Interference Neutralization vs Clean Relaying in Cognitive Radio Networks with Secrecy

Pin-Hsun Lin
Communications Laboratory
Faculty of Electrical and Computer Engineering
Technische Universitat Dresden, Dresden, Germany
Pin-Hsun.Lin@tu-dresden.de

Frédéric Gabry
Mathematics and Algorithmic Sciences Lab
Huawei France Research Center,Paris
frederic.gabry@huawei.com

Ragnar Thobaben
School of Electrical Engineering and the ACCESS Linnaeus Centre
KTH Royal Institute of Technology
Stockholm, Sweden
ragnar.thobaben@ee.kth.se

Eduard Jorswieck
Communications Laboratory
Faculty of Electrical and Computer Engineering
Technische Universitat Dresden, Dresden, Germany
Eduard.Jorswieck@tu-dresden.de

Mikael Skoglund
School of Electrical Engineering and the ACCESS Linnaeus Centre
KTH Royal Institute of Technology
Stockholm, Sweden
skoglund@kth.se

ABSTRACT

In this paper we study cognitive radio networks with secrecy constraints on the primary transmission. In particular we consider several transmission schemes for the secondary transmitter, namely interference neutralization (IN) and cooperative jamming with and without clean relaying (CR). We derive and analyze the achievable secondary rate performance of the schemes. Furthermore we thoroughly investigate the advantages and shortcomings of these schemes through numerical simulations in a geometric model where we highlight the impact of the users' locations and show the important difference in all schemes depending on the topology. Our results show that the secondary transmitter can successfully adapt its transmission scheme (and parameters), i.e., either IN or CR, depending on its location to maximize its rate while insuring perfect secrecy of the primary transmission.

Keywords

physical layer security, cognitive radio, jamming, interference neutralization, relaying

1. INTRODUCTION

Wireless networks have been developed considerably over the last few decades. As a consequence of the broadcast nature of these networks, transmissions can potentially be intercepted by malicious parties, and therefore, security plays a fundamental role in modern wireless communications. There exists a promising direction towards achieving secure communications, namely *information theoretic secrecy*. The information theoretic secrecy approach, developed by Wyner in [14], exploits randomness of the channel codewords to ensure the secrecy of the transmitted messages. As a performance measure for communication systems with secrecy constraints, the *secrecy rate* is defined as a rate at which the message can be transmitted reliably and securely between the legitimate nodes. However, similar to communication networks without secrecy constraints, the overall performance is limited by the channel conditions. In particular, the legitimate parties need to have some advantage over the eavesdropper in terms of channel quality to guarantee secure communications. Many techniques have been proposed to overcome this limitation, such as the use of multiple antenna systems in [10], [11]. To avoid the limitation from channel conditions, there has recently been a substantial interest on exploiting the potential *cooperation* between users to enhance the secrecy of communications [5]. We refer the readers to [1] for a summary of recent advances in the topic of cooperation for secrecy. Cognitive radio technology, introduced by Mitola in [9], proposes an efficient way to sense the spectrum, decode information from detected signals, and use this knowledge to improve the overall performance of communication systems. In cognitive radio networks, secondary users are allowed to use the licensed spectrum as long as they do not degrade the data transmission of the primary users, which are the legacy owners of the spectrum. In recent years, due to the growth of cognitive radio networks (CRN), security issues have been the subject of increasing attention for these networks. While traditional security threats such as jamming and media access control layer (MAC-layer) attacks exist, CRN-specific threats such as exogenous attackers or selfish/intruding nodes exploiting the vulnerability of *ad hoc* cognitive networks must be considered. For eavesdropping attacks, the concept of infor-

MOBIQUITOUS 2015, July 22-24, Coimbra, Portugal

DOI 10.4108/eai.22-7-2015.2260193

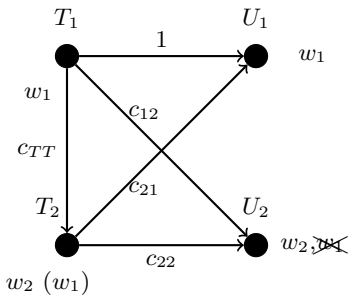

Figure 1: Cognitive channel with secrecy constraints.

mation theoretic secrecy and the corresponding cooperative techniques for secrecy can naturally be applied to cognitive radio networks. In [13], a scenario where an external eavesdropper attempts to decode the primary user's message is considered. In exchange of cooperation from the secondary user to improve its own secrecy rate, the primary user allows the secondary user a share of the spectrum. A different setup is investigated in [6]: the secondary user wants to keep its message confidential from the primary network. That is, the primary receiver is viewed as an eavesdropper from the secondary network perspective.

The concept of the wiretap channel can be applied to cognitive radio channels where the secondary receiver is treated as a potential eavesdropper to the primary transmission. The primary transmitter is assisted in the model by the trustworthy secondary transmitter if the cooperation could improve the secrecy performance, while the secondary transmitter benefits from being awarded a share of the spectrum for its data transmission. Therefore secrecy concerns lay the foundation of mutual cooperation between primary and secondary transmitters. In the present paper, we generalize this model introduced in [3] and we extend previous results in [7]. In particular, We consider the multi-phase signalling scheme where the secondary transmitter learns the primary message w_1 in the first phase. After successfully decoding w_1, the secondary transmitter implements two types of cooperation, namely cooperative jamming, introduced in [12], and relaying of the primary message. Moreover, we use the clean relaying (CR) scheme introduced in [8], where the secondary transmitter splits its transmission into the third phase in which its own message is not broadcasted (thus, the term "clean") to increase the efficiency of relaying/cooperative jamming. We compare clean relaying to another signalling schemes, namely pure cooperative jamming and interference neutralization, where for the latter scheme the secondary transmitter cancels out the primary message at the secondary receiver and hence guarantees perfect secrecy of the primary transmission.

This paper is organized as follows. In Section 2 we introduce our system model. In Section 3 we describe the transmission scheme and derive the achievable secrecy rates for different signalling strategies. Our theoretical results are investigated through numerical simulations in Section 4. Finally, Section 5 concludes this paper.

2. SYSTEM MODEL

2.1 Network Model

In this paper, we investigate the cognitive radio network as shown in Figure 1. The cognitive radio network consists of the following single antenna nodes: a primary transmitter T_1, a cognitive (secondary) transmitter T_2, a primary receiver U_1 and a secondary receiver U_2. T_1 (Alice) wishes to transmit the secret message w_1 to U_1 (Bob), which should be kept secret from U_2 (Eve) and therefore these three nodes form a wiretap channel. Meanwhile, T_2 wants to transmit message w_2 (without secrecy constraints) to the secondary receiver U_2. We assume that all nodes operate in *half duplex* mode. We also assume all channels are complex and static within a codeword length. We assume T_1 transmits at the rate equal to the wiretap channel capacity. We also assume that T_1 perfectly knows the channels from T_1 to U_1 and from T_1 to U_2, while T_2 knows all channels.

One of the possible practical scenarios of the considered model is that, the primary users belong to a licensed system, who sells rights of the spectrum usage to a femtocell system. Here we let the secondary transmitter and receiver as the femtocell base station and users, respectively. However, since the femtocell operator may not be able to guarantee the femtocell users are malicious or not, to provide a secrecy transmission to the primary users, not only the primary base station needs to use the wiretap coding, but also the femtocell base station needs to help to maintain that secrecy transmission for the primary system, which is included into the secure coexistence condition and will be discussed later.

2.2 Transmission Model, Schemes, and Notations

In this paper we consider the following three-phase transmission scheme for the secondary user. The ratios of the intervals of each phase to a codeword are defined as η_1, η_2, and η_3[1], respectively. Assume the time index $t \in \mathbb{N}$. We define the corresponding intervals of the three phases as the following three sets $\mathsf{T}_1 = \{t : 1 \leq t \leq \lfloor \eta_1 n \rfloor\}$, $\mathsf{T}_2 = \{t : \lfloor \eta_1 n \rfloor + 1 \leq t \leq \lfloor (\eta_1 + \eta_2) n \rfloor\}$, $\mathsf{T}_3 = \{t : \lfloor (\eta_1 + \eta_2) n \rfloor + 1 \leq t \leq n\}$, respectively, where n is the length of a codeword.

Phase 1: For $t \in \mathsf{T}_1$, only T_1 broadcasts $\boldsymbol{x}_1^{(1)}$ while T_2 remains silent (i.e., $x_2(t) = 0$ due to the half-duplex assumption) and attempts to decode T_1's message w_1 from the overheard signal $y_T(t)$. The duration of Phase 1 is chosen adaptively to ensure that T_2 successfully decodes T_1's message. The received signals at U_1, U_2, and T_2 within Phase 1 can be respectively described by

$$\boldsymbol{y}_1^{(1)} = \boldsymbol{x}_1^{(1)} + \boldsymbol{n}_1^{(1)}, \tag{1}$$

$$\boldsymbol{y}_2^{(1)} = c_{12}\boldsymbol{x}_1^{(1)} + \boldsymbol{n}_2^{(1)}, \tag{2}$$

$$\boldsymbol{y}_T^{(1)} = c_{TT}\boldsymbol{x}_1^{(1)} + \boldsymbol{n}_T^{(1)}. \tag{3}$$

Without loss of generality, we assume that the noises $n_1(t)$, $n_2(t)$,

[1]In this paper, upper case normal alphabet denotes random variables, lower and upper case bold alphabets denote vectors and matrices, respectively. $\mathcal{C}(x) \triangleq \log(1+x)$ and $a^+ \triangleq \max(0, a)$.

and $n_T(t)$ at the nodes U_1, U_2, and T_1, respectively, are independent and identically distributed additive white Gaussian noises with zero mean and unit variance and are mutually independent for all t.

Phase 2: For $t \in \mathsf{T}_2$, T_2 splits its power $P_2^{(2)}$ in Phase 2 into three parts: jamming, relaying and transmission of own message. In particular the jamming signal is encoded into $a_2(t)$ with power $P_{2a}^{(2)} = \rho_2 P_2^{(2)}$. For relaying, we first note that for T_2 to be able to successfully decode message w_1 in Phase 1, the following *decodability constraint* must be satisfied

$$|c_{TT}| > 1. \tag{4}$$

to guarantee that the channel capacity between T_1 and T_2 is large enough for T_2 to successfully decode T_1's message under $t < n$. We assume that T_2 knows T_1's codebook and w_1 is encoded into $\boldsymbol{v}_1^{(2)}$ with power $P_{2,1}^{(2)} = \gamma(1-\rho_2)P_2^{(2)}$. Finally w_2 is encoded into $\boldsymbol{v}_2^{(2)}$ with power $P_{2,2}^{(2)} = (1-\gamma)(1-\rho_2)P_2^{(2)}$ to be decoded by the secondary user U_2 only. Specifically, in Phase 2 node T_2 transmits

$$x_2(t) = v_2(t) + \sqrt{\frac{P_{2,1}^{(2)}}{P_1}} x_1(t) + a_2^{(2)}(t) \triangleq v_2(t) + v_1^{(2)}(t) + a_2^{(2)}(t), \tag{5}$$

where $v_2(t)$ is the t-th code symbol of the codeword encoding T_2's message w_2, and the received signals at U_1 and U_2 in this phase can be respectively described by

$$\boldsymbol{y}_1^{(2)} = \boldsymbol{x}_1^{(2)} + c_{21}\boldsymbol{x}_2^{(2)} + \boldsymbol{n}_1^{(2)}, \tag{6}$$

$$\boldsymbol{y}_2^{(2)} = c_{12}\boldsymbol{x}_1^{(2)} + c_{22}\boldsymbol{x}_2^{(2)} + \boldsymbol{n}_2^{(2)}. \tag{7}$$

Phase 3: For $t \in \mathsf{T}_3$, node T_2 performs clean relaying by transmitting only $\{x_1(t)\}_{t\in\mathsf{T}_3}$ with power $P_{2,1}^{(3)}$ and the jamming signal with power $P_{2a}^{(3)}$, but no $v_2(t)$. The signal transmitted by T_2 can be written as

$$x_2(t) = \sqrt{P_{2,1}^{(3)}/P_1}\, x_1(t) + a_2^{(3)}(t) \triangleq v_1^{(3)}(t) + a_2^{(3)}(t), \tag{8}$$

where $\{X_1(t)\}_{t\in\mathsf{T}_3}$ is the third part of T_1's codeword. The received signals at U_1 and U_2 in this phase are respectively as

$$\boldsymbol{y}_1^{(3)} = \boldsymbol{x}_1^{(3)} + c_{21}\boldsymbol{x}_2^{(3)} + \boldsymbol{n}_1^{(3)}, \tag{9}$$

$$\boldsymbol{y}_2^{(3)} = c_{12}\boldsymbol{x}_1^{(3)} + c_{22}\boldsymbol{x}_2^{(3)} + \boldsymbol{n}_2^{(3)}. \tag{10}$$

The average transmit power constraints for both transmitters are considered

$$\frac{1}{n}\sum_{k=1}^{n} |x_i(k)|^2 \le P_i \quad \text{for} \quad i \in \{1,2\}. \tag{11}$$

More specifically, at T_2 we require that $\eta_2 P_2^{(2)} + \eta_3 P_2^{(3)} \le P_2$.

A rate pair (R_1, R_2) for the messages w_1 and w_2 is *achievable*, if for $n \to \infty$, $P_{e,1} \triangleq \Pr\{\hat{w}_1 \neq w_1\}$ and $P_{e,2} \triangleq \Pr\{\hat{w}_2 \neq w_2\}$ can be made arbitrarily small, while the message w_1 stays secure from the secondary receiver, i.e.,

$$\max\{P_{e,1}, P_{e,2}\} \le \varepsilon \quad \text{(Reliability)}, \tag{12a}$$

$$\sup |\mathbb{P}_{W\boldsymbol{y}_2} - \mathbb{P}_W \mathbb{P}_{\boldsymbol{y}_2}| \le \varepsilon \quad \text{(Secrecy)}, \tag{12b}$$

for arbitrarily small $\varepsilon > 0$ and $\mathbb{P}$ denotes the distribution. Note that the secrecy metric in (12b) is the *variational distance* [2], which is stronger than the commonly used weak secrecy constraint $\lim_{n\to\infty} \frac{1}{n} I(w_1; \boldsymbol{y}_2) \le \varepsilon$. When T_2 does not transmit, the maximum achievable rate R_1^{WT} under both the reliability and secrecy conditions are fulfilled is known as the secrecy capacity of the wiretap channel [14] and is given by $R_1^{WT} = \big(\mathcal{C}(P_1) - \mathcal{C}(c_{12}^2 P_1)\big)^+$.

3. TRANSMISSION SCHEMES AND ACHIEVABLE RATE REGIONS

In this section we establish our main results. In particular we investigate a cooperative jamming strategy with and without clean relaying in Section 3.1, which acts as a benchmark for the comparison. The reason to introduce clean relay is that, it is a transmission scheme more general than the traditional one, i.e., only one single phase for the transmission of all signals including the relay, jamming, and the secondary user's own signal, which may not be efficient for the relay. And by the following numerical results, we can see the clean relay indeed provides rate gain. In Section 3.2 we consider the interference neutralization scheme considered in [4]. The reason to compare the cooperative jamming with the interference neutralization is that, to the best knowledge of the authors, they are both the most efficient signaling scheme to achieve secure transmission.

3.1 Cooperative Jamming without and with Clean Relay

If the constraint (4) is violated, then the primary user's rate can not be maintained when T_2 transmits his own signal by simultaneously relaying under the assumption that the primary channel is fully loaded. One explicit example is that when T_2 is out of the decodability region, i.e., the region enclosed by the circle with T_1 as the center and the distance between T_1 and U_1 as the radius, when only path loss is considered. Therefore, we implement cooperative jamming as follows. Since in this case T_2 does not need to listen and decode w_1, the signalling in the new phases 1 and 2 is modified respectively as

$$x_2^{(1)}(t) = v_2^{(1)}(t) + j_2^{(1)}(t), \text{ and } x_2^{(2)}(t) = v_2^{(2)}(t) + j_2^{(2)}(t).$$

We parameterize the power allocated to jamming and T_2's own message transmission as $P_{2j}^{(2)} = \rho_2 P_2^{(2)}$, and $P_{2,2} = (1-\rho_2)P_2^{(2)}$, respectively, where $\rho_2 \in [0,1]$ denotes the fraction of the power used for jamming. In the third phase, we only transmit the jamming signal as

$$x_2^{(3)}(t) = j_2^{(3)}(t). \tag{13}$$

PROPOSITION 1. *The achievable rate pair* (R_1^{CJ}, R_2^{CJ}) *for*

the CJ scheme is given by the region $\mathcal{R}_{CJ} = \{(R_1^{CJ}, R_2^{CJ}) :$

$$R_1^{CJ} \leq \Big(\eta_1 R_1^{WT} + \eta_2 \left\{ \mathcal{C}\left(\frac{P_1}{1+|c_{21}|^2 P_2^{(2)}}\right) - \mathcal{C}\left(\frac{|c_{12}|^2 P_1}{1+|c_{22}|^2 \rho_2 P_2^{(2)}}\right)\right\} + \eta_3 \left\{ \mathcal{C}\left(\frac{P_1}{1+|c_{21}|^2 P_2^{(3)}}\right) - \mathcal{C}\left(\frac{c_{12}^2 P_1}{1+|c_{22}|^2 P_2^{(3)}}\right)\right\}\Big)^+, \quad (14)$$

$$R_2^{CJ} \leq \eta_2 \, \mathcal{C}\left(\frac{|c_{22}|^2(1-\rho_2)P_2^{(2)}}{1+|c_{12}|^2 P_1 + |c_{22}|^2 \rho_2 P_2^{(2)}}\right)\Bigg\}. \quad (15)$$

When T_2 is inside the decodability region, we give the achievable rate region in the following proposition for CJ with clean relaying.

PROPOSITION 2. *The achievable rate pair* (R_1, R_2) *for the clean relaying scheme with cooperative jamming is given by the region* $\mathcal{R}_{CR} = \{(R_1^{CR}, R_2^{CR}) :$ (16) *and* (17)$\}$.

Then the optimization problem can be formulated as follows.

DEFINITION 1. *The optimization problem* $\mathcal{P}_{R_{2m}}$ *investigated in this paper is defined as*

$$\max_{\eta_1,\eta_2,\rho_2,\rho_3,\gamma,P_2^{(2)},P_2^{(3)}} R_2$$
$$s.t.\ R_1 \geq R_1^{WT},\ \eta_2 P_2^{(2)} + \eta_3 P_2^{(3)} \leq P_2.$$

3.2 Interference Neutralization

In this section we consider an interference neutralization (IN) strategy as a transmission scheme for T_2. The idea of interference neutralization is to nullify the interference signal from T_1 received at U_2. In our scenario, this strategy could potentially yield to two beneficial effects: the leakage of the primary message to the secondary user is eliminated, while at the same time the quality of the secondary transmission could be improved since there is no more primary interference. The signalling in the first phase is the same as for the relaying schemes, since T_2 needs to decode w_1 in the first phase. Therefore the constraint (4) must be satisfied and η_1 is set as $\mathcal{C}(P_1)/\mathcal{C}(|c_{TT}|^2 P_1)$. In the second phase T_2 transmits:

$$x_2^{(2)}(t) = v_2^{(2)}(t) - \frac{c_{12}}{c_{22}} x_1^{(2)}(t). \quad (18)$$

The received signals in the second phase are given by:

$$\mathbf{y}_1^{(2)} = \mathbf{x}_1^{(2)} + c_{21}\mathbf{x}_2^{(2)} + \mathbf{n}_1^{(2)}, \quad (19)$$
$$\mathbf{y}_2^{(2)} = c_{12}\mathbf{x}_1^{(2)} + c_{22}\mathbf{x}_2^{(2)} + \mathbf{n}_2^{(2)}, \quad (20)$$

which simplifies to

$$\mathbf{y}_1^{(2)} = \left(1 - \frac{c_{12}c_{21}}{c_{22}}\right)\mathbf{x}_1^{(2)} + c_{21}\mathbf{v}_2^{(2)} + \mathbf{n}_1^{(2)}, \quad (21)$$
$$\mathbf{y}_2^{(2)} = c_{22}\mathbf{v}_2^{(2)} + \mathbf{n}_2^{(2)}. \quad (22)$$

Based on this signalling, we obtain the achievable rate region as follows.

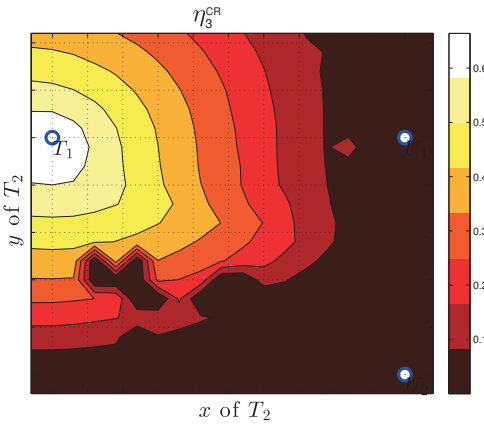

Figure 2: Distribution of η_3 depending on the location of T_2.

PROPOSITION 3. *The achievable rate pair* (R_1^{IN}, R_2^{IN}) *for IN is given by the region* $\mathcal{R}_{IN} = \{(R_1^{IN}, R_2^{IN}) :$

$$R_1^{IN} < \eta_1 R_1^{WT} + \eta_2 \, \mathcal{C}\left(\frac{P_1|1 - \frac{c_{12}c_{21}}{c_{22}}|^2}{1+|c_{21}|^2(P_2^{(2)} - |\frac{c_{12}}{c_{22}}|^2 P_1)}\right), \quad (23)$$

$$R_2^{IN} < \eta_2 \, \mathcal{C}\left(|c_{22}|^2\left(P_2^{(2)} - \left|\frac{c_{12}}{c_{22}}\right|^2 P_1\right)\right)\Bigg\}. \quad (24)$$

Note that from (23) and (24) we can see that if $|c_{12}|$ is too large and/or $|c_{22}|$ is too small such that

$$\eta_2 \left|\frac{c_{12}}{c_{22}}\right|^2 P_1 > P_2, \quad (25)$$

then T_2 may not have enough power to neutralize the interference and therefore IN cannot be implemented.

Finally we should note that the optimization problem $\mathcal{P}_{R_{2m}}$ reduces as given in the following definition.

DEFINITION 2. *The optimization problem for IN* $\mathcal{P}_{R_2^{IN}}$ *is defined as*

$$\max_{\eta_2, P_2^{(2)}} R_2^{IN}, s.t.\ R_1^{IN} \geq R_1^{WT}.$$

Note that IN can achieve Shannon's perfect secrecy $I(W;Z) = 0$, which is stronger than the strong secrecy. Thus from [2] we know that IN can achieve the secrecy based on variational distance.

4. NUMERICAL ILLUSTRATIONS

In this section we present the numerical results and related discussions. We will compare the rate performance clean relaying with cooperative jamming, pure cooperative jamming, relaying without the additional phase and interference neutralization with respect to the particular topology of interest. In particular, we are interested in how the system behaves for different locations of the secondary transmitter.

$$R_1^{CR} \leq \left(\eta_1 R_1^{WT} + \eta_2 \left\{ \mathcal{C}\left(\frac{\left| \sqrt{P_1} + c_{21}\sqrt{(1-\rho_2)\gamma P_2^{(2)}} \right|^2}{1+|c_{21}|^2(1-\gamma+\gamma\rho_2)P_2^{(2)}} \right) - \mathcal{C}\left| \frac{\left(c_{12}\sqrt{P_1} + c_{22}\sqrt{(1-\rho_2)\gamma P_2^{(2)}} \right)^2}{1+|c_{22}|^2\rho_2 P_2^{(2)}} \right| \right\} \right.$$
$$\left. + \eta_3 \left\{ \mathcal{C}\left(\frac{\left| \sqrt{P_1} + c_{21}\sqrt{(1-\rho_3)P_2^{(3)}} \right|^2}{1+|c_{21}|^2\rho_3 P_2^{(3)}} \right) - \mathcal{C}\left(\frac{\left| c_{12}\sqrt{P_1} + c_{22}\sqrt{(1-\rho_3)P_2^{(3)}} \right|^2}{1+|c_{22}|^2\rho_3 P_2^{(3)}} \right) \right\} \right)^+, \quad (16)$$

$$R_2^{CR} \leq \eta_2 \, \mathcal{C}\left(\frac{|c_{22}|^2(1-\rho_2)(1-\gamma)P_2^{(2)}}{1+|c_{22}|^2\rho_2 P_2^{(2)} + \left| c_{22}\sqrt{\gamma(1-\rho_2)P_2^{(2)}} + c_{12}\sqrt{P_1} \right|^2} \right). \quad (17)$$

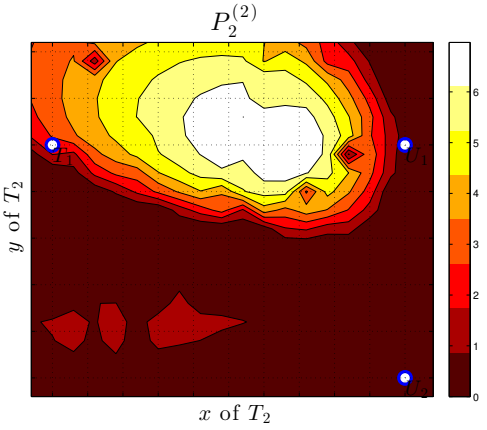

Figure 3: Transmission power $P_2^{(2)}$ in the second phase for the CR scheme depending on the location of T_2.

We will also show how the relaying and time splitting of different strategies are affected by the relative positions of nodes.

In our simulation, we fix the locations of the primary transmitter T_1 and receiver U_1 at the coordinates $(0,0)$ and $(1,0)$, respectively. The secondary receiver is fixed at $(1,-1)$. We assume a path-loss model with path-loss exponent $\alpha = 3$, i.e., $c_{ij} = d_{ij}^{-3}$. The power constraints at both transmitters are $P_1^{\max} = P_2^{\max} = 10$ dB. We scan the parameters $(\rho_2, \rho_3, \gamma, \eta_1, \eta_2, P_2^{(2)}, P_2^{(3)})$ over a sufficiently fine grid and take the maximum achievable rate over all corresponding rates. Note that we also include power control as a possible strategy for T_2; i.e., the transmission power utilized is not necessarily fixed to its maximum $P_2^{\max} = 20$ dB.

4.1 Clean Relaying: Signalling Parameters

In Figure 2 we show the relation between the location of T_2 and the time splitting parameters η_3 for T_2 to implement clean relaying/cooperative jamming in the third phase. The figure shows that the third phase, specific to the clean relaying scheme, is used by the secondary transmitter, which shows the relevance of considering the CR scheme for our cognitive model. We observe that η_3 decreases with the increasing distance between T_2 to T_1. One possible explanation to this observation is that since η_1 becomes larger as T_2 gets further away from T_1, there is less time allowed for clean relaying to be implemented in the third phase. The interesting behavior in the middle-left area can be tentatively explained using the observations from the third phase being solely used for CJ instead of relaying the message in that region, which possibly explains the difference in behavior as the aim of the third phase is changed.

In Figure 3 we depict how the secondary power in the second phase $P_2^{(2)}$ is distributed depending on the location of T_2. This transmission power is constituted of three parts: the power allocated to the primary message, the jamming power, and the power allocated to the secondary message. According to numerical results not depicted here we made the following observations:

1. Most of the transmission power used in the second phase is allocated to the transmission of the secondary message, i.e., the term $(1-\gamma)(1-\rho)P_2^{(2)}$.

2. No power is allocated to the relaying of the primary message in the second phase, i.e., $\gamma = 0$. Instead the power allocated to relaying is concentrated in the third phase.

3. There exists a region where some jamming power is allocated, namely the region inside the decodability circle which is the closest to U_2, since CJ is efficient in this location.

4.2 Comparison with Pure Cooperative Jamming

In Figure 4 we depict the difference in terms of maximal achievable rates between the clean relaying with cooperative jamming strategy and the pure cooperative jamming strategy. The red line represents the coarse boundary under which the clean relaying results in $R_2 = 0$, since the decodability constraint is not satisfied for T_2 located outside this decodability circle. In the region below the red line, pure CJ is efficient while above the red line, the pure CJ

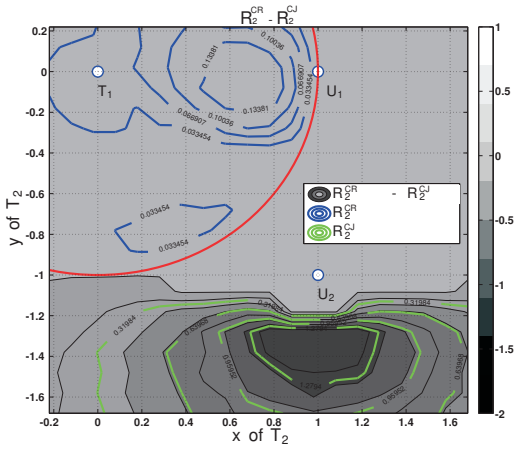

Figure 4: Difference between maximum achievable secondary rates with CR and pure CJ $R_2^{\mathbf{CR}} - R_2^{\mathbf{CJ}}$ as a function of the position of $\mathbf{T}_2$.

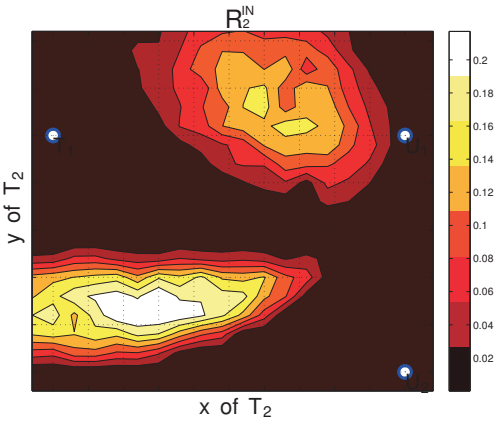

Figure 5: Achievable secondary rate $R_2^{\mathbf{IN}}$ using IN depending on the location of $\mathbf{T}_2$.

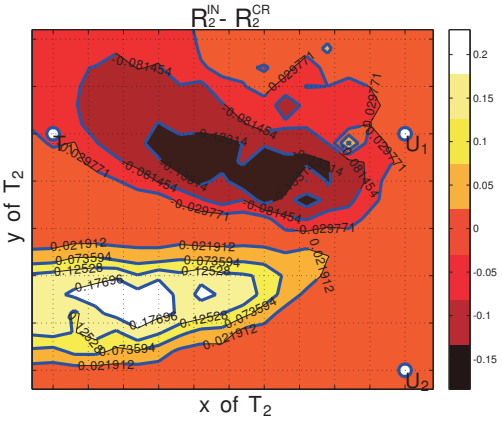

Figure 6: Difference $R_2^{\mathbf{IN}} - R_2^{\mathbf{CR}}$ between the CR and IN schemes depending on the location of $\mathbf{T}_2$.

strategy yields to $R_2 = 0$. The explanations of this phenomenon are two-fold: first, if T_2 is above this region, pure jamming may degrade the main channel more than Eve's channel. Therefore relaying is necessary while jamming is hurtful. Secondly, because T_2 is much closer to U_2 than to U_1 when T_2 is below the red line, the relaying contributes more to the numerator of the second term in the bracket multiplied by η_2 in (16), which degrades the primary user's secrecy rate. The achievable rates by clean relaying and CJ are also labeled in the figure by blue and green lines, respectively. From Figure 4 we observe that pure CJ and CR are achieving strictly positive secondary rates in different regions, and their performance is not comparable for a fixed location of T_2. Thus in the following we restrict our comparison with the other scheme, namely IN. This observation also leads to the idea of an hybrid scheme where T_2 either uses one of the strategies where X_1's knowledge is necessary, or resorts to jamming if X_1 is not decodable, i.e., outside the decodability region.

4.3 Comparison with Interference Neutralization

We now illustrate the performance of the IN scheme. First in Figure 5 we depict the secondary rate achievable using interference neutralization. We observe two separate regions where IN achieves strictly positive secondary rates. First when T_2 is located close to U_2, yet still in the decodability region since X_1 needs to be known by T_2 for the implementation of the scheme, we observe that IN performs well. This is expected since T_2 can neutralize the interference caused by X_1 transmitted by T_1 efficiently. The IN scheme being efficient when T_2 is close to U_1 is surprising however and it can be explained as follows. Since c_{21} is large for that scenario, the negative part of X_1 adding itself to the received signal at U_1 becomes large enough so that the amplitude of the received signal in X_1, is higher than that without the interference caused by T_2. Thus T_2 is effectively relaying X_1 to U_1 in that region.

Finally in Figure 6 we compare CR and IN in terms of achievable secondary rates. We observe that in the region between T_1 and U_1, CR outperforms IN. However in the lower part of the plane, IN outperforms CR, which highlights that IN is more effective than jamming, i.e., that canceling the signal X_1 at U_2 is preferable to exhausting the decoding capabilities of U_2 by jamming using Gaussian signals. However we should note that the IN strategy necessitates a precise knowledge of the channels' CSI to be implemented, while the CJ scheme does not rely on the knowledge of the signal coefficients for its signalling.

5. CONCLUSIONS

In this paper we investigated a four-node cognitive channel with a stronger secrecy metric than the weak secrecy, where the secondary receiver is a potential eavesdropper with respect to the primary transmission. To efficiently allow the secondary system to operate simultaneously with the primary system while leaving the primary user's secrecy rate unchanged, we introduced several schemes, namely interference neutralization and cooperative jamming with and without clean relaying. In particular we analyzed secondary user's achievable rate when interference neutralization is used

to compare with the performance of clean relaying with and without cooperative jamming. We illustrated our results through numerical examples which emphasize the impact of the node geometry on the achievable rates, the optimal power allocation, and the time splitting of the secondary transmitter. Our study demonstrated how the signalling strategies can outperform each other depending on the relative location of the nodes. We conclude from this observation that the position of the users must be taken into account for the design of secure transmissions in cognitive radio networks.

6. ACKNOWLEDGMENTS

This work has been performed in the framework of the European research project DIWINE, which is partly funded by the European Union under its FP7 ICT Objective 1.1 - The Network of the Future.

7. REFERENCES

[1] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. Bloch, S. Ulukus, and A. Yener. Cooperative security at the physical layer. *IEEE Signal Processing Magazine*, (9):6–28, September 2013.

[2] M. R. Bloch and J. N. Laneman. Strong secrecy from channel resolvability. *IEEE Trans. Inform. Theory*, 59(12):8077–8098, Dec. 2013.

[3] F. Gabry, N. Li, M. Girnyk, N. Schrammar, L. K. Rasmussen, and M. Skoglund. On the optimization of the secondary transmitter's strategy in cognitive radio channels with secrecy. *IEEE J. Select. Areas Commun.*, 32(3):451 – 463, 2014.

[4] Z. K. M. Ho, E. Jorswieck, and S. Gerbracht. Information leakage neutralization for the multi-antenna non-regenerative relay-assisted multi-carrier interference channel. 31(9):1672–1686, Sept. 2013.

[5] Y. Liang, H. V. Poor, and S. Shamai (Shitz). Information theoretic security. *Foundations and Trends in Communications and Information Theory*, 5:355–580, April 2009.

[6] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. S. Shamai, and S. Verdú. Capacity of cognitive interference channels with and without secrecy. *IEEE Trans. Inform. Theory*, 55(2):604–619, February 2009.

[7] P.-H. Lin, F. Gabry, R. Thobaben, E. Jorswieck, and M. Skoglund. Clean relaying in cognitive radio networks with variational distance secrecy constraint. In *Proc. IEEE Global Communications conference, GLOBECOM*, December 2014.

[8] P.-H. Lin, S.-C. Lin, H.-J. Su, and Y.-W. Hong. Improved transmission strategies for cognitive radio under the coexistence constraint. *IEEE Trans. Wireless Commun.*, 11(11):4058 – 4073, 2012.

[9] J. Mitola. *Cognitive Radio An integrated agent architecture for software defined radio*. PhD thesis, KTH, May 2000.

[10] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wiretap channel. In *Proc. IEEE International Symposium on Information Theory, Toronto, Canada*, 2008.

[11] S. Shafiee, N. Liu, and S. Ulukus. Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel. *IEEE Trans. Inform. Theory*, 55(9):4033–4039, September 2009.

[12] E. Tekin and A. Yener. The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Trans. Inform. Theory*, 54(6):2735 –2751, June 2008.

[13] Y. Wu and K. J. R. Liu. An information secrecy game in cognitive radio networks. *IEEE Transactions on Information Forensics and Security*, 6(3):831 – 842, September 2011.

[14] A. Wyner. The wire-tap channel. *Bell Systems Technical Journal*, 54(8):1355–1387, October 1975.