Lin et al. EURASIP Journal on Wireless Communications and Networking (2016) 2016:129
DOI 10.1186/s13638-016-0621-5

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Opportunistic relaying and jamming with robust design in hybrid full/half-duplex relay system

Zhi Lin*, Yueming Cai, Weiwei Yang* and Xiaoming Xu

Abstract

Full duplex (FD) protocol has been widely used in wireless communications, which could transmit and receive signals at the meantime. In this paper, considering the worst-case channel uncertainty, opportunistic relaying and jamming strategy in decode-and-forward (DF) hybrid full/half-duplex (HD) relay system is proposed to enhance security. Specifically, the relay works in FD protocol to receive the confidential signals and transmit jamming signals at the first time slot. Then, the relay switches to HD protocol to transmit the decoded signals. Meanwhile, jammers emit cooperative jamming (CJ) signals to interfere the eavesdropper at two transmission slots. Suppose that imperfect eavesdropper channel condition is considered, we propose a worst-case robust design to obtain distributed jamming weights, which is solved through semi-definite program (SDP). Furthermore, we analyze secrecy rate and secrecy outage performance of the proposed scheme. As a benchmark, a traditional relay selection strategy with HD protocol in distributed relay system is listed for comparison. Simulation results demonstrate that our hybrid scheme with robust design outperforms the traditional relay selection scheme, because the traditional scheme does not consider hybrid FD/HD protocols and robust design based on imperfect channel conditions.

1 Introduction

Due to the broadcast nature of wireless channels which makes communication ubiquitously accessible, security becomes one of the most important issues in wireless communications. Traditionally, communication security is guaranteed through high-layer encryption. With the development of interception technology and computing power, encryption needs to be more complex, leading to higher computation burden. Unlike traditional cryptographic approaches, physical layer security (PLS) takes advantage of the physical characteristics of wireless channels to achieve secure transmission. Wyner pointed out that when the legitimate channel has better propagation conditions than eavesdropping channel, secret transmission is theoretically possible without sharing any key [1].

However, if the channel condition of legitimate user is worse than that of the eavesdropping channels, secrecy rate can be very low or even decline to zero [1]. An efficient solution to enhance the legitimate transmission is through cooperative relaying or confusing the eavesdroppers via cooperative jamming. Recently, relay cooperation diversity has attracted more and more attentions, as it can significantly improve the communication coverage area and secrecy performance [2, 3]. To simplify radio hardware in cooperative diversity setups, relay selection strategy is adopted for multiple relay nodes communication. A distributed opportunistic relay selection approach was proposed in cooperative relay system [4]. This relay selection strategy achieves the same secrecy rate performance with low complexity, compared to the scheme that all nodes participate in aiding the communications.

Alternatively, the cooperative nodes can also act as jammers to transmit artificial jamming signals collaboratively to interfere the eavesdroppers. In [5], the cooperative jamming (CJ) was investigated for Gaussian multiple access and two-way channels. The optimal CJ weights for secrecy rate maximization (SRM) problem in the presence of a single eavesdropper were studied in [6]. Furthermore, hybrid relaying and jamming schemes

* Correspondence: lz945@sina.cn; wwyang1981@163.com
College of Communication Engineering, PLA University of Science and Technology, Guanghua Road, Nanjing, China

were proposed to combine the advantages of both strategies in [4, 7].

Full-duplex (FD) operation, which always transmits and receives signals in the entire bandwidth, has attracted extensive attention. And a range of theoretical and practical researches have been investigated to take advantages of characteristic of FD protocol to enhance system performance [8, 9]. An interesting work was proposed in [8], where artificial noise (AN) was sent by a multi-antenna FD receiver. In [8], authors aimed to design the optimal jamming vector that maximizes the secrecy rate and mitigates loop interference. To enhance secrecy performance of a multiple-input-single-output-single-eavesdropper (MISOSE) relay system, a joint information beamforming and jamming beamforming strategy were proposed to guarantee both transmitting security and receiving security for a FD base station in [9]. Some works also make use of the advantages of both FD and HD protocols to improve system performance. The hybrid scheme that switches between FD and HD protocols can be employed to enhance secrecy performance [10, 11].

However, in the above works [8–11], the perfect instantaneous channel state information (CSI) of all links is needed at the nodes which carry out the optimization procedure. Nevertheless, in practical relay communication networks, the perfect CSI is usually unknown and has to be estimated. The mismatch between the real and estimated CSI is caused by some inevitable factors, such as channel estimation errors, feedback delay, and quantization errors. Obviously, the performance of the designs developed in [8–11] could be heavily degraded by the imperfect CSI. Robust algorithm is an effective way to eliminate the influence of estimation errors. Typically, the existing works usually use deterministic uncertainty model (DUM) to characterize imperfect CSI: it assumes that a nominal value of the instantaneous CSI is available but lies in a bounded uncertainty region defined by some norm. The authors in [12] investigated the worst-case robust transmit covariance design problem of secrecy-rate maximization in the presence of multiple eavesdroppers. In [13], cooperative transmission for securing a decode-and-forward (DF) two-hop network was studied, where only the statistical CSI of the eavesdropping channel is available.

To sum up, the researches above only investigate the secrecy performance in FD or HD networks, and little work has been done for hybrid relay networks with opportunistic relay selection. Moreover, cooperative jamming with robust design is not widely considered in multi-relay systems, which can eliminate the influence of estimation errors.

In this paper, we investigate the secrecy performance of opportunistic relaying and jamming in hybrid FD/HD relay network with channel uncertainty. The contributions of the paper are summarized as follows:

- We propose a hybrid FD/HD strategy and opportunistic proactive relay selection approach in our model, where the best relay is selected to switch between FD and HD operation to DF confidential signals. And the other relay nodes send distributed cooperative jamming signals to interfere the receiving signal and interference with noise ratio (SINR) at the eavesdropper.
- In order to eliminate the influence of imperfect CSI to enhance the system security performance, we adopt the worst-case robust design to obtain the CJ beamformer under channel uncertainty. The optimization problem based on robust design is solved by SDP and interior method.
- We derive the secrecy rate and secrecy outage expressions. Furthermore, we compare our scheme with a traditional relay selection scheme. Simulation results clearly show the advantage of our proposed scheme to improve system secrecy performance.

1.1 Notation

Bold uppercase and lowercase letters denote matrices and vectors, respectively. $(\bullet)^T$ and $(\bullet)^H$ stand for transpose and Hermitian's transpose of a matrix or vector, respectively. $\mathbf{I}_N$ is the $N \times N$ identity matrix. $CN(\tau, \sigma^2)$ denotes the circularly symmetric, complex Gaussian distribution of vectors with mean τ and variance σ^2.

2 System model

The system shown in Fig. 1 consists of a source node S, M cooperative nodes, an intended receiver D, and a legitimate user E, in which cooperative nodes are equipped with both the receive antenna and the transmit antenna and other nodes are equipped with single antenna. In this model, the source S sends private message x, which is destined for intended receiver D and kept secret from receiver E. Before the source transmission, the opportunistic relay R has to be selected, which will

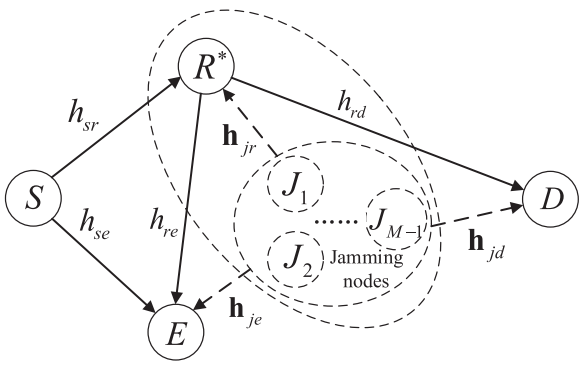

Fig. 1 Hybrid FD/HD relay model

be introduced in Section 3; the other cooperative nodes J_i, $(1 \le i \le M-1)$ are used to send jamming signals.

In particular, we assume the direct path between S and D is blocked by some obstacle so that there is no effective S-D link. Otherwise, if S-D link exits, system has to separate the useful signals from jamming signals, which will complicate the model. h_{sr}, h_{se}, h_{rd}, h_{re}, $\mathbf{h}_{jr}$, $\mathbf{h}_{jd}$, and $\mathbf{h}_{je}$ denote the channel coefficients of S-R, S-E, R-D, R-E, R-R, J_i-R, J_i-D, and J_i-E links, respectively, where $\mathbf{h}_{jr}$, $\mathbf{h}_{jd}$, and $\mathbf{h}_{je}$ are stacked in $M-1\times 1$ vector and other channel coefficients are scalars.

Throughout this paper, the following assumptions are adopted: (1) The channels from transmitting nodes to receiving nodes are symmetric, all the channels involved are considered to remain constant during one operation period and are quasi-static. (2) All the noise distributions are zero-mean circular complex Gaussian with unit variance σ^2. (3) All the channel coefficients experience Rayleigh fading, and the corresponding channel gains are obtained as $\gamma_i = P_i|h_i|^2/\sigma^2$, $(i \in sr, se, rd, re)$ which are independently exponentially distributed with mean of λ_i, $\gamma_k = P_k\left|\mathbf{h}_k^H\mathbf{f}\right|^2$, $(k \in jr, jd, je)$ and $\gamma_k \sim \text{Erlang}(M-1, \lambda_k)$. (4) The self-interference (SI) γ_{rr} is well reduced to a tolerable level by efficient SI suppression. (5) The intended user D and legitimate user E employ maximum radio combination (MRC) technology to receive signals.

At time slot t, source S sends private message $x(t)$, which is destined for opportunistic relay R and kept secret from eavesdropper E, R receive $x(t)$ from S. Meanwhile, opportunistic relay R and cooperative nodes J_i transmit the jamming signal $z_r(t)$ and $j(t)$, respectively. Since we assume that there is no direct link of S-D, legitimate destination cannot receive any useful information except jamming signal at time slot t; thus, we can neglect the receiving signal at D. The receiving signals at the relay R and eavesdropper E are given by

$$y_r(t) = \sqrt{P_S}h_{sr}(t)x(t) + \sqrt{P_R}h_{rr}(t)z_r(t) + \sqrt{P_J}\mathbf{h}_{jr}^H(t)\mathbf{f}_r j(t) + n_r(t) \quad (1)$$

$$y_e(t) = \sqrt{P_S}h_{se}(t)x(t) + \sqrt{P_R}h_{re}(t)z_r(t) + \sqrt{P_J}\mathbf{h}_{je}^H(t)\mathbf{f}_r j(t) + n_e(t), \quad (2)$$

where $x(t)$ and $j(t)$ denote the transmitted useful signals and jamming signals with $E\{|x(t)|^2, |j(t)|^2\} = 1$, respectively. The term n_r and n_e represent naturally occurring noise at best relay R and eavesdropper E. At time slot t, the distributed jamming beamforming weight is stacked in vector $\mathbf{f}_r = [f_{r1}, f_{r2}, \cdots, f_{r(M-1)}]^T$, and since the beamforming weight only determine the transmit direction, we normalize one-dimensional vector $\mathbf{f}_r$ as $\left|\mathbf{f}_r^H\mathbf{f}_r\right| = 1$. We assume that there exist per-node power constraints of all the nodes. P_S denotes the consumed power of the source, P_R denotes the consumed power of the opportunistic relay, while $P_{Ji}(1 \le i \le M-1)$ denotes the consumed power of cooperative node J_i, respectively. And to relax the complexity, we assume $P_{Ji} = P_J$, $(1 \le i \le M-1)$. Thus, we can regard the cooperative jamming nodes as a multi-antenna jammer to emit weighted jamming signals to interfere eavesdropper.

At time slot $t+1$, the chosen relay R switches to HD model and only transmits the previously decoded $x(t)$ to D. At the same time, S transmits the jamming signal $z_s(t+1)$, and cooperative nodes J_i still emit jamming signals $j(t+1)$. The receiving signals at D and E equal

$$y_d(t+1) = \sqrt{P_R}h_{rd}(t+1)x(t) + \sqrt{P_J}\mathbf{h}_{jd}^H(t+1)\mathbf{f}_d j(t+1) + n_d(t+1) \quad (3)$$

$$y_e(t+1) = \sqrt{P_S}h_{se}(t+1)z_s(t+1) + \sqrt{P_R}h_{re}(t+1)x(t) + \sqrt{P_J}\mathbf{h}_{je}^H(t+1)\mathbf{f}_d j(t+1) + n_e(t+1). \quad (4)$$

While at time slot $t+1$, the distributed jamming beamforming weight is stacked in vector $\mathbf{f}_d = [f_{d1}, f_{d2}, \cdots, f_{d(M-1)}]^T$.

Regarding the available CSI in a wireless communication system, the receiver usually estimates the channel using a training sequence (pilot symbols). At the transmitter, the CSI can be obtained through a feedback channel or from previous received signals, exploiting the channel reciprocity in time division duplexing (TDD) (see [14] for an overview of different channel estimation strategies). In this paper, we assume that the CSI $\mathbf{h}_{je}$ is partially known at jammers, and this situation is reasonable while E is a legitimate user but also a potential active eavesdropper in wireless network [15–17]. Since the wireless system tries to enhance secrecy performance through signal processing at distributed jammers, thus, the system requires the receiving nodes feedback corresponding CSI to jammers. The potential eavesdropper additionally exchanges messages with the relay, appearing as a legitimate user. The goal of E is not only to intercept private message but also to feedback false training signals to interfere the estimation on S-E and J_i-E links.

In this correspondence, we consider the additive model for the eavesdropping channel state information (ECSI) available at jamming nodes as follows, which will be used in Section 3.

$$\mathbf{h}_{je} = \tilde{\mathbf{h}}_{je} + \mathbf{e}_{je} \quad (5)$$

where $\tilde{\mathbf{h}}_{je}$ denotes estimation of the channel $\mathbf{h}_{je}$ and $\mathbf{e}_{je}$ denotes channel uncertainty. Since we assume the ECSI at jamming nodes are imperfect, we consider DUM, where the error is deterministically bounded,

i.e., $\mathbf{e}_{je} \in \mathcal{R}\{\mathbf{e} : \|\mathbf{e}\| \le \varepsilon\}$, where ε is assumed to be the upper bound on the channel uncertainty.

3 Opportunistic relaying and jamming

3.1 Opportunistic relaying

Traditionally, there are two strategies of opportunistic relay selection: reactive relay selection and proactive relay selection (Fig. 2). Specifically, the reactive strategy first chooses the nodes to form a collection, which can successfully decode signals between the links of *S*-*R*. Then, the best relay is selected from the collection that maximizes the instantaneous channel gains of *R*-*D* link. Conversely, the proactive selection would choose the best relay prior to the source transmission, which depends on instantaneous channel gains of both *S*-*R* and *R*-*D* links. In this paper, we adopt proactive selection strategy in the hybrid FD/HD relay system.

In opportunistic proactive selection, the best relay R^* is selected from a collection of M possible cooperative nodes prior to the source transmission. It requires that each relay should know its own instantaneous channel gains of *S*-*R* and *R*-*D* links. The best relay is chosen to maximize the minimum of the weighted channel gains between *S*-*R* and *R*-*D* links for all the M relays.

$$\begin{aligned} R^* &= \arg\max W_k,\ k = 1, \ldots, M \\ W_k &= \min\{\zeta\, \gamma_{sk}, (1-\zeta)\gamma_{kd}\}, \end{aligned} \tag{6}$$

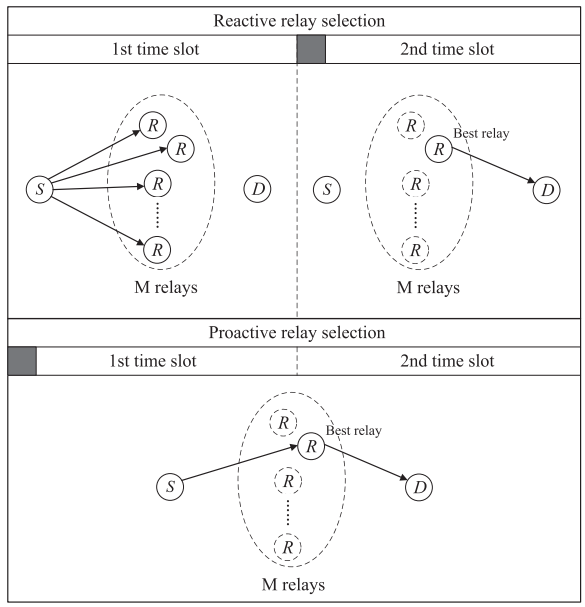

Fig. 2 Relay selection strategy: opportunistic relay selection can be performed proactively before the source transmission or reactively after the source transmission [21]. The grade band indicates when relay selection occurs

where ζ denotes power allocation at the source. In this case, the communication through the best relay would fail to outage while either S-R^* or R^*-D links occur outage.

Since the minimum of two independent exponential distributed variables also follows exponential distribution with the sum of the two parameters, which is shown as follows:

$$W_k \sim E\left(\frac{1}{\zeta\, \lambda_{sk}} + \frac{1}{(1-\zeta)\lambda_{kd}}\right). \tag{7}$$

From (7), we obtain the outage probability of opportunistic proactive relay system as follows:

$$\begin{aligned} P_{\text{Opp-pro}}^{\text{outage}} &= \Pr\left\{W_k < \frac{N_0\left(2^{2R}-1\right)}{P_{\text{tot}}}\right\} \\ &= \Pr\left\{\max W_k < \frac{N_0\left(2^{2R}-1\right)}{P_{\text{tot}}}\right\} \\ &= \prod_{k=1}^{M} \Pr\left\{W_k < \frac{N_0\left(2^{2R}-1\right)}{P_{\text{tot}}}\right\} \\ &= \prod_{k=1}^{M}\left[1-\exp\left\{-\frac{N_0\left(2^{2R}-1\right)}{P_{\text{tot}}}\left(\frac{1}{\zeta\, \lambda_{sk}} + \frac{1}{(1-\zeta)\lambda_{kd}}\right)\right\}\right]. \end{aligned} \tag{8}$$

In proactive selection strategy, selecting a single relay before the source transmission could potentially results in degraded performance. On the other hand, selecting a single relay for information forwarding before source transmission simplifies the receiver design and the overall network operation, since proactive selection is equivalent to routing. Although active selection is more precise because it depends on instantaneous CSI during the communication, it would cost additional spectrum during transmission to select best relay. Conversely, proactive selection can facilitate the receiver operation and system design while all the cooperative nodes stay idle except the opportunistic relay during the transmission. Thus, our opportunistic proactive relay strategy can be viewed as energy efficient.

3.2 Cooperative jamming with robust design

Unlike traditional opportunistic relay selection, except the chosen relay, the remaining nodes would stay idle. In our proposed scheme, the other cooperative nodes operate as jammers to suppress the eavesdropping process.

If the ECSI is known (for instance, the eavesdropper is an active user in the wireless network, it has to feed back its CSI), the source transmits designed CJ beamformer to enhance the security of system, which suppresses or eliminates the information leakage to eavesdropper. During the two time slots, cooperative jamming beamformer depends on *J*-*R* and *J*-*D* links, respectively; thus,

jamming signals would have no influence on the chosen relay and legitimate D.

First, under the assumption that ECSI is available, we apply zero-forcing (ZF) algorithm on the jamming beamforming design, which requires that $\mathbf{h}_{jr}^H\mathbf{f}_r = 0$. At time slot t, we assume that beamformer $\mathbf{f}_r$ is a unit-normalized one-dimensional vector for the cooperative jamming. For the case of perfect CSI, the constraint of ZF algorithm is given by

$$\begin{aligned} &\max_{\mathbf{f}} \ \left|\mathbf{h}_{je}^H\mathbf{f}_r\right| \\ &\text{s.t. } \mathbf{h}_{jr}^H\mathbf{f}_r = 0, \ \left|\mathbf{f}_r^H\mathbf{f}_r\right| = 1. \end{aligned} \tag{9}$$

The solution of (9) is referred as the null-steering beamformer, which is written as

$$\mathbf{f}_r = \frac{(\mathbf{I}_M - \mathbf{H})\mathbf{h}_{je}}{\left\|(\mathbf{I}_M - \mathbf{H})\mathbf{h}_{je}\right\|}, \tag{10}$$

where $\mathbf{H} = \mathbf{h}_{jr}\left(\mathbf{h}_{jr}^H\mathbf{h}_{jr}\right)^{-1}\mathbf{h}_{jr}^H$ is the orthogonal matrix onto the subspace spanned by $\mathbf{h}_{jr}$. On the other hand, the optimal CJ beamformer $\mathbf{f}_d$ at time slot $t+1$ can be obtained with the same way.

However, it is impractical for the relay to obtain perfect ECSI in some cases (channel estimation errors, feedback delay, and quantization errors), and we cannot optimize system performance without knowledge of the eavesdropper's CSI. Thus, we follow the robust approach of [12] to find the optimal CJ beamformer under imperfect CSI. And the optimization problem becomes

$$\begin{aligned} &\max_{\mathbf{Q}_z} \min_{\mathbf{e}} \ \left(\tilde{\mathbf{h}}_{je} + \mathbf{e}_{je}\right)^H\mathbf{Q}_z\left(\tilde{\mathbf{h}}_{je} + \mathbf{e}_{je}\right) \\ &\text{s.t.} \quad \mathbf{h}_{jr}^H\mathbf{Q}_z\mathbf{h}_{jr} = 0, \end{aligned} \tag{11}$$

where $\mathbf{Q}_z = \mathbf{f}_r\mathbf{f}_r^H$ denotes jamming matrix; problem (11) can be transformed to

$$\begin{aligned} &\max_{\mathbf{Q}_z} \ \mathrm{tr}\left[(\mathbf{Q}_z - \boldsymbol{\xi})\tilde{\mathbf{h}}_{jr}\tilde{\mathbf{h}}_{jr}^H\right] - \kappa\varepsilon^2 \\ &\text{s.t.} \quad \begin{bmatrix} \boldsymbol{\xi} & \mathbf{Q}_z \\ \mathbf{Q}_z & \kappa\mathbf{I}_M + \mathbf{Q}_z \end{bmatrix} \succeq 0 \\ &\qquad \mathbf{Q}_z \succeq 0, \quad \kappa \geq 0 \\ &\qquad \boldsymbol{\xi} \succeq \mathbf{Q}_z(\kappa\mathbf{I}_M + \mathbf{Q}_z)^H\mathbf{Q}_z \\ &\qquad \tilde{\mathbf{h}}_{jr}^H\mathbf{Q}_z\tilde{\mathbf{h}}_{jr} = 0. \end{aligned} \tag{12}$$

Proof See Appendix.

Problem (12) is a SDP with a set of linear matrix inequality (LMI) constraints. Note that $\mathbf{e}_{je}$ is not explicit in (12), the optimal robust matrix $\mathbf{Q}_z^*$ is derived from the hidden $\mathbf{e}_{je}$, which can be obtained through the following problem:

$$\begin{aligned} &\min_{\mathbf{e}} \ \left(\tilde{\mathbf{h}}_{je} + \mathbf{e}_{je}\right)^H\mathbf{Q}_z^*\left(\tilde{\mathbf{h}}_{je} + \mathbf{e}_{je}\right) \\ &\text{s.t.} \ \ \left\|\mathbf{e}_{je}\right\| \leq \varepsilon. \end{aligned} \tag{13}$$

Using the Lagrange theorem, the problem (13) can be written as

$$\begin{aligned} L(\mathbf{e}_{je}, \lambda) = \mathbf{e}_{je}^H(\mathbf{Q}_z^* + \lambda\mathbf{I}_M)\mathbf{e}_{je} + 2\mathrm{Re}\left(\mathbf{e}_{je}^H\mathbf{Q}_z^*\tilde{\mathbf{h}}_{je}\right) \\ + \tilde{\mathbf{h}}_{je}^H\mathbf{Q}_z^*\tilde{\mathbf{h}}_{je} - \lambda\varepsilon^2, \end{aligned} \tag{14}$$

where $\lambda \geq 0$. When $\mathbf{e}_{je} = -\tilde{\mathbf{h}}_{je}^H\mathbf{Q}_z^*\left(\mathbf{Q}_z^* + \lambda\mathbf{I}_M\right)^{-1}$, the minimum of $L(\mathbf{e}_{je}, \lambda)$ is achieved. The problem (13) is written as

$$\begin{aligned} &\max_{\lambda} \tilde{\mathbf{h}}_{je}^H\mathbf{Q}_{\mathbf{z}}^*\tilde{\mathbf{h}}_{je} - \lambda\varepsilon^2 - \tilde{\mathbf{h}}_{je}^H\mathbf{Q}_z^*\left(\mathbf{Q}_z^* + \lambda\mathbf{I}_M\right)\mathbf{Q}_z^{*H}\tilde{\mathbf{h}}_{je} \\ &\text{s.t.} \ \ \mathbf{Q}_z^* + \lambda\mathbf{I}_M \succeq 0, \ \ \mathbf{Q}_z^{*H}\tilde{\mathbf{h}}_{je} \in R\left(\mathbf{Q}_z^* + \lambda\mathbf{I}_M\right), \end{aligned} \tag{15}$$

where λ is solution of the following problem:

$$\begin{aligned} &\max_{\lambda \geq 0, \eta} \ \ \eta \\ &\text{s.t.} \ \ \begin{bmatrix} \mathbf{Q}_z^* + \lambda\mathbf{I}_M & \mathbf{Q}_z^{*H}\tilde{\mathbf{h}}_{je} \\ \tilde{\mathbf{h}}_{je}^H\mathbf{Q}_z^* & \tilde{\mathbf{h}}_{je}^H\mathbf{Q}_z^*\tilde{\mathbf{h}}_{je} - \lambda\varepsilon^2 - \eta \end{bmatrix} \succeq 0. \end{aligned} \tag{16}$$

Problem (16) can be efficiently solved by well-studied interior-point algorithm-based package SeDuMi [18]. After $\mathbf{Q}_z^*$ and $\mathbf{e}_{je}$ are obtained, then, we can get the optimal $\mathbf{f}_d$. Meanwhile, the optimal $\mathbf{f}_r$ can be obtained with the same approach.

4 Performance analysis

4.1 Secrecy rate

The hybrid FD/HD technology is adopted at the relay to strengthen the interference on eavesdropper to enhance system secrecy performance. However, the whole transmission is divided into two time slots; the source uses two time slots to transmit a same data packet. Thus, the capacity is computed by a one-half coefficient, which is given by

$$\begin{aligned} C_{sr} &= \frac{1}{2}\log_2\left(1 + \frac{P_S|h_{sr}|^2}{P_R|h_{rr}|^2 + P_J\left|\mathbf{h}_{jr}^H\mathbf{f}_r\right|^2 + \sigma^2}\right) \\ &= \frac{1}{2}\log_2\left(1 + \frac{P_S|h_{sr}|^2}{P_R|h_{rr}|^2 + \sigma^2}\right) \\ &= \frac{1}{2}\log_2\left(1 + \frac{\gamma_{sr}}{\gamma_{rr} + 1}\right). \end{aligned} \tag{17}$$

Since jammers emit cooperative jamming signals in the null space of *J-R* and *J-E* links, respectively, jamming signals have no effect on the relay and destination D. The channel capacity of *R-D* link is given by

$$\begin{aligned} C_{rd} &= \frac{1}{2}\log_2\left(1+\frac{P_R|h_{rd}|^2}{P_J\left|\mathbf{h}_{jd}^H\mathbf{f}_d\right|^2+\sigma^2}\right) \\ &= \frac{1}{2}\log_2\left(1+\frac{P_R|h_{rd}|^2}{\sigma^2}\right) \\ &= \frac{1}{2}\log_2(1+\gamma_{rd}). \end{aligned} \tag{18}$$

Thus, the capacity of main channel is

$$\begin{aligned} C_D &= \min(C_{sr}, C_{rd}) \\ &= \frac{1}{2}\log_2\left(1+\min\left(\frac{\gamma_{sr}}{\gamma_{rr}+1}, \gamma_{rd}\right)\right). \end{aligned} \tag{19}$$

On the other hand, from (1)–(4), the capacity of eavesdropping channel is obtained as

$$\begin{aligned} C_E = \frac{1}{2}\log_2\Bigg(1 &+ \frac{P_S|h_{se}|^2}{P_R|h_{re}|^2+P_J\left|\tilde{\mathbf{h}}_{je}^H\mathbf{f}_r\right|^2+\sigma^2} \\ &+ \frac{P_R|h_{re}|^2}{P_S|h_{se}|^2+P_J\left|\tilde{\mathbf{h}}_{je}^H\mathbf{f}_d\right|^2+\sigma^2}\Bigg) \\ = \frac{1}{2}\log_2&\left(1+\frac{\gamma_{se}}{\gamma_{re}+\gamma_{jer}+1}+\frac{\gamma_{re}}{\gamma_{se}+\gamma_{jed}+1}\right), \end{aligned} \tag{20}$$

where $\gamma_{jer} = P_J\left|\tilde{\mathbf{h}}_{je}^H\mathbf{f}_r\right|^2/\sigma^2, \gamma_{jed} = P_J\left|\tilde{\mathbf{h}}_{je}^H\mathbf{f}_d\right|^2/\sigma^2$.

Thus, the secrecy rate of this hybrid FD/HD system can be written as

$$\begin{aligned} C_{\mathrm{HFD}} = \frac{1}{2}\Bigg[&\log_2\left(1+\min\left(\frac{\gamma_{sr}}{\gamma_{rr}+1}, \gamma_{rd}\right)\right) \\ &-\log_2\left(1+\frac{\gamma_{se}}{\gamma_{re}+\gamma_{jer}+1}+\frac{\gamma_{re}}{\gamma_{se}+\gamma_{jed}+1}\right)\Bigg]^+, \end{aligned} \tag{21}$$

where $[G]^+ = \max(G, 0)$.

4.2 Secrecy outage probability

Secrecy outage refers to the event that the secrecy rate falls below a prescribed transmission rate, equals $P\{C_{\mathrm{HFD}} < R_{th}\}$. In this part, we will analyze the outage performance. At first, letting $X = \min\left(\frac{\gamma_{sr}}{\gamma_{rr}+1}, \gamma_{rd}\right)$, $Y = \frac{\gamma_{se}}{\gamma_{re}+\gamma_{jer}+1} + \frac{\gamma_{re}}{\gamma_{se}+\gamma_{jed}+1}$ and $Z = \frac{1+X}{1+Y}$, the secrecy outage probability of the transmission is written as

$$\begin{aligned} P_{\mathrm{HFD}} &= P(C_{\mathrm{HFD}} < R_{th}) \\ &= P\left(\frac{1+X}{1+Y} < 2^{2R_{th}}\right) \\ &= F_Z\left(2^{2R_{th}}\right) \\ &= \int_0^{\infty}\int_0^{(1+y)2^{2R_{th}}-1} f_X(x)f_Y(y)\mathrm{d}x\mathrm{d}y. \end{aligned} \tag{22}$$

The cumulative distribution function (CDF) of X can be obtained as

$$F_X(x) = 1-\frac{\lambda_{sr}e^{-\frac{\lambda_{sr}+\lambda_{rd}}{\lambda_{sr}\lambda_{rd}}}}{\lambda_{sr}+\lambda_{rr}x}. \tag{23}$$

Thus, the probability density function (PDF) of X is given as

$$f_X(x) = e^{-\frac{\lambda_{sr}+\lambda_{rd}}{\lambda_{sr}\lambda_{rd}}}\left(\frac{\lambda_{sr}+\lambda_{rr}x}{(\lambda_{sr}+\lambda_{rr}x)\lambda_{rd}}+\frac{\lambda_{sr}}{(\lambda_{sr}+\lambda_{rr}x)^2}\right). \tag{24}$$

Since $\gamma_{jer} = P_J|\mathbf{h}_{je}^H\mathbf{f}_r|^2/\sigma^2, \gamma_{jed} = P_J|\mathbf{h}_{je}^H\mathbf{f}_d|^2/\sigma^2$, which follow Erlang distribution of $M-1$ orders with parameter λ_{je}. The PDF and CDF of γ_{jer} and γ_{jed} can be expressed as

$$f(t) = \lambda_{je}\frac{(\lambda_{je}t)^{M-2}}{(M-2)!}e^{-\lambda_{je}t} \quad t\geq 0 \tag{25}$$

$$\begin{aligned} F(t) &= \sum_{k=M-1}^{+\infty}\frac{(\lambda_{je}t)^k}{k!}e^{-\lambda_{je}t} \\ &= 1-\sum_{k=0}^{M-2}\frac{(\lambda_{je}t)^k}{k!}e^{-\lambda_{je}t} \quad t\geq 0. \end{aligned} \tag{26}$$

To simplify the deduce, we assume $\gamma_{re}+\gamma_{jer} \gg 1$, $\gamma_{se}+\gamma_{jed} \gg 1$. Then, Y is written as $Y = \frac{\gamma_{se}}{\gamma_{re}+\gamma_{jer}} + \frac{\gamma_{re}}{\gamma_{se}+\gamma_{jed}}$. Thus, the PDF of Y is obtained as

$$\begin{aligned} f_Y(y) = \frac{\lambda_{se}\lambda_{re}}{2}&\left[\left(\frac{\lambda_{je}}{|\lambda_{je}-\lambda_{re}|}\right)^{M-1}+\left(\frac{\lambda_{je}}{|\lambda_{je}-\lambda_{se}|}\right)^{M-1}\right] \\ &\cdot\sum_{k=M-1}^{\infty}(k+1)\left(\frac{|\lambda_{je}-\lambda_{re}|^k}{(\lambda_{je}+\lambda_{se}z)^{k+2}}+\frac{|\lambda_{je}-\lambda_{se}|^k}{(\lambda_{je}+\lambda_{re}z)^{k+2}}\right). \end{aligned} \tag{27}$$

Substituting (24) and (27) into (22), the secrecy outage probability is given by

$$P_{\mathrm{HFD}} = \int_0^{\infty} f_Y(y)\left[1-\frac{e^{-\frac{(\lambda_{sr}+\lambda_{rd})\left(2^{R_{th}}(y+1)-1\right)}{\lambda_{sr}\lambda_{rd}}}}{\lambda_{rr}\left(2^{R_{th}}(y+1)-1\right)+\lambda_{sr}}\right]\mathrm{d}y. \tag{28}$$

4.3 Comparison with existing work

As shown above, an opportunistic relaying strategy with CJ is proposed in distributed relay networks. In

comparison, cooperative transmission for securing a DF dual-hop network where massive cooperative nodes coexist with a potential single eavesdropper is investigated. In [19], it adopts opportunistic relay strategy and works in HD model. Besides, it assumes instantaneous perfect CSI of the eavesdropper's channel is available.

In [19], a conventional relay selection strategy is proposed during the second phase of the protocol. The existing solutions are summarized as follows:

(1) Conventional selection (CS): This solutions does not take the eavesdropper channels into account, and the relay node is selected based on the instantaneous CSI of the *S-D* links. Although it is an effective solution for non-eavesdropper environments, it cannot support systems with secrecy constraints. The conventional selection is written as

$$R^* = \arg \max_{R_i, i=1,\ldots,M} \left\{ \gamma_{R_i D} \right\}. \tag{29}$$

(2) Optimal selection (OS): The optimal selection scheme takes the relay-eavesdropper links into account and decides the relay node based on the knowledge of both *R-D* and *R-E* links. The optimal selection maximizes the secrecy capacity and is given as

$$R^* = \arg \max_{R_i, i=1,\ldots,M} \left\{ \frac{\gamma_{R_i D}}{\gamma_{R_i E}} \right\}. \tag{30}$$

(3) Suboptimal selection (SS): The suboptimal selection consists of a practical implementation of the optimal selection as it avoids the instantaneous estimate of the *R-E* links by deciding the appropriate relay based on the knowledge of expectation of *R-E* CSI. It is a solution which efficiently fills the gap between optimal and conventional selection with a low implementation/complexity overhead. The suboptimal selection is expressed as

$$R^* = \arg \max_{R_i, i=1,\ldots,M} \left\{ \frac{\gamma_{R_i D}}{E\left[\gamma_{R_i E}\right]} \right\}. \tag{31}$$

In this comparison, we assume opportunistic relay selection strategy in [19] adopts reactive relay selection and OS, which is optimal in the above three strategy. However, due the effect of estimation errors, we assume the instantaneous knowledge of the eavesdropping channel is imperfect.

The difference between our proposed scheme and relay selection scheme in [19] can be described as follows:

- The authors in [19] deal with relay selection in cooperative networks with secrecy constraints. The proposed scheme in [19] enables an opportunistic selection of relay nodes to increase secrecy performance. The selected relay assists the source to deliver confidential information to destination via DF strategy. The proposed selection technique protects the primary destination against interference and eavesdropping. However, the approach is analyzed based on instantaneous perfect knowledge of the eavesdropper channels, which is assumed imperfect.
- Unlike the traditional relay selection strategy in [19], after the best relay is selected, it would not select the optimal jammer to transmit artificial jamming signals. Our proposed scheme selects the best relay to switch between FD and HD operation to deteriorate the receiving SINR at the eavesdropper. At the first time slot, the best relay works in FD protocol to receive useful signals from source and emit artificial jamming signals to interfere eavesdropper. At the second time slot, source transmits artificial jamming signals and relay switch to HD protocol to DF the confidential signals. It can simultaneously avoid the interference at destination from the source and degrade the receiving at eavesdropper.
- Besides, the instantaneous knowledge of all links and average knowledge of the eavesdropper links are considered in [19]. However, in practical, the perfect CSI is usually unknown and has to be estimated. The performance of the designs based on imperfect CSI will be heavily degraded. In our proposed scheme, we propose a worst-case robust design to obtain the CJ beamformer under channel uncertainty to improve secrecy performance, while traditional relay selection scheme [19] is based on estimated ECSI. Our robust algorithm can be viewed as an effective way to eliminate the influence of estimation errors.

5 Numerical analysis

In this section, we present simulation results to illustrate the performance analysis mentioned in Section 4 and compare our proposed scheme with [19]. For convenience, we assume the noise power $\sigma^2 = 1$ and number of cooperative nodes is $M = 5$. To simplify the deducing, we consider Gaussian's noise in the channel estimation and define spherical uncertainty regions with a radius equal to $\varepsilon = g\left\|\tilde{\mathbf{h}}_{je}\right\|, 0 \le g \le 1$. Note that for these uncertainty regions, $\mathbf{h}_{je} = \tilde{\mathbf{h}}_{je} + \mathbf{e}_{je} \ne \mathbf{0}, \forall \mathbf{e}_{je} \in \mathfrak{R}$.

In Fig. 3, we present the secrecy rate comparison against transmit SNR between our proposed scheme

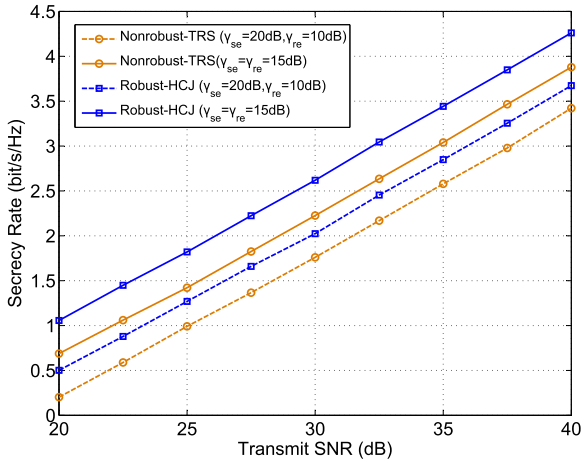

Fig. 3 Secrecy rate versus transmit SNR $\gamma_{sr} = \gamma_{rd}$, the channel error parameter is set $g = 0.3$

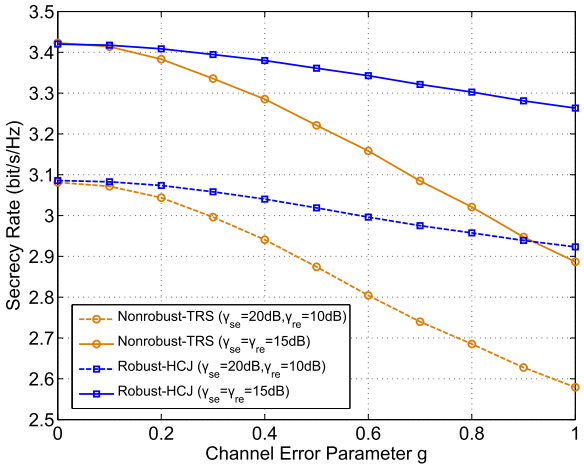

Fig. 5 Secrecy rate versus channel error parameter g, the transmit SNR is fixed as $\gamma_{sr} = \gamma_{rd} = 40$ dB

(HCJ) and traditional relay selection scheme (TRS), where we let $\gamma_{sr} = \gamma_{rd}$ and $\gamma_{rr} = 5$ dB, assuming that the channel error parameter is $g = 0.3$. It can be intuitively shown that, when *S-E* and *R-E* channels have similar gains ($\gamma_{se} = \gamma_{re} = 15$ dB), secrecy rate is higher than the situation when one of the eavesdropping channels is weak ($\gamma_{se} = 20$ dB, $\gamma_{re} = 15$ dB). HCJ scheme far outperforms TRS scheme because of cooperative jamming based on robust design and hybrid FD/HD protocols.

Figure 4 presents the secrecy outage probability of different methods versus secrecy rate threshold, where we let channel error parameter $g = 0.3$, $\gamma_{sr} = \gamma_{rd} = 40$ dB and $\gamma_{rr} = 5$ dB. As seen in the figure, TRS scheme yields higher outage probability than HCJ scheme. When the secrecy rate threshold increases, outage probability of HCJ and TRS schemes would get close since the secrecy rate of two schemes is far less than the threshold rate.

Figure 5 plots the secrecy rate for the legitimate destination as a function of the channel error parameter g, where we let $\gamma_{sr} = \gamma_{rd} = 40$ dB and $\gamma_{rr} = 5$ dB. It can be observed from Fig. 5 that the secrecy rate of the TRS scheme is deeply affected by the channel errors, while the influence on HCJ is much less. Furthermore, when the channel error bound ε increases, the robust HCJ scheme guarantees better secrecy rate, while the non-robust design violates decline quite seriously especially for large g.

In Fig. 6, we present the secrecy rate comparison for different transmit antennas M and assume $\gamma_{sr} = \gamma_{rd} = 40$ dB and $\gamma_{rr} = 5$ dB. Since the increase of cooperative nodes can provide a better relay as the best relay to DF useful signals and it generates stronger interference to

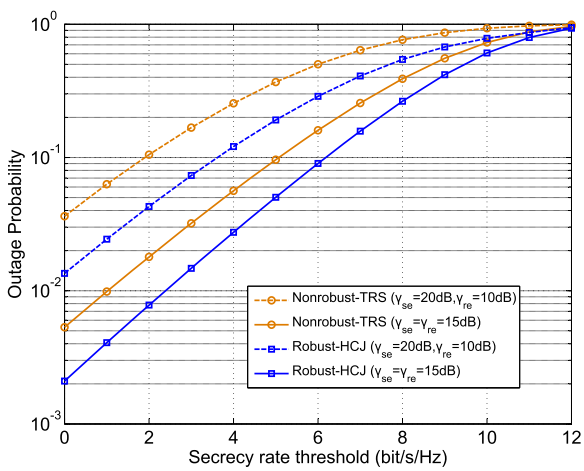

Fig. 4 Secrecy outage probability versus secrecy rate threshold, the channel error parameter is set $g = 0.3$

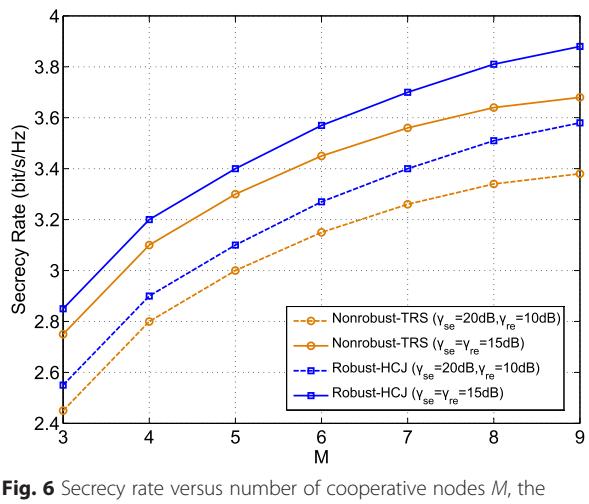

Fig. 6 Secrecy rate versus number of cooperative nodes M, the transmit SNR is fixed as $\gamma_{sr} = \gamma_{rd} = 40$ dB and the channel error parameter is set $g = 0.3$

confuse eavesdropper, the secrecy rate of the two schemes gets better while the number of nodes increases. Not surprisingly, the secrecy rate performance of hybrid scheme is better than the traditional one under the same condition. Moreover, we observe that the secrecy rate achieved by TRS scheme increased slowly compared with our proposed scheme, while the cooperative nodes increase.

Finally, we compare the computational complexity of our proposed scheme and TRS scheme. For the sake of notational simplicity, we evaluate how the computational complexity of both schemes scale with the number of nodes M. In our proposed scheme, the complexity of the opportunistic relay selection is $O(M)$. The complexity order of obtain $\mathbf{f}_r$ and $\mathbf{f}_d$ through solving the SDP problem (11)–(16) is $O(M^5)$ [20]. Thus, the computational complexity of our proposed scheme is $O(M^5)$. For the TRS scheme, the major computation task is how to obtain best relay R^* based on imperfect CSI (30), which has complexity order of $O(M)$. Thus, the computational complexity of traditional CJ scheme is $O(M)$. Based on the analysis above, we find that our proposed scheme has a higher complexity than traditional one. However, the proposed scheme outperforms TRS scheme both on secrecy rate and secrecy outage probability.

6 Conclusions

In this paper, we addressed a hybrid opportunistic relaying and jamming strategy in multi-relay system under imperfect channel estimation. A proactive opportunistic relay selection is proposed, in which the criteria are based on the channel conditions. To enhance secrecy performance of cooperative jamming under channel uncertainty, we transform the optimization problem into a SDP with some LMI constraints, which is solved by the interior point approach. Furthermore, we derive the secrecy rate and deduce the outage probability. Since our proposed scheme takes advantages of cooperative jamming with robust design and increases interference on eavesdropper through hybrid FD/HD protocols, simulation results demonstrated that the proposed scheme leads to significant improvement than TRS strategy in distributed relay system.

Appendix

The problem (11) can be transformed to

$$\begin{aligned} &\max_{\mathbf{Q}_z,u} \ u \\ &\text{s.t.} \quad \left(\tilde{\mathbf{h}}_{je}+\mathbf{e}_{je}\right)^H \mathbf{Q}_z \left(\tilde{\mathbf{h}}_{je}+\mathbf{e}_{je}\right) \geq u \\ &\qquad \mathbf{e}_{je}^H \mathbf{e}_{je} \leq \varepsilon^2. \end{aligned} \tag{32}$$

The constraints of (32) can be rewritten as

$$\begin{aligned} \text{s.t.} \quad & \mathbf{e}_{je}^H \mathbf{Q}_z \mathbf{e}_{je} + 2\mathrm{Re}\left(\tilde{\mathbf{h}}_{je}^H \mathbf{Q}_z \tilde{\mathbf{h}}_{je}\right) + \tilde{\mathbf{h}}_{je}^H \mathbf{Q}_z \tilde{\mathbf{h}}_{je} - u \geq 0 \\ & -\mathbf{e}_{je}^H \mathbf{e}_{je} + \varepsilon^2 \geq 0. \end{aligned} \tag{33}$$

According to the S-procedure, there exists an $\mathbf{e}_{je}$ satisfying above inequalities only if there exists a $\kappa \geq 0$ such that

$$\begin{bmatrix} \kappa \mathbf{I}_M + \mathbf{Q}_z & \mathbf{Q}_z \tilde{\mathbf{h}}_{je} \\ \tilde{\mathbf{h}}_{je}^H \mathbf{Q}_z & \tilde{\mathbf{h}}_{je}^H \mathbf{Q}_z \tilde{\mathbf{h}}_{je} - \kappa\varepsilon^2 - u \end{bmatrix} \succeq 0. \tag{34}$$

Applying the Schur complement, (34) can be expressed as

$$-\kappa\varepsilon^2 + \tilde{\mathbf{h}}_{je}^H \mathbf{Q}_z \tilde{\mathbf{h}}_{je} - \tilde{\mathbf{h}}_{je}^H \mathbf{Q}_z (\kappa \mathbf{I}_M + \mathbf{Q}_z)^\dagger \mathbf{Q}_z \tilde{\mathbf{h}}_{je} \geq u \tag{35}$$

Then, the problem (35) becomes

$$\max_{\mathbf{Q}_z, \kappa \geq 0} \ -\kappa\varepsilon^2 + \tilde{\mathbf{h}}_{je}^H \mathbf{Q}_z \tilde{\mathbf{h}}_{je} - \tilde{\mathbf{h}}_{je}^H \mathbf{Q}_z (\kappa \mathbf{I}_M + \mathbf{Q}_z)^\dagger \mathbf{Q}_z \tilde{\mathbf{h}}_{je}, \tag{36}$$

which equals to

$$\begin{aligned} &\max_{\mathbf{Q}_z, \kappa \geq 0, \boldsymbol{\xi}} \ -\kappa\varepsilon^2 + \tilde{\mathbf{h}}_{je}^H \mathbf{Q}_z \tilde{\mathbf{h}}_{je} - \tilde{\mathbf{h}}_{je}^H \boldsymbol{\xi} \tilde{\mathbf{h}}_{je} \\ &\text{s.t.} \quad \mathbf{Q}_z (\kappa \mathbf{I}_M + \mathbf{Q}_z)^\dagger \mathbf{Q}_z \preceq \boldsymbol{\xi}. \end{aligned} \tag{37}$$

Therefore, we use the Schur complement to transform above constraints into LMI and the problem (11) can be written

$$\begin{aligned} &\max_{\mathbf{Q}_z} \ \mathrm{tr}\left[(\mathbf{Q}_z - \boldsymbol{\xi}) \tilde{\mathbf{h}}_{jd} \tilde{\mathbf{h}}_{jd}^H\right] - \kappa\varepsilon^2 \\ &\text{s.t.} \quad \begin{bmatrix} \boldsymbol{\xi} & \mathbf{Q}_z \\ \mathbf{Q}_z & \kappa \mathbf{I}_M + \mathbf{Q}_z \end{bmatrix} \succeq 0 \\ &\qquad \mathbf{Q}_z \succeq 0, \quad \kappa \geq 0 \\ &\qquad \boldsymbol{\xi} \succeq \mathbf{Q}_z (\kappa \mathbf{I}_M + \mathbf{Q}_z)^H \mathbf{Q}_z \\ &\qquad \tilde{\mathbf{h}}_{jd}^H \mathbf{Q}_z \tilde{\mathbf{h}}_{jd} = 0, \end{aligned} \tag{38}$$

and the proof is completed.

Competing interests
The authors declare that they have no competing interests.

Acknowledgements
This work is supported by the National Natural Science Foundation of China (No.61371122 and No. 61471393) and the China Postdoctoral Science Foundation under a Special Financial Grant No. 2013T60912.

Received: 1 September 2015 Accepted: 24 April 2016
Published online: 10 May 2016

References

1. AD Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)
2. GF Pivaro, G Fraidenraich, CF Dias, Outage probability for MIMO relay channel. IEEE Trans. Commun. **62**(11), 3791–3800 (2014)
3. C Chien, H Su, H Li, Joint beamforming and power allocation for MIMO relay broadcast channel with individual sinr constraints. IEEE Trans. Veh. Technol. **63**(4), 1660–1677 (2014)

4. C Wang, H Wang, X Xia, Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks. IEEE Trans. Inf. Theory **14**(2), 589–605 (2015)
5. E Tekin, A Yener, The general Gaussian multiple access and two-way wire-tap channels: achievable rates and cooperative jamming. IEEE Trans. Inf. Theory **54**(6), 2735–2751 (2008)
6. G Zheng, LC Choo, KK Wong, Optimal cooperative jamming to enhance physical layer security using relays. IEEE Trans. Signal Process. **59**(3), 1317–1322 (2011)
7. JC Chen, RQ Zhang, LY Song, Z Han, BL Jiao, Joint relay and jammer selection for secure two-way relay networks. IEEE Trans. Inf. Fore. Theory **7**(1), 310–320 (2012)
8. G Zheng, I Krikidis, J Li, Joint relay and jammer selection for secure two-way relay networks. IEEE Trans. Signal Process. **61**(20), 4962–4974 (2013)
9. F Zhu, F Gao, M Yao, H Zou, Joint information- and jamming-beamforming for physical layer security with full duplex base station. IEEE Commun. Lett. **62**(24), 6391–6401 (2014)
10. T Riihonen, S Werner, R Wichman, Hybrid full-duplex/half-duplex relaying with transmit power adaptation. IEEE Trans. Wireless Commun. **10**(9), 3074–3085 (2011)
11. J Lee, TQS Quek, Hybrid full-/half-duplex system analysis in heterogeneous wireless networks. IEEE Trans. Wireless Commun. **14**(5), 2883–2895 (2015)
12. J Huang, AL Swindlehurst, Robust secure transmission in MISO channels based on worst-case optimization. IEEE Trans. Signal Process. **60**(3), 1696–1707 (2012)
13. C Wang, H Wang, Joint relay selection and artificial jamming power allocation for secure DF relay networks. IEEE International Conference on Communication (ICC2014), 819–824 (2015)
14. M Bengtsson, B Ottersten, Optimal and suboptimal transmit beamforming, in *Handbook of Antennas in Wireless Communications, Florida, U. S*, 2001
15. M Bloch, J Barros, MRD Rodrigues, SW McLaughlin, Wireless information-theoretic security. IEEE Trans. Inf. Theory **54**(6), 2515–2534 (2008)
16. VNQ Bao, NL Trung, M Debbah, Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers. IEEE Trans. Wireless Commun. **12**(12), 6076–6085 (2013)
17. Y Zou, X Wang, W Shen, Optimal relay selection for physical-layer security in cooperative wireless networks. IEEE J. Select. Areas Commun. **31**(10), 2099–2111 (2013)
18. J Sturm, Using sedumi 1.02: a Matlab toolbox for optimization over symmetric cones. Opt. Meth. Software **11–12**, 625–653 (1999)
19. I Krikidis, JS Thompson, Relay selection for secure cooperative networks with jamming. IEEE Trans. Wireless Commun. **8**(10), 5003–5011 (2009)
20. Y Nesterov, A Nemirovsky, Interior-point polynomial methods in convex programming. Studies in Applied Mathematics **13**, 8–30 (1994)
21. A Bletsas, H Shin, MZ Win, Cooperative communications with outage-optimal opportunistic relaying. IEEE Trans. Wireless Commun. **6**(9), 3450–3460 (2007)