EURASIP Journal on Advances in Signal Processing
a SpringerOpen Journal

RESEARCH Open Access

Security-reliability performance of cognitive AF relay-based wireless communication system with channel estimation error

Qi Gu[1], Gongpu Wang[1*], Li Gao[2] and Mugen Peng[3]

Abstract

In this paper, both the security and the reliability performance of the cognitive amplify-and-forward (AF) relay system are analyzed in the presence of the channel estimation error. The security and the reliability performance are represented by the outage probability and the intercept probability, respectively. Instead of perfect channel state information (CSI) predominantly assumed in the literature, a certain channel estimation algorithm and the influence of the corresponding channel estimation error are considered in this study. Specifically, linear minimum mean square error estimation (LMMSE) is utilized by the destination node and the eavesdropper node to obtain the CSI, and the closed form for the outage probability and that for the intercept probability are derived with the channel estimation error. It is shown that the transmission security (reliability) can be improved by loosening the reliability (security) requirement. Moreover, we compare the security and reliability performance of this relay-based cognitive radio system with those of the direct communication system without relay. Interestingly, it is found that the AF relay-based system has less reliability performance than the direct cognitive radio system; however, it can lower the sum of the outage probability and the intercept probability than the direct communication system. It is also found that there exists an optimal training number to minimize the sum of the outage probability and the intercept probability.

Keywords: Channel estimation error; Secure wireless communication; Cognitive radio; Security-reliability performance; Amplify-and-forward; Relay network

1 Introduction

Nowadays, the increasing demand for high data rate wireless access and services brings about the problem of spectrum scarcity [1]. Cognitive radio (CR) [2,3] has been recognized as a promising technology to improve spectrum utilization efficiency and solve the spectrum scarcity problem. CR can enable unlicensed users, also referred to as cognitive users or secondary users, to communicate with each other over licensed bands. FCC [4] gives a formal definition of CR: ‘A cognitive radio is a radio that can change its transmitter parameters based on interaction with the environment it operates’.

Typically, a cognitive transmission process consists of two essential phases: spectrum sensing phase and data transmission phase. In the spectrum sensing phase, cognitive users attempt to find the spectrum hole, which is a frequency band assigned to the primary users but is not being utilized by the users at a particular time and specific geographic location [5]. The spectrum hole is typically located through the following techniques: energy detection [6], matched filter, and cyclostationary detection [7]. In the data transmission phase, cognitive users transmit data to each other through the detected spectrum hole. Different transmission techniques have been studied in [8-11] and references therein.

Due to the broadcasting nature of wireless channel and the openness of cognitive radio architecture where various unknown wireless devices are allowed to access the licensed spectrum, cognitive radio systems face a challenge of physical layer security. For example, one receiver located near the cognitive source can receive the signal from it and recover the original information.

*Correspondence: gpwang@bjtu.edu.cn
[1] School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China
Full list of author information is available at the end of the article

Much attention has been given to physical layer security in wireless communication systems [12-14]. It is Wyner who firstly investigated the physical-layer security problem in an information-theoretic sense [15] in 1975. Shortly after, the authors in [16] extended Wyner's results to Gaussian wiretap channels and derived the secrecy capacity. In recent years, a multiple-input single-output (MISO) wiretap channel is considered in [12], and a multiple-input multiple-output (MIMO) wiretap channel is studied in [13]. Besides, cooperative relay-aided secure communication has been suggested in [14]. Furthermore, the authors in [17] characterize the security-reliability trade-off performance of conventional direct transmission from source to destination in the presence of an eavesdropper, where the security and reliability are evaluated by the intercept probability at the eavesdropper and the outage probability at the destination, respectively.

All the previous works for traditional point-to-point networks [12-14] and relay-based systems [17-19] about secure wireless communication assumed perfect channel state information (CSI). However, in a practical situation, perfect CSI cannot be obtained. For most practical wireless communication systems, training symbols are transmitted so that the receiver can estimate the channel [20].

Almost in every situation, channel estimation error exists. To our best knowledge, secure wireless communication for relay-based networks has not been addressed in the case of the presence of channel estimation error, which motivates our present work.

In this paper, we study the security and reliability performance of the cognitive amplify-and-forward (AF) relay system in the presence of channel estimation error, and we compare its performance with that of the direct communication cognitive radio system. Specifically, we assume that all communication systems utilize linear minimum mean square error estimation (LMMSE) to obtain channel parameters and derive the corresponding channel estimation error. Based on channel estimates, the detection of data symbols can be found and the channel capacity in the presence of channel estimation error can be obtained. Next, we derive the outage probability and the intercept probability to evaluate the reliability and security performance, respectively. We find that the transmission security (reliability) can be improved by loosening the reliability (security) requirement. Moreover, comparing the security and the reliability performance of this relay-based system with those of the direct communication system without relay, we find that the AF relay-based system has less reliability performance than the direct system; however, it can lower the sum of the outage probability and the intercept probability than the direct communication system. We also show that there exists an optimal training number to minimize the sum of the outage probability and the intercept probability.

This paper is organized as follows: Section 2 gives the system model and Section 3 shows the sensing performance of the cognitive system. Next, the capacity analysis in the presence of channel estimation error is presented in Section 4. The security and the reliability performance are analyzed in Section 5, and numerical results are provided in Section 6 to corroborate our proposed studies. Finally, Section 7 concludes the paper.

2 System model

Consider a joint existence of the primary network and a cognitive system (Figure 1). The primary network consists of two primary users: PU_1 and PU_2, that are communicating over certain licensed bands. The secondary network is a cognitive one-way relay network with one source, one destination, and one relay. One eavesdropper is assumed to intercept the cognitive transmission from the source to the destination. The solid and dash lines in Figure 1 represent the main links (one from the source via the relay to the destination and the other from the source directly to the destination) and wiretap links (from the source and from the relay to the eavesdropper), respectively.

The cognitive wireless system works in a slotted structure, and the whole communication from the source to the destination has two processes: the sensing process and the transmission process (Figure 2). The source will sense the spectrum hole for S symbols' period at the beginning of each slot and will start the transmission process when sensing the spectrum whole and stop after N symbols are transmitted. The whole slot contains $L_{slot} = S + 2N$ symbols.

The transmission process involves two phases. In the first phase, the source node broadcasts signals to the relay node and the destination node; in the second phase, the relay node employs the amplify-and-forward (AF) protocol to resend the received signal to the destination node. That is, the relay node amplifies its received signal with a constant factor α and then forwards it to the destination.

Suppose the subslot transmitted from the source contains N symbols that consist of K training symbols $p(n)$ and M data symbols $s(n)$, as shown in Figure 2. Clearly, $N = K + M$. Let $\mathcal{T}_p$ denote the index set of the training symbols while denote $\mathcal{T}_d$ as the index set of data symbols. The full time index set is then $\mathcal{T} = \mathcal{T}_d \bigcup \mathcal{T}_p = \{n = 1, 2, \ldots, N\}$.

Let H_p represent whether or not there is a spectrum hole for the current time slot. Specifically, $H_p = H_0$ represents that a spectrum hole is available, i.e., the channel is unoccupied by the primary users; otherwise, $H_p = H_1$.

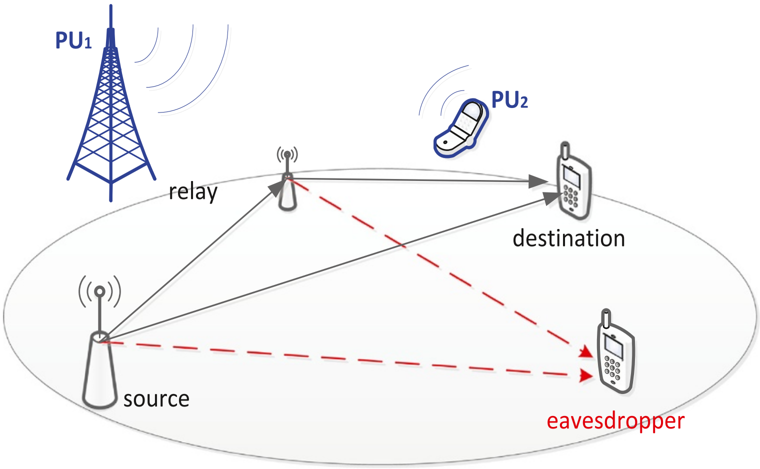

Figure 1 A cognitive AF relay-based system against an eavesdropper.

Without loss of generality, we suppose PU$_1$ is transmitting signal $x_p(n)$ to PU$_2$ in the case of $H_p = H_1$. As did in [21], we model H_p as a Bernoulli random variable with parameter $P_\emptyset$ (the probability of the channel being available for secondary users), i.e., $\Pr(H_p = H_0) = P_\emptyset$ and $\Pr(H_p = H_1) = 1 - P_\emptyset$.

Let $\hat{H}_s$ represent the sensing decision by the source node, i.e., $\hat{H}_s = H_0$ or $\hat{H}_s = H_1$.

For notational convenience, the channels are defined in Table 1. We assume that all channels are Rayleigh fading. In addition, the noise produced in the transmission on the channel h_{ab} from node a to node b is denoted as w_{ab} which is assumed as a zero-mean complex Gaussian variable with variance N_0.

2.1 Source

At the beginning of each slot, the source will sense the licensed channel and decide its existence or not. If it decides $\hat{H} = H_0$, then the source will transmit N symbols to the relay and the destination, and next the relay will forward the received N symbols to the destination.

The signal received by the source at the first S symbol periods is

$$s(n) = f_{\text{ps}}\sqrt{P_p}\,\theta(n) + w_{\text{ps}}(n), \quad 1 \le n \le S, \tag{1}$$

where $w_{\text{ps}}(n)$ is the noise at the source node and $\theta(n)$ is the signal transmitted from the PU

$$\theta(n) = \begin{cases} 0, & H_p = H_0 \\ x_p(n), & H_p = H_1. \end{cases} \tag{2}$$

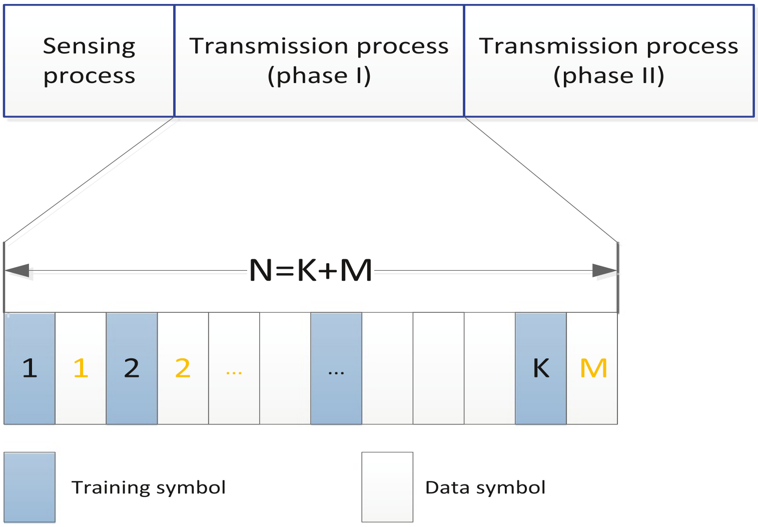
Sensing process
Transmission process (phase I)
Transmission process (phase II)
N=K+M
1
1
2
2
...
...
K
M
Training symbol
Data symbol

Figure 2 One slot includes two parts: the sensing part and the transmission part. The transmission process involves two phases, and each phase contains *N* symbols: *K* training symbols and *M* data symbols.

Table 1 List of the channel notations

Notation	Definition	Distribution
h_{sd}	Channel from source to destination	$\mathcal{CN}(0,\sigma_{\mathrm{sd}}^2)$
h_{sr}	Channel from source to relay	$\mathcal{CN}(0,\sigma_{\mathrm{sr}}^2)$
h_{rd}	Channel from relay to destination	$\mathcal{CN}(0,\sigma_{\mathrm{rd}}^2)$
g_{se}	Channel from source to eavesdropper	$\mathcal{CN}(0,\sigma_{\mathrm{se}}^2)$
g_{re}	Channel from relay to eavesdropper	$\mathcal{CN}(0,\sigma_{\mathrm{re}}^2)$
f_{ps}	Channel from PU$_1$ to source	$\mathcal{CN}(0,\sigma_{\mathrm{ps}}^2)$
f_{pr}	Channel from PU$_1$ to relay	$\mathcal{CN}(0,\sigma_{\mathrm{pr}}^2)$
f_{pd}	Channel from PU$_1$ to destination	$\mathcal{CN}(0,\sigma_{\mathrm{pd}}^2)$
f_{pe}	Channel from PU$_1$ to eavesdropper	$\mathcal{CN}(0,\sigma_{\mathrm{pe}}^2)$

2.2 Relay

Suppose the transmission power at the source node and at the PU$_1$ is P_s and P_p, respectively. The signal received at the relay node is

$$r(n) = h_{\mathrm{sr}}\sqrt{P_s}x(n) + w_{\mathrm{sr}}(n) + f_{\mathrm{pr}}\sqrt{P_p}\theta(n), \tag{3}$$

where the transmitted signal $x(n)$ is defined as

$$x(n) = \begin{cases} p(n), & n \in \mathcal{T}_p \\ s(n), & n \in \mathcal{T}_d \end{cases} \tag{4}$$

and $\theta(n)$ is the signal transmitted from the PU defined in (2).

In the next phase, the relay will amplify the received signal $r(n)$ with a factor α and forward it to the destination node. The factor α is defined as

$$\alpha = \sqrt{\frac{P_r}{P_s\sigma_{\mathrm{sr}}^2 + N_0}}. \tag{5}$$

2.3 Destination

The signal received at the destination in the first phase and in the second phase can be respectively expressed as

$$d_1(n) = h_{\mathrm{sd}}\sqrt{P_s}x(n) + f_{\mathrm{pd}}\sqrt{P_p}\theta(n) + w_{\mathrm{sd}}(n), \tag{6}$$

$$\begin{aligned} d_2(n) &= \alpha h_{\mathrm{r}d}\sqrt{P_r}r(n) + f_{\mathrm{pd}}\sqrt{P_p}\theta(n+N) + w_{\mathrm{rd}}(n) \\ &= \alpha h_{\mathrm{sr}}h_{\mathrm{r}d}\sqrt{P_rP_s}x(n) + w_{\mathrm{srd}}(n) + I_{\mathrm{pd}}(n), \end{aligned} \tag{7}$$

where $I_{\mathrm{pd}}(n)$ is the interference from the primary user

$$I_{\mathrm{pd}}(n) = \alpha h_{\mathrm{rd}}f_{\mathrm{pr}}\sqrt{P_rP_p}\theta(n) + f_{\mathrm{pd}}\sqrt{P_p}\theta(n+N) \tag{8}$$

and $w_{\mathrm{srd}}(n)$ is the combined noise defined as

$$w_{\mathrm{srd}}(n) = \alpha h_{\mathrm{r}d}\sqrt{P_r}w_{\mathrm{sr}}(n) + w_{\mathrm{rd}}(n). \tag{9}$$

Clearly, the combined noise $w_{\mathrm{srd}}(n)$ is zero-mean Gaussian-distributed with variance

$$N_{\mathrm{srd}} = |\alpha|^2\sigma_{\mathrm{rd}}^2P_rN_0 + N_0. \tag{10}$$

2.4 Eavesdropper

The signals received at the eavesdropper during the first phase and the second phase can be respectively expressed as

$$e_1(n) = g_{\mathrm{se}}\sqrt{P_s}x(n) + w_{\mathrm{se}}(n) + f_{\mathrm{pe}}\sqrt{P_p}\theta(n), \tag{11}$$

$$\begin{aligned} e_2(n) &= \alpha g_{\mathrm{re}}\sqrt{P_r}r(n) + w_{\mathrm{re}}(n) + f_{\mathrm{pe}}\sqrt{P_p}\theta(n+N) \\ &= \alpha h_{\mathrm{sr}}g_{\mathrm{re}}\sqrt{P_rP_s}x(n) + w_{\mathrm{sre}}(n) + I_{\mathrm{pe}}(n), \end{aligned} \tag{12}$$

where $w_{\mathrm{sre}}(n)$ is the combined noise defined as

$$w_{\mathrm{sre}}(n) = \alpha g_{\mathrm{re}}\sqrt{P_r}w_{\mathrm{sr}}(n) + w_{\mathrm{re}}(n) \tag{13}$$

and $I_{\mathrm{pe}}(n)$ is the interference from the primary user

$$I_{\mathrm{pe}}(n) = \alpha g_{\mathrm{re}}f_{\mathrm{pr}}\sqrt{P_rP_p}\theta(n) + f_{\mathrm{pe}}\sqrt{P_p}\theta(n+N). \tag{14}$$

Obviously, the combined noise $w_{\mathrm{sre}}(n)$ is zero-mean Gaussian-distributed with variance

$$N_{\mathrm{sre}} = |\alpha|^2\sigma_{\mathrm{re}}^2P_rN_0 + N_0. \tag{15}$$

3 Sensing performance

With the assumption of the energy detector utilized by the source node, we can find the false alarm probability P_f as

$$\begin{aligned} P_f &= \{\hat{H}_s = H_1 | H_p = H_0\} \\ &= \Pr\left\{\sum_{n=1}^{S}|w_{\mathrm{ps}}(n)|^2 > \lambda_{\mathrm{E}D}\right\}, \end{aligned} \tag{16}$$

where $\lambda_{\mathrm{E}D}$ is the decision threshold of the energy detector. Note that $\sum_{n=1}^{S}|w_{\mathrm{ps}}(n)|^2$ can be considered as a central chi-squared random variable $\mathcal{X}_{2S}^2$ with $2S$ degrees of freedom [22]. Therefore, Equation 16 can be found as [23]

$$P_f = \exp\left(-\frac{\lambda_{\mathrm{ED}}}{N_0}\right)\sum_{k=0}^{S-1}\frac{\left(\frac{\lambda_{\mathrm{E}D}}{N_0}\right)^k}{k!}. \tag{17}$$

In the case of $H_p = H_1$, the signal received at the source is $x_p(n)$ plus noise. The individual detection probability P_d at the source node can be thus obtained as

$$\begin{aligned} P_d &= \Pr\{\hat{H}_s = H_1 | H_p = H_1\} \\ &= \Pr\left\{\sum_{k=0}^{S-1}|\sqrt{P_p}f_{\mathrm{ps}}x_p(k) + w_{\mathrm{ps}}(k)|^2 > \lambda_{\mathrm{ED}}\right\} \\ &= \Pr\left\{\sum_{k=1}^{S}\frac{|\sqrt{P_p}f_{\mathrm{ps}}x_p(k) + n_i(k)|^2}{(P_p\sigma_{\mathrm{ps}}^2 + N_0)/2} > \frac{2\lambda_{\mathrm{ED}}}{P_p\sigma_{\mathrm{ps}}^2 + N_0}\right\}. \end{aligned} \tag{18}$$

Note that $\sum_{k=1}^{S} \frac{|\sqrt{P_p} f_{\mathrm{ps}} x_p(k)+n_i(k)|^2}{(P_p\sigma_{\mathrm{ps}}^2+N_0)/2}$ can be also considered as a central chi-squared random variable $\mathcal{X}_{2S}^2$ with $2S$ degrees of freedom [22]. Hence, we can further obtain (16) as

$$P_d = \exp\left(-\frac{\lambda_{\mathrm{ED}}}{P_p\sigma_{\mathrm{ps}}^2+N_0}\right)\sum_{k=0}^{S-1}\frac{\left(\frac{\lambda_{ED}}{P_p\sigma_{\mathrm{ps}}^2+N_0}\right)^k}{k!}. \tag{19}$$

4 Channel capacity with estimation error

In this section, the channel estimation and data detection process at the destination and also at the eavesdropper are analyzed. The LMMSE method is chosen due to its optimal estimation performance for Gaussian signals [24]. Based on the analysis of estimation and detection process, the mathematical expressions for channel capacity with estimation error are derived.

The source will begin transmission in the two cases of $\hat{H}_s = H_0$: one is that it successfully detects the existence of the spectrum hole when there is no transmission between the primary users; the other is that it mistakenly detects the appearance of the spectrum hole when the primary users are communicating. In the former case, the nodes in the cognitive system can communicate without any interference from the primary users. Suppose the achievable channel capacity in this case is C_{I}. In the latter case, both PU_1, the cognitive source and the cognitive relay will transmit signals and will interfere with each other. In such case, the cognitive system can also obtain certain channel capacity $C_{\mathrm{I}I}$. However, the capacity gain is limited and negligible especially when P_p, the transmission power of PU_1, is high [21]. Thus, in the following capacity analysis, we focus on the first case.

4.1 Signal processing at destination

4.1.1 The first phase

In the case of $H_p = H_0$, the item $\theta(n)$ in Equation (6) is zero. Stack $d_1(n)$, $p(n)$, and $w_{\mathrm{sd}}(n)$ from the set $\mathcal{T}_p$ into $K \times 1$ vectors $\mathbf{d}_{1p}$, $\mathbf{p}$, and $\mathbf{w}_{d1p}$, respectively. We can obtain the following equation from (6)

$$\mathbf{d}_{1p} = h_{\mathrm{sd}}\sqrt{P_s}\mathbf{p} + \mathbf{w}_{d1p}. \tag{20}$$

Multiplying both sides of Equation 20 with $\mathbf{p}^H$ will give

$$\mathbf{p}^H\mathbf{d}_{1p} = h_{\mathrm{sd}}\sqrt{P_s}\mathbf{p}^H\mathbf{p} + \mathbf{p}^H\mathbf{w}_{d1p}. \tag{21}$$

Let $y_{1p} = \mathbf{p}^H\mathbf{d}_{1p}$. Utilizing the LMMSE method, the estimate of the channel h_{sd} can be found from (21) as

$$\hat{h}_{\mathrm{sd}} = E(h_{\mathrm{sd}}y_{1p}^H)(E(y_{1p}y_{1p}^H))^{-1}y_{1p} \tag{22}$$

$$= \frac{\sqrt{P_s}\sigma_{\mathrm{sd}}^2\mathbf{p}^H\mathbf{d}_{1p}}{P_s\sigma_{\mathrm{sd}}^2\mathbf{p}^H\mathbf{p}+N_0}, \tag{23}$$

where $E(.)$ denotes the statistical expectation throughout this paper. The mean of the channel estimate $\hat{h}_{\mathrm{sd}}$ is zero and the variance is

$$\varsigma_{\mathrm{sd}}^2 = \frac{P_s\sigma_{\mathrm{sd}}^4\mathbf{p}^H\mathbf{p}}{P_s\sigma_{\mathrm{sd}}^2\mathbf{p}^H\mathbf{p}+N_0}. \tag{24}$$

Therefore, the estimation error of the channel h_{sd} is

$$\epsilon_{\mathrm{sd}} = \hat{h}_{\mathrm{sd}} - h_{\mathrm{sd}} \tag{25}$$

$$= \frac{\sqrt{P_s}\sigma_{\mathrm{sd}}^2\mathbf{p}^H\mathbf{w}_{d1p} - h_{\mathrm{sd}}N_0}{P_s\sigma_{\mathrm{sd}}^2\mathbf{p}^H\mathbf{p}+N_0}. \tag{26}$$

It can be readily checked that the channel estimation error ϵ_{sd} is zero-mean Gaussian-distributed with variance

$$\varrho_{\mathrm{sd}}^2 = \frac{\sigma_{\mathrm{sd}}^2N_0}{P_s\sigma_{\mathrm{sd}}^2\mathbf{p}^H\mathbf{p}+N_0}. \tag{27}$$

In order to detect data symbols with channel estimate $\hat{h}_{\mathrm{sd}}$, Equation 6 will be rewritten as

$$d_1(n) = \hat{h}_{\mathrm{sd}}\sqrt{P_s}s(n) - \epsilon_{\mathrm{sd}}\sqrt{P_s}s(n) + w_{\mathrm{sd}}(n), \tag{28}$$

for $n \in \mathcal{T}_d$.

4.1.2 The second phase

In the case of $H_p = H_0$, the item $I_{\mathrm{pd}}(n)$ in Equation 7 is zero. Stack $d_2(n)$ and $w_{\mathrm{srd}}(n)$ from the set $\mathcal{T}_p$ into $K \times 1$ vectors $\mathbf{d}_{2p}$ and $\mathbf{w}_{d2p}$, respectively. We can obtain the following equation from (7)

$$\mathbf{d}_{2p} = \alpha h_{\mathrm{sr}}h_{\mathrm{rd}}\sqrt{P_sP_r}\mathbf{p} + \mathbf{w}_{d2p}. \tag{29}$$

Multiplying both sides of (29) with $\mathbf{p}^H$ will produce

$$\mathbf{p}^H\mathbf{d}_{2p} = \alpha h_{\mathrm{sr}}h_{\mathrm{rd}}\sqrt{P_sP_r}\mathbf{p}^H\mathbf{p} + \mathbf{p}^H\mathbf{w}_{d2p}. \tag{30}$$

Suppose $y_{2p} = \mathbf{p}^H\mathbf{d}_{2p}$ and define the combined channel $h_{\mathrm{srd}} = h_{\mathrm{sr}}h_{rd}$. Clearly, the mean of h_{srd} is zero and the variance of h_{srd} is $\sigma_{\mathrm{srd}}^2 = \sigma_{\mathrm{sr}}^2\sigma_{\mathrm{rd}}^2$.

We can obtain the estimate of the combined channel h_{srd} with the LMMSE method as

$$\hat{h}_{\mathrm{srd}} = E(h_{\mathrm{srd}}y_{2p}^H)(E(y_{2p}y_{2p}^H))^{-1}y_{2p}$$

$$= \frac{\alpha\sigma_{\mathrm{srd}}^2\sqrt{P_sP_r}\mathbf{p}^H\mathbf{d}_{2p}}{\alpha^2\sigma_{\mathrm{srd}}^2P_sP_r\mathbf{p}^H\mathbf{p}+N_{\mathrm{srd}}}. \tag{31}$$

The channel estimate $\hat{h}_{\mathrm{srd}}$ has zero mean and its variance is

$$\varsigma_{\mathrm{srd}}^2 = \frac{\alpha^2 \sigma_{\mathrm{srd}}^4 P_s P_r \mathbf{p}^H \mathbf{p}}{\alpha^2 \sigma_{\mathrm{srd}}^2 P_s P_r \mathbf{p}^H \mathbf{p} + N_{\mathrm{srd}}} \tag{32}$$

The estimation error of the combined channel h_{srd} can be found as

$$\begin{aligned}\epsilon_{\mathrm{srd}} &= \hat{h}_{\mathrm{srd}} - h_{\mathrm{srd}} \\ &= \frac{\alpha \sigma_{\mathrm{srd}}^2 \sqrt{P_s P_r} \mathbf{p}^H \mathbf{w}_{d2p} - h_{\mathrm{srd}} N_{\mathrm{srd}}}{\alpha^2 \sigma_{\mathrm{srd}}^2 P_s P_r \mathbf{p}^H \mathbf{p} + N_{\mathrm{srd}}}.\end{aligned} \tag{33}$$

Clearly, $E(\epsilon_{\mathrm{srd}}) = 0$ and the variance of the channel estimation error ϵ_{srd} is

$$\varrho_{\mathrm{srd}}^2 = \frac{\sigma_{\mathrm{srd}}^2 N_{\mathrm{srd}}}{\alpha^2 \sigma_{\mathrm{srd}}^2 P_s P_r \mathbf{p}^H \mathbf{p} + N_{\mathrm{srd}}}. \tag{34}$$

To perform data detection with the estimate, Equation 7 will be rewritten as

$$d_2(n) = \alpha \hat{h}_{\mathrm{srd}} \sqrt{P_s P_r} s(n) - \alpha \epsilon_{\mathrm{srd}} \sqrt{P_s P_r} s(n) + w_{\mathrm{srd}}(n), \tag{35}$$

for $n \in \mathcal{T}_d$.

Remark 1. Only the LMMSE method can produce the result that the channel estimation error is uncorrelated with the channel estimate, that is,

$$E(\hat{h}_{\mathrm{sd}} \epsilon_{\mathrm{sd}}^H) = 0, \qquad E(\hat{h}_{\mathrm{srd}} \epsilon_{\mathrm{srd}}^H) = 0. \tag{36}$$

This will guarantee that the interference which resulted from the channel estimation error can be translated into a sort of noise independent from the source signals [25], which will facilitate the capacity analysis in the following part.

4.1.3 Channel capacity

Next, from (28) we can find the capacity of the direct channel h_{sd} as

$$C_{\mathrm{sd}} = \frac{M}{L_{slot}} \log_2 \left(1 + \frac{|\hat{h}_{\mathrm{sd}}|^2 P_s}{|\epsilon_{\mathrm{sd}}|^2 P_s + N_0} \right). \tag{37}$$

In addition, from (35) we can obtain the capacity of the AF relay channel $h_s rd$ as

$$C_{\mathrm{srd}} = \frac{M}{L_{slot}} \log_2 \left(1 + \frac{\alpha^2 |\hat{h}_{\mathrm{srd}}|^2 P_r P_s}{\alpha^2 |\epsilon_{\mathrm{srd}}|^2 P_r P_s + N_{\mathrm{srd}}} \right). \tag{38}$$

Assume that the destination chooses selection diversity combining, i.e., when two signals are received at the destination, a signal copy with higher signal-to-noise ratio (SNR) than the other will be employed for decoding the source message. Thus, the capacity achieved at the destination in the case that the source successfully detects the existence of the spectrum hole is

$$C_{\mathrm{I}} = \max(C_{\mathrm{sd}}, C_{\mathrm{srd}}). \tag{39}$$

Finally, we can express the total achievable capacity at the destination as

$$\begin{aligned} C_d &= P_\emptyset \Pr(\hat{H}_s = H_0 | H_p = H_0) C_{\mathrm{I}} \\ &\quad + (1 - P_\emptyset) \Pr(\hat{H}_s = H_0 | H_p = H_1) C_{\mathrm{II}} \\ &= P_\emptyset (1 - P_f) C_{\mathrm{I}} + (1 - P_\emptyset)(1 - P_d) C_{\mathrm{II}} \\ &\approx P_\emptyset (1 - P_f) \max(C_{\mathrm{sd}}, C_{\mathrm{srd}}), \end{aligned} \tag{40}$$

where P_f is the false alarm probability defined in (17) and P_d is the detection probability defined in (19). The approximation is due to that C_{II} represents the channel capacity in the case that the cognitive users mistakenly detect the appearance of the spectrum hole when the primary users are communicating. In such case, both PU1, the cognitive source, and the cognitive relay will interfere with each other, which will result in a small value of C_{II} as in [21,26]. Moreover, we can adjust the threshold so that the detection probability P_d can approach 1. Therefore, the item $(1 - P_\emptyset)(1 - P_d)C_{II}$ in (40) is negligible.

4.2 Signal processing at the eavesdropper

Since the eavesdropper will take a similar estimation and detection process as the destination, the process is described briefly in this subsection.

4.2.1 The first phase

Stack $e_1(n)$ and $w_{\mathrm{se}}(n)$ from the set $\mathcal{T}_p$ into $K \times 1$ vectors $\mathbf{e}_{1p}$ and $\mathbf{w}_{e1p}$. We can find from (11) the following equation:

$$\mathbf{e}_{1p} = g_{\mathrm{se}} \sqrt{P_s} \mathbf{p} + \mathbf{w}_{e1p}. \tag{41}$$

Using the same LMMSE method in Section 4.1, the estimate of the channel h_{se} can be obtained as

$$\hat{g}_{\mathrm{se}} = \frac{\sqrt{P_s} \sigma_{\mathrm{se}}^2 \mathbf{p}^H \mathbf{e}_{1p}}{P_s \sigma_{\mathrm{se}}^2 \mathbf{p}^H \mathbf{p} + N_0}. \tag{42}$$

Clearly, $E(\hat{g}_{\mathrm{se}}) = 0$ and the variance of the channel estimate $\hat{g}_{\mathrm{se}}$ is

$$\varsigma_{\mathrm{se}}^2 = \frac{P_s \sigma_{\mathrm{se}}^4 \mathbf{p}^H \mathbf{p}}{P_s \sigma_{\mathrm{se}}^2 \mathbf{p}^H \mathbf{p} + N_0}. \tag{43}$$

The channel estimation error is

$$\begin{aligned}\epsilon_{\mathrm{se}} &= \hat{g}_{\mathrm{se}} - g_{\mathrm{se}} \\ &= \frac{\sqrt{P_s} \sigma_{\mathrm{se}}^2 \mathbf{p}^H \mathbf{e}_{1p} - h_{\mathrm{se}} N_0}{P_s \sigma_{\mathrm{se}}^2 \mathbf{p}^H \mathbf{p} + N_0}.\end{aligned} \tag{44}$$

Also, we have $E(\epsilon_{\mathrm{se}}) = 0$ and the variance of the channel estimation error ϵ_{se} is

$$\varrho_{\mathrm{se}}^2 = \frac{\sigma_{\mathrm{se}}^2 N_0}{P_s \sigma_{\mathrm{se}}^2 \mathbf{p}^H \mathbf{p} + N_0}. \tag{45}$$

To detect data symbols with channel estimate $\hat{h}_{\mathrm{se}}$, Equation 11 will be rewritten as

$$e_1(n) = \hat{g}_{\mathrm{se}} \sqrt{P_s} s(n) - \epsilon_{\mathrm{se}} \sqrt{P_s} s(n) + w_{\mathrm{se}}(n), \tag{46}$$

for $n \in \mathcal{T}_d$.

4.2.2 *The second phase*

Stack $e_2(n)$ and $w_{\mathrm{sre}}(n)$ from the set $\mathcal{T}_p$ into $K \times 1$ vectors $\mathbf{e}_{2p}$ and $\mathbf{w}_{e2p}$, respectively. We can obtain the following equation from (12):

$$\mathbf{e}_{2p} = \alpha h_{\mathrm{sr}} g_{\mathrm{re}} \sqrt{P_s P_r} \mathbf{p} + \mathbf{w}_{e2p}. \tag{47}$$

Define the combined channel $g_{\mathrm{sre}} = h_{\mathrm{sr}} g_{\mathrm{re}}$. Clearly, $E(g_{\mathrm{sre}}) = 0$ and the variance of g_{sre} is $\sigma_{\mathrm{sre}}^2 = \sigma_{\mathrm{sr}}^2 \sigma_{\mathrm{re}}^2$.

We can obtain the estimate of the combined channel g_{sre} with the LMMSE method as

$$\hat{g}_{\mathrm{sre}} = \frac{\alpha \sigma_{\mathrm{sre}}^2 \sqrt{P_s P_r} \mathbf{p}^H \mathbf{e}_{2p}}{\alpha^2 \sigma_{\mathrm{sre}}^2 P_s P_r \mathbf{p}^H \mathbf{p} + N_{\mathrm{sre}}}. \tag{48}$$

Also, we can have $E(\hat{h}_{\mathrm{sre}}) = 0$ and the variance of the channel estimate $\hat{h}_{\mathrm{sre}}$ is

$$\varsigma_{\mathrm{sre}}^2 = \frac{\alpha^2 \sigma_{\mathrm{sre}}^4 P_s P_r \mathbf{p}^H \mathbf{p}}{\alpha^2 \sigma_{\mathrm{sre}}^2 P_s P_r \mathbf{p}^H \mathbf{p} + N_{\mathrm{sre}}}. \tag{49}$$

The estimation error of the combined channel g_{sre} is

$$\begin{aligned}\epsilon_{\mathrm{sre}} &= \hat{g}_{\mathrm{sre}} - g_{\mathrm{sre}} \\ &= \frac{\alpha \sigma_{\mathrm{sre}}^2 \sqrt{P_s P_r} \mathbf{p}^H \mathbf{e}_{d2p} - h_{\mathrm{sre}} N_{\mathrm{sre}}}{\alpha^2 \sigma_{\mathrm{sre}}^2 P_s P_r \mathbf{p}^H \mathbf{p} + N_{\mathrm{sre}}}.\end{aligned} \tag{50}$$

Clearly, $E(\epsilon_{\mathrm{sre}}) = 0$ and the variance of the channel estimation error ϵ_{sre} is

$$\varrho_{\mathrm{sre}}^2 = \frac{\sigma_{\mathrm{sre}}^2 N_{\mathrm{sre}}}{\alpha^2 \sigma_{\mathrm{sre}}^2 P_s P_r \mathbf{p}^H \mathbf{p} + N_{\mathrm{sre}}}. \tag{51}$$

To perform data detection with the estimate, Equation 7 will be rewritten as

$$e_2(n) = \alpha \hat{g}_{\mathrm{sre}} \sqrt{P_s P_r} s(n) - \alpha \epsilon_{\mathrm{sre}} \sqrt{P_s P_r} s(n) + w_{\mathrm{sre}}(n), \tag{52}$$

for $n \in \mathcal{T}_d$.

4.2.3 *Channel capacity*

From (46) we can find the capacity of the direct channel h_{se} as

$$C_{\mathrm{se}} = \frac{M}{L_{slot}} \log_2 \left(1 + \frac{|\hat{g}_{\mathrm{se}}|^2 P_s}{|\epsilon_{\mathrm{se}}|^2 P_s + N_0} \right) \tag{53}$$

In addition, from (52) we can obtain the capacity of the AF relay channel h_{sre} as

$$C_{\mathrm{sre}} = \frac{M}{L_{slot}} \log_2 \left(1 + \frac{\alpha^2 |\hat{g}_{\mathrm{sre}}|^2 P_r P_s}{\alpha^2 |\epsilon_{\mathrm{sre}}|^2 P_r P_s + N_{\mathrm{sre}}} \right). \tag{54}$$

Similar to the derivation of (40), the total capacity achievable at the eavesdropper can be approximated as

$$C_e \approx P_{\emptyset}(1 - P_f) \max(C_{\mathrm{se}}, C_{\mathrm{sre}}). \tag{55}$$

5 Security-reliability performance

5.1 Outage probability

When the channel capacity becomes less than the data rate R, the destination node is unable to recover the source signal and an outage event will occur in this case. Thus, the outage probability of the main links is given as

$$\begin{aligned}P_{out}^{(R)} &= \Pr\left(P_{\emptyset}(1 - P_f) C_d < R\right) \\ &= \Pr\left(\max(C_{\mathrm{sd}}, C_{\mathrm{srd}}) < \frac{R}{P_{\emptyset}(1 - P_f)}\right) \\ &= \Pr\left(C_{\mathrm{sd}} < \frac{R}{P_{\emptyset}(1 - P_f)}\right) \Pr\left(C_{\mathrm{srd}} < \frac{R}{P_{\emptyset}(1 - P_f)}\right).\end{aligned} \tag{56}$$

The first part in (56) can be found as

$$\begin{aligned}\Pr\left(C_{\mathrm{sd}} < \frac{R}{P_{\emptyset}(1 - P_f)}\right) &= \Pr\left(\frac{|\hat{h}_{\mathrm{sd}}|^2 P_s}{|\epsilon_{\mathrm{sd}}|^2 P_s + N_0} < \kappa_1\right) \\ &= \Pr(|\hat{h}_{\mathrm{sd}}|^2 < \kappa_1 |\epsilon_{\mathrm{sd}}|^2 + \kappa_1/\gamma_s),\end{aligned} \tag{57}$$

where $\kappa_1 = 2^{\frac{RL_{slot}}{MP_{\emptyset}(1-P_f)}} - 1$ and $\gamma_s = P_s/N_0$. Note that both $|\hat{h}_{\mathrm{sd}}|^2$ and $|\epsilon_{\mathrm{sd}}|^2$ follow exponential distribution; we can thus find

$$\begin{aligned}\Pr\left(C_{\mathrm{sd}} < \frac{R}{P_{\emptyset}(1 - P_f)}\right) &= \int_0^{\infty} \frac{1}{\varrho_{\mathrm{sd}}^2} \exp\left(-\frac{y}{\varrho_{\mathrm{sd}}^2}\right) dy \\ &\quad \int_0^{\kappa_1 y + \kappa_1/\gamma_s} \frac{1}{\varsigma_{\mathrm{sd}}^2} \exp\left(-\frac{x}{\varsigma_{\mathrm{sd}}^2}\right) dx\end{aligned} \tag{58}$$

After several straight mathematical calculations, we can obtain

$$\Pr\left(C_{\mathrm{sd}} < \frac{R}{P_{\emptyset}(1 - P_f)}\right) = 1 - \frac{\exp\left(-\frac{\kappa_1}{\gamma_s \varsigma_{\mathrm{sd}}^2}\right)}{1 + \kappa_1 \varrho_{\mathrm{sd}}^2 / \varsigma_{\mathrm{sd}}^2}. \tag{59}$$

Substituting (24) and (27) into (59) will give

$$\Pr\left(C_{\text{sd}} < \frac{R}{P_{\emptyset}(1-P_f)}\right) = 1 - \frac{\exp\left(-\frac{\kappa_1}{\gamma_s \varsigma_{\text{sd}}^2}\right)}{1+\kappa_1/(\gamma_s \sigma_{\text{sd}}^2 \mathbf{p}^H \mathbf{p})}. \tag{60}$$

Using (38), we can find the second part in (56) as

$$\begin{aligned}\Pr\left(C_{\text{srd}} < \frac{R}{P_{\emptyset}(1-P_f)}\right) &= \Pr\left(\frac{|\hat{h}_{\text{srd}}|^2 P_r P_s}{|\epsilon_{\text{srd}}|^2 P_r P_s + N_{\text{srd}}} < \kappa_1\right)\\ &= \Pr\left(|\hat{h}_{\text{srd}}|^2 < \kappa_1 |\epsilon_{\text{srd}}|^2 + \kappa_1/\gamma_r\right),\end{aligned} \tag{61}$$

where $\gamma_r = \alpha^2 P_r P_s / N_{\text{srd}}$. Considering that both $|\hat{h}_{\text{sd}}|^2$ and $|\epsilon_{\text{sd}}|^2$ follow exponential distribution, we can further obtain

$$\begin{aligned}\Pr\left(C_{\text{srd}} < \frac{R}{P_{\emptyset}(1-P_f)}\right) &= \int_0^{\infty} \frac{1}{\varrho_{\text{srd}}^2} \exp\left(-\frac{y}{\varrho_{\text{srd}}^2}\right) dy\\ &\quad \int_0^{\kappa_1 y + \kappa_1/\gamma_r} \frac{1}{\varsigma_{\text{srd}}^2} \exp\left(-\frac{x}{\varsigma_{\text{srd}}^2}\right) dx.\end{aligned} \tag{62}$$

After straight calculation steps, we can get

$$\Pr\left(C_{\text{srd}} < \frac{R}{P_{\emptyset}(1-P_f)}\right) = 1 - \frac{\exp\left(-\frac{\kappa_1}{\gamma_r \varsigma_{\text{srd}}^2}\right)}{1+\kappa_1 \varrho_{\text{srd}}^2/\varsigma_{\text{srd}}^2}. \tag{63}$$

Substituting (32) and (34) into (63) will produce

$$\Pr\left(C_{\text{srd}} < \frac{R}{P_{\emptyset}(1-P_f)}\right) = 1 - \frac{\exp\left(-\frac{\kappa_1}{\gamma_r \varsigma_{\text{srd}}^2}\right)}{1+\kappa_1/\left(\gamma_r \varsigma_{\text{srd}}^2 \mathbf{p}^H \mathbf{p}\right)}. \tag{64}$$

Finally, the outage probability can be obtained as

$$P_{out}^{(R)} = \left(1 - \frac{\exp\left(-\frac{\kappa_1}{\gamma_s \varsigma_{\text{sd}}^2}\right)}{1+\kappa_1/(\gamma_s \sigma_{\text{sd}}^2 \mathbf{p}^H \mathbf{p})}\right)\left(1 - \frac{\exp\left(-\frac{\kappa_1}{\gamma_r \varsigma_{\text{srd}}^2}\right)}{1+\kappa_1/(\gamma_r \varsigma_{\text{srd}}^2 \mathbf{p}^H \mathbf{p})}\right) \tag{65}$$

5.2 Intercept probability

If the wiretap channel capacity is greater than the data rate, the eavesdropper is able to decode the source message. Thus, an intercept event happens when the wiretap channel capacity becomes larger than the data rate R. Hence, the intercept probability for both channels h_{se} and h_{sre} is

$$\begin{aligned}P_{\text{int}}^{(R)} &= \Pr\left(\max(C_{\text{se}}, C_{\text{sre}}) > \frac{R}{P_{\emptyset}(1-P_f)}\right)\\ &= 1 - \Pr\left(C_{\text{se}} < \frac{R}{P_{\emptyset}(1-P_f)}\right) \Pr\left(C_{\text{sre}} < \frac{R}{P_{\emptyset}(1-P_f)}\right).\end{aligned} \tag{66}$$

With the same process in obtaining (60), we can find

$$\Pr\left(C_{\text{se}} < \frac{R}{P_{\emptyset}(1-P_f)}\right) = 1 - \frac{\exp\left(-\frac{\kappa_1}{\gamma_s \varsigma_{\text{se}}^2}\right)}{1+\kappa_1/(\gamma_s \sigma_{\text{se}}^2 \mathbf{p}^H \mathbf{p})}. \tag{67}$$

Also, using the same method in finding (64), we can obtain

$$\Pr\left(C_{\text{sre}} < \frac{R}{P_{\emptyset}(1-P_f)}\right) = 1 - \frac{\exp\left(-\frac{\kappa_1}{\gamma_e \varsigma_{\text{sre}}^2}\right)}{1+\kappa_1/(\gamma_e \sigma_{\text{sre}}^2 \mathbf{p}^H \mathbf{p})}, \tag{68}$$

where $\gamma_e = \alpha^2 P_r P_s / N_{\text{sre}}$.

Finally, the intercept probability can be obtained as

$$\begin{aligned}P_{\text{int}}^{(R)} &= 1 - \left(1 - \frac{\exp\left(-\frac{\kappa_1}{\gamma_s \varsigma_{\text{se}}^2}\right)}{1+\kappa_1/(\gamma_s \sigma_{\text{se}}^2 \mathbf{p}^H \mathbf{p})}\right)\\ &\quad \times \left(1 - \frac{\exp\left(-\frac{\kappa_1}{\gamma_e \varsigma_{\text{sre}}^2}\right)}{1+\kappa_1/(\gamma_e \sigma_{\text{sre}}^2 \mathbf{p}^H \mathbf{p})}\right).\end{aligned} \tag{69}$$

5.3 Approximation

When $\mathbf{p}^H \mathbf{p} \gg N_0$ or at high SNR, i.e., $P_s \gg N_0$ and $P_r \gg N_0$, we can have the following approximation:

$$\varsigma_{\text{sd}}^2 \approx \sigma_{\text{sd}}^2, \quad \varsigma_{\text{se}}^2 \approx \sigma_{\text{se}}^2, \quad \varsigma_{\text{srd}}^2 \approx \sigma_{\text{srd}}^2, \quad \varsigma_{\text{sre}}^2 \approx \sigma_{\text{sre}}^2.$$

Suppose BSPK or QPSK modulation is adopted, and thus, $\mathbf{p}^H \mathbf{p} = K$. Also assume that

$$\sigma_{\text{sd}}^2 = \sigma_{\text{sr}}^2 = \sigma_{\text{rd}}^2 = \sigma_h^2, \quad \sigma_{\text{se}}^2 = \sigma_{\text{re}}^2 = \sigma_g^2. \tag{70}$$

Therefore, we can rewrite the outage probability and intercept probability as

$$P_{\mathrm{out}}^{(R)} = \left(1 - \frac{\exp\left(-\frac{\kappa_1}{\gamma_s \sigma_h^2}\right)}{1 + \frac{\kappa_1}{\gamma_s \sigma_h^2 K}}\right)\left(1 - \frac{\exp\left(-\frac{\kappa_1}{\gamma_r \sigma_h^4}\right)}{1 + \frac{\kappa_1}{\gamma_r \sigma_h^4 K}}\right), \tag{71}$$

$$P_{\mathrm{int}}^{(R)} = 1 - \left(1 - \frac{\exp\left(-\frac{\kappa_1}{\gamma_s \sigma_g^2}\right)}{1 + \frac{\kappa_1}{\gamma_s \sigma_g^2 K}}\right)\left(1 - \frac{\exp\left(-\frac{\kappa_1}{\gamma_e \sigma_g^4}\right)}{1 + \frac{\kappa_1}{\gamma_e \sigma_g^4 K}}\right). \tag{72}$$

5.4 Comparison with direct channel

If there is no relay, that is, there are only two channels h_{sd} and g_{se}, the outage probability and intercept probability can be found as

$$P_{out}^{(D)} = 1 - \frac{\exp\left(-\frac{\kappa_2}{\gamma_s \varsigma_{\mathrm{sd}}^2}\right)}{1 + \kappa_2/(\gamma_s \sigma_{\mathrm{sd}}^2 \mathbf{p}^H \mathbf{p})}, \tag{73}$$

$$P_{\mathrm{int}}^{(D)} = \frac{\exp\left(-\frac{\kappa_2}{\gamma_s \varsigma_{\mathrm{se}}^2}\right)}{1 + \kappa_2/(\gamma_s \sigma_{\mathrm{se}}^2 \mathbf{p}^H \mathbf{p})}, \tag{74}$$

where $\kappa_2 = 2^{\frac{RL_{slot}}{MP_{\emptyset}(1-P_f)}} - 1$. Please refer to [27] for the detailed derivation process.

When $\mathbf{p}^H \mathbf{p} \gg N_0$ or at high SNR, we can further simplify (73) and (74) as

$$P_{out}^{(D)} = 1 - \frac{\exp\left(-\frac{\kappa_2}{\gamma_s \sigma_h^2}\right)}{1 + \frac{\kappa_2}{\gamma_s \sigma_h^2 K}}, \tag{75}$$

$$P_{\mathrm{int}}^{(D)} = \frac{\exp\left(-\frac{\kappa_2}{\gamma_s \sigma_g^2}\right)}{1 + \frac{\kappa_2}{\gamma_s \sigma_g^2 K}}. \tag{76}$$

Proposition 1. The outage probability for the relay-based transmission is larger than that for direct transmission, while the intercept probability for the relay-based transmission is smaller than that for direct transmission.

$$P_{out}^{(R)} > P_{out}^{(D)}, \quad P_{\mathrm{int}}^{(R)} < P_{\mathrm{int}}^{(D)}. \tag{77}$$

Proposition 2. Suppose the total probability is the sum of the outage probability and the intercept probability and is a function of data rate R. The minimum value of the total probability for the relay-based transmission is less than that for direct transmission, i.e.,

$$\min_R \left(P_{out}^{(R)} + P_{\mathrm{int}}^{(R)}\right) < \min_R \left(P_{out}^{(D)} + P_{\mathrm{int}}^{(D)}\right). \tag{78}$$

Note that the sum of the outage probability and the intercept probability $P_{out}^{(R)} + P_{\mathrm{out}}^{(R)}$ can be considered as a parameter to measure the overall performance. It needs to be pointed out that the strictly mathematical proof of the two propositions is challenging; however, they can be numerically verified through computer simulations[a].

6 Simulation results

In this section, we numerically evaluate both the security and reliability performance of the cognitive relay system with channel estimation error. Let us fix the slot length $L_{slot} = 1{,}000$ and sensing duration $S = 2$ and choose the threshold of the energy detector $\lambda_{ED} = 9.2$ so that the false alarm probability in (17) $P_f = 0.01$.

First, we set $K = 10, P_s = P_r = 1{,}000, N_0 = 1, \sigma_{\mathrm{sd}}^2 = \sigma_{\mathrm{sr}}^2 = \sigma_{\mathrm{rd}}^2 = 8$, and $\sigma_{\mathrm{se}}^2 = \sigma_{\mathrm{re}}^2 = 2$. Increasing the data rate R from 0 to 12 bps/Hz, we can obtain the outage probability and the intercept probability from (65) and (69), respectively. For comparison, the outage probability and the intercept probability of direct transmission without relay are also found from (73) and (74). The outage probability and intercept probability versus data rate R is plotted in Figure 3. The sum of outage probability and intercept probability versus data rate R in the case of one relay and no relay is also plotted in Figure 4.

Second, we increase the transmission power $P_s = P_r$ from 0 to 1,000 and increase the number of training symbols K from 1 to 100, and then we can find the minimum value of the probability sum for the relay-based transmission and direct transmission, respectively. The minimum

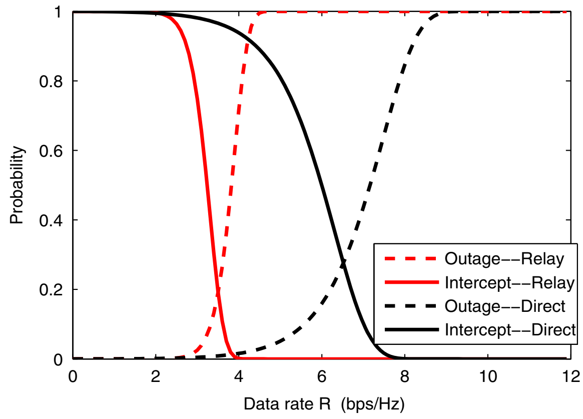

Figure 3 Outage probability and intercept probability versus data rate *R*.

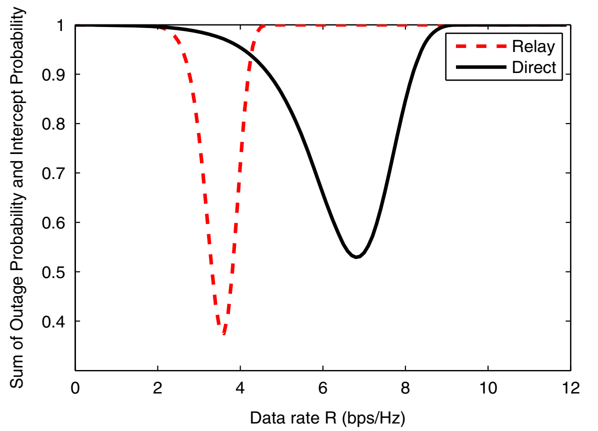

Figure 4 Sum of outage probability and intercept probability versus data rate *R*.

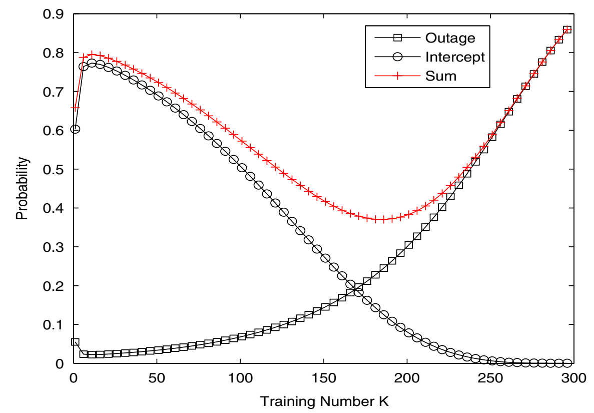

Figure 6 Outage probability and intercept probability versus the number of training symbols *K*.

sum of the outage probability and the intercept probability versus the transmission power and the training number is plotted in Figure 5. It can be seen that the relay-base transmission system can obtain lower probability sum than the direct transmission system, which implies better joint security and reliability performance of the relay-based transmission system than the direct transmission system.

Next, we increase the number of training symbols K from 1 to 300 and obtain the outage probability and the intercept probability from (65) and (69), respectively. Figure 6 plots the outage probability, the intercept probability, and the sum of the two probabilities versus the training number K. The increasing value of the training number K will result in less data symbols M and thus reduced channel capacity C_d. Therefore, given data rate R, the outage probability will increase while the intercept probability will decrease with the larger training number K. However, it can be seen from Figure 6 that the sum of the outage probability and the intercept probability first decreases and then increases when the training number K increases from 1 to 400. Clearly, there exists an optimal value of K so that the probability sum can be minimized.

We also examine the approximation performance of the outage probability and the intercept probability. The approximate value and the exact value for the outage probability are obtained from (71) and (65), respectively. So are those for the intercept probability from (72) and (69). Figure 7 shows the nice agreement of approximate values with theoretical ones.

7 Conclusion

This paper evaluated both the security and the reliability performance of the cognitive amplify-and-forward (AF) relay system in the presence of the channel estimation error. Specifically, LMMSE is utilized by the destination node and the eavesdropper node to obtain the CSI, and the closed form for the outage probability and that for the intercept probability are derived. Based on these, the security and the reliability performance were evaluated

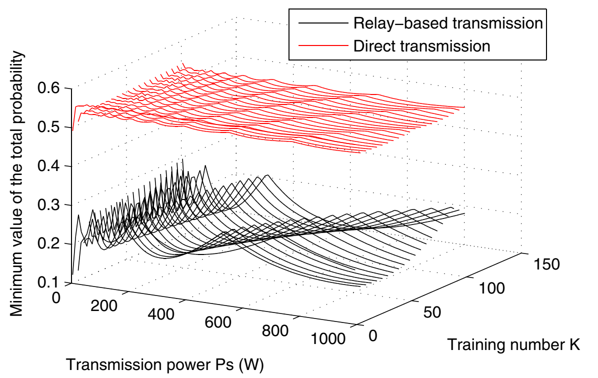

Figure 5 The minimum value of the total probability for relay-based transmission and direct transmission.

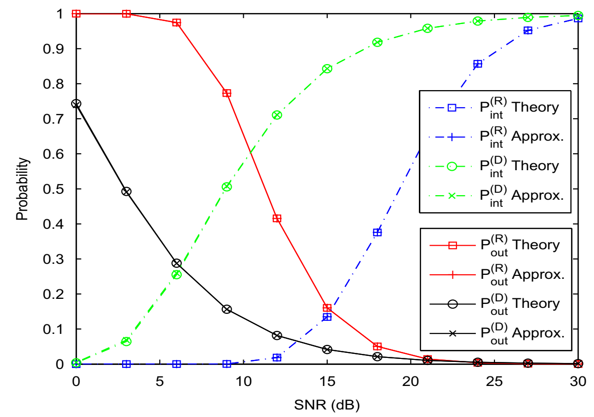

Figure 7 Theoretical and approximate outage/intercept probability versus SNR.

in the form of the outage probability and the intercept probability, respectively. It was shown that the transmission security (reliability) could be improved by loosening the reliability (security) requirement. Moreover, the security and the reliability performance of this relay-based system were compared with those of the direct communication system without relay. Interestingly, it was found that the AF relay-based system has less reliability performance than the direct system; however, it can lower the sum of the outage probability and the intercept probability than the direct system. It was also found that there exists an optimal training number to minimize the sum of the outage probability and the intercept probability.

Endnote

[a] This is the reason for the name of proposition, instead of theorem.

Competing interests

The authors declare that they have no competing interests.

Acknowledgements

This study is supported in part by the Key Laboratory of Universal Wireless Communications, Ministry of Education, China. This study is also supported in part by the National Natural Science Foundation of China (No. 61201202, No. 61372116, and No. 61071077) and by Tsinghua-Tencent Joint Laboratory for Internet Innovation Technology.

Author details

[1]School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China. [2]State Key Laboratory of Information Photonics and Optical Communications, School of Digital Media and Design Arts, Beijing University of Posts and Telecommunications, Beijing 100876, China. [3]School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China.

Received: 23 November 2013 Accepted: 29 January 2014
Published: 5 March 2014

References

1. S Haykin, Cognitive radio: brain-empowered wireless communications. IEEE J. Sel. Areas Commun. **23**(2), 201–220 (2005)
2. J Mitola, Cognitive radio for flexible mobile multimedia communications, in *Proc. IEEE International Workshop on Mobile Multimedia Communications (MoMuC)*, (San Diego, CA, Nov. 1999), pp. 3–10
3. J Mitola, *Cognitive radio: an integrated agent architecture for software defined radio*. Ph.D. dissertation, KTH Royal Institute of Technology, 2000
4. FCC, 2003, ET Docket No. 03-222, No.ice of proposed rule making and order. Tech. Rep., December, 2003
5. P Kolotzy, Next generation communications: kickoff meeting, in *Proc. DARPA*, Vol. 10, (2001)
6. H Urkowitz, Energy detection of unknown deterministic signals. Proc. IEEE. **55**(4), 523–531 (1967)
7. WA Gardner, CM Spooner, Signal interception: performance advantages of cyclic-feature detectors. IEEE Trans. Commun. **40**, 149–159 (1992)
8. JN Laneman, DNC Tse, GW Wornell, Cooperative diversity in wireless networks: efficient protocols and outage behavior. IEEE Trans. Inf. Theory. **50**(12), 3062–3080 (2004)
9. TE Hunter, S Sanayei, A Nosratinia, Outage analysis of coded cooperation. IEEE Trans. Inf. Theory. **52**(2), 375–391 (2006)
10. Y Zou, B Zheng, J Zhu, Outage analysis of opportunistic cooperation over Rayleigh fading channels. IEEE Trans. Wireless Commun. **8**(6), 3077–3385 (2009)
11. A Bletsas, H Shin, MZ Win, A Lippman, A simple cooperative diversity method based on network path selection. IEEE J. Sel. Areas Commun. **24**(3), 659–672 (2006)
12. A Khisti, GW Wornell, Secure transmission with multiple antennas: the MISOME wiretap channel. IEEE Trans. Inf. Theory. **56**(7), 3088–3104 (2010)
13. F Oggier, B Hassibi, The secrecy capacity of the MIMO wiretap channel. IEEE Trans. Inf. Theory. **57**(8), 4961–4972 (2011)
14. L Dong, Z Han, AP Petropulu, HV Poor, Improving wireless physical layer security via cooperating relays. IEEE Trans. Signal Process. **58**(3), 1875–1888 (2010)
15. AD Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)
16. SK Leung-Yan-Cheong, ME Hellman, The Gaussian wiretap channel. IEEE Trans Inf. Theory. **24**, 451–456 (1978)
17. Y Zou, X Wang, W Shen, L Hanzo, Security versus reliability analysis of opportunistic relaying. 10.1109/TVT.2013.2292903
18. C Xing, M Xia, F Gao, Y Wu, Robust transceiver with Tomlinson-Harashima precoding for amplify-and-forward MIMO relaying systems. IEEE J. Sel. Areas Commun. **30**(8), 1370–1382 (2012)
19. C Xing, S Ma, Z Fei, Y Wu, H Vincent Poor, A general robust linear transceiver design for multi-hop amplify-and-forward MIMO relaying systems. IEEE Trans Signal Process. **61**(5), 1196–1209 (2013)
20. J Cavers, An analysis of training symbol assisted modulation for Rayleigh fading channels [mobile radio]. IEEE Trans. Veh. Technol. **40**(4), 686–693 (1991)
21. Y Zou, YD Yao, B Zheng, Cognitive transmissions with multiple relays in cognitive radio networks. IEEE Trans. Wireless Commun. **10**(2), 648–659 (2011)
22. SM Kay, *Fundamentals of Statistical Signal Processing: Detection Theory*. (Prentice-Hall, Englewood Cliffs, 1993)
23. M Abramowitz, IA Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*. (Dover, New York, 1972)
24. SM Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. (Prentice-Hall, Englewood Cliffs, 1993)
25. B Hassibi, B Hochwald, How much training is needed in multiple-antenna wireless links. IEEE Trans. Inf. Theory. **49**(4), 951–963 (2003)
26. G Wang, Y Zou, J Lu, C Tellambura, Cognitive transmission and performance analysis for amplify-and-forward two-way relay networks, in *Proc. IEEE ICC*, (Sydney, June 2014), pp. 1–6
27. G Wang, Y Zou, F Gao, Z Zhong, Secuirity-reliability tradeoff for secure wireless communications with channel estimation error, in *Proc. IEEE HMWC*, (Shanghai, Nov. 2013), pp. 1–4

doi:10.1186/1687-6180-2014-28
Cite this article as: Gu *et al.*: Security-reliability performance of cognitive AF relay-based wireless communication system with channel estimation error. *EURASIP Journal on Advances in Signal Processing* 2014 **2014**:28.