Relay Selection for Security Enhancement in Cognitive Relay Networks


Published in:
IEEE Wireless Communications Letters

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal

Publisher rights
©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.

General rights
Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.
Relay Selection for Security Enhancement in Cognitive Relay Networks

Yuanwei Liu, Lifeng Wang, Tran Trung Duy, Maged Elkashlan, and Trung Q. Duong

Abstract—This letter proposes several relay selection policies for secure communication in cognitive decode-and-forward (DF) relay networks, where a pair of cognitive relays are opportunistically selected for security protection against eavesdropping. The first relay transmits the secrecy information to the destination, and the second relay, as a friendly jammer, transmits the jamming signal to confound the eavesdropper. We present new exact closed-form expressions for the secrecy outage probability. Our analysis and simulation results strongly support our conclusion that the proposed relay selection policies can enhance the performance of secure cognitive radio. We also confirm that the error floor phenomenon is created in the absence of jamming.

Index Terms—Cognitive radio, cooperative networks, physical layer security

I. INTRODUCTION

Cognitive radio networks are confronted with new privacy and security risks, due to the broadcast nature of wireless channels. Such security threats of eavesdropping are further escalated by the distributed nature of future multi-tier cognitive radio deployments. Physical (PHY) layer security, as an appealing approach to achieve secure transmission, has aroused wide-spread interest [1]. With this in mind, PHY layer security has been considered in cognitive radio networks [2]. Also, several recent efforts have considered PHY layer security in cooperative communications [3–8]. Among them [3] introduced cooperative transmission for security enhancement with single antenna and with multiple antennas. In [4], several cooperative relaying schemes were proposed to increase the secrecy rate, including decode-and-forward (DF), amplify-and-forward (AF), and cooperative jamming (CJ). In [5], collaborative relay weights for CJ were optimized to maximize the secrecy rate. In [6], two secrecy transmission schemes were proposed in opportunistic relaying. Joint relay and jammer selection for security enhancement was examined in one-way DF relay networks [7] and in two-way AF relay networks [8], where jamming was considered as a useful approach to resist security attacks.

Contrary to previous efforts, we focus on the security of cognitive relay networks where the transmit power of the cognitive relay is constrained. In this network, a pair of cognitive relays are selected. The first relay, as a helper, transmits the confidential messages to the legitimate destination, while the malicious eavesdropper tries to overhear the communication.

The second relay, as a friendly jammer, transmits a jamming signal to corrupt the received signals at the eavesdropper. Our contributions are at least two-fold: 1) we propose and compare four relay selection policies, namely random relay and random jammer (RRRJ), random jammer and best relay (RJBR), best relay and best jammer (BRBJ), and best relay and no jammer (BRNJ); and 2) we characterize the joint impact of the proposed relay selection policies and the interference power constraint on the secrecy performance by deriving new exact closed-form expressions for the secrecy outage probability. We show that the proposed policies offer a secrecy performance/implementation trade-off. We also show that the absence of the jammer gives rise to the outage saturation phenomenon.

II. NETWORK MODEL

We consider the secure communication in a cognitive relay network consisting of one secondary user (SU) source (S), M + 1 DF cognitive relays \( \{ R_m \} \) \( (m = 1, 2, \ldots, M + 1) \), one primary user (PU) receiver (P), one SU destination (D), and one eavesdropper (E). All the nodes are equipped with a single antenna and operate in half-duplex mode. In such a network, the cognitive relays are allowed to share the same spectrum as the PU under interference power constraint. Because of the absence of the direct links, the signal transmitted by S cannot be received by the eavesdropper, hence the transmission during broadcast phase is secure. Assuming that the source and the relays are located in the same cluster, yielding high received SNRs at the DF relays for successful decoding of messages [7], we concentrate on the cooperative phase in the presence of eavesdropping\(^1\). A pair of relays are selected among \( M + 1 \) relays, such that the first relay, denoted as \( R_m \), transmits the secrecy information; and the second relay, denoted as \( R_j \), transmits the jamming signal as a jammer. We consider the active eavesdropper scenario where the channel state information (CSI) between the relays and the eavesdropper is available\(^2\) [4, 9]. Such a scenario is particularly applicable in multicast and unicast networks where the users play dual roles as legitimate receivers for some signals and eavesdroppers for others [4].

All the channels are subject to slow, flat, block Rayleigh fading, where the fading coefficients are constant during a codeword transmission. Let us denote \( \gamma_{m}^{D}, \gamma_{m}^{P} \), and \( \gamma_{m}^{E} \) as the channel power gains of \( R_m \rightarrow D \), \( R_m \rightarrow P \), and \( R_m \rightarrow E \) links, respectively. The channel power gains \( \gamma_{m}^{D}, \gamma_{m}^{P}, \) and \( \gamma_{m}^{E} \)

\(^1\)In DF relay networks, the transmission of the broadcast phase has little effect on our proposed schemes of the secure transmission in the cooperative phase.

\(^2\)The CSI among all the nodes can be obtained at the SU source with the assistance of the relays.
Based on (2) and (3), the secrecy rate is expressed as \[7–9\] secrecy outage probability. These new results will enable us to find that increasing the instantaneous received SNR at the destination increases the secrecy rate. On the other hand, decreasing the instantaneous received SNIR at the eavesdropper increases the secrecy rate. With this in mind, we propose and analyze four different relay selection policies in cognitive relay networks, namely random relay and random jammer (RRRJ), random jammer and best relay (RJBR), best relay and best jammer (BRBJ), and best relay and no jammer (BRNJ).

A. Random Relay and Random Jammer (RRRJ)

We first consider the RRRJ policy as a baseline for comparison purposes. In this case, the relay \( R_c \) and the jammer \( R_j \) are selected randomly. As such, the secrecy outage probability for RRRJ is formulated as

\[
P_{\text{out}}^{\text{RRRJ}} = \Pr (I_{RRRJ} < R_{\text{th}}) = \Pr \left( \frac{1 + \alpha Q_T \gamma_c^p / \gamma_c^p}{\gamma_c^p (1 + (1 - \alpha) Q_T \gamma_j^p / \gamma_j^p)} < \rho \right),
\]

where \( R_{\text{th}} \) is the expected secrecy rate and \( \rho = 2^{R_{\text{th}}} \).

**Theorem 1:** The secrecy outage probability for RRRJ is given by

\[
P_{\text{out}}^{\text{RRRJ}} = \frac{\omega_1 \lambda_E (1 - \omega_2) \lambda_E (1 - \omega_3) + \lambda_E \lambda_R \rho \omega_2}{\lambda_E (1 - \omega_3) + \lambda_E \rho} \ln \left( \frac{\lambda_E + \lambda_E \rho}{\lambda_E \omega_2} \right),
\]

where \( \omega_1 = \lambda_E \alpha Q_T / (\lambda_E \alpha Q_T + \lambda_E (\rho - 1)) \) and \( \omega_2 = \lambda_E (1 - \alpha) Q_T / \lambda_E \).

**Proof:** See Appendix A.

From (6), we see that the secrecy outage probability for RRRJ is independent of the number of relays.

B. Random Jammer and Best Relay (RJBR)

In this policy, we first select a random jammer \( R_j \). Without loss of the generality, we assume that the jammer is \( R_j = R_{m+1} \). As such, the instantaneous secrecy rate at the relay \( R_m (m = 1, 2, \ldots, M) \) is calculated as

\[
P_{\text{out}}^{\text{RJBR}} = \Pr \left( \max_{m=1,2,\ldots,M} \left( \frac{1 + \alpha Q_T \gamma_m^p / \gamma_m^p}{1 + \frac{\alpha Q_T \gamma_m^p}{\gamma_m^p (1 + Y_1)}} \right) < \rho \right).
\]

**Theorem 2:** The secrecy outage probability for RJBR is given by

\[
P_{\text{out}}^{\text{RJBR}} = (1 - \omega_1)^M + \sum_{m=1}^{M} \left( \frac{M}{m} \right) (1 - \omega_1)^{M-m} \omega_2 (\omega_3 - 1)^m \times \left[ a_1 \ln \left( \frac{\omega_2}{\omega_3} \right) + \frac{a_2}{\omega_2} + \sum_{t=2}^{m} \frac{a_t}{(l - 1) (\omega_3)^{l-1}} \right],
\]

where \( \omega_3 = 1 + \lambda_E / \lambda_E, a_1 = \frac{m}{(\omega_3 - \omega_2)^{m+1}}, a_2 = \frac{1}{(\omega_3 - \omega_2)^{m}} \), and \( a_t = \frac{\omega_2}{(\omega_3 - \omega_2)^{t+1}} \).

**Proof:** See Appendix B.
C. Best Relay and Best Jammer (BRBJ)

In this policy, we first select the best relay that maximizes the channel power gain between the relay and the destination. Without loss of generality, we assume that the best relay $R_c$ is $R_{M+1}$, i.e., $\gamma_{M+1} = \max_{m=1,2,\ldots,M+1} (\gamma_m)$. Then, the best jammer $R_j$ is selected among the remaining $M$ relays to maximize the interference power at the eavesdropper, such that $R_j = \arg\max_{m=1,2,\ldots,M} ((1 - \alpha) Q_t \gamma_{m} / \gamma_0)$. In such a policy, the instantaneous secrecy rate is expressed as

$$I_{BRBJ} = \log_2 \left( \frac{1 + \alpha Q_t Y_2 / \gamma_{M+1}^p}{1 + \alpha Q_t (1 + Y_3)} \right),$$

where $Y_2 = \max_{m=1,2,\ldots,M+1} (\gamma_{m})$ and $Y_3 = \max_{m=1,2,\ldots,M} ((1 - \alpha) Q_t \gamma_{m} / \gamma_0)$. Then, the secrecy outage probability for BRBJ is formulated as

$$P_{out}^{BRBJ} = \Pr \left( Y_2 < \frac{\rho - 1}{\alpha Q_t} \gamma_{M+1}^p + \rho \gamma_{M+1}^p / (1 + Y_3) \right).$$

**Theorem 3:** The secrecy outage probability for BRBJ is given in (12) at the top of next page, where $\vartheta = \frac{\alpha (1 - \omega_i + m \lambda_0)}{\lambda_0 + m \lambda_0}$ and $\mathcal{F}_1 (\cdot; \cdot; \cdot)$ is the Gauss hypergeometric function [12, Eq. (9.142)].

**Proof:** The proof can be done in the similar way as the proof of Theorem 1.

D. Best Relay and No Jammer (BRNJ)

In this policy, no jamming protection is utilized. As such, the instantaneous secrecy rate at relay $R_m$ ($m = 1, 2, \ldots, M + 1$) is calculated as

$$I_{BRNJ} = \log_2 \left( \frac{1 + Q_t Y_2 / \gamma_m^p}{1 + Q_t Y_2 / \gamma_m^p} \right).$$

The best relay $R_c$ is selected so as to maximize the secrecy rate, such that $R_c = \arg\max_{m=1,2,\ldots,M+1} I_{BRNJ}^m$. Therefore, the secrecy outage probability for BRNJ is derived as

$$P_{out}^{BRNJ} = \Pr \left( \max_{m=1,2,\ldots,M+1} \left( \frac{1 + Q_t \gamma_m^p / \gamma_0}{1 + Q_t \gamma_m^p / \gamma_0} < \rho \right) \right)\left( 1 - \frac{\lambda_0 \lambda_0}{\lambda_f} \right)^{M+1}.$$
After some manipulations, (A.1) is given by

\[
F_Z(\omega) = \frac{\lambda_\rho \alpha Q_\alpha + m \lambda_\rho (\rho - 1)}{\lambda_\rho \alpha Q_\alpha + m \lambda_\rho (\rho - 1)} \sum_{n=1}^{M} \binom{M}{n/n!} \int_0^\infty f_1(x) f_2(z) \, dx \, dz .
\]

(A.1)

Here, \( f_Z(z) \) is the PDF of \( Z \), we remind that the cumulative density function (CDF) and probability density function (PDF) of the random variables (RVs) \( \gamma_m^X, X \in \{D, P, E\} \) are

\[
F_m^X(x) = 1 - e^{-\lambda x} \quad \text{and} \quad f_m^X(x) = \lambda x e^{-\lambda x},
\]

respectively. By substituting the CDF \( F_m^X(x) \) and PDF \( f_m^X(x) \) into (A.1), after some manipulations, (A.1) is given by

\[
P_{\text{BBRJ}} = \int_0^\infty \left( 1 - \omega_1 e^{-\lambda \rho z} \right) f_Z(z) \, dz,
\]

(A.2)

where \( \omega_1 = \lambda_\rho \alpha Q_\alpha / (\lambda_\rho \alpha Q_\alpha + m \lambda_\rho (\rho - 1))\). To obtain \( f_Z(z) \), we first calculate the CDF of \( Y_1 \) as

\[
F_{Y_1}(y) = 1 - \frac{\sum_{n=1}^\infty \frac{(-1)^n \lambda_\rho}{n!} (\omega_2)^n}{1 + \omega_2},
\]

Taking the derivative of \( F_{Y_1}(y) \) with respect to \((w.r.t.) y\), we obtain the PDF of \( Y_1 \) as

\[
f_{Y_1}(y) = \frac{\omega_2}{(y + \omega_2)^2}.
\]

(A.3)

Then, the CDF of \( Z \) can be formulated as

\[
F_Z(z) = \int_0^\infty \left( 1 - e^{-\lambda(z+y)} \right) f_{Y_1}(y) \, dy.
\]

(A.4)

By substituting (A.3) into (A.4), the CDF of \( Z \) is derived as

\[
F_Z(z) = 1 - e^{-\lambda z} + \lambda_\rho \omega_2 e^{-\lambda_\rho (1+\omega_2)} f_1(\lambda_\rho \omega_2 z),
\]

(A.5)

where \( E_1(x) \) is the exponential integral function given by

\[
E_1(x) = \int_1^\infty e^{-zt} \frac{dz}{z^2}.
\]

Taking the derivative of \( F_Z(z) \) given in (A.5) \(w.r.t\ z\), we obtain the PDF of \( Z \). Then substituting the PDF of \( Z \) into (A.2) and using [12, Eq. (6.227.1)], we obtain the desired result in (6).

### Appendix B: Proof of Theorem 2

Based on (8), we first calculate the secrecy outage probability conditioned on \( Y_1 \) as

\[
P_{\text{out}}_{\text{BBRJ}}(Y_1) = \prod_{m=1}^M Pr\left( \frac{\gamma_m^p}{\alpha Q_\alpha} - 1 + Y_1 \right) (1 - \omega_1)^m + \sum_{m=1}^M \left( \frac{m \lambda_\rho (\omega_2)^m}{(Y_1 + \omega_3)^m} \right).
\]

(B.1)

The \( P_{\text{out}}_{\text{BBRJ}} \) is derived as

\[
P_{\text{out}}_{\text{BBRJ}} = \int_0^\infty f_{Y_1}(y) P_{\text{out}}_{\text{BBRJ}}(y) \, dy.
\]

(B.2)

Substituting (A.3) and (B.1) into (B.2), we get the desired result in (9).

### References


