Improving the secrecy rate by turning foes to allies: An auction scheme*

Ma Ya-Yan(马亚燕) and Wang Bao-Yun(王保云)†

College of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, *China*

(Received 13 February 2015; revised manuscript received 22 April 2015; published online 21 July 2015)

Security against eavesdroppers is a critical issue in cognitive radio networks (CRNs). In this paper, a scenario consisting of one primary pair and multiple secondary pairs is considered. The secondary transmitters (STs) work in half-duplex mode and they are potential eavesdroppers on the primary transmission unless they are allowed to simultaneously transmit with the primary transmitter (PT). A modified second-price sealed-bid auction scheme is employed to model the interaction between the PT and STs. With the proposed auction scheme, the hostile relationship between the PT and STs is transformed into a cooperative relationship. An iterative algorithm based on the max–min criteria is proposed to find the optimal bidding power of the STs for an access chance in the presence of multiple eavesdroppers. Numerical results show that the proposed auction scheme not only improves the PT's security but also increases the access opportunities of the STs.

Keywords: security, auction, cooperation, cognitive radio networks

PACS: 02.50.Le, 03.67.Dd **DOI:** 10.1088/1674-1056/24/9/090209

1. Introduction

Currently, demand for the wireless spectrum is increasing thanks to the rapid development of wireless communication. The cognitive radio network (CRN)[1] is a promising technique to solve this problem because it allows unlicensed users to coexist with licensed users.[2] However, it also introduces more security issues, which have attracted considerable attention.

Game theory is not only a proper mathematical tool but it is also a social science that can be used to analyze the behavior of rational nodes.[3,4] In order to improve the wireless communication security in CRNs, many researchers have employed game theory to study potential cooperation among nodes.[5,6]

In Ref. [5], the author proposed a game theoretic scheme in which users that have their own information to transmit can reinforce the secure communication of the primary link by acting as cooperative jammers if they are granted access to the spectrum to separately transmit their own data. In Ref. [6] the secondary transmitter (ST) cooperates with the primary transmitter (PT) to deliver information securely by relaying the PT's data, in return it is granted spectrum access opportunities. Both of these studies have assumed that cooperative nodes are trusted. If the cooperative nodes are malicious, it is possible for them to act as eavesdroppers. The cooperation between such nodes becomes complex[7,8] because it is not clear if cooperation can enhance security.

In Ref. [9], a scenario was considered where an untrusted ST is willing to cooperate with the PT by relaying the PT's data for the chance of using the licensed spectrum. The cooperation takes effect but the ST has the opportunity to decode the PT's messages. An information-theoretic approach was adopted to solve this question. If the PT can secure the message from the STs by encoding a message into a codeword for the eavesdropping channel, then the ST will be allowed to relay the PT's data and transmit its own data. A different cognitive scenario was considered in Ref. [10], where the primary transmission must be secured from the secondary receiver. The ST is permitted to access the legitimate spectrum if it is willing to relay the PT's information or employ some Gaussian jamming to help the PT to lessen the probable leakage to the secondary receiver. First, the author found achievable rate regions and investigated several optimization problems. Furthermore, a Stackelberg game was employed to analyze the cooperation between the PT and STs. In Ref. [11], the STs work at half-duplex form, i.e., they can choose to either eavesdrop or transmit at any given time slot, and they prefer to transmit than eavesdrop. Hence, they are potential eavesdroppers on the primary traffic when they are not allowed to send their own data. Thus, it will increase the achievable secrecy rate for the PT to select an appropriate ST to transmit simultaneously. The author modeled the interaction between the PT and STs as a Stackelberg game in which the PT is a leader and the STs are followers. The drawback of this approach is that the STs only passively choose to eavesdrop or transmit with a fixed power level. This scheme works but it fails to fully exploit the rational and selfish features of multiple STs, which can lead to further improvement for the secrecy rate of the PT and the access chance of the STs.

In this paper, another kind of game theory: the second-price sealed-bid auction,[12,13] is employed to model the interaction between the PT and untrusted STs, which are considered as the auctioneer and bidders, respectively. The bid is

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61271232 and 61372126) and the University Postgraduate Research and Innovation Project in Jiangsu Province, China (Grant No. CXZZ12-0472).

†Corresponding author. E-mail: bywang@njupt.edu.cn

© 2015 Chinese Physical Society and IOP Publishing Ltd

the achievable secrecy rate at the primary receiver (PR) when the bidder simultaneously transmits its own data with the PT. The strategy of each ST is its power choice, and the winning ST will be rewarded with the right of using the licensed spectrum and will only be required to provide the second largest bid. Because the STs prefer to transmit than eavesdrop, they will improve the PT's secrecy rate as far as possible. The main contributions of this work are summarized as follows:

(i) With the proposed auction scheme, the hostile relationship between the PT and untrusted STs is transformed into a cooperative relationship. Therefore, the PT's secrecy rate and the STs' access chance are both increased.

(ii) An iterative algorithm based on the maxmin rule is proposed to find the optimal bidding power of STs for the access chance in the presence of multiple eavesdroppers.

The remainder of the paper is organized as follows. In Section 2, the system model is presented. In Section 3, the interaction between the PT and STs is modeled as the second-price sealed-bid auction, and some preliminaries are introduced. In Sections 4 and 5, we consider the cooperation between the PT and multiple STs using the proposed auction scheme and obtain the equilibrium. Simulation results are provided in Section 6, which is followed by the conclusion in Section 7.

2. System model

We consider a CRN model consisting of one primary pair and multiple secondary pairs ($i = 1, 2, \ldots, N$), as depicted in Fig. 1.

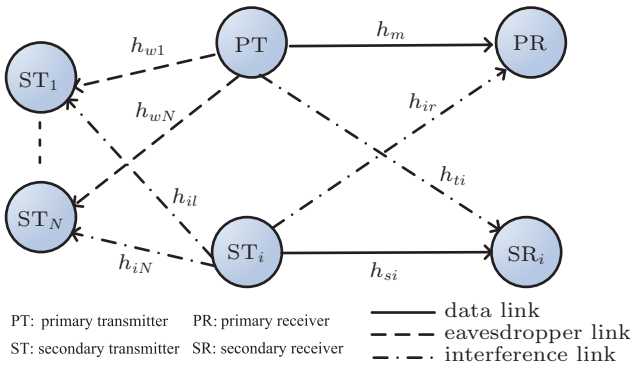


Fig. 1. (color online) System model.

Table 1. Parameters.

Parameters	Meanings
h_m	The instantaneous power channel gain between the PT and PR
h_{wi}	The instantaneous power channel gain between the PT and ST i
h_{ij}	The instantaneous power channel gain between the ST i and ST j
h_{si}	The instantaneous power channel gain between the ST i and SR i
h_{ir}	The instantaneous power channel gain between the ST i and PR
h_{ti}	The instantaneous power channel gain between the PT and SR i
P_p	The transmitted power for the PT
P_{si}	The transmitted power for the ST i
$P^{\max}$	The maximum transmitted power for the STs
σ^2	The noise power for all the links
c_{si}	The cost per unit transmission power
$R_s(P_{si}, i, j)$	The achievable secrecy rate at the PR in the presence of ST j
$R_s(P_{si}, i)$	The achievable secrecy rate at the PR in the presence of all unselected STs
$U_{si}(P_{si})$	The bidder i's utility if it won the auction
${R_s}^0$	The reserve price set by the PT
v	The index of the winning bidder
${R_s}^2$	The second highest bid
$A(i,j)$	$h_{ij}h_{ir}(h_{ij}h_m - h_{wj}h_{ir})$
$B(i,j)$	$2h_{ij}h_{ir}\sigma^2(h_m - h_{wj})$
$C(i,j)$	$\sigma^4(h_{ir}h_m - h_{wj}h_{ij}) + \sigma^2 h_m h_{wj} P_p(h_{ir} - h_{ij})$
D_{si}	$\partial U_{si}(P_{si})/\partial P_{si}\big\|_{P_{si}=0}$
${P_{si}}^0$	The nonzero solution of $U_{si}(P_{si}) = 0$
${P_{si}}^{\lim}$	$\min({P_{si}}^0, P^{\max})$
${P_{sij}}^{\max}$	$\arg\max_{P_{si}} R_s(P_{si}, i, j)$ $\ s.t.\ $ $P_{si} \geq 0$
${P_{si}}^{\text{bid}}$	The dominant bidding strategy of the bidder i
${R_{si}}^{\text{bid}}$	The bid of the bidder i
${P_{sv}}^*$	The proper power selected by the winning bidder v
${P_{s_v}}^{\text{opt}}$	The power maximizing the utility of the winning bidder v
k	$\arg\max_{i=1\ldots N}(h_{wi})$
b	$\arg\max_{i\neq k}(h_{wi})$
K	If $i \neq k$ then $K = k$, otherwise $K = b$
P^{sh}, P^{sl}	The winning bidder's transmitted power levels which let the achievable secrecy rate equal to ${R_s}^2$ ($P^{\text{sh}} > P^{\text{sl}}$) when $N = 2$
P^{SH}, P^{SL}	The winning bidder's transmitted power levels which let the achievable secrecy rate equal to ${R_s}^2$ ($P^{\text{SH}} > P^{\text{SL}}$) when $N \geq 3$ (see Fig. 5)
${P_{si}}^{\text{L}}$, ${R_{si}}^{\text{L}}$	Please see Remark 4 and Fig. 5
${P_{si}}^{\text{R}}$, ${R_{si}}^{\text{R}}$	Please see Algorithm 2 and Fig. 5
LRN_{si}, LLN_{si}	Please see Remark 4 and Fig. 5
RRN_{si}, RLN_{si}	Please see Algorithm 2 and Fig. 5

The STs work at half-duplex mode, i.e., they can choose to eavesdrop or transmit, and they prefer to transmit than eavesdrop. Therefore, they are potential eavesdroppers on the primary transmission when they are not allowed to send their own data. It is assumed that the STs do not collude. Clearly, when the channel between the primary pair is worse than the eavesdropping channel, the secrecy rate is zero. In this model the receivers are assumed to regard the information from unintended transmitters as noise. In some cases the selected STs cause more interference to unselected STs; i.e., the eavesdroppers than to the PR. To improve the secrecy rate, the PT would select one appropriate ST to transmit simultaneously using the licensed spectrum.

The instantaneous power channel gain between the PT and PR is denoted as h_m, between the PT and ST i as h_{wi}, and between the ST i and ST j as h_{ij}. Similarly, we have h_{si}, h_{ir}, and h_{ti} as depicted in Fig. 1. The transmitted powers for the PT and ST i are P_p and P_{si}, respectively. The maximum transmitted power for the STs is $P^{\max}$. Without loss of generality, we assume that the noise power is the same for all of the links, denoted by σ^2. For better readability, the parameters of this paper are summarized in Table 1.

If the ST i is selected by the PT, then other unselected STs eavesdrop as usual and the achievable secrecy rate at the PR in the presence of ST j is

$$R_s(P_{si},i,j) = \left[\log\left(1+\frac{P_p h_m}{\sigma^2+P_{si}h_{ir}}\right)-\log\left(1+\frac{P_p h_{wj}}{\sigma^2+P_{si}h_{ij}}\right)\right]^+, \quad (1)$$

where $[x]^+ = \max(x,0)$. The achievable secrecy rate at the PR in the presence of all unselected STs is

$$R_s(P_{si},i) = \min_{j\neq i}\left[\log\left(1+\frac{P_p h_m}{\sigma^2+P_{si}h_{ir}}\right)-\log\left(1+\frac{P_p h_{wj}}{\sigma^2+P_{si}h_{ij}}\right)\right]^+. \quad (2)$$

The achievable rate at the secondary receiver i is defined as

$$R_{si}(P_{si}) = \log\left(1+\frac{P_{si}h_{si}}{\sigma^2+P_p h_{ti}}\right), \quad (3)$$

where $P_{si} \leq P^{\max}$.

3. Game theory model and preliminaries

3.1. Game theory model

Throughout this paper the nodes are assumed to be rational and selfish.[14] Game theory is not only a proper mathematical tool but also a social science that can be used to analyze the behavior of such nodes. Auction, a kind of game theory, is a promising scheme to analyze how to realize efficient resource allocations in an environment where each bidder has its own preference. Auctions are generally classified into four types, which are: English auction (ascending price auction), Dutch auction (descending price auction), the first-price sealed-bid auction, and the second-price sealed-bid auction.[14] The former two auctions are open-outcry auctions because the bids of all of the bidders are disclosed to each other during the auction.[14] However, it is impossible that the private information (including the bid) of each ST is known by each other in the CRN. The latter two are sealed-bid auctions in which the privacy of the bidders is protected. When a sealed-bid auction is exploited to assign the object, the bidders submit bids simultaneously. The object is given to the bidder who submits the highest bid, in exchange for a payment. In a first-price sealed-bid auction scheme, the payment of the winning bidder is the price that it bids, and in a second-price sealed-bid auction scheme the payment of the winning bidder is the second highest bid among all of the bids. A second-price sealed-bid auction, which is known as a Vickrey auction, is individually rational for each bidder to bid truthfully with its own valuation, i.e., the maximum amount, it would like to pay for the object. To provide an intuitive understanding about this truthful bidding property, the winning opportunity of the bidder is reduced if the bid is less than its own valuation. If the bid is larger than its own valuation, then it would increase the winning opportunity of the bidder and its payoff would be negative. Moreover, such a truthful strategic choice is the dominant strategy equilibrium (DSE), which is defined as a strategy profile in which all of the players find the perfect strategy, no matter how the other players may play.[14] Therefore, in the DSE for a second-price sealed-bid auction, the strategy of every bidder is irrespective of the information on other bidders.

In summary, the second-price sealed-bid auction is employed to model the interaction between the PT and untrusted STs. The PT acts as the auctioneer and the STs are bidders. The object is the usage right of the licensed spectrum if it won the auction, and zero otherwise. The bidder's strategy is its transmitted power P_{si} and its utility is defined by

$$U_{si}(P_{si}) = \left[\log(1+\frac{P_{si}h_{si}}{\sigma^2+P_p h_{ti}}) - c_{si}P_{si}\right]^+, \quad (4)$$

where c_{si} is the cost per unit transmission power.

The bid of ST i is the secrecy rate defined by Eq. (2). This implies that the bidder i must know the PT's parameters h_m and h_{wi} ($i = 1,2,\ldots,N$). The PT sets the reserve price as

$${R_s}^0 = \min_{i=1,\ldots,N}\left[\log\left(1+\frac{P_p h_m}{\sigma^2}\right)-\log\left(1+\frac{P_p h_{wi}}{\sigma^2}\right)\right]^+. \quad (5)$$

The PT only accepts a bid larger than ${R_s}^0$.

The winning ST will be rewarded with the right of using the licensed spectrum and is only charged the second largest bid. Denoting the strategy of bidder i in the DSE as ${P_{si}}^{\text{bid}}$, the index of the winning bidder is

$$v = \arg\max_{i=1,\ldots,N} R_s\left({P_{si}}^{\text{bid}}, i\right), \quad (6)$$

if $R_s(P_{sv}, v) > {R_s}^0$, otherwise no ST is chosen. In the case of multiple equal highest offers, it is resolved randomly. Furthermore, the second highest bid is

$$ {R_s}^2 = \max_{i \neq v}(\max(R_s(P_{si}, i), {R_s}^0). \tag{7} $$

3.2. Preliminaries

In order to find the DSE, in this subsection we will introduce some properties of the functions relevant to (1) and (4) in advance.

Denoting

$$ \begin{aligned} &{R_s}'(P_{si}, i, j) \\ &= \log\left(1 + \frac{P_p h_m}{\sigma^2 + P_{si} h_{ir}}\right) - \log\left(1 + \frac{P_p h_{wj}}{\sigma^2 + P_{si} h_{ij}}\right), \end{aligned} \tag{8} $$

thus $[{R_s}'(P_{si}, i, j)]^+ = R_s(P_{si}, i, j)$, where $R_s(P_{si}, i, j)$ is defined as (1). Now, the properties of the function ${R_s}'(P_{si}, i, j)$ are given by Theorem 1.

Theorem 1 For $P_{si} \geq 0$, the function ${R_s}'(P_{si}, i, j)$ is a continuous function and has the following properties.

(i) If $A(i, j) > 0, C(i, j) < 0, B(i, j) > 0$, then ${R_s}'(P_{si}, i, j)$ is a quasi-concave function in P_{s_i} and will be a positive value in the range of $P_{si} \geq 0$;

(ii) If $A(i, j) > 0, C(i, j) < 0, B(i, j) \leq 0$, then ${R_s}'(P_{si}, i, j)$ is a quasi-concave function in P_{s_i} and will be a positive value in the range of $P_{si} > -B(i, j)/2A(i, j)$;

(iii) If $A(i, j) \geq 0, C(i, j) > 0, B(i, j) > 0$, then ${R_s}'(P_{si}, i, j)$ is a decreasing function in P_{s_i} and will be a positive value in the range of $P_{si} \geq 0$;

(iv) If $A(i, j) < 0, C(i, j) > 0, B(i, j) > 0$, then ${R_s}'(P_{si}, i, j)$ is a quasi-convex function in P_{s_i} and will be a positive value in the range of $0 \leq P_{si} < -B(i, j)/2A(i, j)$;

(v) When the above conditions are not satisfied, there is no proper value of P_{s_i} which makes ${R_s}'(P_{si}, i, j)$ rise above zero.

Here,

$$ \begin{aligned} A(i, j) &= h_{ij} h_{ir} (h_{ij} h_m - h_{wj} h_{ir}), \\ B(i, j) &= 2 h_{ij} h_{ir} \sigma^2 (h_m - h_{wj}), \\ C(i, j) &= \sigma^4 (h_{ir} h_m - h_{wj} h_{ij}) + \sigma^2 h_m h_{wj} P_p (h_{ir} - h_{ij}). \end{aligned} $$

The first four cases are depicted in Fig. 2.

Proof Firstly, let ${R_s}'(P_{s_i}, i, j) > 0$, we can then obtain

$$ -A(i, j) P_{si} < B(i, j)/2. \tag{9} $$

Secondly, set the derivative of ${R_s}'(P_{s_i}, i, j)$ with respect to P_{si} to zero and rearrange it, we can then obtain

$$ A(i, j) {P_{si}}^2 + B(i, j) P_{si} + C(i, j) = 0. \tag{10} $$

The two solutions of Eq. (10) are

$$ P_{si}(1) = \frac{-B(i, j) + \sqrt{B(i, j)^2 - 4A(i, j)C(i, j)}}{2A(i, j)}, $$

$$ P_{si}(2) = \frac{-B(i, j) - \sqrt{B(i, j)^2 - 4A(i, j)C(i, j)}}{2A(i, j)}. $$

If $A(i, j) > 0, C(i, j) < 0$, and $B(i, j) \geq 0$, then $\partial {R_s}'(P_{si}, i, j)/\partial P_{si}|_{P_{si}=0} > 0$, $P_{si}(1) > 0$, $P_{si}(2) < 0$. When $P_{si} \to \infty$, ${R_s}'(P_{s_i}, i, j)$ approaches zero. Thus, ${R_s}'(P_{si}, i, j)$ is an increasing function with respect to P_{s_i} in the range of $0 \leq P_{si} \leq P_{si}(1)$ and a decreasing function with respect to P_{s_i} in the range of $P_{si} \geq P_{si}(1)$. Moreover, ${R_s}'(P_{si}, i, j)$ is a continuous function for $P_{si} \geq 0$, so ${R_s}'(P_{si}, i, j)$ is a quasi-concave function with respect to P_{s_i} in the range of $P_{si} \geq 0$.[15] From Eq. (9) we can obtain the range of $P_{si} > -B(i, j)/2A(i, j)$, i.e., $P_{si} \geq 0$, in which the value ${R_s}'(P_{si}, i, j)$ is positive.

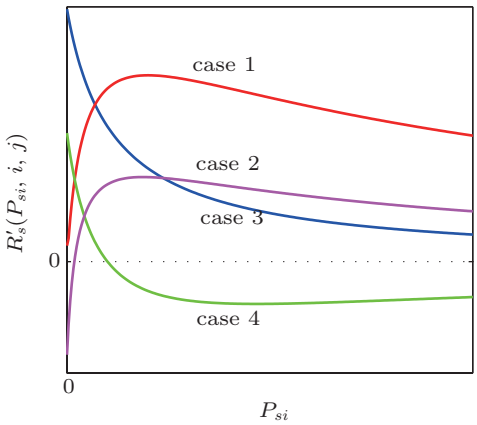


Fig. 2. (color online) Theorem 1's illustration.

Other cases can be proved similarly.

Next, the properties of the winning bidder's utility $U_{si}(P_{si})$ are introduced by Theorem 2.

Theorem 2 The function $U_{si}(P_{si})$ $(P_{si} \geq 0)$ is concave in P_{si} and will be a positive value in the range of $0 \leq P_{si} \leq {P_{si}}^0$, if the following condition is satisfied:

$$ D_{si} > 0, \ \text{i.e.,} \ h_{si} > c_{si} \ln 2 (P_p h_{ti} + \sigma^2), \tag{11} $$

where $D_{si} = \partial U_{si}(P_{si})/\partial P_{si}|_{P_{si}=0}$, ${P_{si}}^0$ is the nonzero solution of $U_{si}(P_{si}) = 0$ and c_{si} is the cost per unit transmission power.

Proof It is easy to see that $U_{si}(P_{si})$ is concave in P_{si} and below zero when $P_{si} \to \infty$. Because $U_{si}(0)$ equals zero, for the function $U_{si}(P_{si})$ to be a positive value over the range of $0 \leq P_{si} \leq {P_{si}}^0$, the condition $D_{si} = \partial U_{si}(P_{si})/\partial P_{si}|_{P_{si}=0} > 0$ must be satisfied.

According to Theorem 2, only the condition (11) is satisfied, and the ST i is willing to participate in the bidding.

4. Auction scheme with two secondary transmitters

In this section, the cooperation between the PT and two STs is presented using the second-price sealed-bid auction.

In such a case, when the ST i has won the auction, the achievable secrecy rate at the PR is

$$R_s(P_{si},i) = \left[\log\left(1+\frac{P_p h_m}{\sigma^2+P_{si}h_{ir}}\right) - \log\left(1+\frac{P_p h_{wj}}{\sigma^2+P_{si}h_{ij}}\right)\right]^+, \quad (12)$$

where $j \neq i$. The utility of winning ST is defined as (4).

4.1. Equilibrium

Assume $k = \arg\max_{i=1\ldots N}(h_{wi})$, $b = \arg\max_{i\neq k}(h_{wi})$, let

$$K = \begin{cases} k, & i \neq k, \\ b, & i = k, \end{cases} \quad (13)$$

thus the ST K is the eavesdropper when the ST i simultaneously transmits with the PT.

When $D_{si}>0, A(i,K)>0, C(i,K)<0$, and $B(i,K)>0$, the condition of Case 1 in Theorem 1 is satisfied, the ST i's cooperation can increase the achievable secrecy rate at the PR. From Fig. 2, it can be observed that in the case of $D_{si}>0$, $A(i,K)>0$, $C(i,K)<0$, and $B(i,K)\leq 0$, ${R_s}^0$ equals zero. In such a case, if $P_{si} > -B(i,K)/2A(i,K)$, the achievable secrecy rate at the PR in the presence of ST K is larger than ${R_s}^0$. In the case of $D_{si}>0, C(i,K)>0, B(i,K)>0$, the condition of Case 3 or 4 in Theorem 1 is satisfied. Under this circumstance, the security can be enhanced if $i=k$ and the ST i simultaneously transmits with the PT. Above all, the achievable secrecy rate can be improved due to the ST i's cooperation if one of the following conditions is satisfied:

$$\text{(i)}\quad D_{si}>0,\ A(i,K)>0,\ C(i,K)<0,\ B(i,K)>0; \quad (14)$$

$$\text{(ii)}\quad D_{si}>0,\ A(i,K)>0,\ C(i,K)<0,\ B(i,K)\leq 0,\ {P_{si}}^{\lim} > -B(i,K)/2A(i,K); \quad (15)$$

$$\text{(iii)}\quad i=k,\ D_{si}>0,\ C(i,K)>0,\ B(i,K)>0, \quad (16)$$

where

$${P_{si}}^{\lim} = \min({P_{si}}^0, P^{\max}). \quad (17)$$

Recall that a second-price sealed-bid auction is individually rational for each bidder to bid truthfully with its own valuation, so they will bid with the maximum amount they would be willing to pay for the object. As mentioned in subsection 3.1, the game-theoretic concept of the DSE is such a truthful strategic choice.

On the basis of the above discussion, the dominant bidding strategy ${P_{si}}^{\text{bid}}$ and the bid ${R_{si}}^{\text{bid}}$ of a bidder i $(i=1,2)$ are given by Theorem 3.

Theorem 3 If one of the conditions (14)–(16) is satisfied, then the achievable secrecy rate $R_s(P_{si},i)$ can be improved due to a bidder i's cooperation. The dominant bidding strategy ${P_{si}}^{\text{bid}}$ and the bid ${R_{si}}^{\text{bid}}$ of a bidder i $(i=1,2)$ are given as

$${P_{si}}^{\text{bid}} = \min({P_{si}}^{\lim}, {P_{siK}}^{\text{smax}}), \quad (18)$$

$${R_{si}}^{\text{bid}} = R_s\left({P_{si}}^{\text{bid}}, i, K\right), \quad (19)$$

where K and ${P_{si}}^{\lim}$ are given by Eqs. (13) and (17), and ${P_{siK}}^{\text{smax}}$ is expressed as

$${P_{siK}}^{\text{smax}} = \arg\max_{P_{si}} R_s(P_{si},i,K), \quad \text{s.t. } P_{si}\geq 0. \quad (20)$$

Proof Recall that the ST i likes transmitting better than eavesdropping, so it will do its best to improve the PT's secrecy rate to maximize its winning opportunity. As $R_s(P_{si},i,j) = [{R_s}'(P_{si},i,j)]^+$, three cases are discussed according to the values of $D_{si}, A(i,K), C(i,K), B(i,K)$ and k.

(i) $D_{si}>0, A(i,K)>0, C(i,K)<0, B(i,K)>0$.

This case corresponds to Case 1 in Theorem 1. When ${P_{siK}}^{\text{smax}} \leq {P_{si}}^{\lim}$, the dominant strategy of ST i is bidding with ${P_{siK}}^{\text{smax}}$ to maximize its winning opportunity as ${P_{siK}}^{s\max}$ maximizes $R_s(P_{s_i},i,K)$. When ${P_{siK}}^{\text{smax}} > {P_{si}}^{\lim}$, ${P_{siK}}^{\text{smax}}$ is out of the power range that the ST i can accept. Under this circumstance $R_s(P_{s_i},i,K)$ increases in the range of $0\leq P_{s_i}\leq {P_{si}}^{\lim}$, so the dominant strategy of ST i is bidding with ${P_{si}}^{\lim}$ to improve its winning opportunity.

(ii) $D_{si}>0, A(i,K)>0, C(i,K)<0, B(i,K)\leq 0, {P_{si}}^{\lim} > -B(i,k)/2A(i,k)$.

In the case of $A(i,K)>0$, $C(i,K)<0$, $B(i,K)\leq 0$, if ${P_{si}}^{\lim} \leq -B(i,K)/2A(i,K)$, the achievable secrecy rate at the PR in the presence of ST K is limited by ${P_{si}}^{\lim}$ and equal to ${R_s}^0$, i.e., 0. When ${P_{si}}^{\lim} > -B(i,K)/2A(i,K)$, it can be proven as above.

(iii) $i=k, D_{si}>0, C(i,K)>0$, and $B(i,K)>0$.

Now $K=b$. This case corresponds to Case 3 or Case 4 in Theorem 1. From Fig. 2, it is easy to see that the dominant strategy of ST i is bidding with zero and ${P_{siK}}^{\text{smax}}=0$. It is proved.

Remark 1 The scheme that we employed is a second-price sealed-bid auction, and the winning ST is only required to offer the second highest achievable secrecy rate. If the ST whose bidding strategy is zero wins the auction, then it can transmit with a power larger than zero.

Remark 2 When $h_{wk}=h_{wb}$, if one of the conditions (14) and (15) is satisfied, the achievable secrecy rate at the PR can be improved due to the ST i's cooperation and the ST i bids with the power of $\min({P_{si}}^{\lim}, {P_{siK}}^{\text{smax}})$.

4.2. Power of the winning secondary transmitter

The index of the winning bidder v is defined as (6).

In traditional auction theory, the utilities of the auctioneer and the winning bidder are monotonically increasing and decreasing, respectively, as the price increases; namely, one's utility increase causes another's utility decrease. However, in this paper, because of their concavity, the utilities of the auctioneer and winning bidder v (i.e., $R_s(P_{sv},v)$ and $U_{sv}(P_{sv})$) may have the same monotonicity in some specific ranges of P_{sv}, as shown in the red dashed rectangular areas of Fig. 3.

Hence, we will introduce a modification of the second-price sealed-bid auction:[5] the winning bidder is charged at least the second highest bid by the auctioneer. In this setting, it can be seen from Fig. 3 that the winning bidder v may select a proper transmitted power to maximize its utility $U_{sv}(P_{sv})$ with the limitation $R_s(P_{sv}, v) \geq {R_s}^2$, which can bring the simultaneous increase of $R_s(P_{sv}, v)$ and $U_{sv}(P_{sv})$. It is worth noting that this modification does not harm the benefits of the auctioneer and bidder, even if their concavity is not satisfied.

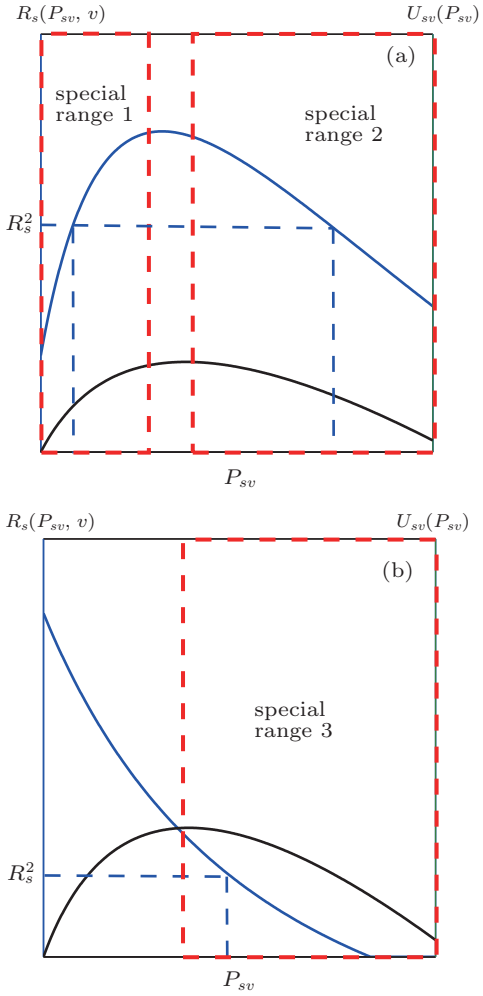


Fig. 3. (color online) Illustration of the auction scheme's modification. (a) Case 1 or case 2 in Theorem 1; (b) case 3 or 4 in Theorem 1.

In short, the outcome of this auction is given by Theorem 4.

Theorem 4 The proper power ${P_{sv}}^*$ selected by the winning ST v is

$$
{P_{sv}}^* = \begin{cases} P^{\mathrm{sh}}, & {P_{sv}}^{\mathrm{opt}} > P^{\mathrm{sh}},\ {R_s}^2 > 0, \\ P^{\mathrm{sl}}, & {P_{sv}}^{\mathrm{opt}} < P^{\mathrm{sl}},\ {R_s}^2 > 0, \\ {P_{sv}}^{\mathrm{opt}}, & P^{\mathrm{sl}} \leq {P_{sv}}^{\mathrm{opt}} \leq P^{\mathrm{sh}},\ {R_s}^2 > 0, \\ {P_{sv}}^{\mathrm{opt}}, & {R_s}^2 = 0, \end{cases} \tag{21}
$$

where ${R_s}^2$ is given by (7), and ${P_{s_v}}^{\mathrm{opt}}$ is the power maximizing utility of the winning ST v and can be expressed as

$$
{P_{sv}}^{\mathrm{opt}} = \left[\frac{1}{c_{sv} \ln 2} - \frac{P_p h_{tv} + \sigma^2}{h_{sv}} \right]_0^{P^{\max}}, \tag{22}
$$

P^{sh} and P^{sl} (the winning ST's transmitted power levels which make the achievable secrecy rate equal to ${R_s}^2$) are given by

(i) If $R_s(0, v) \geq {R_s}^2$, then $P^{\mathrm{sl}} = 0$; otherwise, P^{sl} is the solution of $R_s(P_{sv}, v)) = {R_s}^2$ lying in the range of $0 < P_{sv} < {P_{sv}}^{\mathrm{bid}}$;

(ii) If $R_s\left({P_{sv}}^{\mathrm{lim}}, v\right)) \geq {R_s}^2$, then $P^{\mathrm{sh}} = {P_{sv}}^{\mathrm{lim}}$; otherwise, P^{sh} is the solution of $R_s(P_{sv}, v)) = {R_s}^2$ lying in the range of ${P_{sv}}^{\mathrm{bid}} < P_{sv} < P_{sv}^{\mathrm{lim}}$.

Proof Recall that the winning ST v is charged at least the second highest bid by the PT, so it will maximize its utility $U_{sv}(P_{sv})$ on the basis that the utility of the PT $R_s(P_{sv}, v)$ is no less than ${R_s}^2$, and its selection for ${P_{sv}}^*$ is illustrated in Fig. 4.

If traditional auction theory is employed in our system model, then the utilities of the PT and winning ST v are ${R_s}^2$ and $U_{sv}\left(P^{\mathrm{sl}}\right)$(or $U_{sv}\left(P^{\mathrm{sh}}\right)$), respectively. From formula (21) and Fig. 4, for the case $P^{\mathrm{sl}} \leq {P_{sv}}^{\mathrm{opt}} \leq P^{\mathrm{sh}}$, it can be seen that the modification of the second-price sealed-bid auction increases these two utilities to $R_s({P_{sv}}^{\mathrm{opt}}, v))$ and $U_{sv}\left(P_{sv}^{\mathrm{opt}}\right)$ separately. Hence, the modified auction scheme simultaneously improves the performance of the PT and STs.

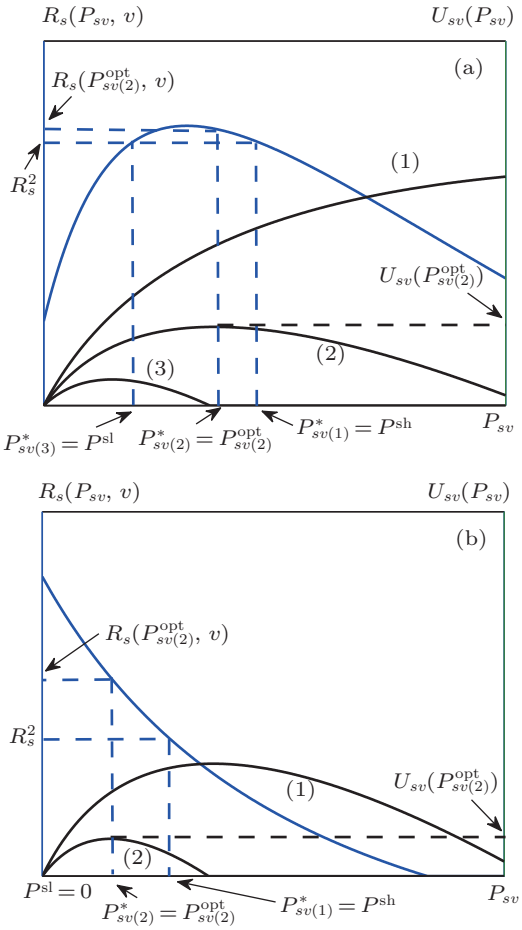


Fig. 4. (color online) Illustration of Theorem 4. (a) Case 1 or case 2 in Theorem 1. (b) Case 3 or case 4 in Theorem 1.

5. Auction scheme with more than two secondary transmitters

In this section, we consider the cooperation between the PT and more than two STs using the modified second-price

sealed-bid auction. In this case, if the ST i has won the auction, then the PT transmits with the help of ST i in the presence of multiple eavesdroppers, i.e., unselected STs. The achievable secrecy rate at the PR is defined as (2). The utility of the winning ST is defined as (4).

5.1. Equilibrium

Recall that the ST i will do its best to improve the PT's secrecy rate to maximize its winning opportunity, so ${P_{si}}^{\text{bid}}$ is the solution of the following max–min problem:

$$\begin{aligned} {P_{si}}^{\text{bid}} &= \arg\max_{P_{si}} R_s(P_{si},i) \\ &= \arg\max_{P_{si}} \min_{j\neq i} R_s(P_{si},i,j) \\ &= \arg\max_{P_{si}} \min_{j\neq i} {R_s}'(P_{si},i,j), \\ \text{s.t.} \quad & 0\le P_{si}\le {P_{si}}^{\lim}, \quad R_s(P_{si},i) > {R_s}^0, \end{aligned} \tag{23}$$

where $R_s(P_{si},i)$, $R_s(P_{si},i,j)$, and ${R_s}'(P_{si},i,j)$ are defined as (2), (1), and (8), respectively, ${P_{si}}^{\lim}$ and ${R_s}^0$ are given by (17) and (5), respectively.

Therefore, the dominant bidding strategy ${P_{si}}^{\text{bid}}$ and the bid ${R_{si}}^{\text{bid}}$ of a bidder i $(i=1\ldots N, N\ge 3)$ are given by Theorem 5.

Theorem 5 If one of the conditions (14)–(16) is satisfied, then the achievable secrecy rate $R_s(P_{si},i)$ can be improved due to a bidder i's cooperation. The dominant bidding strategy ${P_{si}}^{\text{bid}}$ and the bid ${R_{si}}^{\text{bid}}$ of a bidder i $(i=1\ldots N, N\ge 3)$ are given by Algorithm 1.

Algorithm 1 Maxmin algorithm for the dominant strategy equilibrium

Initialize $t_i=1$, ${P_{si}}^{\text{L}}(1)=0$, ${R_{si}}^{\text{L}}(1)=R_s(0,i,K)$, $\text{LLN}_{si}(1)=0$, $\text{LRN}_{si}(1)=K$, ${P_{si}}^{\text{inter0}}=0$.

Step 1 **If** $i=k$, $D_{si}>0$, $C(i,K)>0$ and $B(i,K)>0$,
then ${P_{si}}^{\text{bid}}=0$, ${R_{si}}^{\text{bid}}=R_s\left({P_{si}}^{\text{bid}},i,K\right)$ and the bidder i 's bidding is over.
else if $D_{si}>0$, $A(i,K)>0$ and $C(i,K)<0$,
then $t_i=2$ and go to step 2,
else the bidder i quits from the bidding,
end if
end if

Step 2 Let ${R_s}'(P_{si},i,K)={R_s}'(P_{si},i,m)(m=1,2,\ldots,N,m\neq i,K)$, denote the obtained power levels as ${P_{si}}^{\text{inter}}(K,m)$.

Step 3 Obtain l by $l=\arg\min_{m\neq K,i} {P_{si}}^{\text{inter}}(K,m)$, s.t. ${P_{si}}^{\text{inter}}(K,m)>{P_{si}}^{\text{inter0}}$.

Step 4 Calculate ${D_{iK}}^{l}=\left.\frac{\partial {R_s}'(P_{si},i,K)}{\partial P_{si}}\right|_{P_{si}={P_{si}}^{\text{inter}}(K,l)}$, ${D_{il}}^{K}=\left.\frac{\partial {R_s}'(P_{si},i,l)}{\partial P_{si}}\right|_{P_{si}={P_{si}}^{\text{inter}}(K,l)}$.

Step 5 **If** one of the following three conditions is satisfied:
${P_{si}}^{\text{inter}}(K,l)\notin[0,{P_{si}}^{\lim}]$ or $\max_{m\neq K,i}({P_{si}}^{\text{inter}}(K,m))\le {P_{si}}^{\text{inter0}}$ or
${D_{iK}}^{l}<0$ and ${D_{il}}^{K}<0$ and ${P_{si}}^{\text{inter}}(K,l)\in({P_{si}}^{\text{inter0}},{P_{si}}^{\lim}]$,
then
${P_{si}}^{\text{bid}}=\min({P_{si}}^{\lim},{P_{siK}}^{\text{smax}})$, ${R_{si}}^{\text{bid}}=R_s\left({P_{si}}^{\text{bid}},i,K\right)$, ${P_{si}}^{\text{L}}(t_i)={P_{si}}^{\text{bid}}$, ${R_{si}}^{\text{L}}(t_i)={R_{si}}^{\text{bid}}$, $\text{LLN}_{si}(t_i)=K$, $\text{LRN}_{si}(t_i)=K$.
else if ${D_{iK}}^{l}>0$ and ${D_{il}}^{K}<0$
then if $B(i,K)<0$ and ${P_{si}}^{\text{inter}}(K,l)<-B(i,K)/2A(i,K)$
then the bidder i quits from the bidding.
else
${P_{si}}^{\text{bid}}={P_{si}}^{\text{inter}}(K,l)$, ${R_{si}}^{\text{bid}}=R_s\left({P_{si}}^{\text{bid}},i,K\right)$, ${P_{si}}^{\text{L}}(t_i)={P_{si}}^{\text{bid}}$,
${R_{si}}^{\text{L}}(t_i)={R_{si}}^{\text{bid}}$, $\text{LLN}_{si}(t_i)=K$, $\text{LRN}_{si}(t_i)=l$.
end
else if ${D_{iK}}^{l}>0$ and ${D_{il}}^{K}>0$
then
${P_{si}}^{\text{L}}(t_i)={P_{si}}^{\text{inter}}(K,l)$, $\text{LLN}_{si}(t_i)=K$, $\text{LRN}_{si}(t_i)=l$,
${R_{si}}^{\text{L}}(t_i)=R_s\left({P_{si}}^{\text{inter}}(K,l),i,K\right)$.
update $t_i=t_i+1$, $K=l$, ${P_{si}}^{\text{inter0}}={P_{si}}^{\text{inter}}(K,l)$
return to step 2.
end
end
end

Proof Similar to Section 4, the achievable secrecy rate $R_s(P_{si},i)$ may be larger than ${R_s}^0$ if one of the conditions (14)–(16) is satisfied.

Let ${R_s}'(P_{si},i,K)={R_s}'(P_{si},i,m)$ $(m=1,2,\ldots,N,m\neq i,K)$, we will obtain ${P_{si}}^{\text{inter}}(K,m)=\sigma^2(h_{wK}-h_{wm})/(h_{wm}h_{iK}-h_{wK}h_{im})$. It is obvious that the two curves, ${R_s}'(P_{si},i,K)$ and ${R_s}'(P_{si},i,m)$, as the functions of P_{si}, have one and only one intersection. According to Theorem 1, ${R_s}'(P_{si},i,j)$ is a continuous function for $P_{si}>0$. ${R_s}'(0,i,K)<{R_s}'(0,i,m)$ because the ST K is the eavesdropper whose eavesdropping capability is the strongest among the unselected STs. Above all, ${R_s}'(P_{si},i,K)<{R_s}'(P_{si},i,m)$ in the range of $0\le P_{si}<{P_{si}}^{\text{inter}}(K,m)$ and ${R_s}'(P_{si},i,K)>{R_s}'(P_{si},i,m)$ in the range of $P_{si}>{P_{si}}^{\text{inter}}(K,m)$.

Assume ${P_{si}}^{\rm ra} > {P_{si}}^{\rm inter}(K,m)$ and

$$D_{iK}{}^{m} = \frac{\partial {R_s}'(P_{si},i,K)}{\partial P_{si}}\Big|_{P_{si}={P_{si}}^{\rm inter}(K,m)} < 0,$$

then ${R_s}'({P_{si}}^{\rm ra},i,K) < {R_s}'\left({P_{si}}^{\rm inter}(K,m),i,K\right)$ according to Theorem 1. Because ${R_s}'({P_{si}}^{\rm ra},i,K) > {R_s}'({P_{si}}^{\rm ra},i,m)$ and ${R_s}'\left({P_{si}}^{\rm inter}(K,m),i,K\right) = {R_s}'\left({P_{si}}^{\rm inter}(K,m),i,m\right)$, we get

$$D_{im}{}^{K} = \frac{\partial {R_s}'(P_{si},i,m)}{\partial P_{si}}\Big|_{P_{si}={P_{si}}^{\rm inter}(K,m)} < 0,$$

i.e., ${R_s}'({P_{si}}^{\rm ra},i,m) < {R_s}'\left({P_{si}}^{\rm inter}(K,m),i,m\right)$.

Above all, the values of $D_{iK}{}^{m}$ and $D_{im}{}^{K}$ can be divided into three categories: i) $D_{iK}{}^{m} < 0$, $D_{im}{}^{K} < 0$; ii) $D_{iK}{}^{m} > 0$, $D_{im}{}^{K} < 0$; and, iii) $D_{iK}{}^{m} > 0$, $D_{im}{}^{K} > 0$.

To solve the max–min problem (23), two situations are analyzed according to the values of $A(i,K)$, $B(i,K)$, $C(i,K)$, D_{si}, and k .

(i) $i = k$, $D_{si} > 0$, $C(i,K) > 0$, and $B(i,K) > 0$.

If $D_{si} > 0, C(i,K) > 0$, and $B(i,K) > 0$, the condition of Case 3 or Case 4 in Theorem 1 is satisfied. It is seen from Fig. 2 that $D_{iK}{}^{m} < 0$ and ${R_s}'(P_{si},i,K)$ is a decreasing and continuous function in P_{si} in the range that ${R_s}'(P_{si},i,K) > 0$. Define $l = \arg\min_{m\neq K,i} {P_{si}}^{\rm inter}(K,m)$, s.t., ${P_{si}}^{\rm inter}(K,m) > 0$, we can obtain $D_{il}{}^{K} < 0$ as above. Similarly, if there are other curves ${R_s}'(P_{si},i,n)$ $(n = 1,2,\ldots,N, n \neq i,K,l)$ that intersect with ${R_s}'(P_{si},i,l)$ in the range of $P_{si} \geq {P_{si}}^{\rm inter}(K,l)$, then we can have $D_{im}{}^{n} < 0$. It is clear that $\min_{j\neq i} {R_s}'(P_{si},i,j) = {R_s}'(P_{si},i,K)$ in the range of $0 \leq P_{si} \leq {P_{si}}^{\rm inter}(K,l)$, and $\min_{j\neq i} {R_s}'(P_{si},i,j) \leq {R_s}'(P_{si},i,K) \leq {R_s}'\left({P_{si}}^{\rm inter}(K,l),i,K\right)$ in the range of $P_{si} \geq {P_{si}}^{\rm inter}(K,l)$. Hence, $\min_{j\neq i} {R_s}'(P_{si},i,j)$ is also a decreasing and continuous function in P_{si} in the range that $\min_{j\neq i} {R_s}'(P_{si},i,K) > 0$. In such a case, the security can be enhanced due to the ST i's cooperation if the ST i is the ST whose eavesdropping capability is the strongest among all of the STs; i.e., $i = k$, and the dominant strategy of the ST k is bidding with zero, as given by the analysis in Section 4.

(ii) $D_{si} > 0, A(i,K) > 0, C(i,K) < 0$.

As mentioned above, we can get $\min_{j\neq i} R_s(P_{si},i,j) = R_s(P_{si},i,K)$ in the range of ${P_{si}}^{\rm inter0} \leq P_{si} \leq {P_{si}}^{\rm inter}(K,l)$.

Firstly, we assume the situation that $D_{iK}{}^{m} > 0$ and $D_{il}{}^{K} > 0$ does not happen. Let ${P_{si}}^{\rm inter0} = 0$, three different cases are analyzed according to various situations of the intersection ${P_{si}}^{\rm inter}(K,l)$.

(i) ${P_{si}}^{\rm inter}(K,l) \notin ({P_{si}}^{\rm inter0}, {P_{si}}^{\rm lim}]$ or $\max_{m\neq K,i}({P_{si}}^{\rm inter}(K,m)) \leq {P_{si}}^{\rm inter0}$.

In such a case, the optimization problem (23) can be expressed as (24).

$$\begin{aligned} &{P_{si}}^{\rm bid} = \arg\max_{P_{si}} R_s(P_{si},i,K), \\ &\text{s.t. } {P_{si}}^{\rm inter0} < P_{si} \leq {P_{si}}^{\rm lim}. \end{aligned} \tag{24}$$

Hence, ${P_{si}}^{\rm bid} = \min({P_{si}}^{\rm lim}, {P_{si}K}^{\rm smax})$, ${R_{si}}^{\rm bid} = R_s\left({P_{si}}^{\rm bid},i,K\right)$.

(ii) $D_{iK}{}^{l} < 0$ and $D_{il}{}^{K} < 0$, ${P_{si}}^{\rm inter}(K,l) \in ({P_{si}}^{\rm inter0}, {P_{si}}^{\rm lim}]$.

As $D_{il}{}^{K} < 0$, the function ${R_s}'(P_{si},i,l)$ is a decreasing function in P_{si} for $P_{si} > {P_{si}}^{\rm inter}(K,l)$ and approaches zero when $P_{si} \to \infty$ if the conditions of $A(i,l) > 0$ and $C(i,l) < 0$ are met. Otherwise, if $C(i,l) > 0$ and $B(i,l) > 0$, the function ${R_s}'(P_{si},i,l)$ is monotonically decreasing in the range of ${P_{si}}^{\rm inter}(K,l) < P_{si} < -B(i,l)/2A(i,l)$ and below zero when $P_{si} > -B(i,l)/2A(i,l)$. Since ${R_s}'\left({P_{si}}^{\rm inter}(K,l),i,l\right) = {R_s}'\left({P_{si}}^{\rm inter}(K,l),i,K\right)$, $\min_{j\neq i} {R_s}'(P_{si},i,j) \leq {R_s}'(P_{si},i,l) \leq {R_s}'\left({P_{si}}^{\rm inter}(K,l),i,K\right)$, for $P_{si} > {P_{si}}^{\rm inter}(K,l)$.

Then, we can reformulate (23) as

$$\begin{aligned} &{P_{si}}^{\rm bid} = \arg\max_{P_{si}} R_s(P_{si},i,K), \\ &\text{s.t. } {P_{si}}^{\rm inter0} < P_{si} \leq {P_{si}}^{\rm inter}(K,l). \end{aligned} \tag{25}$$

As $D_{iK}{}^{l} < 0$ and $R_s(P_{si},i,K)$ is concave in P_{si} for $P_{si} > {P_{si}}^{\rm inter0}$, the solution of (25) is ${P_{si}}^{\rm bid} = \min({P_{si}}^{\rm lim}, {P_{si}K}^{\rm smax})$.

(iii) $D_{iK}{}^{l} > 0$ and $D_{il}{}^{K} < 0$, ${P_{si}}^{\rm inter}(K,l) \in ({P_{si}}^{\rm inter0}, {P_{si}}^{\rm lim}]$.

Similarly, in this case the problem (23) is rewritten as (25). As $D_{iK}{}^{l} > 0$ and ${R_s}'(P_{si},i,K)$ is concave in P_{si} for $P_{si} > 0$, the problem can be solved by ${P_{si}}^{\rm bid} = {P_{si}}^{\rm inter}(K,l)$.

In such a case, it can be observed from Fig. 2 that $\min_{j\neq i} {R_s}'(P_{si},i,j) = {R_s}'(P_{si},i,K) = {R_s}^{0} = 0$ and the bidder i quits from the bidding if ${P_{si}}^{\rm inter}(K,l) < -B(i,K)/2A(i,K)$ and $B(i,K) < 0$.

Next, we consider the case of $D_{iK}{}^{l} > 0$ and $D_{il}{}^{K} > 0$.

(iv) $D_{iK}{}^{l} > 0$ and $D_{il}{}^{K} > 0$, ${P_{si}}^{\rm inter}(K,l) \in ({P_{si}}^{\rm inter0}, {P_{si}}^{\rm lim}]$.

As $D_{iK}{}^{l} > 0$ and $D_{il}{}^{K} > 0$, ${R_s}'(P_{si},i,K)$ and ${R_s}'(P_{si},i,l)$ are both concave in P_{si} for $P_{si} > 0$ according to Theorem 1. ${R_s}'(P_{si},i,K)$ is monotonically increasing in the range of ${P_{si}}^{\rm inter0} \leq P_{si} \leq {P_{si}}^{\rm inter}(K,l)$. When $P_{si} > {P_{si}}^{\rm inter}(K,l)$, ${R_s}'(P_{si},i,l) > {R_s}'\left({P_{si}}^{\rm inter}(K,l),i,l\right)$ and ${R_s}'\left({P_{si}}^{\rm inter}(K,l),i,l\right) = {R_s}'\left({P_{si}}^{\rm inter}(K,l),i,K\right)$. The problem (23) becomes

$$\begin{aligned} &{P_{si}}^{\rm bid} = \arg\max_{P_{si}} \min_{j\neq i} {R_s}'(P_{si},i,j), \\ &\text{s.t. } {P_{si}}^{\rm inter}(K,l) < P_{si} \leq {P_{si}}^{\rm lim}, \\ &\quad R_s(P_{si},i) > {R_s}^{0}. \end{aligned} \tag{26}$$

Because ${R_s}'(P_{si},i,l)$ is concave in P_{si} for $P_{si} > {P_{si}}^{\rm inter}(K,l)$ and ${R_s}'\left({P_{si}}^{\rm inter}(K,l),i,l\right) < {R_s}'\left({P_{si}}^{\rm inter}(K,l),i,n\right)$ $(n \neq i,l,K)$, we can find the solution of (26) by regarding the curve ${R_s}'(P_{si},i,l)$ as ${R_s}'(P_{si},i,K)$, ${P_{si}}^{\rm inter}(K,l)$ as ${P_{si}}^{\rm inter0}$.

All of the above steps can be summarized as Algorithm 1 "maxmin algorithm for the dominant strategy equilibrium".

Because N and ${P_{si}}^{\rm lim}$ are both finite values, the problem (23) must have a solution if one of the conditions (14)–(16) is satisfied.

Remark 3 Similar to Remark 2, in a case where there are multiple equal largest h_{wi}, the ST who meets the condition (14) or (15) bids according to Algorithm 1, but the ST who meets the conditions (16) quits from the bidding.

Remark 4 In Algorithm 1, the arrays $P_{si}{}^{\mathrm{L}}$ and $R_{si}{}^{\mathrm{L}}$ are used to record the power value and the achievable secrecy rate corresponding to the intersections lying on the curve $\min_{j\neq i} R_s(P_{si}, i, j)$ before the dominant bidding strategy $P_{si}{}^{\mathrm{bid}}$ is found. LRN_{si} and LLN_{si} are applied to store the sequence numbers of the eavesdroppers corresponding to these intersections. For ease of calculation in the next steps, we regard the zero point and bidding one as the intersections.

5.2. Power of the winning secondary transmitter

The index of the winning bidder v is defined as (6). It has to provide the PT, at least ${R_s}^2$, given by Eq. (7).

Similar to Algorithm 1, Algorithm 2 is used to calculate the information of the intersections lying on the curve $\min_{j\neq v} R_s(P_{sv}, v, j)$ after the dominant bidding strategy is found. For ease of calculation, in the next steps we consider the bidding point and the point of $P_{sv} = P_{sv}{}^{\mathrm{lim}}$ as the intersections.

Algorithm 2: max–min algorithm for the winning bidder's secrecy rate

Initialize $w_v = 2$, $\mathrm{RLN}_{sv}(1) = \mathrm{LLN}_{sv}(t_v)$, $\mathrm{RRN}_{sv}(1) = r = \mathrm{LRN}_{sv}(t_v)$, $P_{sv}{}^{\mathrm{R}}(1) = P_{sv}{}^{\mathrm{bid}}$, $R_{sv}{}^{\mathrm{R}}(1) = R_{sv}{}^{\mathrm{bid}}$, $P_{sv}{}^{\mathrm{Rinter0}} = P_{sv}{}^{\mathrm{L}}(t_v)$.

Step 1 Let $R_s(P_{sv}, v, r) = R_s(P_{sv}, v, m)$ $(m = 1, 2, \ldots, N, m \neq v, r)$, denote the obtained power level as $P_{sv}{}^{\mathrm{Rinter}}(r, m)$.

Step 2 Obtain l by $l = \arg\min_{m\neq r,v} P_{sv}{}^{\mathrm{Rinter}}(r, m)$, s.t. $P_{sv}{}^{\mathrm{Rinter}}(r, m) > P_{sv}{}^{\mathrm{Rinter0}}$

Step 3 **If** $P_{sv}{}^{\mathrm{Rinter}}(r, l) \notin [0, P_{sv}{}^{\mathrm{lim}}]$ or $\max_{m\neq r,v}(P_{sv}{}^{\mathrm{Rinter}}(r, m)) \leq P_{sv}{}^{\mathrm{Rinter0}}$

then

$P_{sv}{}^{\mathrm{R}}(w_v) = P_{sv}{}^{\mathrm{lim}}$, $\mathrm{RLN}_{sv}(w_v) = r$, $\mathrm{RRN}_{sv}(w_v) = 0$, $R_{sv}{}^{\mathrm{R}}(w_v) = R_s\left(P_{sv}{}^{\mathrm{lim}}, v, r\right)$.

else

$P_{sv}{}^{\mathrm{R}}(w_v) = P_{sv}{}^{\mathrm{Rinter}}(r, l)$, $\mathrm{RLN}_{sv}(w_v) = r$, $\mathrm{RRN}_{sv}(w_v) = l$, $R_{sv}{}^{\mathrm{R}}(w_v) = R_s\left(P_{sv}{}^{\mathrm{R}}(w_v), v, r\right)$,

update $w_v = w_v + 1$, $r = l$, $P_{sv}{}^{\mathrm{Rinter0}} = P_{sv}{}^{\mathrm{Rinter}}(r, l)$

return to step 1.

end

Similar to subsection 4.2, the modified second-price sealed-bid auction scheme is employed and the outcome of the auction is given by Theorem 6.

Theorem 6 The proper power ${P_{sv}}^*$ selected by the winning ST v is

$$ {P_{sv}}^* = \begin{cases} P^{\mathrm{SH}}, & P_{sv}{}^{\mathrm{opt}} > P^{\mathrm{SH}}, {R_s}^2 > 0, \\ P^{\mathrm{SL}}, & P_{sv}{}^{\mathrm{opt}} < P^{\mathrm{SL}}, {R_s}^2 > 0, \\ P_{sv}{}^{\mathrm{opt}}, & P^{\mathrm{SL}} \leq P_{sv}{}^{\mathrm{opt}} \leq P^{\mathrm{SH}}, {R_s}^2 > 0, \\ P_{sv}{}^{\mathrm{opt}}, & {R_s}^2 = 0, \end{cases} \tag{27} $$

where ${R_s}^2$ and $P_{s_v}{}^{\mathrm{opt}}$ are given by (7) and (22), respectively, P^{SH} and P^{SL} (the winning ST's transmitted power levels which make the achievable secrecy rate exactly equal to ${R_s}^2$) are given by

(i) If $R_{sv}{}^{\mathrm{L}}(1) \geq {R_s}^2$,then $P^{\mathrm{SL}} = 0$; otherwise, if $R_{sv}{}^{\mathrm{L}}(T) < {R_s}^2 \leq R_{sv}{}^{\mathrm{L}}(T+1)$ $(1 \leq T < t_v)$, let $x = \mathrm{LRN}(T)$, then P^{SL} is the solution of $R_s(P_{sv}, v, x) = {R_s}^2$;

(ii) If $R_{sv}{}^{\mathrm{R}}(w_v) \geq {R_s}^2$, then $P^{\mathrm{SH}} = P_{sv}{}^{\mathrm{lim}}$; otherwise, if $R_{sv}{}^{\mathrm{R}}(W) < {R_s}^2 \leq R_{sv}{}^{\mathrm{R}}(W-1)$, $(1 < W \leq w_v)$, let $y = RLN(W)$, then P^{SH} is the solution of $R_s(P_{sv}, v, y) = {R_s}^2$.

Proof The proof is similar to Theorem 4 but there are some differences from Theorem 4 in the selection for P^{SH} and P^{SL}. Recall that the arrays $P_{sv}{}^{\mathrm{L}}$ and $R_{sv}{}^{\mathrm{L}}$ have recorded the power value and the achievable secrecy rate corresponding to the intersections lying on the curve $\min_{j\neq v} R_s(P_{s_v}, v, j)$ before the dominant bidding strategy $P_{sv}{}^{\mathrm{bid}}$ is found. If $R_{sv}{}^{\mathrm{L}}(1) \geq {R_s}^2$, then the winning ST v only keeps silent and does not eavesdrop, and the achievable secrecy rate at the PR will be larger than ${R_s}^2$. Otherwise, if $R_{sv}{}^{\mathrm{L}}(T) < {R_s}^2 \leq R_{sv}{}^{\mathrm{L}}(T+1)$ $(1 \leq T < t_v)$, let $x = \mathrm{LRN}(T)$ and P^{SL} is the solution of $R_s(P_{sv}, v, x) = {R_s}^2$. The selection for P^{SH} can be proven similarly.

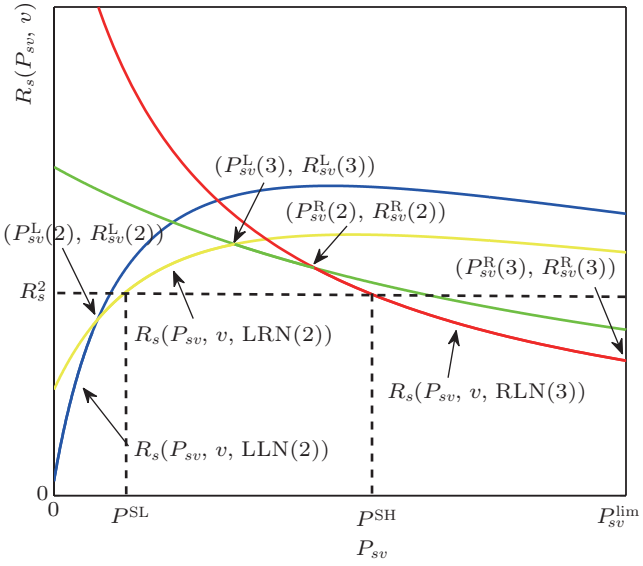


Fig. 5. (color online) Illustration of the selection for P^{SH} and P^{SL}. Here, $w_v = t_v = 3$. The thick curve indicates the value of $\min_{j\neq v} R_s(P_{sv}, v, j)$, P^{SL} is the solution of $R_s(P_{sv}, v, \mathrm{LRN}(2)) = {R_s}^2$, P^{SH} is the solution of $R_s(P_{sv}, v, \mathrm{RLN}(3)) = {R_s}^2$.

One illustration of the selection for P^{SH} and P^{SL} is shown in Fig. 5. In Fig. 5, the thick curve indicates the value of $\min_{j\neq v} R_s(P_{sv}, v, j)$. Because $R_{sv}{}^{\mathrm{L}}(2) < {R_s}^2 \leq R_{sv}{}^{\mathrm{L}}(3)$ and $R_{sv}{}^{\mathrm{R}}(3) < {R_s}^2 \leq R_{sv}{}^{\mathrm{R}}(2)$, P^{SL} and P^{SH} are the solutions of $R_s(P_{sv}, v, \mathrm{LRN}(2)) = {R_s}^2$ and $R_s(P_{sv}, v, \mathrm{RLN}(3)) = {R_s}^2$, respectively.

6. Numerical results

In this section, we present the numerical results to illustrate the proposed auction scheme. We consider a simple geometrical model where the STs are all placed at approximately the same normalized distance from the PT and the PR. A flat Rayleigh fading environment is considered, with the average power channel gains are given by $E[h_m] = E[h_{si}] = E[h_{wi}] = 1$, $E[hij] = E[hir] = E[h_{ti}] = 0.1$, P_p, $P^{\max}$, and noise power σ^2 are set to 10 mW, 10 mW, and 1 mW, respectively. The cost per unit transmission power c_{si} is set to be c, as shown in the figures. The displayed results are obtained through 10^5 trials .

Figures 6–8 show the average secrecy rate of the PT versus the number N of STs, the average eavesdropping power channel gain h_{wi} and the average interference power channel gain h_{ir}, respectively, using our proposed auction scheme and the Stackelberg scheme proposed in Ref. [11]. Figures 9–11 demonstrate the average utility of the selected ST as a function of the number N of STs, the average eavesdropping power channel gain h_{wi} and the average interference power channel gain h_{ir}, respectively, using the same two schemes. In Figs. 7–8 and Figs. 10–11, the parameter N is set to 5.

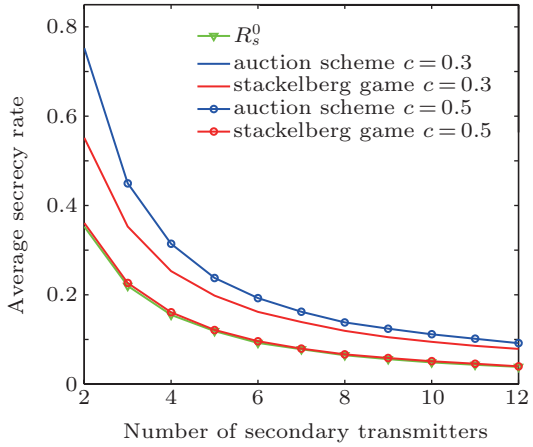


Fig. 6. (color online) Average secrecy rate versus the number of STs.

From Figs. 6–11, it is seen that both two schemes can improve the average secrecy rate of the PT and the average utility of the selected ST compared with a situation where no ST is selected. It is worth noting that the utilities and rates of STs which are not selected are zero. When the Stackelberg scheme is used, the STs can only choose to eavesdrop or transmit with a fixed power $P^{\max}$. The larger cost per unit transmission power c_{si} leads to a higher possibility that the utility of the selected ST is not positive. The STs may be willing to eavesdrop for a large enough c_{si}. In the case of $c_{si} = 0.5$, the Stackelberg scheme could hardly improve the performance of the PT and the selected ST. Due to competitiveness of the STs, greater performance improvements are achieved for the PT with our proposed auction scheme than with the Stackelberg scheme proposed in Ref. [11], as shown in Figs. 6–8. A similar phenomenon holds for the performance of the selected ST as shown in Figs. 9–11 because our auction scheme increases the access chance of the STs.

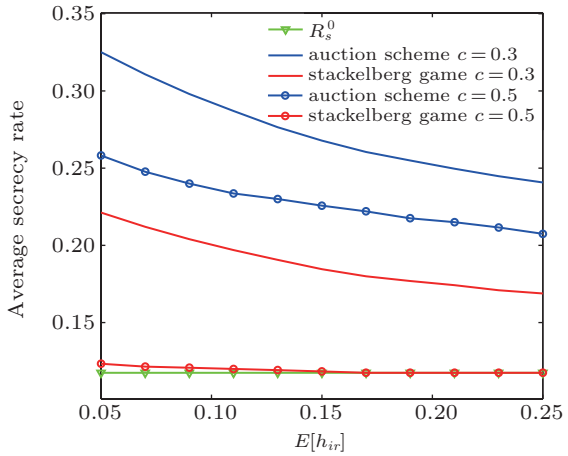


Fig. 7. (color online) Average secrecy rate versus average power channel gain h_{ir}.

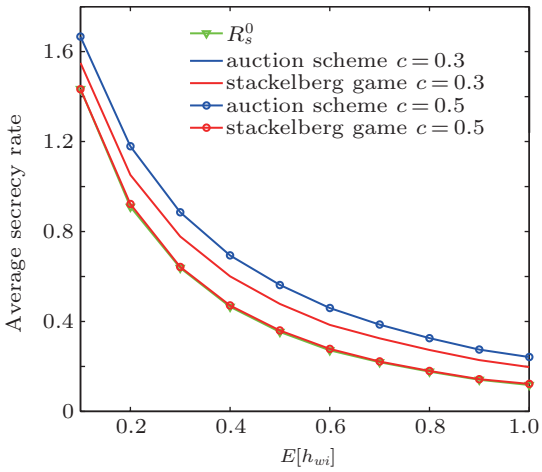


Fig. 8. (color online) Average secrecy rate versus average eavesdropping channel gain h_{wi}.

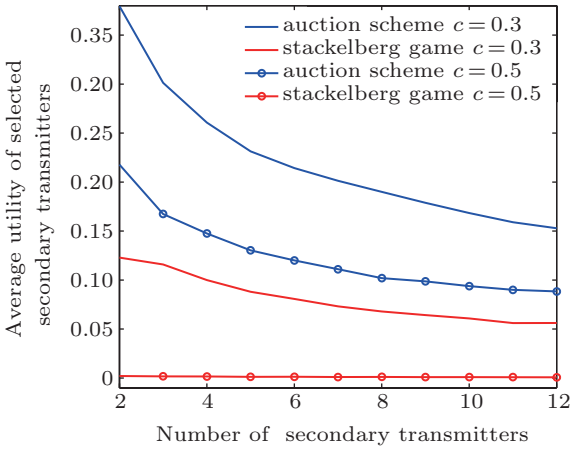


Fig. 9. (color online) Average utility of the selected ST versus the number of STs.

As the number of STs increases, the average secrecy rates with these two schemes obviously decrease, as shown in Fig. 6, since the number of eavesdroppers increases at the

same time. A similar case holds for the selected ST's performance due to competitiveness, as shown in Fig. 9.

With the increase in the interference power channel gain h_{ir}, the advantage of these two schemes diminishes, as shown in Figs. 7 and 10, because the selected ST causes more interference to the PR. This implies that the larger values of h_{ir} compared to h_{ij} benefit these two schemes.

Above all, significant performance improvements can be achieved for the PT and the selected ST with our proposed scheme.

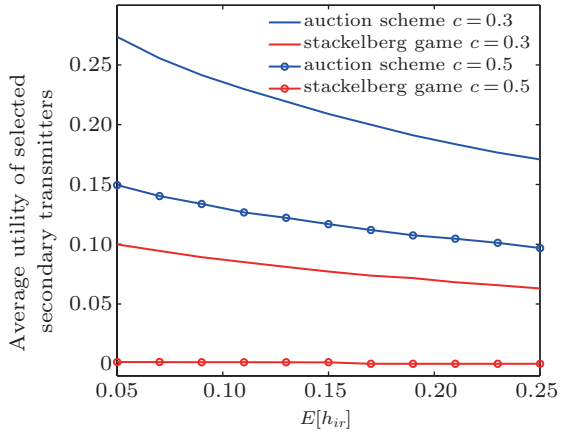


Fig. 10. (color online) Average utility of the selected ST versus average power channel gain h_{ir}.

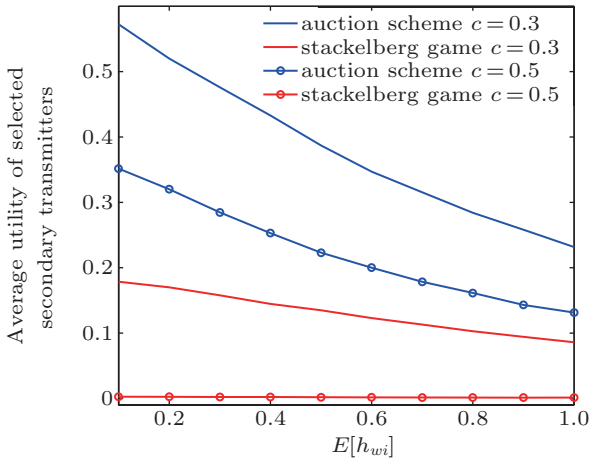


Fig. 11. (color online) Average utility of the selected ST versus average eavesdropping channel gain h_{wi}.

7. Conclusion

In this paper, we considered a scenario in which the multiple half-duplex STs threaten the security performance of the primary link by eavesdropping when they are not allowed to use the licensed spectrum.

A modified second-price sealed-bid auction scheme was proposed to analyze the interaction between the PT and untrusted STs. With the presented scheme, the PT and STs became allies instead of foes. Based on the max–min rule, an iterative algorithm was proposed to find the optimal bidding power of the STs in the presence of multiple eavesdroppers. If a proper ST is granted to access the licensed spectrum, it will help the PT to enhance the security by creating more interference to other unselected STs than to the PR. Numerical results show that both the PT and the selected ST can achieve significant performance improvements with our proposed scheme because it not only helps the PT select one proper cooperating ST but also increases the access chance of the STs. In our further work, the scenario in which the power of the PT can be adjusted will be investigated.

References

[1] Goldsmith A, Jafar S A, Maric I and Srinivasa S 2009 *IEEE Proceedings* **97** 894

[2] Qi P H, Li Z, Si J B and Gao R 2014 *Chin. Phys. B* **23** 128401

[3] Yang J, Yang D, Huang B, *et al.* 2014 *Acta Phys. Sin.* **63** 020501 (in Chinese)

[4] Wu C, Jiang H and You X J 2014 *Acta Phys. Sin.* **63** 088801 (in Chinese)

[5] Stanojev I and Aylin Y 2013 *IEEE Trans. Wireless Communications* **12** 134

[6] Zhang N, Lu N, Cheng N, Mark J W and Shen X S 2013 *IEEE Trans. Selected Areas in Communications* **31** 2453

[7] He X and Yener A 2010 *IEEE Trans. Inf. Theory* **56** 3807

[8] Yuksel M, Liu X and Erkip E 2011 *IEEE Trans. Inf. Forens. Security* **6** 818

[9] Hyoungsuk J, Steven W M, Il-Min K and Jeongseok H 2014 *IEEE Trans. Wireless Communications* **13** 1970

[10] Frédéric G, Li N, Nicolas S, Maksym G, Lars K R and Mikael S 2014 *IEEE Trans. Selected Areas in Communications* **32** 451

[11] Karim K and Eylem E 2013 *in Proc. Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)*, Tsukuba Science City, May 13–17, 2013, p. 194

[12] Klemperer P 1999 *J. Economics Surveys* **13** 227

[13] Wang T, Song L, Han Z, Cheng X and Jiao B 2012 *in Proc. International Conference on Communications*, Ottawa, Canada, June 10–15, 2012, p. 1683

[14] Osborne M J and Rubenstein A 1994 *A Course in Game Theory* (Cambridge: MIT Press) pp. 18–30

[15] Stephen B and Lieven V 2004 *Convex Optimization* (Cambridge: Cambridge University Press) pp. 95–103