IET Communications

Research Article

IET Journals
The Institution of Engineering and Technology

Cooperative jamming-based physical-layer security of cooperative cognitive radio networks: system model and enabling techniques

ISSN 1751-8628
Received on 16th April 2018
Revised 5th November 2018
Accepted on 10th December 2018
E-First on 6th February 2019
doi: 10.1049/iet-com.2018.5216
www.ietdl.org

Yuhang Zhang[1], Rongxing Lu[2], Bin Cao[1,3] ✉, Qinyu Zhang[1,3]

[1]*Harbin Institute of Technology (Shenzhen), Shenzhen, Guangdong, People's Republic of China*
[2]*University of New Brunswick, Fredericton, NB, Canada*
[3]*Shenzhen Cyberspace Laboratory, Shenzhen, Guangdong, People's Republic of China*
✉ *E-mail: caobin@hit.edu.cn*

Abstract: The aim of this work is to improve the secrecy capacity of primary users (PUs), meanwhile, spectrum utilisation and energy efficiency are considered. the authors present a communication system model with secondary users (SUs). The SUs are provided access to the spectrum. Also, by means of beamforming, their signals will not interfere the PUs but eavesdropper, and the PUs' transmissions are protected. By leveraging the SUs instead of traditional jamming nodes can also make the energy efficiency higher. They formulate the system model, signalling plan, and key enabling techniques to enhance the spectrum efficiency and PUs' physical-layer security with SUs' participation. They provide theoretic analysis of a sum capacity maximisation under a certain power constraint to evaluate the performance of this system. Numerical results show that the proposed scheme not only improves PU's secrecy capacity but also enhances the spectrum utilisation.

1 Introduction

Security is a very important issue in the field of wireless communication due to its vulnerability to eavesdropping. Traditionally, cryptography is used to solve this problem. In recent years, physical layer security technologies that protect communication security through information such as channel characteristics have received widespread attention. Wyner's pioneering work [1] investigated the theoretical basis of this area, which introduced the wiretap channel and demonstrated that when the eavesdropper's channel is a degraded version of the legitimate receiver, secret messages can be sent to the destination while keeping the eavesdropper from getting anything about the message. Then, in [2], Cheong and Hellman investigated the secrecy capacity of a Gaussian wire-tap channel. Later, Csiszar and Korner generalised Wyner's approach by considering the transmission of secret messages over broadcast channels [3]. Recently, physical-layer security in fading channels has been studied in [4, 5].

Basically, physical layer security and secrecy capacity are the capacity difference between the main channel and the eavesdropping channel. When the eavesdropping channel's performance is better than the main channel, there is no security. If the opposite, there is a certain amount of secrecy capacity. As a natural extension, approaches for physical layer security have been investigated in cooperative relaying networks [6–9]. In such a paradigm, one or more relays generate jamming at the eavesdropper to enhance security [10–12]. Employing jamming nodes for jamming has also been studied [13–19]. Especially in [18], the authors considered a scenario in which they introduced secondary users (SUs) with a single antenna instead of relaying and jamming nodes. Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks was analysed in [19], and the main focus of this work was on the security capacity of the user.

Unlike the aforementioned work, we not only focus on increasing the secrecy capacity, but also on pursuing higher spectral efficiency. To this end, this study proposes collaboration strategies for a half-duplex two-hop multiple antennas relay system in which the eavesdropper can wiretap the channels during both transmission phases. Also, SUs are introduced to replace relaying and jamming nodes. The aim of this work is to present a scheme, which improves both physical layer security and spectrum utilisation. To achieve our goal, we propose to build a cooperative network. In this study, the primary users (PUs) communicate as usual and the SUs assist PUs to forward information. Meanwhile, the SUs communicate with each other, causing interference to eavesdroppers, but will not affect the PUs. In this way not only can we save the energy of jamming, but also enhance the utilisation of spectrum. To evaluate the performance of the proposed strategy, we formulate and tackle the problem as a sum achievable capacity maximisation problem under a certain rate and power constraints. Simulations are provided to verify the solution approach and strategy performance.

The organisation of the rest paper is as follows. Section 2 describes the system model considered throughout the paper. In Section 3, the problem formulation and solution are presented. The performance of the proposed strategy is discussed in Section 4, and conclusions are drawn in Section 5.

The following notations are used in the paper: $()^{\mathrm{H}}$ denotes the Hermitian transpose. $\{x\}^+$ denotes $\max\{0, x\}$. Tr() is the trace operator and $\boldsymbol{I}$ is an identity matrix of appropriate dimension.

2 System model and signalling plan

2.1 System description

As shown in Fig. 1, we consider a two-phase five-terminal relay system composed of PUs, SUs and an eavesdropper Eve. In such a system, considering the scenario that the eavesdropper denoted as Eve tries to intercept signals and get the information from the primary network. The channel conditions between the PUs may be worse than those between PUs and Eve due to various reasons, such as buildings blocked and long distance. In this situation, it will be easier for Eve to get the information from the PUs. To enhance the quality of service, the PUs can employ SUs as relays to forward the information, as shown in Fig. 1.

With the help of relaying PU's signal, SUs are enabled to access the PUs' spectrum for secondary communication. Traditionally, a cooperative jammer requiring extra energy is always taken into account to protect the communications of PUs by generating and

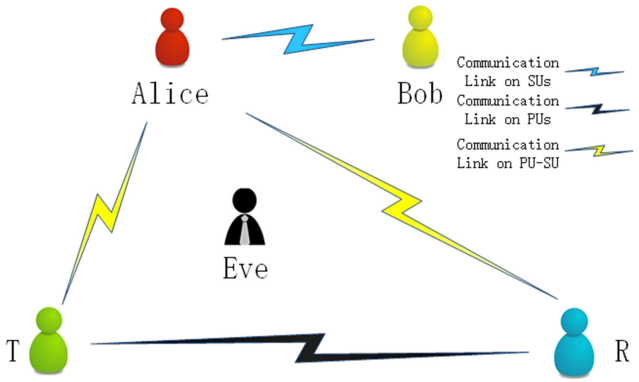

Fig. 1 *System model*

transmitting jamming signals. As mentioned above, the eavesdropper is only aiming at the communication of PUs and the information exchange between SUs is out of eavesdropper's concern, which means the signals transmitted between SUs are equivalent to jamming signals for Eve and can protect the information security of PUs as well. Compared with the traditional method, the advantage of introducing SUs is to achieve higher energy and spectral efficiency.

In this study, we denote T, R as PUs and Alice, Bob as SUs, as shown in Fig. 1. It is assumed that each terminal is equipped with multiple antennas, and the channel state information between all nodes can be perfectly obtained or estimated. The number of antennas of T, R, Alice, Bob and Eve is denoted by $N_{\mathrm{T}}, N_{\mathrm{R}}, N_{\mathrm{A}}, N_{\mathrm{B}}$, and N_{E}, respectively. In order to implement the above strategy, the PUs inform SUs to enter into this cooperation. A detailed process of SUs' selection is omitted here since it is not the focus of this study. After selecting Alice and Bob as partners, T and Alice–Bob pair start a two-phase cooperation. In the first phase, T broadcasts its signal $X_{\mathrm{T}} \in \mathbb{C}^{N_{\mathrm{T}}\times 1}$, meanwhile Bob transmits its signal $X_{\mathrm{B}} \in \mathbb{C}^{N_{\mathrm{B}}\times 1}$ to Alice. The signal received by Eve and Alice is a mixture version from T and Bob. By zero-forcing and projection techniques, the signal X_{B} can be nullified at R, and Alice can separate the two signals while Eve cannot differentiate them. The signal X_{B} here is equivalent of interference to Eve. In the second phase, Alice forwards the signal X_{T}, which received in the first phase to R and transmits the signal $X_{\mathrm{A}} \in \mathbb{C}^{N_{\mathrm{A}}\times 1}$ to Bob. For the same reason, signal X_{A} does not affect R at all, and Eve cannot separate the two signals. Although these two signals go through the same channel between Alice and Bob, Bob cannot separate them by means of projection, however, Bob can still obtain a certain communication capacity. In this way, with the assistance of SUs, the PUs get better quality of service. Meanwhile, Alice and Bob obtain the opportunity for their own communication, which improves spectrum efficiency.

2.2 Signalling plan

In the first phase, both T and Bob transmit the information signals to Alice and R. The signal received by R, Alice and Eve can be expressed as

$$Y_{\mathrm{r1}} = \sqrt{P_{\mathrm{T}}}H_{\mathrm{RT}}X_{\mathrm{T}} + \sqrt{P_{\mathrm{B}}}H_{\mathrm{RB}}\boldsymbol{T}_{\mathrm{B}}X_{\mathrm{B}} + Z_{r1}, \tag{1}$$

$$Y_{\mathrm{a}} = \sqrt{P_{\mathrm{T}}}H_{\mathrm{AT}}X_{\mathrm{T}} + \sqrt{P_{\mathrm{B}}}H_{\mathrm{AB}}\boldsymbol{T}_{\mathrm{B}}X_{\mathrm{B}} + Z_{a}, \tag{2}$$

$$Y_{\mathrm{e1}} = \sqrt{P_{\mathrm{T}}}H_{\mathrm{ET}}X_{\mathrm{T}} + \sqrt{P_{\mathrm{B}}}H_{\mathrm{EB}}\boldsymbol{T}_{\mathrm{B}}X_{\mathrm{B}} + Z_{e1}, \tag{3}$$

where $\boldsymbol{T}_{\mathrm{B}}$ is the zero-forcing matrix used by Bob. $Z_{\mathrm{r1}} \in \mathbb{C}^{N_{\mathrm{R}}\times 1}$, $Z_{\mathrm{a}} \in \mathbb{C}^{N_{\mathrm{A}}\times 1}$, $Z_{\mathrm{e1}} \in \mathbb{C}^{N_{\mathrm{E}}\times 1}$ are additive white Gaussian noise (AWGN) at R, Alice and the eavesdropper with covariance $\delta^2 I$, respectively. In general, $\boldsymbol{H}_{ij} \in \mathbb{C}^{N_i\times N_j}$ represents the channel matrix from nodes j to i, with $i, j \in \{T, R, A, B, E\}$. These channel matrices are fixed over the whole process. P_{T}, P_{B} are the transmit power used at T and Bob and $\mathrm{Tr}(X_{\mathrm{T}}X_{\mathrm{T}}^{\mathrm{H}}) = 1, \mathrm{Tr}(X_{\mathrm{B}}X_{\mathrm{B}}^{\mathrm{H}}) = 1$. Since the signal X_{B} would interfere the PU R, we can design T_{B} by zero-forcing to make the signal completely nulled at node R [12]. Here we can obtain the zero-forcing matrix by SVD decomposition of the channel matrix. After SVD decomposition, the channel matrix $\boldsymbol{H}_{ij} \in \mathbb{C}^{N_i\times N_j}$ can be expressed as $\boldsymbol{H}_{ij} = U\Sigma V$. $V = \{V_1 V_2\} \in \mathbb{C}^{N_j\times N_j}$. The zero-forcing matrix can be expressed as $\boldsymbol{T} = \{V_2 V_1\}^{\mathrm{H}}$. As aforementioned, Alice can separate the two signals from different nodes by projection. In this case, the signals received in this phase can be expressed as

$$Y_{\mathrm{r1}} = \sqrt{P_{\mathrm{T}}}H_{\mathrm{RT}}X_{\mathrm{T}} + Z_{\mathrm{r1}}, \tag{4}$$

$$Y_{\mathrm{a1}} = \sqrt{P_{\mathrm{T}}}H_{\mathrm{AT}}X_{\mathrm{T}} + Z_{\mathrm{a}}, \tag{5}$$

$$Y_{\mathrm{a2}} = \sqrt{P_{\mathrm{B}}}H_{\mathrm{AB}}T_{\mathrm{B}}X_{\mathrm{B}} + Z_{\mathrm{a}}, \tag{6}$$

$$Y_{\mathrm{e1}} = \sqrt{P_{\mathrm{T}}}H_{\mathrm{ET}}X_{\mathrm{T}} + \sqrt{P_{\mathrm{B}}}H_{\mathrm{EB}}T_{\mathrm{B}}X_{\mathrm{B}} + Z_{\mathrm{e1}}. \tag{7}$$

In Phase 2, Alice forwards the signal from PT by decode-and-forward (DF) protocol. Meanwhile, Alice communicates with Bob, therefore the received signal at R and Bob can be expressed as

$$Y_{\mathrm{r2}} = \sqrt{P_{\mathrm{A1}}}H_{\mathrm{RA}}X_{\mathrm{T}} + \sqrt{P_{\mathrm{A2}}}H_{\mathrm{RA}}\boldsymbol{T}_{\mathrm{A}}X_{\mathrm{A}} + Z_{\mathrm{r2}}, \tag{8}$$

$$Y_{\mathrm{b}} = \sqrt{P_{\mathrm{A1}}}H_{\mathrm{BA}}X_{\mathrm{T}} + \sqrt{P_{\mathrm{A2}}}H_{\mathrm{BA}}\boldsymbol{T}_{\mathrm{A}}X_{\mathrm{A}} + Z_{\mathrm{b}}. \tag{9}$$

The signal that Eve received is

$$Y_{\mathrm{e2}} = \sqrt{P_{\mathrm{A1}}}H_{\mathrm{EA}}X_{\mathrm{T}} + \sqrt{P_{\mathrm{A2}}}H_{\mathrm{EA}}\boldsymbol{T}_{\mathrm{A}}X_{\mathrm{A}} + Z_{\mathrm{e2}}, \tag{10}$$

where $\boldsymbol{T}_{\mathrm{A}}$ is the zero-forcing matrix used by Alice. The same as phase 1, $Z_{\mathrm{r2}}, Z_{\mathrm{b}}, Z_{\mathrm{e2}}$ are AWGN and $\mathrm{Tr}(X_{\mathrm{A}}X_{\mathrm{A}}^{\mathrm{H}}) = 1$. P_{A1} and P_{A2} are the power consumed by forwarding the signal X_{T} and communication with Bob, respectively. As aforementioned, the signal X_{A} corresponds to an interference to Eve and it will not interfere with R. Thus, the signal received at R in phase 2 is obtained as

$$Y_{\mathrm{r2}} = \sqrt{P_{\mathrm{A1}}}H_{\mathrm{RA}}X_{\mathrm{T}} + Z_{\mathrm{r2}}. \tag{11}$$

3 Problem formulation and solution approach

In this section, we first discuss the SNR or SINR and capacity of each node. Then the optimal problem of maximising the sum capacity under certain constraints is formulated. Finally, solutions to the problem are derived when $N_{\mathrm{t}} + N_{\mathrm{b}} > N_{\mathrm{e}}$ and $N_{\mathrm{a}} > N_{\mathrm{e}}$.

3.1 Problem formulation

For a two-hop DF-based relay channel via maximal ratio combining at all nodes, the mutual information between T and R through the relay link can be written as

$$C_s = \frac{1}{2}\min\{\log_2(1+\Gamma_{RT}+\Gamma_{RA}), \log_2(1+\Gamma_{AT})\}, \tag{12}$$

$$\Gamma_{RT} = \frac{P_T X_T^H H_{RT}^H H_{RT} X_T}{\delta^2}, \tag{13}$$

$$\Gamma_{RA} = \frac{P_{A1} X_T^H H_{RA}^H H_{RA} X_T}{\delta^2}, \tag{14}$$

$$\Gamma_{AT} = \frac{P_T X_T^H H_{AT}^H H_{AT} X_T}{\delta^2} \tag{15}$$

and the first formula in C_s is the capacity of R and the second one is the achievable throughput of relaying at Alice. $\frac{1}{2}$ appears because the transmission is divided into two phases, and Γ_{ij} is the SNR or SINR at node i of the signal from node j. Similarly, Alice and Bob's capacities can be written as

$$C_a = \frac{1}{2}\log_2(1+\Gamma_{AB}), \tag{16}$$

$$C_b = \frac{1}{2}\log_2(1+\Gamma_{BA}), \tag{17}$$

$$\Gamma_{AB} = \frac{P_B X_B^H T_B^H H_{AB}^H H_{AB} T_B X_B}{\delta^2}, \tag{18}$$

$$\Gamma_{BA} = \frac{P_{A2} X_A^H T_A^H H_{BA}^H H_{BA} T_A X_A}{P_{A1} X_T^H H_{BA}^H H_{BA} X_T + \delta^2}. \tag{19}$$

Through maximal ratio combining, Eve's capacity can be expressed as

$$C_e = \frac{1}{2}(\log_2(1+\Gamma_{EA}+\Gamma_{ET})), \tag{20}$$

where

$$\Gamma_{ET} = \frac{P_T X_T^H H_{ET}^H H_{ET} X_T}{P_B X_B^H T_B^H H_{EB}^H H_{EB} T_B X_B + \delta^2}, \tag{21}$$

$$\Gamma_{EA} = \frac{P_{A1} X_T^H H_{EA}^H H_{EA} X_T}{P_{A2} X_A^H T_A^H H_{EA}^H H_{EA} T_A X_A + \delta^2}. \tag{22}$$

In this context, PU's secrecy capacity is

$$C_r = \{C_s - C_e\}^+. \tag{23}$$

As mentioned before, we will consider the sum achievable capacity maximisation problem under certain constraints to evaluate the system performance. The power allocation leads to a trade-off in sum achievable capacity under both global power constraints ($P_T + P_B \le P$ in the first phase and $P_{A1} + P_{A2} \le P$ in the second phase). In addition, every user's capacity constraints should be considered to keep cooperation by ensuring every user's benefit. This is an optimisation problem and we would find the optimal power allocation.

For power allocation, the problem of maximising the sum capacity can be written as

$$\max_{P_T, P_B, P_{A1}, P_{A2}} \quad C_{max} = C_r + C_a + C_b \tag{24}$$

$$\text{s.t.} \quad P_T + P_B \le P, \quad 0 \le P_T, P_B, \tag{25}$$

$$P_{A1} + P_{A2} \le P, \quad 0 \le P_{A1}, P_{A2}, \tag{26}$$

$$C_0 \le C_r, \tag{27}$$

$$C_1 \le C_a, \tag{28}$$

$$C_2 \le C_b, \tag{29}$$

where (25) and (26) are the power constraints. C_0 is the lower limit of secrecy capacity required by the PUs. After cooperation with PUs, if the capacities Alice and Bob obtained no more than C_1, C_2, respectively, they do not have the motivation to participate in the cooperation and the cooperation ends.

In the above problem, obviously a larger P_T in phase 1 is beneficial for R, Eve and Alice's signal reception, however, this will result in a lower available power of P_B, which means the interference to Eve and the capacity of Bob may be lower. Similarly, P_{A1} not only affects the signal reception of Eve and R but also affects the communication capacity of Alice and the interference effect on Eve. As above mentioned, power changes on each node can have an indeterminate impact on system performance. Unfortunately, this problem appears to be a non-convex optimisation problem in general.

3.2 Solution approach

In order to solve the optimisation problem of (24), we need to simplify it first. As given in (12), the secrecy capacity of PUs is the minimum throughput of signal X_T obtained by Alice and R. In this case, when the two capacities are equal, system efficiency is the highest and there is no energy waste. In this way, (12) can be written as

$$C_s = \frac{1}{2}\log_2(1+\Gamma_{RT}+\Gamma_{RA}), \tag{30}$$

where

$$\log_2(1+\Gamma_{RT}+\Gamma_{RA}) = \log_2(1+\Gamma_{AT}). \tag{31}$$

We can expand (31) as

$$\begin{aligned} &P_T \frac{X_T^H H_{AT}^H H_{AT} X_T}{\delta^2} \\ &\quad = P_T \frac{X_T^H H_{RT}^H H_{RT} X_T}{\delta^2} + P_{A1} \frac{X_T^H H_{RT}^H H_{RT} X_T}{\delta^2}. \end{aligned} \tag{32}$$

Here, we denote P_T as aP_{A1}, a is a constant. Therefore, this equation can be expressed as

$$\begin{aligned} &aP_{A1} \frac{X_T^H H_{AT}^H H_{AT} X_T}{\delta^2} \\ &\quad = aP_{A1} \frac{X_T^H H_{RT}^H H_{RT} X_T}{\delta^2} + P_{A1} \frac{X_T^H H_{RT}^H H_{RT} X_T}{\delta^2}. \end{aligned} \tag{33}$$

As assumed that the quality of the channel between T and Alice is better than that between T and R, i.e. $X_T^H H_{RT}^H H_{RT} X_T < X_T^H H_{AT}^H H_{AT} X_T$, we further have

$$a = \frac{X_T^H H_{RT}^H H_{RT} X_T}{X_T^H H_{AT}^H H_{AT} X_T - X_T^H H_{RT}^H H_{RT} X_T}. \tag{34}$$

The problem of maximising the sum capacity can be rewritten as

$$\max_{P_B, P_{A1}, P_{A2}} \quad C_{max} = C_r + C_a + C_b, \tag{35}$$

$$\text{s.t.} \quad aP_{A1} + P_B \le P, \quad 0 \le P_{A1}, P_B, \tag{36}$$

$$P_{A1} + P_{A2} \le P, \quad 0 \le P_{A1}, P_{A2}, \tag{37}$$

$$C_0 \le C_r, \tag{38}$$

$$C_1 \le C_a, \tag{39}$$

$$C_2 \le C_b, \tag{40}$$

On account of the last three constraints being complicated, even non-convex, we would reduce these constraints by constructing the penalty function. Then take advantage of the heuristic algorithm to solve this problem and obtain the overall optimal solution. Here, we use the annealing algorithm. From (38)–(40), a penalty function can be built as

$$\begin{aligned} F = q(&\max\{(C_0 - C_r), 0\}^2 \\ &+ \max\{(C_1 - C_a), 0\}^2 + \max\{(C_2 - C_b), 0\}^2), \end{aligned} \tag{41}$$

where q is the penalty coefficient, which is a positive number. The converted problem is as follows, (36) and (37) are the domains of power

$$\max_{P_B, P_{A1}, P_{A2}} \quad C_{max} = C_r + C_a + C_b - F, \tag{42}$$

$$\text{s.t.} \quad aP_{A1} + P_B \le P, \quad 0 \le P_{A1}, P_B, \tag{43}$$

$$P_{A1} + P_{A2} \le P, \quad 0 \le P_{A1}, P_{A2}. \tag{44}$$

Then, we can solve this optimisation problem by the following algorithm, which is summarised in Algorithm 1 (see Fig. 2).

In Algorithm 1 (Fig. 2), T and t are the initial and end temperatures, respectively. θ is the gain coefficient of q, which is larger than 1. η here is the annealing coefficient, which is a little bit < 1. α is the number of cycles at the same temperature. ε means the limit of error, which is a very small positive number, in general. We initialise P_{A1}, P_B, P_{A2} in the domain of power, and can obtain the optimal solution of the problem through this algorithm.

4 Analytical and simulation results

To validate our theoretical results and proposed algorithms, we consider a secrecy network in the presence of an eavesdropper. T, R, Alice, Bob and Eve's coordinates are assumed to be located at $(-0.5, 0)$, $(0.5, 0)$, $(0, 0)$, $(0.5, -0.5)$ and $(0, -0.5)$ respectively, where distances are expressed in kilometres. We assume the path-loss coefficient is 2, and the background noise power $\delta^2 = -60$ dBm at all nodes. We would examine the system performance via Matlab simulations. In this simulation, it is assumed that the PUs, Bob, Eve are equipped with two antennas ($N_T = N_R = N_B = N_E = 2$), whereas Alice is equipped with four antennas ($N_a = 4$). The maximum available transmission power at both phases is considered to be 1000 mW. C_0, C_1, C_2 are set as $1, 0.5, 0.5$ bps/Hz, respectively. On the setting of the constants of the annealing algorithm, we set $T = 100$, $t = 10^{-10}$, $\theta = 1.2$, $q = 20$, $\eta = 0.98$, $\alpha = 100$ and $\varepsilon = 0.5$. The step length in the algorithm is 10.

The relationship between the maximum communication capacity and the forwarding power P_{A1} obtained by each node is shown in Fig. 3, here we can observe that as P_{A1} changes, the maximum capacity that each node changes accordingly. When the value of P_{A1} is very small, the secrecy capacity obtained by the PU cannot meet the requirement and this cooperation cannot be established. With the increase of P_{A1}, the secrecy capacity of the PU gradually increases. At the same time, the SU's capacity decreases and the maximum values of P_B and P_{A2} also decrease. When the P_{A1} increases to a certain value, the communications of the SUs cannot effectively interfere eavesdroppers. At this time, continuing to increase P_{A1} will result in the decrease of the PU's secrecy capacity. When P_{A1} is very large, SUs cannot get adequate communication capacity and the cooperation is terminated. As for the sum capacity, it is affected by three values: C_s, C_b and C_a. The sum capacity increases firstly and then decreases with the increase of P_{A1}. The circle mark in Fig. 3 is the maximum capacity point obtained by our algorithm.

1: Initialize:$P_{A1}, P_B, P_{A2}, T, t, q, \theta, \eta, \alpha, \varepsilon$,$(P_{A1}, P_B, P_{A2})$ is regarded as coordinates of a point
2: F=1
3: while($\varepsilon \le F$)
4: while($t \le T$)
5: calculate C_{max}
6: initialize $i = 0$
7: while ($i \le \alpha$)
8: randomly generate a step $l = (x, y, z)$ with fixed length
9: (P'_{A1}, P'_B, P'_{A2}) =$(P_{A1}, P_B, P_{A2}) + l$
10: if (P'_{A1}, P'_B, P'_{A2}) is out of the domain of definition
11: goto step (7)
12: end
13: calculate C'_{max} with (P'_{A1}, P'_B, P'_{A2})
14: if $C_{max} < C'_{max}$
15: $C_{max} = C'_{max}$, $(P_{A1}, P_B, P_{A2}) = (P'_{A1}, P'_B, P'_{A2})$
16: else if $rand(0, 1) \le e^{\frac{C'_{max} - C_{max}}{T}}$
17: $C_{max} = C'_{max}$, $(P_{A1}, P_B, P_{A2}) = (P'_{A1}, P'_B, P'_{A2})$
18: end
19: i=i+1
20: end
21: $T = T * \eta$
22: end
23: calculate F
24: $q = q * \theta$
25: end

Fig. 2 *Algorithm 1: capacity maximisation algorithm*

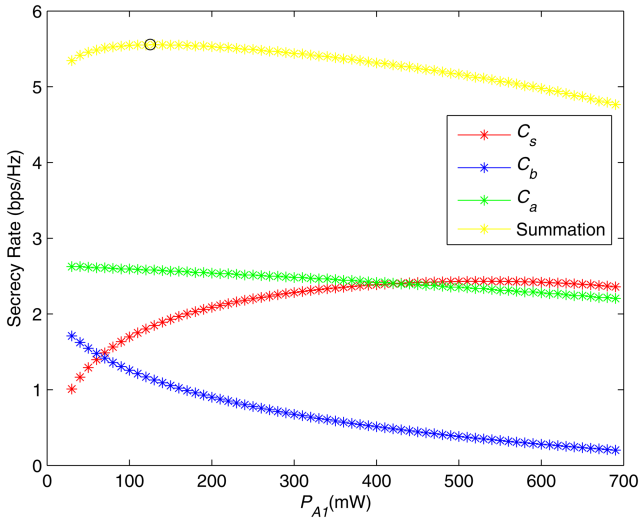

Fig. 3 *Capacity performance with respect to* P_{A1}

To further verify the feasibility of the algorithm, we calculated the classified capacity at different power P in Fig. 4. Here we change the value of P, the actual value and the calculated value of the maximum capacity are shown in the figure. Obviously, these two values are very close.

Fig. 5 shows the effect of distance on the PU's secrecy capacity. We keep the other nodes in the same position, then we change the location of Eve on the line of Eve and T. We can find that the closer the two nodes are, the lower the secrecy capacity is. Since the closer they are, the better it is for the eavesdropper's interception. When eavesdropper is close enough to T, we even cannot get the required secrecy capacity.

Then, we consider the effect of the number of antennas on the system. We examine the capacity of each node and sum capacity in the case of Alice equipped with a different number of antennas in Figs. 6–9. Here we can see that the more antennas, the better the performance of the system. At the same time, with the change of P_{A1}, the system performance has the same trend under different antenna numbers. Also, we can see that the number of antennas has

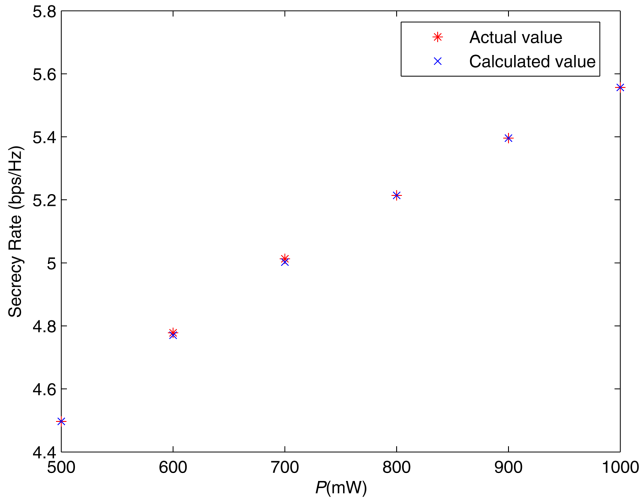

Fig. 4 *Capacity performance with respect to P*

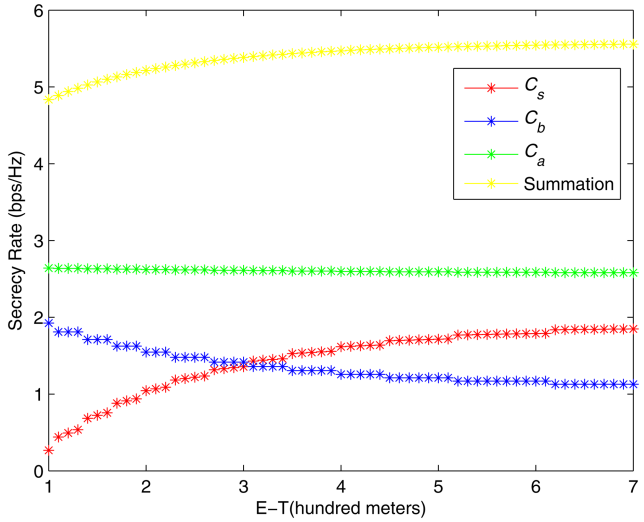

Fig. 5 *Capacity performance with respect to the distance between E–T*

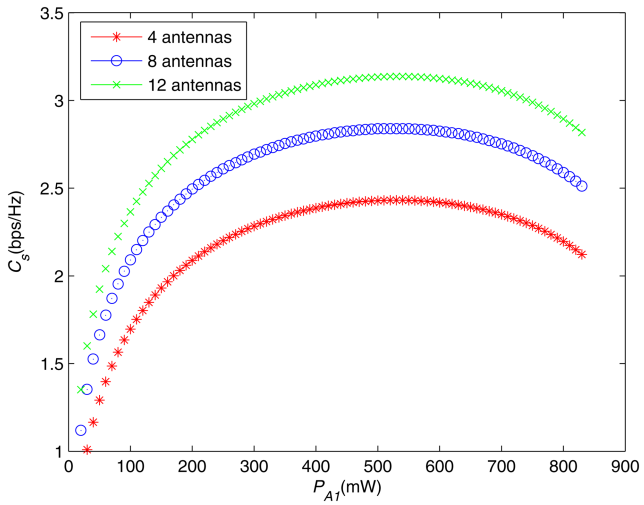

Fig. 6 C_s *with respect to* P_{A1}

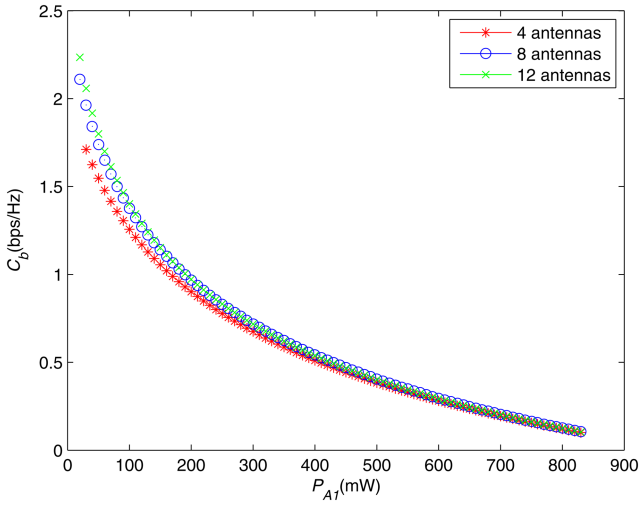

Fig. 7 C_b *with respect to* P_{A1}

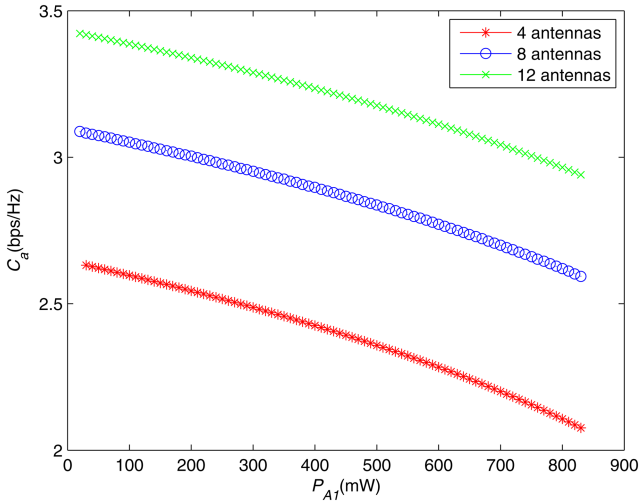

Fig. 8 C_a *with respect to* P_{A1}

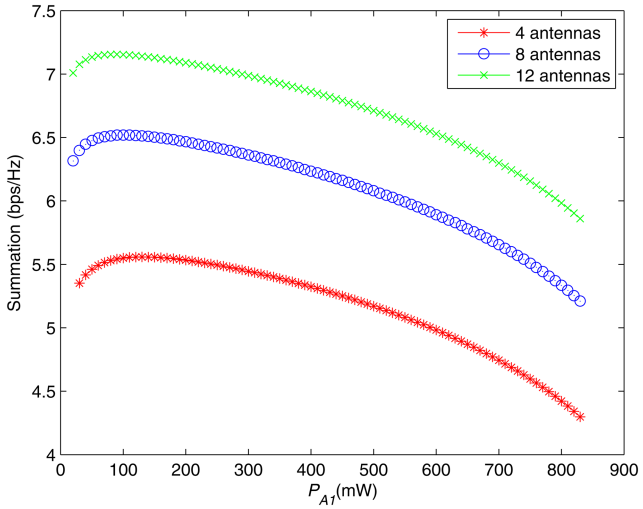

Fig. 9 *Sum capacity performance with respect to* P_{A1}

little effect on the capacity of Bob. This is because both the interfering signal and the useful signal for Bob are sent from Alice. The difference between the number of antennas does not affect the SNR of Bob.

Finally, the performance comparison between our proposed strategy and the traditional method realised by a jamming node are shown in Fig. 10. It is shown that our proposed strategy has better performance under different power constraints. From the simulation result, we can see that the sum of capacity is about twice that of the traditional method, which suggests the proposed strategy can improve the energy and spectral efficiency of the system at the same time.

5 Concluding remarks

Obtaining secure transmission performance and high spectral efficiency at the same time is a problem worth studying in the field

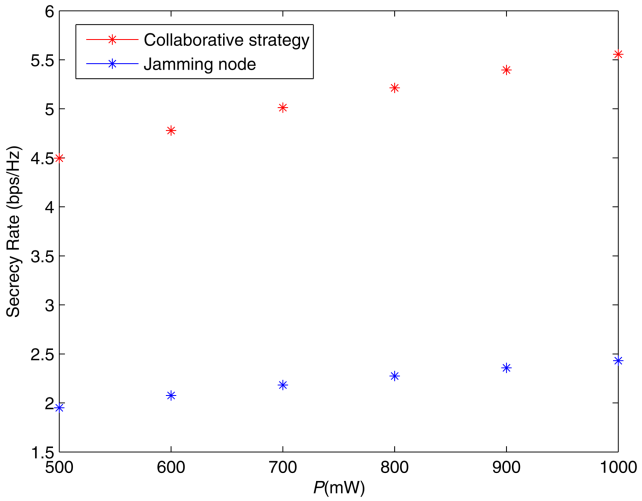

Fig. 10 *Sum capacity performance with respect to P*

of physical layer security. In this study, different from traditional relay communication and cooperative jamming schemes, we propose a strategy with high spectrum utilisation, which also ensures the security performance of the physical layer at the same time. The main idea is to use the communication signals between SUs as interference to eavesdroppers. In such a scenario, the PUs gain required secrecy capacity by allowing SUs to join the spectrum. In the meantime, SUs also get the opportunity to communications. The collaboration between them can achieve a win–win result, not only increases the secrecy capacity of the PUs but also increases the utilisation rate of the spectrum.

6 Acknowledgment

This work was supported by the National Natural Sciences Foundation of China under Grant No. 6150121), the Basic Research Project of Shenzhen under Grant No. JCYJ20160531192013063 and JCYJ20170307151148585, the Natural Sciences Foundation of Guangdong under Grant No. 2017A030313372, the Natural Scientific Research Innovation Foundation in Harbin Institute of Technology, the Natural Sciences Foundation of Jiangxi under Grant No. 20151BAB217001 and 20151BAB217018, and S&T Foundation of Jingdezhen.

7 References

[1] Wyner, A.D.: 'The wire-tap channel', *Syst. Tech. J.*, 1975, **54**, (8), pp. 1355–1387

[2] Leung-Yan-Cheong, S., Hellman, M.E.: 'The Gaussian wire-tap channel', *IEEE Trans. Inf. Theory*, 1978, **24**, (4), pp. 451–456

[3] Csiszar, I., Korner, J.: 'Broadcast channels with confidential messages', *IEEE Trans. Inf. Theory*, 1978, **24**, (3), pp. 339–348

[4] Yang, J., Kim, I.M., Kim, D.I.: 'Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers', *IEEE Trans. Wirel. Commun.*, 2013, **12**, (6), pp. 2840–2852

[5] Huang, J., Swindlehurst, A.L.: 'Cooperative jamming for secure communications in MIMO relay networks', *IEEE Trans. Signal Process.*, 2011, **59**, (10), pp. 4871–4884

[6] Vishwakarma, S., Chockalingam, A.: 'MIMO decode-and-forward relay beamforming for secrecy with cooperative jamming'. 2014 Twentieth National Conf. on Communications (NCC), Kanpur, India, February 2014, pp. 1–6

[7] Dong, L., Han, Z., Petropulu, A, *et al.*: 'Improving wireless physical layer security via cooperating relays', *IEEE Trans. Signal Process.*, 2010, **58**, (3), pp. 1875–1888

[8] Feng, Y., Yang, Z., Yan, S., *et al.*: 'Physical layer security enhancement in multi-user multi-full-duplex-relay networks'. 2017 IEEE Int. Conf. on Communications (ICC), Paris, France, May 2017, pp. 1–7

[9] Zheng, G., Choo, L.C., Wong, K.K.: 'Optimal cooperative jamming to enhance physical layer security using relays', *IEEE Trans. Signal Process.*, 2011, **59**, (3), pp. 1317–1322

[10] Fakoorian, S.A.A., Swindlehurst, A.L.: 'Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer', *IEEE Trans. Signal Process.*, 2011, **59**, (10), pp. 5013–5022

[11] Wang, H.M., Luo, M., Xia, X.G., *et al.*: 'Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI', *IEEE Signal Process. Lett.*, 2013, **20**, (1), pp. 39–42

[12] Chu, Z., Cumanan, K., Ding, Z., *et al.*: 'Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer', *IEEE Trans. Veh. Technol.*, 2015, **64**, (5), pp. 1833–1847

[13] Zhang, G., Xu, J., Wu, Q., *et al.*: 'Wireless powered cooperative jamming for secure OFDM system', *IEEE Trans. Veh. Technol.*, 2018, **67**, (2), pp. 1331–1346

[14] Kolokotronis, N., Athanasakos, M.: 'Improving physical layer security in DF relay networks via two-stage cooperative jamming'. 2016 24th European Signal Processing Conf. (EUSIPCO), Budapest, Hungary, August 2016, pp. 1173–1177

[15] Iwata, S., Ohtsuki, T., Kam, P.Y.: 'A lower bound on secrecy capacity for MIMO wiretap channel aided by a cooperative jammer with channel estimation error', *IEEE Access*, 2017, **5**, pp. 4636–4645

[16] Li, L., Chen, Z., Fang, J., *et al.*: 'Secrecy degrees of freedom of a MIMO Gaussian wiretap channel with a cooperative jammer'. 2016 IEEE Int. Conf. on Acoustics Speech and Signal Processing (ICASSP), March 2016, pp. 3486–3490

[17] Cumanan, K., Alexandropoulos, G.C., Ding, Z., *et al.*: 'Secure communications with cooperative jamming: optimal power allocation and secrecy outage analysis', *IEEE Trans. Veh. Technol.*, 2017, **66**, (8), pp. 7495–7505

[18] Chen, Z., Cao, B., Zhang, Y., *et al.*: 'Creep: cognitive relaying enabled efficiency and physical-layer security preserving framework'. 2014 IEEE Int. Conf. on Communication Systems, Macau, China, November 2014, pp. 258–262

[19] Zhang, R., Cheng, X., Yang, L.: 'Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks', *IEEE Trans. Wirel. Commun.*, 2016, **15**, (8), pp. 5651–5663