Chen G, Gong Y, Xiao P, Chambers JA.

Physical layer network security in the full duplex relay system.

IEEE Transactions on Information Forensics and Security **2015, 10(3), 574-583.**

Copyright:

© 2015 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

DOI link to article:

http://dx.doi.org/10.1109/TIFS.2015.2390136

Date deposited:

08/02/2017

Newcastle University ePrints - eprint.ncl.ac.uk

Physical Layer Network Security in the Full-Duplex Relay System

Gaojie Chen, *Member, IEEE*, Yu Gong, *Member, IEEE*, Pei Xiao, *Senior Member, IEEE*
and Jonathon Chambers, *Fellow, IEEE*

***Abstract*—This paper investigates the secrecy performance of full duplex relay networks. The resulting analysis shows that full duplex relay networks have better secrecy performance than half duplex relay networks, if the self-interference can be well suppressed. We also propose a full duplex jamming relay network, in which the relay node transmits jamming signals while receiving the data from the source. While the full duplex jamming scheme has the same data rate as the half duplex scheme, the secrecy performance can be significantly improved, making it an attractive scheme when the network secrecy is a primary concern. A mathematic model is developed to analyze secrecy outage probabilities for the half duplex, full duplex and full duplex jamming schemes, and simulation results are also presented to verify the analysis.**

***Index Terms*—Physical layer secrecy, cooperative relay networks, full duplex relay, secrecy outage probability**

I. INTRODUCTION

Unlike a traditional cryptographic system [1], physical layer security is based on Shannon theory using channel coding (rather than encryption) to achieve secure transmission [2]–[7]. Due to the broadcast nature of wireless communications, both the intended receiver and eavesdropper may receive data from the source. But if the capacity of the intended data transmission channel is higher than that of the eavesdropping channel, the data can be transmitted at a rate close to the intended channel capacity so that only the intended receiver (not the eavesdropper) can successfully decode the data. This is the principle of physical layer security, where the level of security is quantified by the secrecy capacity which is the capacity difference between the intended data transmission and eavesdropping channels.

It is interesting to notice that both cooperative relay and physical layer security networks relay on wireless broadcasting. This implies that the popular cooperative networks, which have been well investigated to improve transmission capacity, also provide an effective way to improve the secrecy capacity [8], [9]. A typical relay network with an eavesdropper is shown in Fig. 1, where there is one source node S, one relay node R, one destination node D and one eavesdropper node E.

The purpose of physical layer security in the cooperative network is to prevent the eavesdropper from decoding the data transmitted from S or R. This can be achieved by injecting jamming signals into the network with the assumption that the jamming power at the eavesdropper is higher than that at the intended destination (e.g. [10]). The jamming signal must be used with care as it may also deteriorate the intended data transmission. This can be seen for example in [11] where beamforming is used at the destination to reduce the negative effect of the jamming signals at the intended relay node.

Current cooperative networks usually employ half duplex relays (HDR-s) because of easy implementation. But this is at the price of 50% loss in spectral efficiency as two time slots are required to transmit one data packet. Full duplex transmission, which was previously considered impractical due to the associated self-interference, has attracted much attention recently due to the progress in self-interference cancelation techniques ([12], [13]). For example, in [14], multiple antenna were used to suppress the self-interference; in [15], [16], a joint analog and digital cancellation technique was proposed to mitigate the self-interference to the noise floor; in [17], two analog/RF designs were proposed which can avoid using bulky components and/or antenna structures in most existing self-interference approaches. Of particular interest is when the self-interference is significantly suppressed, the impact of full duplex transmission on physical layer security. In [18] and [19], the receiver operates in full duplex mode for better secrecy because it can simultaneously receive the data from the source and send a jamming signal to the eavesdropper. Alternatively, in [20], it is the eavesdropper that is equipped with the full duplex technology, so that the eavesdropper can minimize the secrecy by receiving the data from the source and transmitting jamming signals to the intended receiver at the same time. These approaches consider the secrecy performance of a point-to-point full duplex system, and little work has been done for the full duplex relay network.

In this paper, we investigate the secrecy performance of a full duplex relay network. In the full duplex network, the eavesdropper simultaneously receives signals from the source and relay which interfere with each other, making it harder for the eavesdropper to decode the data. This decreases the eavesdropping capacity, and then improves the secrecy performance. Moreover, because full duplex does not suffer from 50% loss in data rate, there is no $1/2$ factor in both data transmission and eavesdropping capacities, which also leads to better secrecy performance. This will be investigated in detail later in this paper. In order to further increase the

Copyright (c) 2013 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org

G. J. Chen and P. Xiao are with the Institute for Communication Systems (ICS), home of the 5G Innovation Centre, University of Surrey, Guildford, Surrey, UK, Emails: {`gaojie.chen and p.xiao`}`@surrey.ac.uk`.

Y. Gong and J. A. Chambers are with the Advanced Signal Processing Group, School of Electronic, Electrical and Systems Engineering, Loughborough University, Loughborough, Leicestershire, UK, Emails: {`y.gong and j.a.chambers`}`@lboro.ac.uk`.

secrecy performance, we propose a full duplex jamming relay scheme, in which the relay simultaneously receives data from the source and sends jamming signals to the eavesdroppers. The proposed full duplex jamming scheme has good secrecy outage performance, though its data rate is the same as that for the half duplex scheme, making it an attractive scheme when the network secrecy is a primary concern. The contributions of the paper are listed as follows:

- We obtain a closed-form expression of the secrecy outage probability in a half duplex relay network, for the case that the eavesdropper can intercept the data from both the source and destination. To the best of our knowledge, this is the first time this has been done. In [9], the secrecy performance of a relay selection secrecy system is analyzed, but the resulting secrecy outage probability is actually a lower bound. This point will be further explained in Section II.
- We derive the maximum and (approximate) minimum secrecy outage probability of a full duplex relay network, which well approximates the true secrecy outage probability. We also quantitatively compare the secrecy performance of the half duplex and full duplex relay networks.
- We propose a full duplex jamming network and analyze its secrecy outage probability.

The remainder of the paper is organized as follows: Section II- IV analyze the secrecy performance for the half duplex, full duplex and full duplex jamming relay networks respectively; Section V gives numerical simulations to verify the analysis; finally, Section VI summarizes the paper.

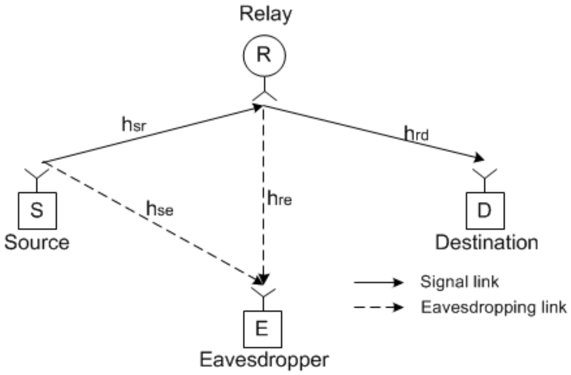


Fig. 1. The secrecy relay network with an eavesdropper.

II. HALF DUPLEX SECRECY RELAY NETWORK

In this section, we derive the secrecy outage probability of the half duplex secrecy network, which is used as a baseline to compare with a full duplex scheme and the newly proposed full duplex jamming scheme. The system model is shown in Fig. 1, where all nodes are equipped with a single antenna, and the eavesdropper can intercept the data from both the source S and relay R, and the relay applies the decode-and-forward (DF) protocol. The channel coefficients for $S \to R$, $R \to D$, $S \to E$ and $R \to E$ are denoted as h_{sr}, h_{rd}, h_{se} and h_{re}, respectively. We assume that all channels experience block Rayleigh fading and that the channels remain constant over one block but vary independently from one block to another. The corresponding channel gains, obtained as $\gamma_j = |h_j|^2$ ($j \in \{sr, rd, se, re\}$), are independently exponentially distributed with mean of λ_j ($j \in \{sr, rd, se, re\}$) respectively. The noise at nodes R, D and E are denoted as $n_r(t)$, $n_d(t)$ and $n_e(t)$ with variances of σ_j^2 ($j \in \{r, d, e\}$) respectively. The transmission powers at S and R are E_s and E_r, respectively.

We particularly note that, in this paper, we assume S and D are well separated so that there is no effective direct $S \to D$ transmission link as in ([9], [21]–[23]). On the other hand, if the direct $S \to D$ link exists, the destination D receives signals from both the source S and relay R which need to be separated. In the half-duplex scheme, this can be easily achieved by letting S and R transmit at odd and even time slots respectively. In the full duplex scheme, other approaches are necessary for the signal separation. For example, multiple antennas can be used to separate signals in the spatial domain and CDMA can be used to separate signals with different spreading codes for S and D respectively. Alternatively, network-coding based approaches may be applied. To be specific, we assume initially at time slot $t = 1$, S transmits data $s(1)$ to both R and D, and R has no data to transmit yet. At time $t = 2$, S and R transmit data $s(2)$ and $s(1)$ to D respectively. Then at the destination D, $s(1)$ and $s(2)$ can be separated by subtracting the previously received $s(1)$ (at time $t = 1$) from the current received signal (at time $t = 2$). This process can be continued until all data are transmitted. This is similar to the two-path transmission in [24], [25]. The detail of this issue is beyond the scope of this paper and will be left as an interesting topic for future study.

A. Secrecy capacity

We assume at time t, the source transmits $x_s(t)$ to the relay R, and the received signal at R is given by

$$y_r(t) = \sqrt{E_s} h_{sr}(t) x_s(t) + n_r(t), \tag{1}$$

and the eavesdropper E intercepts the signal from S as

$$y_e(t) = \sqrt{E_s} h_{se}(t) x_s(t) + n_e(t). \tag{2}$$

At time $(t+1)$, if the relay R successfully decodes $x_s(t)$, it forwards $x_s(t)$ to D. The received signals at D and E are given by

$$\begin{aligned} y_d(t+1) &= \sqrt{E_r} h_{rd}(t+1) x_s(t) + n_d(t+1), \\ y_e(t+1) &= \sqrt{E_r} h_{re}(t+1) x_s(t) + n_e(t+1), \end{aligned} \tag{3}$$

respectively. For notational convenience, the time index t is ignored below unless necessary.

The secrecy capacity is defined as (see [4]),

$$C_s = [C_t - C_e]^+, \tag{4}$$

where $[x]^+ = \max(x, 0)$, C_t and C_e are the capacities for data transmission and eavesdropping respectively. Because the relay applies DF, we have

$$C_t = \min(C_{sr}, C_{rd}), \tag{5}$$

where C_{sr} and C_{rd} are the channel capacities for $S \to R$ and $R \to D$ respectively. In order to concentrate on the secrecy performance of the network, we assume the channel SNR is high enough so that the relay and destination nodes can always decode the data. Then we have

$$\begin{aligned} C_{sr} &= \frac{1}{2}\log_2(1+\frac{E_s|h_{sr}|^2}{\sigma_r^2}) \simeq \frac{1}{2}\log_2(\gamma_{sr}), \\ C_{rd} &= \frac{1}{2}\log_2(1+\frac{E_r|h_{rd}|^2}{\sigma_d^2}) \simeq \frac{1}{2}\log_2(\gamma_{rd}), \end{aligned} \tag{6}$$

where we assume without losing generality that $E_r = E_s = 1$ and $\sigma_r^2 = \sigma_d^2 = 1$, so that the channel gains γ_{sr} and γ_{rd} become the channel SNRs for $S \to R$ and $R \to D$ respectively[1]. Similar assumption is used in the rest of the paper.

Substituting (6) into (5) gives

$$C_t = \min\left\{\frac{1}{2}\log_2(\gamma_{sr}), \frac{1}{2}\log_2(\gamma_{rd})\right\}. \tag{7}$$

On the other hand, because the eavesdropper receives the data $x_s(t)$ twice, from S and R at time t and $(t+1)$ respectively, the eavesdropping capacity is obtained as

$$C_e = \frac{1}{2}\log_2\left(1+\frac{E_s|h_{se}|^2+E_r|h_{re}|^2}{\sigma_r^2}\right) \simeq \frac{1}{2}\log_2(\gamma_{se}+\gamma_{re}), \tag{8}$$

where γ_{se} and γ_{re} are the channel SNRs for $S \to E$ and $R \to E$ respectively. Note that the "1/2" factor in (7) and (8) are due to the half duplex transmission at the relay node.

Substituting (7) and (8) into (4) gives the secrecy capacity of the half duplex scheme as

$$\begin{aligned} C_{HDR} &= \left[\frac{1}{2}\log_2(\min(\gamma_{sr},\gamma_{rd})) - \frac{1}{2}\log_2(\gamma_{se}+\gamma_{re})\right]^+ \\ &= \left[\frac{1}{2}\log_2\left(\frac{\min(\gamma_{sr},\gamma_{rd})}{\gamma_{se}+\gamma_{re}}\right)\right]^+. \end{aligned} \tag{9}$$

B. Secrecy outage probability

From (9), the secrecy outage probability for the half duplex relay scheme is given by

$$P_{HDR} = P(C_{HDR} < R_s) = P\left(\frac{\min(\gamma_{sr},\gamma_{rd})}{\gamma_{se}+\gamma_{re}} < 2^{2R_s}\right), \tag{10}$$

where R_s is the target secrecy rate. Note that, because $R_s \geq 0$, we have $P([x]^+ < R_s) = P(x < R_s)$ so that the operator $[.]^+$ can be removed in (10).

Letting $X = \min(\gamma_{sr},\gamma_{rd})$, $Y = \lambda_{se}+\lambda_{re}$ and $Z = X/Y$, (10) becomes

$$P_{HDR} = F_Z(2^{2R_s}) = \int_0^\infty F_X(2^{2R_s}y) f_Y(y)dy, \tag{11}$$

where $F(.)$ and $f(.)$ are the cumulative density function (CDF) and probability-density-function (PDF) respectively.

The CDF of X can be obtained as

$$F_X(x) = 1 - e^{-\frac{x(\lambda_{sr}+\lambda_{rd})}{\lambda_{sr}\lambda_{rd}}}, \tag{12}$$

and the PDF of Y is given by

$$f_Y(y) = \begin{cases} \frac{ye^{-y/\lambda_{se}}}{\lambda_{se}^2}, & \lambda_{se} = \lambda_{re} \\ \frac{e^{y/\lambda_{re}} - e^{-y/\lambda_{se}}}{\lambda_{se}-\lambda_{re}} e^{-\frac{y(\lambda_{se}+\lambda_{re})}{\lambda_{se}\lambda_{re}}}, & \lambda_{se} \neq \lambda_{re} \end{cases} \tag{13}$$

Substituting (12) and (13) into (11) gives the secrecy outage probability of the half duplex secrecy network as (14) in the top of the next page.

Before we leave this section, it is interesting to point out that, while the eavesdropper listens to S and R at time t and $(t+1)$ for the same data $x_s(t)$ respectively, it can be easily assumed that the secrecy outage probability is the probability that eavesdropper can decode $x_s(t)$ from either S or D. This is however not correct as the eavesdropper will combine the data from S and D together before it decodes the data. Similar mistake unfortunately still appears in some recent publications (e.g. in [26] though it is for the secrecy outage in a relay selection cognitive radio network). Alternatively in [9], the eavesdropping capacity of a relay selection secrecy system is obtained by taking the maximum gain of the $S \to E$ and $R \to E$ channels, which is smaller than the true eavesdropping capacity. And thus the resulting secrecy outage probability is in fact a lower bound.

III. FULL DUPLEX SECRECY RELAY NETWORK

A. System model

The system model of a full duplex secrecy relay network can also be shown in Fig. 1, except that the relay is now equipped with two antennas for receiving and transmission respectively. We assume that, at time slot t, the source S transmits $x_s(t)$ to the relay R. The relay R receives data from S with its receiving antenna, and at the same time uses its transmission antenna to transmit the previously decoded signal $x_s(t-1)$ to the destination. Because R receives and transmits simultaneously, when R is receiving, it is interfered by its own transmission which is called self-interference. Then the received signal at R is given by

$$y_r(t) = \sqrt{E_s}h_{sr}(t)x_s(t) + \sqrt{E_r}h_{rr}(t)x_s(t-1) + n_r(t), \tag{15}$$

where $h_{rr}(t)$ is the residual self-interference after the self-interference cancellation. It is often assumed that the self-interference can be significantly suppressed[2] (e.g. [12], [27]) so that $h_{rr}(t)$ can be regarded as an independent Rayleigh distributed variable (e.g. [28], [29]). The received signal at the destination D is similar to that in the half duplex scheme which is given by

$$y_d(t) = \sqrt{E_r}h_{rd}(t)x_s(t-1) + n_d(t). \tag{16}$$

Because now the source and relay transmit simultaneously,

---

[1] The transmission and noise powers can always be normalized to unity by "absorbing" into the corresponding channel SNR.

[2] Self-interference cancellation algorithms are beyond the scope of this paper.

$$P_{HDR} = \frac{2^{2R_s}\lambda_{se}\lambda_{re}(\lambda_{sr}+\lambda_{rd})^2 + (\lambda_{rd}^2\lambda_{sr}+\lambda_{rd}\lambda_{sr}^2)(\lambda_{re}+\lambda_{se})}{2^{4R_s}\lambda_{se}\lambda_{re}(\lambda_{sr}+\lambda_{rd})^2 + 2^{2R_s}(\lambda_{rd}^2\lambda_{sr}+\lambda_{rd}\lambda_{sr}^2)(\lambda_{re}+\lambda_{se}) + \lambda_{sr}^2\lambda_{rd}^2}. \tag{14}$$

---

at time t, the received signal at the eavesdropper is given by

$$y_e(t) = \sqrt{E_s}h_{se}(t)x_s(t) + \sqrt{E_r}h_{re}(t)x_s(t-1) + n_e(t). \tag{17}$$

It is interesting to observe that (17) is similar to the intersymbol interference (ISI) channel, and thus the eavesdropping capacity is expected to be lower than that in the half duplex scheme. Assuming there are B data packets per block, and stacking the received signals at the eavesdropper for all B data in one block, (17) can be expressed in a matrix/vector form as

$$\mathbf{y}_e = \mathbf{H}\mathbf{x}_s + \mathbf{n}_e, \tag{18}$$

where $\mathbf{y}_e = (y_e[B{+}1], \cdots, y_e[1])^{\mathrm{T}}$, $\mathbf{x}_s = (x_s[B], \cdots, x_s[1])^{\mathrm{T}}$ and $\mathbf{n}_e = (n_e[B{+}1], \cdots, n_e[1])^{\mathrm{T}}$, and $\mathbf{H}$ is the eavesdropping channel matrix which is given by

$$\mathbf{H} = \begin{bmatrix} \sqrt{E_r}h_{re} & & & & \\ \sqrt{E_s}h_{se} & \sqrt{E_r}h_{re} & & & \\ & \sqrt{E_s}h_{se} & \sqrt{E_r}h_{re} & & \\ & & \ddots & & \\ & & & \sqrt{E_s}h_{se} & \sqrt{E_r}h_{re} \\ & & & & \sqrt{E_s}h_{se} \end{bmatrix}_{(B+1)\times B}, \tag{19}$$

and $(.)^{\mathrm{T}}$ denotes the transpose operator.

B. Secrecy capacity

From (15), the channel capacity for $S \to R$ is given by

$$C_{sr} = \log_2\left(1 + \frac{E_s|h_{sr}|^2}{E_r|h_{rr}|^2 + \sigma_r^2}\right) \simeq \log_2\left(\frac{\gamma_{sr}}{\gamma_{rr}+1}\right), \tag{20}$$

where the approximation holds over the high SNR range, and similar to (6) the transmission and noise powers are normalized to unity, so that γ_{rr} and γ_{rr} are the channel gains for the $S \to R$ and self-interference channels, respectively. Because we assume self-interference can be significantly suppressed, when the SNR is sufficiently high, we have $\gamma_{sr} \gg (\gamma_{rr}+1)$ so that the approximation in (20) holds.

The channel capacity for $R \to D$ is similar to that in the half duplex scheme (as is shown in (6)) but without the "1/2" factor due to the full duplex transmission. Then from (5), the transmission capacity of the full duplex scheme is given by

$$C_t = \log_2\left(\min\left\{\frac{\gamma_{sr}}{\gamma_{rr}+1}, \gamma_{rd}\right\}\right). \tag{21}$$

On the other hand, from (18), the eavesdropping capacity can be obtained as

$$C_e = \frac{1}{B}\log_2 \det\{\mathbf{I} + \mathbf{H}^{\mathrm{H}}\mathbf{H}\}, \tag{22}$$

where $\det(.)$ and $(.)^H$ denote the matrix determinant and Hermitian transpose respectively.

Substituting (21) and (22) into (4) gives the secrecy capacity for the full duplex network

$$C_{FDR} = \left[\log_2\left(\min\left(\frac{\gamma_{sr}}{\gamma_{rr}+1}, \gamma_{rd}\right)\right) - \log_2\left((\det\{\mathbf{I}+\mathbf{H}^{\mathrm{H}}\mathbf{H}\})^{\frac{1}{B}}\right)\right]^+. \tag{23}$$

C. Eavesdropping capacity

Below we further investigate the eavesdropping capacity C_e. From the eigen-decomposition of $\mathbf{H}^{\mathrm{H}}\mathbf{H}$, (22) can be reformed as

$$C_e = \frac{1}{B}\log_2\prod_{b=1}^{B}(1+\theta_b), \tag{24}$$

where θ_b is the bth eigenvalue of $\mathbf{H}^{\mathrm{H}}\mathbf{H}$. Because $\mathbf{H}$ is a Toeplitz matrix, θ_b is given by (see [30])

$$\theta_b = (|h_{se}|^2 + |h_{re}|^2) + 2|h_{se}^* h_{re}|\cos\frac{b\pi}{B+1}, \quad b \in \{1, 2, ..., B\}. \tag{25}$$

Substituting (25) into (24) gives

$$C_e = \log_2\left(1 + |h_{se}|^2 + |h_{re}|^2\right) + \frac{1}{B}\sum_{b=1}^{B}\log_2\left(1 + \frac{2|h_{se}^* h_{re}|\cos\frac{b\pi}{B+1}}{1 + |h_{se}|^2 + |h_{re}|^2}\right). \tag{26}$$

Because $2|h_{se}^* h_{re}|\cos\frac{b\pi}{B+1} \le 2|h_{se}^* h_{re}| \le |h_{se}|^2 + |h_{re}|^2 < |h_{se}|^2 + |h_{re}|^2 + 1$, we have

$$\left|\frac{2|h_{se}^* h_{re}|\cos\frac{b\pi}{B+1}}{|h_{se}|^2 + |h_{re}|^2 + 1}\right| \le 1. \tag{27}$$

For simplicity, we let $u = (2|h_{se}^* h_{re}|\cos\frac{b\pi}{B+1})/(|h_{se}|^2 + |h_{re}|^2 + 1)$. Then using a Taylor expansion, we have

$$\begin{aligned} &\frac{1}{B}\sum_{b=1}^{B}\log_2(1+u) \\ &= \frac{1}{B}\sum_{b=1}^{B}\frac{1}{\ln 2}\left(u - \frac{1}{2}u^2 + \frac{1}{3}u^3 - \frac{1}{4}u^4 + \cdots\right) \\ &= \frac{1}{\ln 2}\cdot\frac{1}{B}\left(\sum_{b=1}^{B}u - \sum_{b=1}^{B}\frac{1}{2}u^2 + \sum_{b=1}^{B}\frac{1}{3}u^3 - \sum_{b=1}^{B}\frac{1}{4}u^4 + \cdots\right). \end{aligned} \tag{28}$$

It is interesting to note that $\sum_{b=1}^{B} u^k = 0$ if k is odd. Thus the odd exponents in (28) are all zeros, so that we have

$$\begin{aligned} &\frac{1}{B}\sum_{b=1}^{B}\log_2(1+u) \\ &= -\frac{1}{\ln 2}\cdot\frac{1}{B}\left(\sum_{b=1}^{B}\frac{1}{2}u^2 + \sum_{b=1}^{B}\frac{1}{4}u^4 + \cdots\right) \le 0, \end{aligned} \tag{29}$$

where the equality holds for $|h_{se}| = 0$ or $|h_{re}| = 0$. Letting $\Delta_{C_e} = -1/B\sum_{b=1}^{B}\log_2(1+u)$, and from (26) and (29), we have

$$\begin{aligned} C_e &= \log_2\left(1+|h_{se}|^2+|h_{re}|^2\right)-\Delta_{C_e} \\ &\leq \log_2\left(1+|h_{se}|^2+|h_{re}|^2\right). \end{aligned} \tag{30}$$

This implies that, except for the "1/2" factor, the eavesdropping capacity of the full duplex scheme is smaller than that of the half duplex scheme, unless either the $S \to E$ or $R \to E$ eavesdropping channel gain is zero. This is not surprising because in the full duplex scheme, the simultaneous transmission from S and R interfere with each at the eavesdropper. Below we further show how much such interference (or Δ_{C_e}) affects the eavesdropping capacity. Ignoring the high order terms in (29), we have

$$\begin{aligned} \Delta_{C_e} &= -\frac{1}{B}\sum_{b=1}^{B}\log_2(1+u) \approx \frac{1}{2\ln 2}\cdot\frac{1}{B}\sum_{b=1}^{B}\frac{1}{2}u^2 \\ &= \frac{1}{2\ln 2}\cdot\frac{1}{B}\cdot\left(\frac{2|h_{se}^*h_{re}|}{|h_{se}|^2+|h_{re}|^2+1}\right)^2\sum_{b=1}^{B}\cos^2\frac{b\pi}{B+1} \\ &= \frac{1}{2\ln 2}\cdot\left(\frac{1}{2}+\frac{1}{2B}\right)\cdot\left(\frac{2|h_{se}^*h_{re}|}{|h_{se}|^2+|h_{re}|^2+1}\right)^2. \end{aligned} \tag{31}$$

Further noting that

$$\frac{2|h_{se}^*h_{re}|}{|h_{se}|^2+|h_{re}|^2+1} < \frac{2|h_{se}^*h_{re}|}{|h_{se}|^2+|h_{re}|^2} \leq 1, \tag{32}$$

where equality holds $|h_{se}| = |h_{re}|$, then the maximum Δ_{C_e} is approximately given by

$$\Delta_{C_e,max} = \frac{1}{2\ln 2}\cdot\left(\frac{1}{2}+\frac{1}{2B}\right) \approx \frac{1}{4\ln 2}, \tag{33}$$

where the approximation holds for large block size B.

Substituting (33) into (30), we have the minimum eavesdropping capacity which is approximately given by

$$C_{e,min} \approx \log_2\left(1+|h_{se}|^2+|h_{re}|^2\right)-\frac{1}{4\ln 2}. \tag{34}$$

Recalling that $\Delta_{C_e} \geq 0$, it is clear from (30) that the maximum eavesdropping capacity is given by

$$C_{e,max} = \log_2\left(1+|h_{se}|^2+|h_{re}|^2\right), \tag{35}$$

which is achieved when $\Delta_{C_e} = 0$, or $|h_{se}| = 0$ or $|h_{re}| = 0$.

From the above analysis we conclude that, when either the $S \to E$ or $R \to E$ eavesdropping channels is weak (either $|h_{se}|$ or $|h_{re}|$ is close to zero), the eavesdropping capacity is close to its maximum value which is given by (35). When the $S \to E$ and $R \to E$ channels have similar gains ($|h_{se}| \approx |h_{re}|$), the receiving eavesdropper is most severely interfered with and the eavesdropping capacity is close to its minimum given by (34).

On the other hand, $C_{e,max}$ and $C_{e,min}$ only differ by approximately $1/(4\ln 2)$, which is a constant. When either of the eavesdropping channels is strong enough, i.e. either $|h_{se}|^2$ or $|h_{re}|^2$ is large such that $\log_2\left(1+|h_{se}|^2+|h_{re}|^2\right) \gg 1/(4\ln 2)$, we have $C_e \approx \log_2\left(1+|h_{se}|^2+|h_{re}|^2\right)$. This leads to an interesting result: the interference at the eavesdropper from the simultaneous transmission at S and R has limited effect on the eavesdropping capacity especially for strong eavesdropping channels.

D. Secrecy outage probability

From (23) and (30), the secrecy outage probability of the full duplex scheme can be obtained as

$$\begin{aligned} P_{FDR} &= P(C_{FDR} < R_s) \\ &= P([\log_2\left(\min\left(\frac{\gamma_{sr}}{\gamma_{rr}+1},\gamma_{rd}\right)\right) \\ &\quad -\left(\log_2\left(1+|h_{se}|^2+|h_{re}|^2\right)-\Delta_{C_e}\right)] < R_s) \\ &\approx P([\log_2\left(\min\left(\frac{\gamma_{sr}}{\gamma_{rr}+1},\gamma_{rd}\right)\right) - \\ &\quad \left(\log_2\left(|h_{se}|^2+|h_{re}|^2\right)-\Delta_{C_e}\right)] < R_s), \end{aligned} \tag{36}$$

where the approximation holds at high SNR. While it is hard to obtain a closed form for (36) due to the presence of Δ_{C_e}, we can obtain the minimum and maximum of the secrecy outage probability which gives very good approximation to the true value.

When $\Delta_{C_e} = 0$, we have the maximum secrecy outage probability, or the upper bound of P_{FDR}, as

$$\begin{aligned} P_{FDR,max} &= P\left(\frac{X_F}{Y} < 2^{R_s}\right) \\ &= F_Z(2^{R_s}) = \int_0^{\infty} F_{X_F}(y\gamma_f)f_Y(y)dy, \end{aligned} \tag{37}$$

where $X_F = \min\left(\frac{\gamma_{sr}}{\gamma_{rr}+1},\gamma_{rd}\right)$, $Y = |h_{se}|^2+|h_{re}|^2$ and $Z = X/Y$.

The PDF of Y, $f_Y(y)$, is the same as that in the half duplex scheme which is given by (13). The CDF of X_F can be obtained as

$$F_{X_F}(x) = 1-\frac{\lambda_{sr}e^{-\frac{x(\lambda_{sr}+\lambda_{rd})}{\lambda_{sr}\lambda_{rd}}}}{\lambda_{sr}+\lambda_{rr}x}. \tag{38}$$

Substituting (13) and (38) into (37) gives the upper bound of the secrecy outage probability as (39) in the top of the next page, where $m = \frac{2^{R_s}\lambda_{rd}\lambda_{re}+2^{R_s}\lambda_{re}\lambda_{sr}+\lambda_{rd}\lambda_{sr}}{2^{R_s}\lambda_{rd}\lambda_{re}\lambda_{rr}}$, $n = \frac{2^{R_s}\lambda_{rd}\lambda_{se}+2^{R_s}\lambda_{se}\lambda_{sr}+\lambda_{rd}\lambda_{sr}}{2^{R_s}\lambda_{rd}\lambda_{se}\lambda_{rr}}$, and $\mathrm{Ei}(\cdot)$ is the exponential integral function, that is, $\mathrm{Ei}(a,b) = \int_1^{\infty} e^{-xb}x^{-a}dx$.

On the other hand, when $\Delta_{C_e} = \Delta_{C_e,max} \approx 1/(4\ln 2)$ as is shown in (33), we obtain the approximate minimum secrecy outage probability as

$$P_{FDR,min} = F_Z(2^{R_s-\Delta_{C_e,max}}) \approx F_Z(2^{R_s-\frac{1}{4\ln 2}}). \tag{40}$$

We note that (40) is not a strict lower bound of P_{FDR}, but it gives accurate approximation of the best secrecy performance of the full duplex scheme. This is because of the Tayler series approximation used in (31).

E. Discussion

Compared with the half duplex scheme, there are several factors that affect the secrecy capacity of the full duplex relay. The first is that the full duplex scheme has no "1/2" factor in both the transmission and eavesdropping capacities. This is equivalent to halving the target secrecy rate, which leads

$$
\begin{aligned}
&P_{FDR,max} = F_Z(2^{R_s}) \\
&= \begin{cases} \frac{\left[2^{3R_s}\lambda_{rd}\lambda_{se}^3\lambda_{rr}^2+2^{2R_s}\lambda_{rd}\lambda_{se}^2\lambda_{sr}\lambda_{rr}^2+2^{3R_s}\lambda_{sr}\lambda_{se}^3\lambda_{rr}^2-\lambda_{rd}\lambda_{se}\lambda_{sr}^2\lambda_{rr}2^{R_s}+e^n\mathrm{Ei}(1,n)(\lambda_{rd}\lambda_{se}\lambda_{sr}^2 2^{R_s}+\lambda_{se}\lambda_{sr}^3 2^{R_s}+\lambda_{rd}\lambda_{sr}^3)\right]}{\lambda_{se}^2\lambda_{rr}^2 2^{2R_s}(2^{R_s}\lambda_{rd}\lambda_{se}+2^{R_s}\lambda_{se}\lambda_{sr}+\lambda_{rd}\lambda_{sr})}, & \lambda_{se} = \lambda_{re} \\ \frac{1}{(\lambda_{se}-\lambda_{re})2^{R_s}\lambda_{rr}}\left[2^{R_s}\lambda_{rr}(\lambda_{se}-\lambda_{re})+\lambda_{sr}(e^m\mathrm{Ei}(1,m)-e^n\mathrm{Ei}(1,n))\right], & \lambda_{se} \neq \lambda_{re} \end{cases}
\end{aligned}
\tag{39}
$$

---

to higher secrecy capacity according to the definition of the secrecy capacity.

The second factor is the simultaneous transmission of the source and relay nodes in the full duplex transmission. The influence of the simultaneous transmission on the eavesdropping capacity has been analyzed in Section III-C. From the analysis, we know that the simultaneous transmission in the full duplex scheme does help to improve the secrecy capacity, but the influence is limited. The most influence occurs when the $S \to E$ and $R \to E$ eavesdropping channels have the same gains, which leads to decreasing the target rate by $1/(4\ln 2)$ as is shown in (40). The least influence applies when either of the eavesdropping channels is zero.

The third factor that influences the secrecy performance is the self-interference at the relay due to the full duplex transmission. It is clearly shown in (20) that the self-interference channel γ_{rr} decreases the channel capacities for $S \to R$, which deteriorates the secrecy capacity of the full duplex scheme. The impact of the self-interference on the secrecy capacity will be investigated in the simulation section.

In summary, for the full duplex network, the first and second factors improve the secrecy performance, and the third factor deteriorates the secrecy performance. Because the second factor (the simultaneous transmission) has no significant effect on the secrecy performance, the secrecy performance advantage of the full duplex over the half duplex scheme mainly comes from the "1/2" factor in the capacities, if the self-interference can be sufficiently suppressed as it can in many systems.

IV. FULL DUPLEX JAMMING RELAY NETWORK

A. Secrecy capacity

This section proposes a full duplex jamming relay network. The system model is the similar to that of the full duplex scheme, but the relay R now switches between full and half duplex operation. At time slot t, the relay works in full duplex mode: the source S transmits data $x_s(t)$ to R, R receives and decodes $x_s(t)$ from S. At the same time, R transmits the jamming signal $j_r(t)$ to the eavesdropper E. Then the received signals at R and E at time t are given by

$$
\begin{aligned}
y_r(t) &= \sqrt{E_s}h_{sr}(t)x_s(t) + \sqrt{E_r}h_{rr}(t)j_r(t) + n_r(t), \\
y_e(t) &= \sqrt{E_s}h_{se}(t)x_s(t) + \sqrt{E_r}h_{re}(t)j_r(t) + n_e(t),
\end{aligned}
\tag{41}
$$

respectively. At time $(t+1)$, the relay R works in the half duplex mode that it only transmits the previously decoded $x_s(t)$ to the destination, and switches off its receiving antenna. At the same time, the source S transmits the jamming signal $j_s(t+1)$ to the eavesdropper. Then at time $(t+1)$, the eavesdropper receives the following signal

$$
\begin{aligned}
y_e(t+1) =& \sqrt{E_r}h_{re}(t+1)x_s(t) + \sqrt{E_s}h_{se}(t+1)j_s(t+1) \\
&+ n_e(t+1).
\end{aligned}
\tag{42}
$$

Because we assume no direct link between S and D, the jamming signal $j_s(t{+}1)$ has no effect on D so that the received signal at D is the same as that for the half duplex scheme which is shown in (3). Then the transmission capacity can be obtained as

$$
C_t = \frac{1}{2}\log_2\left(\min\left\{\frac{\gamma_{sr}}{\gamma_{rr}+1}, \gamma_{rd}\right\}\right). \tag{43}
$$

Comparing (21) and (43) shows that the full duplex and full duplex jamming schemes have similar data transmission capacity, except there is a "1/2" factor in the capacity of the latter. This is because the data rate of the full duplex jamming scheme is the same as that of the half duplex scheme.

On the other hand, from (41) and (42), the eavesdropping capacity C_s is given by

$$
C_e = \frac{1}{2}\log_2\left(1 + \frac{\gamma_{se}}{\gamma_{re}} + \frac{\gamma_{re}}{\gamma_{se}}\right). \tag{44}
$$

Substituting (43) and (44) into (4) gives the secrecy capacity for the full duplex jamming scheme at the high SNR region as

$$
\begin{aligned}
&C_{FDJ} = \\
&\left[\frac{1}{2}\log_2\left(\min\left(\frac{\gamma_{sr}}{\gamma_{rr}+1}, \gamma_{rd}\right)\right) - \frac{1}{2}\log_2\left(1 + \frac{\gamma_{se}}{\gamma_{re}} + \frac{\gamma_{re}}{\gamma_{se}}\right)\right]^+.
\end{aligned}
\tag{45}
$$

B. Secrecy outage probability

Letting $X = \min\left(\frac{\gamma_{sr}}{\gamma_{rr}+1}, \gamma_{rd}\right)$, $Y = \frac{\gamma_{se}}{\gamma_{re}} + \frac{\gamma_{re}}{\gamma_{se}}$ and $Z = X/(1+Y)$, the the secrecy outage probability is obtained as

$$
\begin{aligned}
P_{FDJ} = P(C_{FDJ} < R_s) &= P\left(\frac{X}{1+Y} < 2^{2R_s}\right) \\
&= F_Z(2^{2R_s}) = \int_0^\infty \int_0^{2^{2R_s}(1+y)} f_X(x)f_Y(y)dxdy.
\end{aligned}
\tag{46}
$$

Next we calculate the PDF of X and Y to derive (46). First, taking the derivative of the CDF of X (which is shown in (38)) gives the PDF of X as

$$
f_X(x) = \frac{e^{-\frac{(\lambda_{sr}+\lambda_{rd})x}{\lambda_{sr}\lambda_{rd}}}\left[(\lambda_{rd}+\lambda_{sr})(\lambda_{rr}x+\lambda_{sr})+\lambda_{sr}\lambda_{rr}\right]}{(\lambda_{rr}x+\lambda_{sr})^2\lambda_{rd}}. \tag{47}
$$

Then the PDF of Y, $f_Y(y)$, can be obtained as (48) in the top of the next page, where $M = \lambda_{se}/\lambda_{re}$. Substituting (47) and

$$\frac{2M^3\ln\left(\frac{[M+y][My+1]}{M}\right)(M^2+My^2+M+1)+My(M^6+2M^5y+M^4y^2+M^4+2M^3y+M^2y^2+M^2+2My+1)}{(M^7+4M^6y+6M^5y^2+4M^4y^3+M^3y^4+3M^5+9M^4y+9M^3y^2+3M^2y^3+3M^3+6M^2y+3My^2+M+y)(My+1)} \quad (48)$$

(48) into (46) gives

$$P_{FDJ}=\int_0^\infty f_Y(y)\left[1-\frac{\lambda_{sr}e^{-\frac{2^{R_s}(\lambda_{sr}+\lambda_{rd})(y+1)}{\lambda_{sr}\lambda_{rd}}}}{2^{R_s}\lambda_{rr}y+2^{R_s}\lambda_{rr}+\lambda_{sr}}\right]dy. \quad (49)$$

While (49) is in an integral close form, it can be easily obtained numerically with, for example Matlab or Maple [31].

C. Discussion

In either the full duplex or full duplex jamming scheme, the eavesdropper receives signals from both source and relay simultaneously. In the full duplex scheme, both received signals at the eavesdropper are the data so that they can be jointly decoded, leading to the similar eavesdropping capacity to that for the half duplex scheme (except the "$1/2$" factor). This has been clearly shown in Section III. While in the jamming scheme, the eavesdropper always receives data from one node and jamming signal from another node. The jamming signals impose serious interference to the data decoding at the eavesdropper, resulting in significant decrease in the eavesdropping capacity.

On the other hand, for the data transmission, the jamming scheme is still "half duplex" so that there is a "$1/2$" factor in its data and eavesdropping capacities. The "$1/2$" factor, which is equivalent to doubling the secrecy rate compared with the full duplex scheme, deteriorates the secrecy performance in the jamming scheme. It is clear from the definition of the secrecy capacity that such deterioration is more serious for higher target secrecy rate. This leads to an interesting observation: when the target secrecy rate is small, the influence from the "$1/2$" factor is also small, so that the jamming scheme has significant better secrecy performance than the full duplex scheme. But when the target secrecy rate becomes higher, the secrecy difference between the jamming and full duplex scheme becomes smaller. In fact, when the target secrecy rate is high enough, the full duplex scheme may have better secrecy performance than the jamming scheme. These will be very well verified by the simulation in the next section.

We also note that, while the secrecy outage analysis in this paper is for the relay network without a $S\rightarrow D$ direct link, the described half duplex, full duplex and full duplex jamming schemes can be readily applied in the network with a $S\rightarrow D$ direct link. On the other hand, including the $S\rightarrow D$ direct link complicates the performance analysis without gaining more insight into the half-/full- duplex relay which is the main focus of this paper. Finally we would like to point out that, while the secrecy performance analysis in this paper is based on the knowledge of the channel-state-information (CSI) for all channels (including the eavesdropping channels), the implementation of the half duplex, full duplex and full duplex jamming schemes do not rely upon the CSI knowledge.

V. SIMULATIONS

In this section, simulation results are given to verify the above analysis, where "HDR", "FDR" and "FDJ" represent the half duplex, full duplex and full duplex jamming schemes in following figures. In the simulations, the noise variances σ_r^2, σ_d^2 and σ_e^2 and the source and relay transmission powers E_s and E_r are all normalized to unity, and the block size $B=1000$. The simulation results are obtained by averaging over $100,000$ independent runs.

Fig. 2 verifies the secrecy outage analysis of the full duplex scheme in Section III-D, where we let $\gamma_{rr}=0$ dB and $\gamma_{sr}=\gamma_{rd}=40$ dB; the theoretical maximum and minimum of the secrecy outage probability are obtained by (39) and (40) respectively. In is clearly shown that, when the $S\rightarrow E$ and $R\rightarrow E$ eavesdropping channels have similar gains ($\gamma_{se}=\gamma_{re}=15$ dB), the secrecy outage probability is close to the minimum value. While when one of the eavesdropping channels is weak ($\gamma_{se}=25$ dB and $\gamma_{re}=10$ dB), the secrecy outage probability is close to the upper bound. In any case, the difference between the maximum and minimum secrecy outage probabilities are not significant. This verifies the analysis in Section III-D. In following simulations, only the simulation results for the full duplex scheme are shown for better exposition.

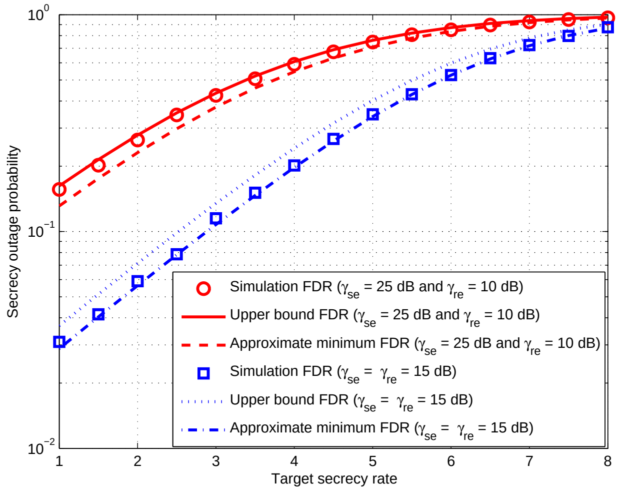


Fig. 2. Theoretical *vs* numerical secrecy outage probabilities for full duplex relay scenario for $\gamma_{sr}=\gamma_{rd}=40$ dB, $\gamma_{rr}=0$ dB.

Fig. 3 shows the secrecy outage probability *vs* data transmission SNR for HDR, FDR and FDJ, where we let $\gamma_{sr}=\gamma_{rd}$, $\gamma_{rr}=0$ dB and $\gamma_{se}=\gamma_{re}=10$ dB. Both the simulation and theoretical results for the half duplex and full duplex jamming schemes are presented, which are shown to be well matched. This verifies the closed-form secrecy outage probabilities for the half duplex and jamming schemes which are given by (14) and (49) respectively. It is shown in Fig. 3 that, when the target secrecy rate is small ($R_s=1$), the jamming scheme has better

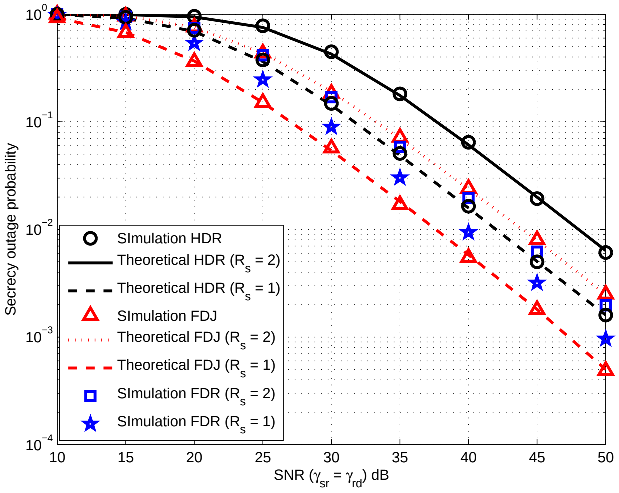


Fig. 3. Secrecy outage probabilities *vs* channel SNR for HDR, FDR and FDJ schemes, where $\gamma_{sr} = \gamma_{rd}$, $\gamma_{se} = \gamma_{re} = 10$ dB and $\gamma_{rr} = 0$ dB.

secrecy performance than the full duplex scheme. But when the target secrecy rate is large ($R_s = 2$), the jamming scheme has slightly worse secrecy outage performance than the full duplex scheme. In all cases, the half duplex has the worst secrecy performance. These observations are exactly what we expected in Section IV-C.

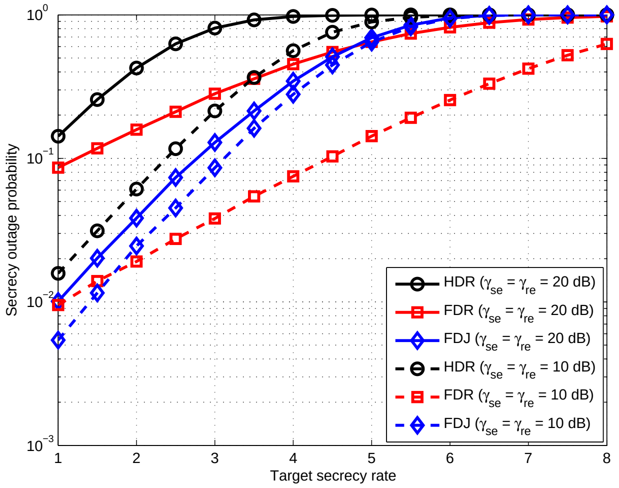


Fig. 4. Secrecy outage probabilities *vs* target secrecy rate for FDR, FDJ and HDR schemes, where $\gamma_{sr} = \gamma_{rd} = 40$ dB and $\gamma_{rr} = 0$ dB.

Fig. 4 shows the secrecy outage probability *vs* target secrecy rate for half duplex, full duplex and jamming schemes, where we let $\gamma_{sr} = \gamma_{rd} = 40$ dB and $\gamma_{rr} = 0$ dB. It is shown that, for $\gamma_{se} = \gamma_{re} = 20$ dB, when the target secrecy rate is small enough ($R_S < 4.7$), the jamming scheme has better secrecy outage performance than the full duplex scheme. This is because the interference from jamming has more influence on the secrecy performance than the "1/2" factor. When the target rate becomes higher, the "$1/2$" factor in the capacities of the jamming scheme starts to have more influence on the secrecy performance. Until the target rate $R_S > 4.7$, the jamming scheme has higher secrecy outage probability than the full duplex scheme. On the other hand, when $\gamma_{se} = \gamma_{re} = 10$ dB, the jamming has less influence on the secrecy performance than that for $\gamma_{se} = \gamma_{re} = 20$ dB. As a result, only when $R_S < 1.7$, the jamming scheme has better secrecy outage than the full duplex scheme. Otherwise, it is the full duplex scheme that has lower secrecy outage probability. This simulation further verifies the analysis in Section IV-C

Fig. 5 shows the secrecy performance *vs* residual self-interference γ_{rr} for different approaches, where we let $\gamma_{sr} = \gamma_{rd} = 40$ dB and $\gamma_{se} = \gamma_{re} = 10$ dB. It is clearly shown that, when the secrecy target $R_s = 2$, the full duplex has better performance than the half duplex scheme when $\gamma_{rr} < 9$ dB. But when $R_s = 1$, the full duplex has better performance than the half duplex scheme only when $\gamma_{rr} < 5$ dB. This is what we expected, because the main reason for the full duplex scheme to have better secrecy performance than the half duplex scheme is the associated "$1/2$" factor in the capacities, whose impact on the secrecy performance goes up with higher data rate. It is also shown in Fig. 5 that, when $R_s = 1$, the jamming scheme has better performance than the full duplex scheme. And when $R_s = 2$, the jamming scheme has slightly worse performance than the full duplex scheme. The reason is the same as that in Fig. 4.

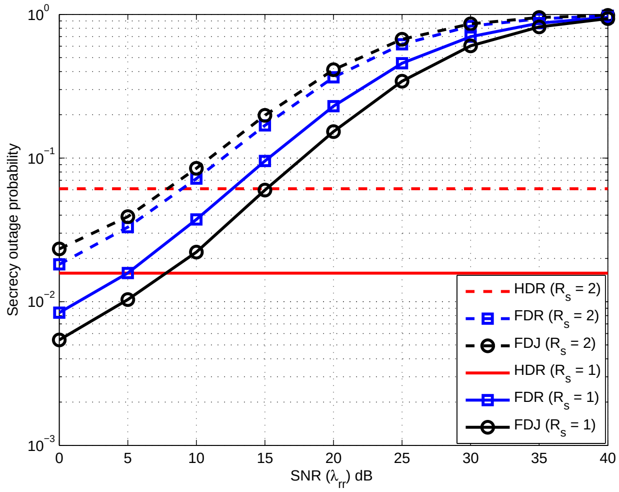


Fig. 5. Secrecy outage probabilities *vs* residual self-interference γ_{rr} for FDR, FDJ and HDR schemes, where $\gamma_{sr} = \gamma_{rd} = 40$ dB and $\gamma_{se} = \gamma_{re} = 10$ dB.

VI. CONCLUSION

In this paper, we investigated the secrecy performance of a full duplex relay network and proposed the full duplex jamming scheme to further improve the secrecy performance. The secrecy outage probability of the half duplex, full duplex and full duplex jamming schemes have been analyzed. The analysis shows that, the full duplex scheme has better secrecy performance than the half duplex scheme. On the other hand, the proposed full duplex jamming scheme has better secrecy performance than the full duplex scheme for small target secrecy rate, and the improvement may disappear when the target rate becomes large. The secrecy improvement of the full duplex jamming scheme is at the price of data rate lose. Numerical examples have been given to verify the analysis.

ACKNOWLEDGEMENTS

We would like to thank the anonymous reviewers and the editor for their constructive comments.

REFERENCES

[1] E. D. Silva, A. L. D. Santos, L. C. P. Albini, and M. Lima, “Identity based key management in mobile ad hoc networks: Techniques and applications,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 5, pp. 46–52, Oct. 2008.

[2] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Inform. Theory*, vol. 54, pp. 2515–2534, June 2008.

[3] Y. Liang, H. V. Poor, and S. Shamai, “Secure communication over fading channels,” *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[4] P. K. Gopala, L. Lai, and H. E. Gamal, “On the secrecy capacity of fading channels,” *IEEE Trans. Inform. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[5] Y. Liang and H. V. Poor, “Multiple-access channels with confidential messages,” *IEEE Trans. Inform. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[6] I. Csiszr and P. Narayan, “Secrecy capacities for multiterminal channel models,” *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2437–2452, June 2008.

[7] A. Khisti, A. Tchamkerten, and G. W. Wornell, “Secure broadcasting over fading channels,” *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2453–2469, June 2008.

[8] P. Popovski and O. Simeone, “Wireless secrecy in cellular systems with infrastructure-Aided cooperation,” *IEEE Trans. Inform. Forensics and Security*, vol. 4, no. 2, pp. 242 – 256, June. 2009.

[9] Y. Zou, X. Wang, and W. Shen, “Physical-layer security with multiuser scheduling in cognitive radio networks,” *IEEE Trans. Wireless Commun.*, vol. 60, no. 12, pp. 5103–5113, Oct. 2013.

[10] E. Tekin and A. Yener, “The general gaussian multiple access and two-way wire-tap channels: achievable rates and cooperative jamming,” *IEEE Trans. Inform. Theory*, vol. 54, pp. 2735–2751, June 2008.

[11] Y. Liu, J. Li, and A. P. Petropulu, “Destination assisted cooperative jamming for wireless physical-lay security,” *IEEE Trans. Inf. Froensics and Security*, vol. 8, no. 4, pp. 682–694, April 2013.

[12] H. Ju, E. Oh, and D. Hong, “Improving efficiency of resource usage in two-hop full duplex relay systems based on resource sharing and interference cancellation,” *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 3933–3938, Aug. 2009.

[13] T. Riihonen, S. Werner, and R. Wichman, “Optimized gain control for single-frequency relaying with loop interference,” *IEEE Trans. Wireless Commun.*, vol. 8, pp. 2801–2806, June 2009.

[14] J. I. Choi, M. Jain, K. Srinivasan, P. Levis, and S. Katti, “Achieving single channel, full duplex wireless communication,” *MobiCom, Chicago, USA*, Sep. 2010.

[15] S. Hong, J. Brand, J. Choi, M. Jain, J. Mehlman, S. Katti, and P. Levis, “Aplications of self-interference cancellation in 5G and beyond,” *IEEE Commun. Magazine*, vol. 52, no. 2, pp. 114–121, Feb. 2014.

[16] D. Bharadia, E. McMilin, and S. Katti, “Full duplex radios,” *ACM SIGCOMM, Hong Kong, China*, Aug. 2013.

[17] B. Debaillie, D. J. Broek, C. Lavin, B. Liempd, E. A. M. Klumperink, C. Palacios, J. Craninckx, B. Nauta, and A. Parssinen, “Analog/RF solutions enabling compact full-duplex radios,” *to appear IEEE J. Sel. Areas Commun.*

[18] W. Li, M. Ghogho, B. Chen, and C. Xiong, “Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis,” *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628–1631, Oct. 2012.

[19] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B.Ottersten, “Improving physical layer secrecy using full-duplex jamming receivers,” *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[20] A. Mukherjee and A. L. Swindlehurst, “A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures,” *in Proc. Asilomar Conf. Sign. Systems Comp., Pacific Grove, CA*, pp. 265–269, Nov. 2011.

[21] I. Krikidis, J. Thompson, and S. Mclaughlin, “Relay selection for secure cooperative networks with jamming,” *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[22] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, “Max-ratio relay selection in secure buffer-aided cooperative wireless networks,” *IEEE Trans. Inform. Forensics and Security*, vol. 9, no. 4, pp. 719–729, Apr. 2014.

[23] Y. Zou, X. Wang, W. Shen, and L. Hanzo, “Security versus reliability analysis of opportunistic relaying,” *IEEE Trans. Veh. Technol.*, vol. 63, no. 6, pp. 2653–2661, July 2014.

[24] C. Luo, Y. Gong, and F. chun Zheng, “Full interference cancellation for two-path relay cooperative networks,” *IEEE Trans. Veh. Technol.*, vol. 60, no. 1, pp. 343–347, Nov. 2010.

[25] H. Wicaksana, S. H. Ting, C. K. Ho, W. H. Chin, and Y. L. Guan, “AF two-path half duplex relaying with inter-relay self interference cancellation: Diversity analysis and its improvement,” *IEEE Trans. Wireless Commun.*, vol. 8, no. 9, pp. 4720–4729, Sep. 2009.

[26] N. Mokari, S. Parsaeefard, H. Saeedi, and P. Azmi, “Cooperative secure resource allocation in cognitive radio networks with guaranteed secrecy rate for primary users,” *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 1058–1073, Feb. 2014.

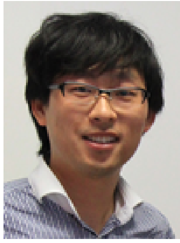
[27] C. R. Anderson, S. Krishnamoorthy, C. G. Ranson, T. J. Lemon, W. G. Newhall, T. Kummetz, and J. H. Reed, “Antenna isolation, wideband multipath propagation measurements and interference mitigation for on-frequency repeaters,” *in Proc. IEEE SoutheastCon*, Mar. 2004.

[28] T. Kwon, S. Lim, S. Choi, and D. Hong, “Optimal duplex mode for DF relay in terms of the outage probability,” *IEEE Trans. Veh. Technol.*, vol. 59, no. 7, pp. 3628–3634, Sep. 2010.

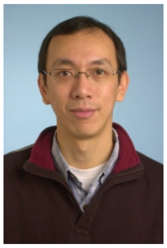
[29] I. Krikidis, H. A. Suraweera, P. J. Smith, and C. Yuen, “Full-duplex relay selection for amplify-and-forward cooperative networks,” *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4381–4393, Dec. 2012.

[30] S. Noschese, L. Pasquini, and L. Reichel, “Tridiagonal toeplitz matrices: Properties and novel applications,” *Numerical Linear Algebra with Applications*, vol. 20, pp. 302–326, April 2012.

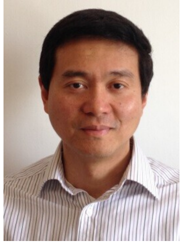
[31] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, “Breaking spectrum gridlock with cognative radios: an information theoretic perspective,” *Proceedings of the IEEE*, vol. 97, no. 5, pp. 894–914, May. 2009.



Gaojie Chen (S’09-M’12) received the B. Eng. and B. Ec. in Electrical Information Engineering and International Economics and Trade from the Northwest University, Shaanxi, China, in 2006, and the M.Sc (Distinction) and Ph.D degrees from Loughborough University, Loughborough, UK, in 2008 and 2012, respectively, all in Electrical and Electronic Engineering. From 2008 to 2009 he worked, as a software engineering in DTmobile, Beijing, China, and from 2012 to 2013 as a Research Associate in the School of Electronic, Electrical and Systems Engineering at the Loughborough University, Loughborough, UK. He is currently a Research Fellow in the Faculty of Engineering and Physical Sciences at the University of Surrey, Guildford, UK. His current research interests include information theory, wireless communications, cooperative communications, cognitive radio and secrecy communications.



Yu Gong is with School of Electronic, Electrical and Systems Engineering, Loughborough University, UK, in July 2012. Dr Gong obtained his BEng and MEng in electronic engineering in 1992 and 1995 respectively, both at the University of Electronics and Science Technology of China. In 2002, he received his PhD in communications from the National University of Singapore. After PhD graduation, he took several research positions in Institute of Inforcomm Research in Singapore and Queen’s University of Belfast in the UK respectively. From 2006 and 2012, Dr Gong had been an academic member in the School of Systems Engineering, University of Reading, UK. His research interests are in the area of signal processing and communications including wireless communications, cooperative networks, non-linear and non-stationary system identification and adaptive filters.



Pei Xiao received the PhD degree from Chalmers University of Technology, Sweden in 2004. Prior to joining the University of Surrey in 2011, he worked as a research fellow at Queens University Belfast and had held positions at Nokia Networks in Finland. He is a Reader at University of Surrey and also the technical leader of 5G Innovation Centre (5GIC), leading and coordinating different areas of 5G research activities. Founded in October 2012 and based in the University of Surrey, 5GIC is the worlds first research centre dedicated to 5G mobile technology. Dr Xiaos research interests and expertise span a wide range of areas in communications theory and signal processing for wireless communications

Jonathon A. Chambers (S'83-M'90-SM'98-F'11) received the Ph.D. and DSc degrees in signal processing from the Imperial College of Science, Technology and Medicine (Imperial College London), London, U.K., in 1990 and 2014. From 1991 to 1994, he was a Research Scientist with the Schlumberger Cambridge Research Center, Cambridge, U.K. In 1994, he returned to Imperial College London, as a Lecturer in signal processing and was promoted as a Reader (Associate Professor) in 1998. From 2001 to 2004, he was the Director of the Centre for Digital Signal Processing and a Professor of signal processing with the Division of Engineering, King's College London, London. From 2004 to 2007, he was a Cardiff Professorial Research Fellow with the School of Engineering, Cardiff University, Wales, U.K. In 2007, he joined the Department of Electronic and Electrical Engineering, Loughborough University, Loughborough, U.K., where he heads the Advanced Signal Processing Group and serves as the Associate Dean (Research) for Loughborough University in London. He is a coauthor of the books Recurrent Neural Networks for Prediction: Learning Algorithms, Architectures and Stability (New York, NY, USA: Wiley, 2001) and EEG Signal Processing (New York, NY, USA: Wiley, 2007). He has advised more than 50 researchers through to Ph.D. graduation and published more than 350 conference proceedings and journal articles, many of which are in IEEE journals. His research interests include adaptive and blind signal processing and their applications. Dr. Chambers is a Fellow of the Royal Academy of Engineering, U.K., and the Institution of Electrical Engineers (IEE). He was the Technical Program Chair of the 15th International Conference on Digital Signal Processing and the 2009 IEEE Workshop on Statistical Signal Processing, both held in Cardiff, U.K., and a Technical Program Cochair for the 36th IEEE International Conference on Acoustics, Speech, and Signal Processing, Prague, Czech Republic. He received the first QinetiQ Visiting Fellowship in 2007 for his outstanding contributions to adaptive signal processing and his contributions to QinetiQ?as a result of his successful industrial collaboration with the international defense systems company QinetiQ. He has served on the IEEE Signal Processing Theory and Methods Technical Committee for six years, the IEEE Signal Processing Society Awards Board for three years and is currently a member of the IEEE Signal Processing Conference Board, and the European Signal Processing Society Best Paper Awards Selection Panel. He has also served as an Associate Editor of the IEEE TRANSACTIONS ON SIGNAL PROCESSING for three terms over the periods 1997-1999, 2004-2007, and 2011- (and is currently a Senior Area Editor).