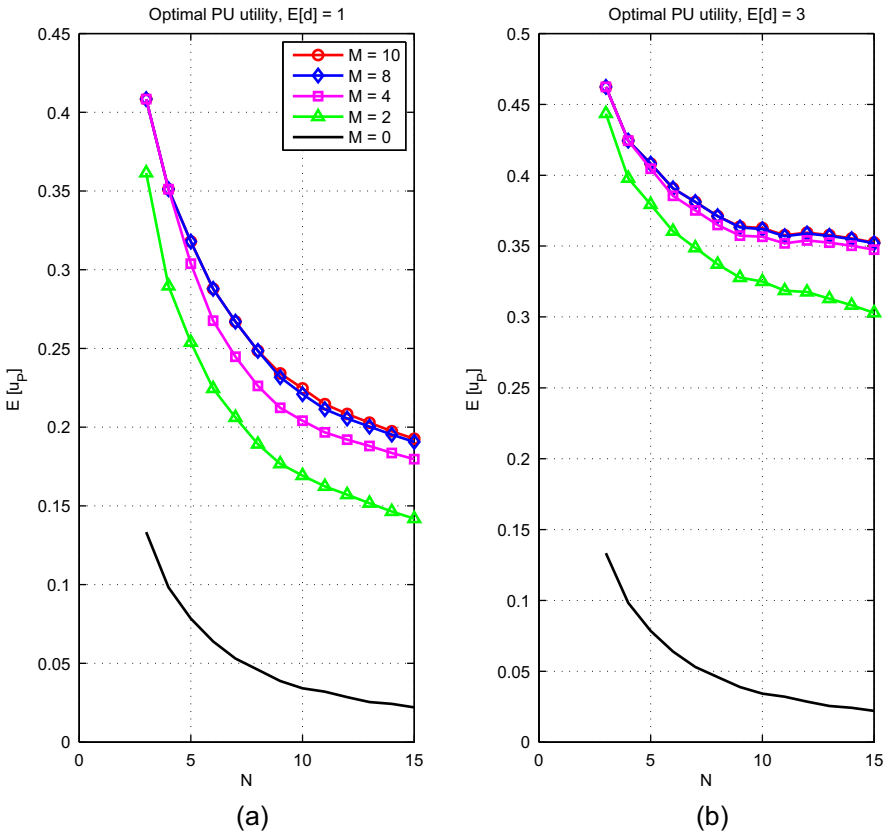

Fig. 5. Optimal PU utility vs. total number of ESUs when $\mathbb{E}[b_i] = \mathbb{E}[c_i] = 1,\ \forall i$: (a) when $\mathbb{E}[d] = 1$ and (b) when $\mathbb{E}[d] = 3$.

$$u_P(\mathbf{s}) = \left[\log_2\left(1+\frac{a}{1+\sum_{i=1}^{N} c_i s_i}\right) - \log_2\left(1+\max_{i\in\mathcal{N}}\left\{\frac{b_i \bar{s}_i}{1+\sum_{j\in\mathcal{N}-\{i\}} d_{ij} s_j}\right\}\right)\right]^+ \quad (22)$$

$$u_i(\mathbf{s}) = s_i\left[\log_2\left(1+\frac{c_i}{1+a+\sum_{j\in\mathcal{N}-\{i\}} c_j s_j}\right) \mathbb{1}_{i\in\mathcal{A}} - R_i^{\min}\right], i \in \mathcal{N}. \quad (23)$$

Here, an extended version of the ESU selection algorithm in Section 4.1 can also be adopted by the base station (note that the definitions (17)–(20) extends naturally to include the case when $N > 2$). In particular, we define $\mathcal{W}$ and $\mathcal{F}$ as subsets of the power set of $\mathcal{N}$ where each element has a cardinality less than or equal M such that $\forall \tau \in \mathcal{W}, \Delta R_i > 0\ \forall i \in \tau$ and $\forall \eta \in \mathcal{F}, R_0^{\eta} > R_0^0$. It is then the duty of the primary system to find the subset of ESUs $\mathcal{A}^* \in \mathcal{W} \cap \mathcal{F}$ that maximizes PU's utility.

It is easy to see that the problem of finding the optimal set $\mathcal{A}^*$ is combinatorial in nature and thus has worst case exponential complexity. In fact, the worst case complexity scales as $O\left(\sum_{k=1}^{M}\binom{N}{k}\right)$. Thus, the parameter M represents the tradeoff between optimality and complexity ($M = N$ has complexity of $O(2^N)$ while $M = 1$ has complexity of $O(N)$).

To address the large computational complexity of finding the optimal subset of ESUs to be granted spectrum when M and N are large, we propose a polynomial-complexity ESU selection algorithm, (Algorithm 1) that iteratively constructs a set of up to $C^{\max}$ ESUs at each iteration until at most M ESUs are selected at the conclusion of the algorithm. Let $\mathcal{C}$ be an arbitrary subset of $\mathcal{N}$ with $|\mathcal{C}| \leqslant C^{\max}$. For the disjoint sets $\mathcal{A}, \mathcal{C}$, we have the following definitions:

$$\tilde{u}_P(\mathcal{C},\mathcal{A}) = \left[\log_2\left(1+\frac{a}{1+\sum_{i\in\mathcal{C}\cup\mathcal{A}} c_i}\right) - \log_2\left(1+\max_{i\in\mathcal{A}^c-\mathcal{C}}\frac{b_i}{1+\sum_{k\in\mathcal{C}\cup\mathcal{A}} d_{ik}}\right)\right]^+,$$

$$\tilde{u}_j(\mathcal{C},\mathcal{A}) = \log_2\left(1+\frac{c_j}{1+a+\sum_{i\in\mathcal{A}\cup\mathcal{C}-j} c_i}\right) - R_j^{\min}. \quad (24)$$

In a given iteration of Algorithm 1, the set $\mathcal{A}$ represents the ESUs selected so far. To guarantee that the ESUs added to the set $\mathcal{A}$ at each iteration may only improve the primary utility, the set $\mathcal{F}_m$ is constructed as in (26). In other words, the subsets of ESUs considered are those that can only improve the primary utility given the jamming and noise effect of the ESUs admitted so far. Since Algorithm 1 sequentially finds at most M candidate[4] ESUs to be granted access, the algorithm stops whenever $\mathcal{A} = M$ or primary utility cannot be improved ($\mathcal{F}_m = \phi$). In each iteration, up to $C^{\max}$ ESUs are selected. Thus, the parameter $C^{\max}$ characterizes the complexity of the algorithm as $O(N^{C^{\max}})$. When $C^{\max} = 1$, then at each iteration of the algorithm, only the best ESU (or no ESU) is selected from the remaining ESUs according to optimal ESU spectrum access algorithm in Section 4. The selected ESU is then removed from the set

[4] Note that for a given maximum number of selected ESUs $M \leqslant N, |\mathcal{A}^*| = K$, where $K \leqslant M$. Thus, it might be the case that only selecting $K < M$ out of N ESUs maximizes $u_P(\mathbf{s})$ when at most M ESUs are allowed access.

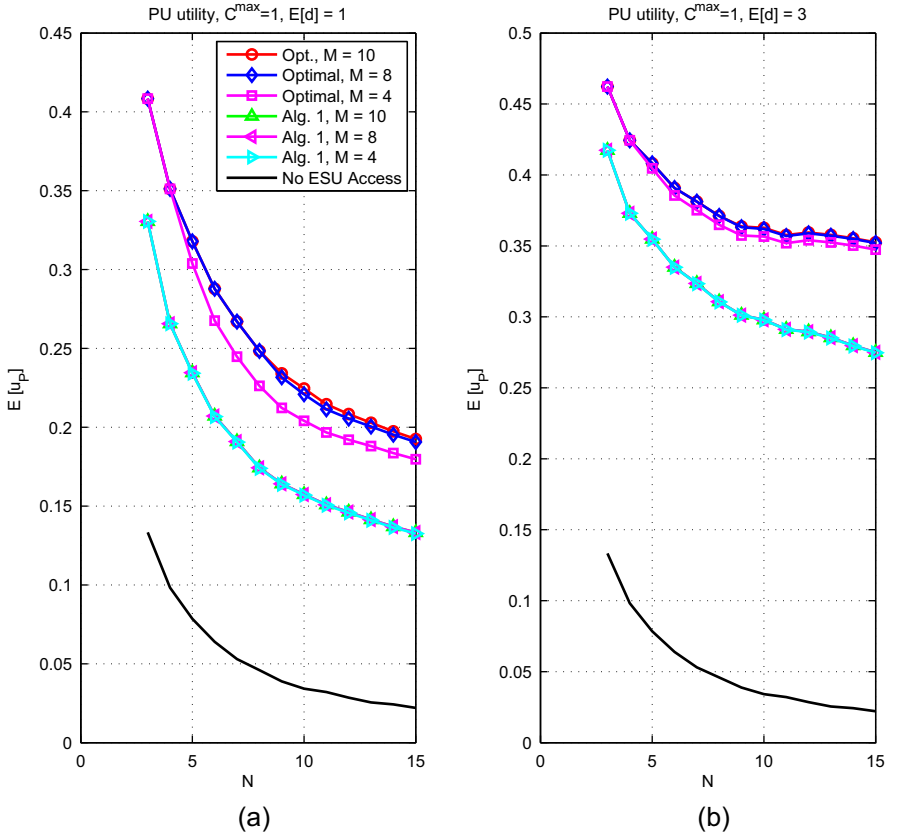

Fig. 6. Performance of Algorithm 1 when $C^{\max} = 1, \mathbb{E}[b_i] = \mathbb{E}[c_i] = 1, \ \forall i$: (a) when $\mathbb{E}[d] = 1$ and (b) when $\mathbb{E}[d] = 3$.

of remaining ESUs and added to $\mathcal{A}$ to affect the selection of the next ESU in the next iteration. In Section 6, we show that increasing M yields only a diminishing gain for the primary system for the symmetric case where ESUs have similar (Rayleigh) channel statistics. It follows that increasing $C^{\max}$ yields a diminishing gain as well.

Algorithm 1. Iterative ESU Selection

Input: $M, C^{\max}, P_0, a, \gamma_i, P_i, b_i, c_i, d_{ij} \ \forall i \neq j \in \mathcal{N}$
Output: $\mathcal{A} : |\mathcal{A}| \leqslant M$
Initialize $\mathcal{A} = \phi, m = 0$
while $m < M$ **do**
  Construct the sets $\mathcal{W}_m, \mathcal{F}_m$ such that

$$\mathcal{W}_m = \{\mathcal{C} \subset \mathcal{N}, |\mathcal{C}| \leqslant C^{\max} : \forall j \in \mathcal{C}, \tilde{u}_j(\mathcal{C}, \mathcal{A}) > 0\}, \quad (25)$$
$$\mathcal{F}_m = \{\mathcal{C} \subset \mathcal{N}, |\mathcal{C}| \leqslant C^{\max} : \tilde{u}_P(\mathcal{C}, \mathcal{A}) > \tilde{u}_P(\phi, \mathcal{A})\} \quad (26)$$

  if $\mathcal{W}_m \cap \mathcal{F}_m = \phi$ **then**
    break
  else
    $\mathcal{C}^* = \arg\max_{\mathcal{W}_m \cap \mathcal{F}_m} \tilde{u}_P(\mathcal{C}, \mathcal{A})$
    $\mathcal{A} = \mathcal{A} \cup \mathcal{C}^*$
    $m = m + |\mathcal{C}^*|$
  end if
end while

The complexity of Algorithm 1 is function in the parameters M, N and $C^{\max}$. In particular, the parameter $C^{\max}$ is introduced in the algorithm to reduce the complexity compared to the optimal algorithm that finds best M ESUs. It can be seen that the worst case complexity is given by $O\left(M \sum_{k=1}^{C^{\max}} \binom{N}{k}\right)$ while the best complexity is $O\left(\frac{M}{C^{\max}} \sum_{k=1}^{C^{\max}} \binom{N}{k}\right)$. For example, when $C^{\max} = M = N$, the complexity is $O(2^N)$. However, when $C^{\max} = 1$, the complexity is $O(MN)$.

It can be seen that primary utility achieved with Algorithm 1 approaches the optimal utility in some special cases. For example, it can be shown that Algorithm 1 is asymptotically optimal as the values of d_{ij} increases for all i, j (for example, when ESUs are collocated and channel gain from each ESU to another ESU is large), or as eavesdropper channel gains are small compared to the primary and secondary channel gains, which will be verified numerically in the next section. Specifically, in Section 6.2, we evaluate the performance of Algorithm 1 and compare it to the upper bound optimal case $C^{\max} = M$.

6. Performance evaluation

In this section, we evaluate the performance of the primary network for different ESU spectrum access schemes. First, we study the case where at most one ESU is granted

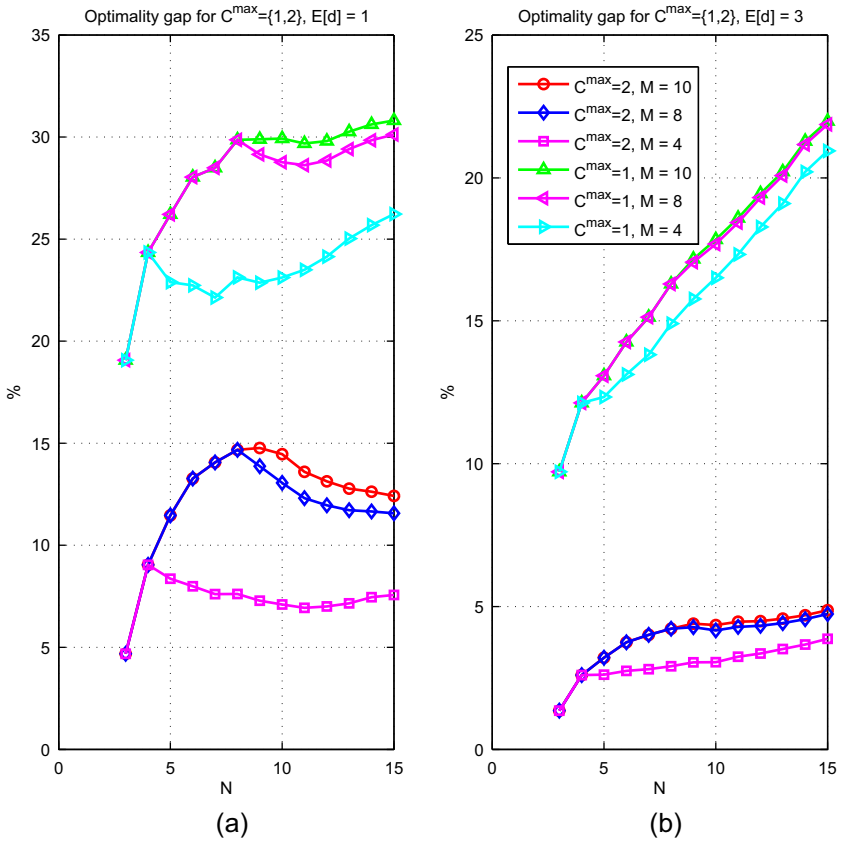

Fig. 7. Performance gap between optimal ESU selection and Algorithm 1, $\mathbb{E}[b_i] = \mathbb{E}[c_i] = 1,\ \forall i$: (a) when $\mathbb{E}[d] = 1$ and (b) when $\mathbb{E}[d] = 3$.

spectrum access. Then we move to the case when multiple ESUs can be granted spectrum simultaneously.

6.1. Only one ESU spectrum access

Here, we compare the achievable utility when spectrum access is not granted to ESUs vs. when access is granted based on the outcome of the multiple ESU game presented in Section 4. The comparison is done for varying average of PU channel gain and varying number of ESUs.

First, we present an example of a one-shot game, i.e., a single time slot. Consider the scenario when $N = 3$. Let $P_0 = 1, \gamma_i = 0.5, P_i = 1, i \in \mathcal{N}$. We generate a random sample of the channel gains a, b_i, c_i, d_{ij}, for $i,j \in \mathcal{N}, i \neq j$, according to an exponential distribution with unit mean. In this example, $a = 0.8253$, $b = [1.4219\ 2.24087\ 0.2103]$, $c = [0.3226\ 0.9174\ 0.1677]$, $d_{12} = d_{21} = 5.7693$, $d_{13} = d_{31} = 0.4287$ and $d_{23} = d_{32} = 1.1485$. Given theses, values, rates can be calculated from as $R_0^0 = 0$, $R_0^1 = 0.2870$, $R_0^2 = 0.2414$ and $R_0^3 = 0$. For the ESUs, only $\Delta R_1, \Delta R_2 > 0$. Thus, ESU 3 is not willing to switch to transmit mode. Since $R_0^1 > R_0^2 > R_0^0$, the base station grants ESU 1 access to spectrum by choosing $s_P = 1$. Note that ESU 2 is the most capable eavesdropper in this example.

Next, we evaluate the performance over many time slots. We focus on Rayleigh fading channels, where the channel gains are exponentially distributed. We calculate the average utility over a simulation period of 100,000 time slots, where we assume channel gains to be i.i.d across time slots. In this case, we assume that the number of ESUs is fixed during the entire simulation period to $N = 5$. In addition, we consider the uniform case across ESUs where average channel gains are set to $\mathbb{E}[b_i] = \mathbb{E}[c_i] = \mathbb{E}[d_{ij}] = 2, i,j \in \mathcal{N}, i \neq j$. Power cost parameters are set to $\gamma_i = 0.1, i \in \mathcal{N}$ and unit transmission power is assumed for all nodes in the network. In Fig. 3, the utility of the primary system is plotted against $\mathbb{E}[a]$ when the base station grants spectrum access to a selected ESU according to the algorithm in Section 4. The solid curve shows the utility achieved by the primary system when ESUs are not granted access. It is clear that granting access to SUs yields improved primary utility for all values of PU average channel gain.

We then study how PU utility varies with the number of ESUs in the network for the same value of parameters considered in the previous part. In Fig. 4, we plot $\mathbb{E}[u_0]$ against a varying number of ESUs for two different values of $\mathbb{E}[d_{ij}]$. It is shown that the advantage of granting spectrum access to ESUs diminishes for large number of ESUs, since the probability of existence of more than one ESU with large

eavesdropper channel gain increases. However, this advantage diminishes at a lower rate if $\mathbb{E}[d_{ij}]$ is increased (e.g., for nearby ESUs).

6.2. Multiple ESU spectrum access

In this section, we also consider Rayleigh fading channels and focus on a uniform case where all ESUs have the same channels statistics, transmission power constraints and transmission costs. The performance of Algorithm 1 is evaluated for different values of $C^{\max}$.

We fix $P_0 = P_i = 1, \gamma_i = 0.01, \forall i$. To cover different scenarios for the channel conditions, we consider different regimes for the eavesdropper and secondary channel parameters. In particular, we fix the primary channel average gain $\mathbb{E}[a]$ and study the cases where $\mathbb{E}[b_i] = \mathbb{E}[c_i], \mathbb{E}[b_i] < \mathbb{E}[c_i]$ and $\mathbb{E}[b_i] > \mathbb{E}[c_i]$ respectively. For each of these scenarios, we present the results for both the cases of small and large $\mathbb{E}[d_{ij}]$.

First, in Fig. 5, we plot the optimal average primary utility vs. the total number of ESUs for different M, the maximum number of ESUs to be granted spectrum. Exhaustive search is employed to perform the optimal ESU selection over the set $\mathcal{W}_m \cap \mathcal{F}_m$ each time slot. Here, $\mathbb{E}[b_i] = \mathbb{E}[c_i] = 1, \ \forall i$ and we consider two values for $\mathbb{E}[d_{ij}]$. The utility of the primary system decreases with N for any value of M, as in the case in Section 6.1. In addition, it can be seen that the gain achieved by granting access to a larger set of ESUs is diminishing for larger values of M. We also note that the same trend of the achieved utility for the other regimes (e.g., Fig. 8). Moreover, for larger $\mathbb{E}[d_{ij}]$, this gain diminishes faster. This result can be justified from (22) by noting that less ESUs are needed to be granted spectrum access and reduce the eavesdropping rate of other EUS when inter-ESU channels are stronger.

In Fig. 6, we plot the expected primary utility vs. N for both the optimal selection rule and Algorithm 1 with $C^{\max} = 1$ for different values of M and $\mathbb{E}[d_{ij}]$. It can be seen that the primary utility achieved by Algorithm 1 exhibits the same behavior with N, M and $\mathbb{E}[d_{ij}]$ as in the optimal case, however with reduced performance.

We also plot the primary utility gap (in percentage) between the suggested algorithm and the optimal utility in Fig. 7. First, the gap generally increases with N. For small values of N, curves matches for the plotted values of M since all available ESUs can be granted spectrum access. In addition, we note that the rate of increase in the optimality gap diminishes with increasing M, since both the optimal utility and that achieved by Algorithm 1 saturate with M (see Fig. 6). The performance of Algorithm 1 improves for larger ESU mutual interference $\mathbb{E}[d]$ (e.g., when different ESUs are physically closer to each other).

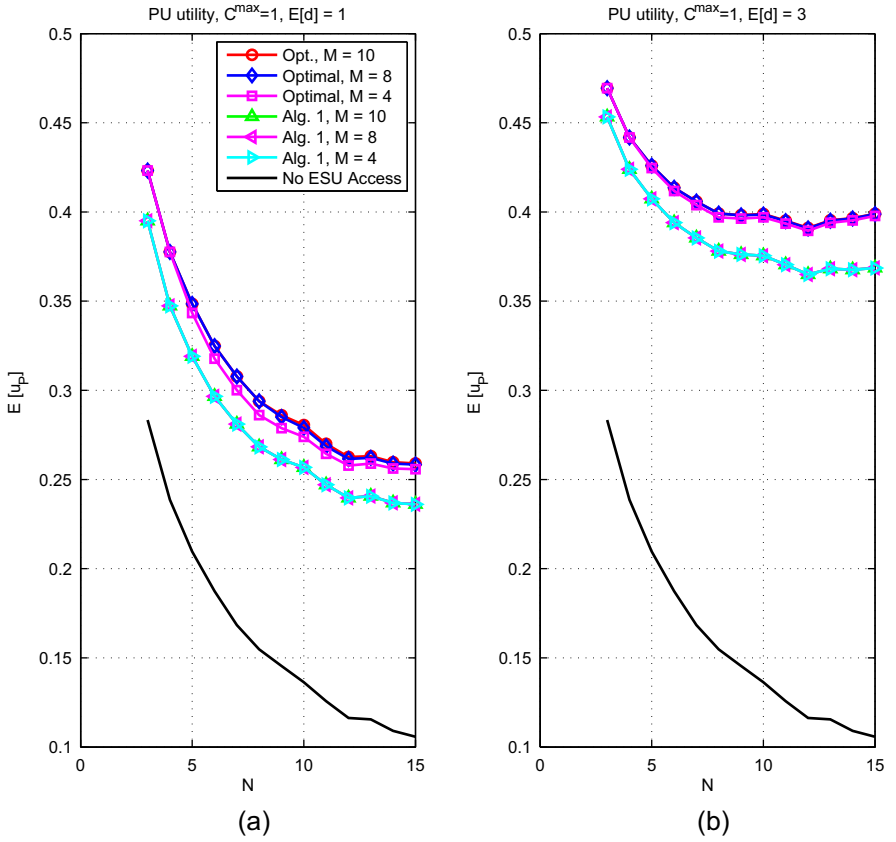

Fig. 8. Performance of Algorithm 1 when $C^{\max} = 1, \mathbb{E}[b_i] = 0.5, \mathbb{E}[c_i] = 2, \ \forall i$: (a) when $\mathbb{E}[d] = 1$ and (b) when $\mathbb{E}[d] = 3$.

However, since the optimality gap can be as large as 30%, we also study the optimality gap for Algorithm 1 when $C^{\max} = 2$. It can be seen that by increasing the complexity from $O(MN)$ to $O(MN^2)$, the optimality gap can be largely decreased (as large as 50% reduction). For example, for large $\mathbb{E}[d_{ij}]$, the gap is reduced from 18% to less than 5% for $N = 10, M = 9$. In addition, the rate of increase of the optimality gap with N is also largely reduced.

Next, we study the optimal primary utility and the performance of Algorithm 1 for a different regime in which ESUs are physically nearer to the destination than to PU. Here, we assume that $\mathbb{E}[b_i] = 0.5$ and $\mathbb{E}[c_i] = 2$ for all i. We plot the achieved average utilities and optimality gaps in Figs. 8 and 9, respectively. It can be seen that even though the values of the achieved optimal primary utility are only slightly changed with respect to those achieved in the former regime of channel parameters, the optimality gap of Algorithm 1 is much smaller, suggesting the favorable properties of the low complexity algorithm in this regime. We also observe the same trends of the primary utility with $N, M, \mathbb{E}[d_{ij}]$ and $C^{\max}$, for the regime with $\mathbb{E}[b_i] = 2$ and $\mathbb{E}[c_i] = 0.5$, however, with larger absolute values for the optimality gap (e.g., optimality gap at $\mathbb{E}[d_{ij}] = 1$ is reduced from 35% to 10% for $N = 10, M = 4$ when $C^{\max}$ is increased from 1 to 2).

Finally, we study the average rates achieved by ESUs. Without loss of generality, we focus on ESU 1 since all ESUs have same channels statistics and cost parameters. In Fig. 10, we plot the average rate $\mathbb{E}[u_1]$ for different values of M for three different schemes; the optimal primary selection rule (exhaustive search), Algorithm 1 with $C^{\max} = 2$ and Algorithm 1 with $C^{\max} = 1$. We also focus on the channel parameters regime $\mathbb{E}[b_i] = \mathbb{E}[c_i] = 1, \forall i$. First, it is clear that the achievable ESU rate decreases with N since chances that the primary system admits other ESUs with better channel parameters increase as N increases. Next, we study the average ESU rate with respect to the different strategies that can be employed by the primary system. For a given value of $\mathbb{E}[d_{ij}]$, we note that as the primary system employs a more complex ESU selection scheme (thus making more accurate ESU admission decisions and improving $u_P(\cdot)$), ESU achieves larger rate. In other words, increasing M and/or $C^{\max}$ improves both the achieved average ESU rate as well as the average primary utility. Lastly, we study the variation of ESU rate with $\mathbb{E}[d_{ij}]$. While the primary system achieves better utilities as $\mathbb{E}[d_{ij}]$ increases, this is only the case for ESU rate when Algorithm 1 is employed. We also observe the same behavior of ESU rate with different parameters for other $\mathbb{E}[b_i]$ and $\mathbb{E}[c_i]$ regimes.

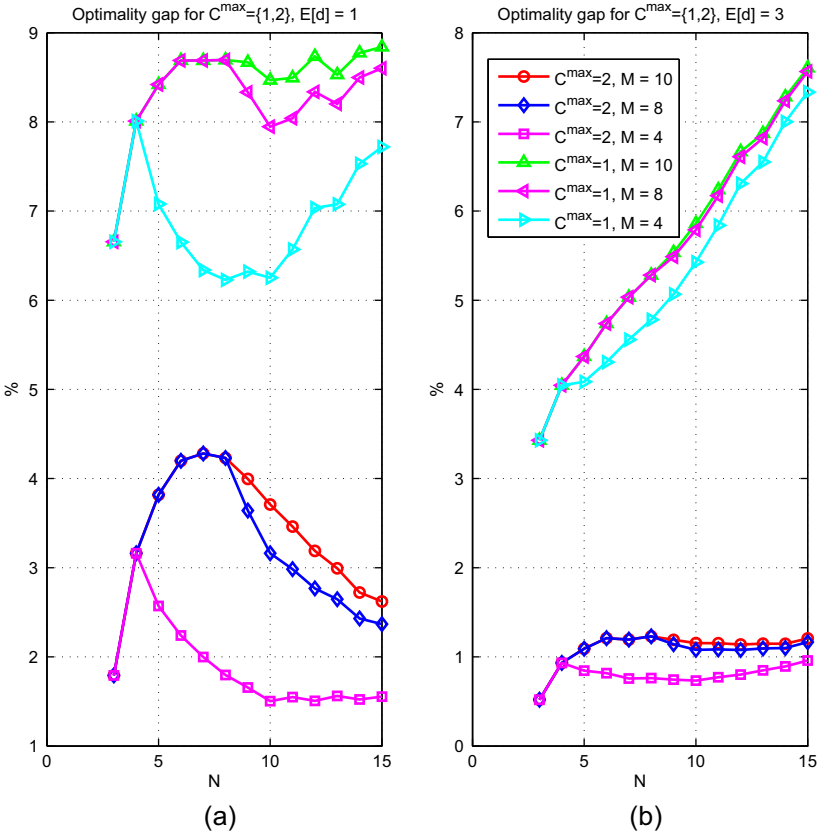

Fig. 9. Performance gap between optimal ESU selection and Algorithm 1, $\mathbb{E}[b_i] = 0.5, \mathbb{E}[c_i] = 2, \forall i$: (a) when $\mathbb{E}[d] = 1$ and (b) when $\mathbb{E}[d] = 3$.

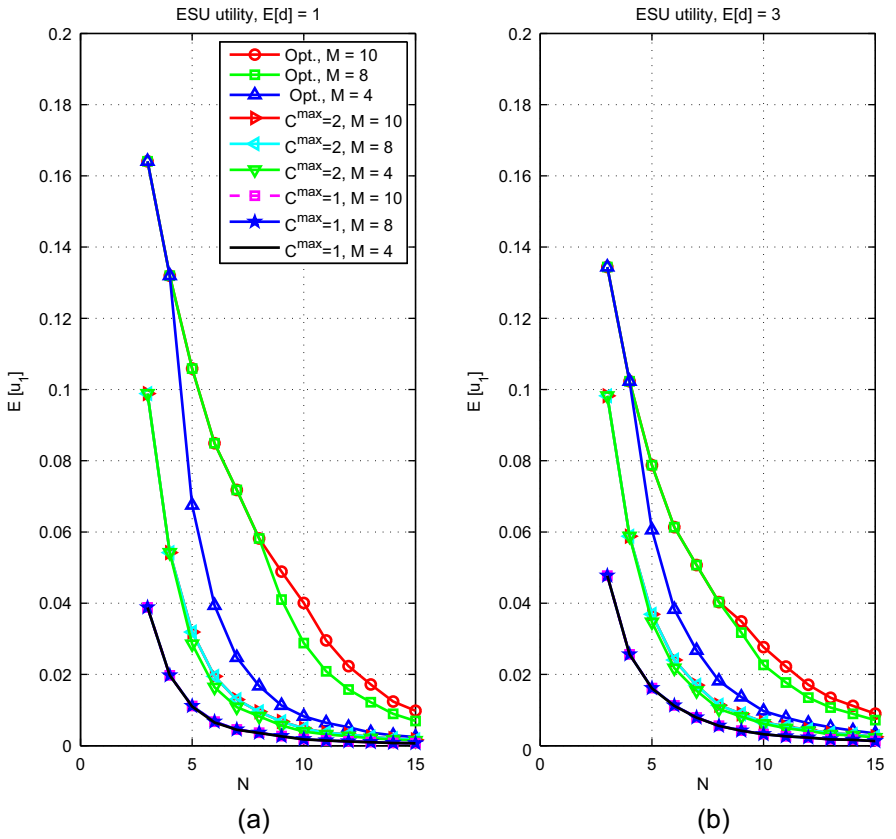

Fig. 10. Average rate for ESU 1 for different selection schemes when $\mathbb{E}[b_i] = \mathbb{E}[c_i] = 1$, $\forall i$: (a) when $\mathbb{E}[d] = 1$ and (b) when $\mathbb{E}[d] = 3$.

7. Conclusion

We presented a non-cooperative game theoretical formulation that models eavesdropping and jamming threats of secondary users to primary systems. In the presented games, the primary system allows a subset of ESUs to transmit their information to the common destination, simultaneously with the primary user's transmission, to improve its secure rate. Equilibria of the game, in which the base station is the leader and ESUs are the followers, were characterized, where we showed that discrete strategy sets for ESUs are not restrictive for practical scenario with non-zero transmission cost. The outcome of the Stackelberg game with multiple eavesdropping ESUs implies a recruiting process. Specifically, the primary system selects ESUs that effectively jam other ESUs while having minimum interference effect on the signal of PU. Finally, we proposed a low complexity algorithm to select a subset of ESUs to be granted spectrum access and evaluated its performance through simulations.

References

[1] K. Khalil, E. Ekici, Multiple access game with a cognitive jammer, in: Proceedings of the 46th Asilomar Conference on Signals, Systems and Computers, 2012.
[2] K. Khalil, E. Ekici, Multiple Access Games with a Cognitive Eavesdropper, arXiv preprint arXiv:1211.4053.
[3] K.J.R. Liu, B. Wang, Cognitive Radio Networking and Security, Cambridge University Press, 2011.
[4] C.E. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J. 28 (4) (1949) 656–715.
[5] A.D. Wyner, The wire-tap channel, Bell Syst. Tech. J. 54 (1974) 1355–1387.
[6] M. Bloch, J. Barros, Physical-Layer Security: From Information Theory to Security Engineering, Cambridge University Press, 2011.
[7] R. Liu, W. Trappe, Securing Wireless Communications at the Physical Layer, 1st Edition., Springer Publishing Company, Inc., 2009.
[8] L. Lai, H. El Gamal, The relay–eavesdropper channel: cooperation for secrecy, IEEE Trans. Inf. Theory 54 (9) (2008) 4005–4019.
[9] X. He, A. Yener, Cooperative jamming: the tale of friendly interference for secrecy, in: R. Liu, W. Trappe (Eds.), Securing Wireless Communications at the Physical Layer, Springer, US, 2010, pp. 65–88 (here, He and Yener discusses briefly their work in secrecy with cooperative jammer in different models).
[10] T. Basar, G.J. Olsder, Dynamic Noncooperative Game Theory, Academic Press, 1995.
[11] Y. Liang, H.V. Poor, S. Shamai (Shitz), Information theoretic security, Found. Trends Commun. Inf. Theory 5 (4) (2009) 355–580, http://dx.doi.org/10.1561/0100000036. http://dx.DOI.org/10.1561/0100000036.
[12] R. Liu, W. Trappe, Securing Wireless Communications at the Physical Layer, first ed., Springer Publishing Company, Incorporated, 2009.
[13] T.M. Cover, J.A. Thomas, Elements of Information Theory, Wiley-Interscience, 1991.
[14] I.F. Akyildiz, W.Y. Lee, M. Vuran, S. Mohanty, NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey, Comput. Netw. 50 (13) (2006) 2127–2159.
[15] I. Csiszar, J. Korner, Broadcast channels with confidential messages, IEEE Trans. Inf. Theory 24 (1978) 339–348.

[16] O. Simeone, I. Stanojev, S. Savazzi, Y. Bar-Ness, U. Spagnolini, R. Pickholtz, Spectrum leasing to cooperating secondary ad hoc networks, IEEE J. Sel. Areas Commun. 26 (1) (2008) 203–213, http://dx.doi.org/10.1109/JSAC.2008.080118.

[17] K. Khalil, M. Karaca, O. Ercetin, E. Ekici, Optimal scheduling in cooperate-to-join cognitive radio networks, in: Proceedings of the 30th IEEE International Conference on Computer Communications (INFOCOM 2010), 2011, pp. 3002–3010, http://dx.doi.org/10.1109/INFCOM.2011.5935142.

Karim Khalil received the B.S. degree in electronics and communications engineering from Cairo University, Cairo, Egypt, in 2007, and the M.S. degree in wireless communications from Nile University, Cairo, Egypt, in 2009. He received the Ph.D. degree in electrical and computer engineering from The Ohio State University, Columbus, OH, in 2014. From February 2013 to August 2013, he was with Wireless Communications group, Fujitsu Laboratories of America, Sunnyvale, CA, as a research intern. In Summer 2014, he was with the Wireless Development group, Cisco Systems, Richfield, OH, as a Hardware Engineering intern. His research interests are wireless communications, cognitive radio networks, information-theoretic security, and game theory. He has three pending patents. He is the recipient of the Ohio State University Fellowship Award.

Eylem Ekici has received his BS and MS degrees in Computer Engineering from Bogazici University, Istanbul, Turkey, in 1997 and 1998, respectively. He received his Ph.D. degree in Electrical and Computer Engineering from Georgia Institute of Technology, Atlanta, GA, in 2002. Currently, he is an associate professor in the Department of Electrical and Computer Engineering of The Ohio State University, Columbus, OH. He is an associate editor of IEEE/ACM Transactions on Networking, Computer Networks Journal (Elsevier), and ACM Mobile Computing and Communications Review. He also served as the general co-chair of ACM MobiCom 2012. He is the recipient of 2008 and 2014 Lumley Research Award of the College of Engineering at OSU. His current research interests include wireless sensor networks, vehicular communication systems, and next generation wireless systems, with a focus on routing and medium access control protocols, resource management, and analysis of network architectures and protocols. He is a Senior Member of IEEE and a member of ACM.