The Cognitive Multiple Access Wire-Tap Channel

Osvaldo Simeone
CWCSPR, ECE Dept.,
New Jersey Institute of Technology

Aylin Yener
Dept. of Electrical Engineering
Pennsylvania State University

***Abstract*—A cognitive Multiple Access Channel with a Wire-tapper (cMAC-WT) is studied, where one of the two encoders is *cognitive*, in the sense that it knows a priori the message of the other encoder. Both the discrete and Gaussian models are considered. General achievable rates and outer bounds to the secrecy capacity region are derived, and the secrecy capacity region is identified for the special cases of *less noisy* discrete cMAC-WT, *degraded Gaussian* cMAC-WT and degraded Gaussian cMAC-WT *with orthogonal components*. Numerical results are provided to illustrate the main findings.**

I. Introduction

Information-theoretic approaches that aim at providing security as well as reliability of communication emerge as powerful tools to provide an alternative to, or to complement or strengthen, the more traditional computation-based security strategies. As an example, information-theoretic security, when channel conditions are (or can be made to be) favorable, enables the confidential exchange of a key between two nodes of a network in the absence of a certified authority. Recent works have addressed information-theoretic security in a number of networks of interest, including broadcast [1] [2], multiple access [3] [4] [5], interference [2] and relay channels [6], as well as multiantenna (MIMO) links [7] [8]. In this body of work, a recurring theme is that of assessing how much the availability of a certain communication resource can help improving the secrecy level in a given network. Examples are the possibility to deploy multiantenna terminals [7] [8], to leverage synergies in multi-terminal networks, possibly via cooperation [6] [5] or jamming [4] [2], or to exploit the side information available at certain (cognitive) nodes regarding the messages to be conveyed by other nodes [9]. In this work, we further explore the latter two issues by studying a model that relate to both the multiple access channel with a wire-tapper (also referred to as eavesdropper) of [3] [4] and the cognitive interference channel of [9]. Specifically, we consider the scenario in Fig. 1, in which two users communicate with an intended receiver in the presence of an eavesdropper. The difference with the model of [3] [4] (see also [10]) is that here one of the two users is *cognitive*, in the sense that it knows the message of the other encoder. Moreover, the model differs from the one in [9] in that here we are interested, as in [3] [4], in keeping both users' messages secret from the eavesdropper, whereas in [9] the "eavesdropping" node is actually a legitimate receiver for one of the messages, but not for the other.

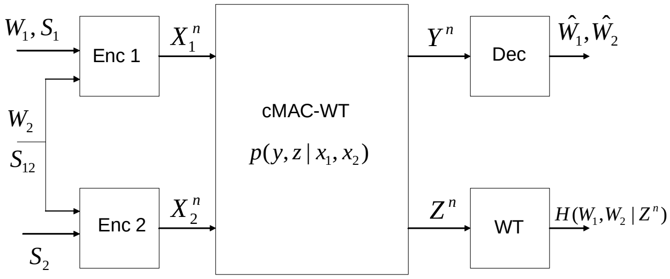

Fig. 1. A cognitive Multiple Access Channel with a Wiretapper (cMAC-WT). Variables W_1, W_2 represent finite-rate messages and S_1, S_2, S_{12} random variables of arbitrary entropy that can be used for stochastic encoding.

We derive general achievable rates and outer bounds to the secrecy capacity region for the model in Fig. 1, referred to as Cognitive Multiple Access Wiretap Channel (cMAC-WT). Furthermore, we identify the capacity region for the special cases of *less noisy* discrete cMAC-WT, *degraded Gaussian* cMAC-WT and degraded Gaussian cMAC-WT *with orthogonal components* [10].

Notation: Instances of a random variable, identified by a given capital letter, are denoted by the corresponding lower-case font. We use the standard sequence notation $x^n = (x_1, ..., x_n)$.

II. System Model

A cMAC-WT, illustrated in Fig. 1, is characterized by two independent and uniformly distributed messages $W_1 \in [1, 2^{nR_1}]$ and $W_2 \in [1, 2^{nR_2}]$ of rates R_1 and R_2 (bits/channel use), where n is the coding block size, two encoders (users), a legitimate destination that receives Y^n and a wire-tapper that receives Z^n. User 1 is the cognitive user and encodes both W_1 and W_2 via an encoder $f_{1,n}$ into a codeword X_1^n and user 2 encodes W_2 via an encoder $f_{2,n}$ into a codeword X_2^n as

$$X_1^n = f_{1,n}(W_1, W_2, S_1, S_{12}) \tag{1a}$$

$$X_2^n = f_{2,n}(W_2, S_2, S_{12}), \tag{1b}$$

where S_1, S_2 and S_{12} are independent random variables of arbitrary entropy. Since $f_{1,n}, f_{2,n}$ are deterministic functions, S_1, S_2 and S_{12} are used to randomize the mapping between messages and codewords (stochastic encoders). Notice that variable S_{12} provides common randomness shared by the two encoders. The codewords are transmitted over a discrete memoryless channel characterized by a conditional distribution $p(y, z|x_1, x_2)$. Decoding at the intended receiver takes place via a function g_n as $(\hat{W}_1, \hat{W}_2) = g_n(Y^n)$ based on the received sequence Y^n. The secrecy level is measured by the equivocation at the wire-tapper upon reception of the sequence Z^n as $H(W_1, W_2|Z^n)$. A pair of rates (R_1, R_2) is said to be *achievable* if for $n \to \infty$, the probability of error at the intended destination vanishes, i.e.,

$$P_e^{(n)} = \Pr[g_n(Y^n) \neq (W_1, W_2)] \to 0, \tag{2}$$

and the equivocation tends to the messages' entropy:

$$H(W_1, W_2|Z^n)/H(W_1, W_2) \to 1. \tag{3}$$

Notice that the secrecy constraint (3) implies secrecy also for each user in the sense of the normalized equivocation, i.e., $H(W_j|Z^n)/H(W_j) \to 1$ for $j = 1, 2$ [3]. The secrecy capacity region is defined as the closure of the set of all achievable rates. It is finally remarked that the secrecy capacity region depends only on the marginals $p(y|x_1, x_2)$ and $p(z|x_1, x_2)$ (see, e.g., Lemma 1 of [5]).

A *stochastically degraded cMAC-WT* (or in short *degraded*) is defined as being such that the marginal $p(z|x_1, x_2)$ is the same as that of a *physically degraded channel* (for which $p(y, z|x_1, x_2) = p(y|x_1, x_2)p(z|y)$ or equivalently the Markov chain condition $(X_1, X_2) - Y - Z$ holds), i.e., we have $p(z|x_1, x_2) = \sum_{y \in \mathcal{Y}} p(y|x_1, x_2)p'(z|y)$ for some conditional distribution $p'(z|y)$. We also say that the cMAC-WT is *less noisy* (more precisely, the main channel is less noisy than the wire-tapper's channel) if for every set of variables satisfying the Markov chain $V - (X_1, X_2) - (Y, Z)$ we have $I(V; Y) - I(V; Z) \geq 0$ [1].

We also consider the Gaussian cMAC-WT defined by

$$Y = X_1 + X_2 + N_y \tag{4a}$$

$$Z = \sqrt{h_1}X_1 + \sqrt{h_2}X_2 + N_z, \tag{4b}$$

with N_y and N_z Gaussian random variables with unit power, and individual average power constraints P_1 and P_2 for the two users: $1/n \sum_{i=1}^n x_{ji}^2 \leq P_j$ for $j = 1, 2$ and any codeword. As noted above, the secrecy capacity region depends only on the marginal distributions, and hence the correlation of N_y and N_z is immaterial. Moreover, it can be seen that the Gaussian cMAC-WT is *(stochastically) degraded* if $h_1 = h_1 = h \leq 1$ [3].

We finally remark that if we set $R_1 = 0$, the model at hand reduces to a special case of the relay channel studied in [11] (see "case 2" therein and assume a noiseless channel between source and relay). The results presented below are consistent with the findings of [11] when specialized to the case $R_1 = 0$.

III. Achievable Secrecy Regions

We first review, and generalize, an achievable region derived in [3] [4], which applies to the "non-cognitive" Multiple Access Wiretap Channel (MAC-WT). In this setting, user 1 does not know message W_2 and encoding is limited to functions of the type $x_1^n = f_{1,n}(w_1, s_1)$ and $x_2^n = f_{2,n}(w_2, s_2)$. Clearly, this achievable secrecy rate region sets a reference result for the scenario at hand, in which the more general form of encoding (1) is possible.

Proposition 1 (Achievable secrecy region for MAC-WT): For a discrete MAC-WT, the following is an achievable rate region

$$\begin{aligned} \bigcup\{(R_1, R_2) \quad &: \quad R_1, R_2 \geq 0, \\ R_1 \quad &\leq \quad I(V_1; Y|V_2, Q) - I(V_1; Z|Q) && \text{(5a)} \\ R_2 \quad &\leq \quad I(V_2; Y|V_1, Q) - I(V_2; Z|Q) && \text{(5b)} \\ R_1 + R_2 \quad &\leq \quad I(V_1, V_2; Y|Q) && \text{(5c)} \\ & \qquad -I(V_1, V_2; Z|Q)\}, \end{aligned}$$

where the union is taken over all joint distributions that factorize as

$$p(q)p(x_1, v_1|q)p(x_2, v_2|q)p(y, z|x_1, x_2)$$

such that the right-hand sides in (5) are non-negative. Moreover, for the Gaussian MAC-WT, assuming without loss of generality $h_1 \geq h_2$, the following rate region is achievable:

$$\begin{aligned} \bigcup\{(R_1, R_2) \quad &: \quad R_1, R_2 \geq 0, \\ R_1 \quad &\leq \quad \frac{1}{2}\sum_{i=1}^{N} \lambda_i (\log(1 + a_i P_{1i}) && \text{(6a)} \\ & \qquad - \log\left(1 + \frac{h_1 P_{1i}}{1 + h_2 P_{2i}}\right)\Bigg) \\ R_2 \quad &\leq \quad \frac{1}{2}\sum_{i=1}^{N} \lambda_i (\log\left(1 + \frac{P_{2i}}{1 + \bar{a}_i P_{1i}}\right) && \text{(6b)} \\ & \qquad - \log\left(1 + \frac{h_2 P_{2i}}{1 + h_1 P_{1i}}\right)\Bigg) \\ R_1 + R_2 \quad &\leq \quad \frac{1}{2}\sum_{i=1}^{N} \lambda_i \log\Bigg(\frac{1 + P_{1i} + P_{2i}}{1 + h_1 P_{1i} + h_2 P_{2i}} \\ & \qquad \cdot \frac{1 + \bar{a}_i h_1 P_{1i}}{1 + \bar{a}_i P_{1i}}\Bigg)\Bigg\}, && \text{(6c)} \end{aligned}$$

where the union is taken over all choices of parameters $\lambda_i, P_{1i}, P_{2i}, a_i$ such that $\lambda_i, P_{1i}, P_{2i} \geq 0$, $\sum_{i=1}^N \lambda_i = 1$, $\sum_{i=1}^N \lambda_i P_{ji} \leq P_j$ for $j = 1, 2$, $a_i \in \{0, 1\}$ (with definition $\bar{a}_i = 1 - a_i$) such that the right-hand sides in (6) are non-negative . Moreover, we can set $N \leq 5$ without loss of generality.

Remark 1: The proposition above is a generalization of the region obtained by time-sharing the "superposition", "TDMA" and *cooperative jamming* schemes of [3] [4] (see Theorem 1 of [4]), since we allow for a more general form of time-sharing, and we treat also the discrete model. For the discrete model, variable Q in the achievable region (5) is a time-sharing variable, auxiliary variables V_1, V_2 represent the codebooks of the two users, and the transmitted signals X_1, X_2 are obtained as the output of "artificial" channels $p(x_1|v_1, q)$ and $p(x_2|v_2, q)$ employed at the two users to further confuse the wire-tapper (see, e.g., [5] [6]). This may provide the opportunity for cooperative jamming. Cooperative jamming amounts, in the Gaussian model, to sending additional noise from a given transmitter so as to jam the wire-tapper's reception [4]. In the achievable region (6) for the Gaussian model, we define variables a_i to define whether user 1, who has the better channel to the wire-tapper, performs cooperative jamming ($a_i = 0$) or not ($a_i = 1$). Notice that, as explained in [4], here it is optimal for user 1 to either perform cooperative jamming or not, without performing more general forms of power allocation between signal and additional noise (see also Remark 4 below).

Remark 2: The achievable rate region of Proposition 1 generally does not exhaust the secrecy capacity region, even when restricting the setting to the MAC-WT. However, it was shown in [3] that the sum-capacity for the *degraded* MAC-WT is given by (6c) with $\lambda_1 = 1$ and no cooperative jamming ($a_1 = 1$) for the Gaussian model, and, it can be seen similarly, by (5c) with Q constant and $V_j = X_j$, for $j = 1, 2$, for the discrete case. Moreover, assuming $h_1, h_2 < 1$, it was shown in [10] that, for the Gaussian case, the region (6) is within 0.5 bits/channel use of the capacity region of the MAC-WT along the individual rate dimensions. Another sum-capacity result of [10] for a different Gaussian model is recalled in Remark 5.

Proof: The proof of achievability of (5) follows similarly to [3] [4] by using a random coding argument (see also discussion in Appendix A for related discussion). In particular, the codewords at the two encoders are generated by first drawing a typical time-sharing sequence q^n according to distribution $p(q)$, which is revealed at all nodes (including the eavesdropper), and then generating codebooks v_1^n and v_2^n in the set of conditionally typical sequences with respect to distributions $p(v_1|q)$ and $p(v_2|q)$ respectively, which are used for stochastic encoding. Stochastic encoding and randomization via the channels $p(x_1|v_1, q)$ and $p(x_2|v_2, q)$ is made possible by the available sources of randomness S_1 and S_2 at the two transmitters. For the Gaussian model, starting from (5), we set $Q = i$ with probability λ_i, we select $p(v_j|q = i)$ so that V_j, conditioned on $Q = i$, is Gaussian with power P_{ji}, we choose $p(x_j|v_j, q = i)$ in (5) so that $X_{1i} = a_i V_{1i} + \bar{a}_i X'_{1i}$ and $X_{2i} = V_{2i}$, where X'_{1i} is a Gaussian variable independent of all other variables and with power P_{1i}. Finally, the constraint on N for (6) follows from Theorem 2 in [12]. ■

Proposition 2 (Achievable secrecy region for cMAC-WT): The following secrecy rate region is achievable for the discrete cMAC-WT

$$\bigcup \{(R_1, R_2) : R_1, R_2 \geq 0$$
$$R_1 \leq I(V_1; Y|V_2, Q) \tag{7a}$$
$$R_1 + R_2 \leq (I(V_1, V_2; Y|Q) \tag{7b}$$
$$- I(V_1, V_2; Z|Q))^+\},$$

where the union is taken over all joint distributions that factorize as

$$p(q)p(v_1, v_2|q)p(x_2|v_2, q)p(x_1|x_2, v_1, v_2, q)p(y, z|x_1, x_2).$$

Moreover, the following rate region is achievable for the Gaussian cMAC-WT

$$\bigcup \{(R_1, R_2) : R_1, R_2 \geq 0$$
$$R_1 \leq \frac{1}{2}\sum_{i=1}^{N} \lambda_i \log\left(1 + \frac{a_{1i}P_{1i}(1-\rho_i^2)}{1 + \bar{a}_{1i}P_{1i} + \bar{a}_{2i}P_{2i}}\right) \tag{8a}$$
$$R_1 + R_2 \leq \frac{1}{2}\sum_{i=1}^{N} \lambda_i \log\left(\frac{\Psi_1(P_{1i}, P_{2i}, \rho_i, a_{1i}, a_{2i})}{\Psi_2(P_{1i}, P_{2i}, a_{1i}, a_{2i})}\right)^+\}, \tag{8b}$$

with

$$\Psi_1 = \frac{1 + P_{1i} + P_{2i} + 2\rho_i\sqrt{a_{1i}a_{2i}P_{1i}P_{2i}}}{1 + h_1P_{1i} + h_2P_{2i} + 2\rho_i\sqrt{h_1h_2a_{1i}a_{2i}P_{1i}P_{2i}}}$$
$$\text{and } \Psi_2 = \frac{1 + \bar{a}_{1i}P_{1i} + \bar{a}_{2i}P_{2i}}{1 + \bar{a}_{1i}h_1P_{1i} + \bar{a}_{2i}h_2P_{2i}},$$

and where the union is taken over all choices of parameters $\lambda_i, P_{1i}, P_{2i}, a_{1i}, a_{2i}, \rho_i$ such that $\lambda_i, P_{1i}, P_{2i} \geq 0$, $\sum_{i=1}^{N} \lambda_i = 1$, $\sum_{i=1}^{N} \lambda_i P_{ji} \leq P_j$, $0 \leq a_{ji} \leq 1$ (with definition $\bar{a}_i = 1 - a_i$), for $j = 1, 2$, and $-1 \leq \rho_i \leq 1$. Moreover, we can set $N \leq 4$ without loss of generality.

Proof: See Appendix A. ■

Remark 3: In the absence of an eavesdropper ($Z = \emptyset$), the region (7) reduces to the capacity result for a cognitive MAC of [13] by setting $V_1 = X_1$, $V_2 = X_2$ and Q constant. In particular, in this case, no time-sharing is necessary since the left-hand sides of (7) are concave in $p(x_1, x_2|q)$. Moreover, it can be seen that the rate regions of Proposition 2 include those of Proposition 1.

Remark 4: In the Gaussian region of Proposition 2, time-sharing is implemented as explained in Remark 1. Moreover, parameter $\bar{a}_{ji}$ represents the fraction of power used by user j for jamming when $Q = i$ (see also proof in Appendix A). Notice that in the cMAC-WT, it is not always true that users should either jam or transmit information, so that we allow for more general forms of power allocation ($0 \leq a_{ji} \leq 1$). We also remark that cooperative jamming is implemented, as in Proposition 1, by injecting independent noise at the two users. However, in the cMAC-WT, one could potentially obtain better performance by *correlating the two jamming noises* thanks to the available common randomness S_{12}, but this is not further pursued here. On a related note, as explained in Appendix A, region (8) is achieved without exploiting the "private" randomness S_1 and S_2, but only the common randomness S_{12}. Finally, the region (8) can be proved to be attainable by simple time-division/ frequency-division following Theorem 1 in [12].

A. Numerical Results

Consider a system in which $h_1 > 0$ and $h_2 = 0$, that is, user 2 is not heard by the wire-tapper. In this case, it is not always clear that user 2 can always benefit from cognition, since the cognitive user is heard by the wire-tapper due to the fact that $h_1 > 0$. Fig. 2 shows the sum-rate $R_1 + R_2$ obtained for the MAC-WT (no cognition) in

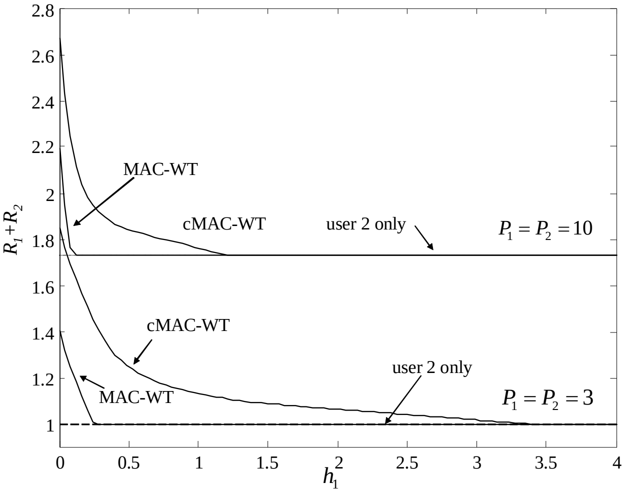

Fig. 2. Sum-rate $R_1 + R_2$ obtained for the MAC-WT (no cognition) in Proposition 1 and for the cMAC-WT in Proposition 2 for $P_1 = P_2 = 3$ or 10, versus h_1, compared to the sum-rate achievable if only user 2 transmits ($R_1 + R_2 = R_2 = 1/2 \log(1 + P_2)$, dashed line).

Proposition 1 (with $N = 1$ to simplify), and for the cMAC-WT in Proposition 2, for $P_1 = P_2 = 3$ and 10, versus h_1, compared to the sum-rate achievable if only user 2 transmits ($R_1 + R_2 = R_2 = 1/2 \log(1 + P_2)$, in dashed lines). It can be seen that, as expected, if h_1 is sufficiently large, the maximum achievable rates with and without cognition coincide with the rate of user 2 only, that is, cognition is not useful. However, cognition leads to substantial sum-rate benefits if h_1 is sufficiently small and the gains are more pronounced for low SNR P, as it is in this regime that coherent power gains ("beamforming") are most relevant.

IV. Outer Bounds and Capacity Results

In this section we derive a general outer bound to the achievable rate region of the discrete cMAC-WT and obtain a number of capacity results.

Proposition 3 (*Outer bound for the discrete cMAC-WT*): The capacity region for the cMAC-WT is included in the set of rates satisfying

$$R_1 \leq I(X_1; Y|X_2) \tag{9a}$$

$$R_1 + R_2 \leq (I(V_1, V_2; Y|Q) - I(V_1, V_2; Z|Q))^+, \tag{9b}$$

for some joint distribution

$$p(q)p(v_1, v_2|q)p(x_1, x_2|v_1, v_2)p(y, z|x_1, x_2).$$

Proof: Similarly to Appendix I of [6], we can obtain the upper bound (9b), starting from the inequality $R_1 + R_2 \leq 1/n \cdot H(W_1, W_2|Z^n)$, which is due to the equivocation constraint (3), and using Fano's inequality $H(W_1, W_2|Y^n) \leq n\epsilon_n$ (with $\epsilon_n \to 0$ for $n \to \infty$), which is due to (2). We use the following definitions for the auxiliary random variables: $Q = (J, Y^{J-1}, Z^n_{J+1})$, where J is a random variable independent of any other variable and uniformly distributed in $[1, n]$, $V_1 = (J, Z^n_{J+1}, W_1)$, $V_2 = (J, Y^{J-1}, W_2)$, $X_1 = X_{1,J}$, $X_2 = X_{2,J}$, $Y = Y_J$ and $Z = Z_J$. The upper bound (9a) is a direct consequence of the converse of a regular MAC and the concavity of $I(X_1; Y|X_2)$ in $p(x_1, x_2)$. ■

The outer bound of Proposition 3 and the achievable region of Proposition 2 do not match in general, but in some special cases provide the capacity region, as shown next.

Proposition 4 (Capacity region for the less noisy discrete cMAC-WT and degraded Gaussian cMAC-WT) For the less noisy discrete cMAC-WT, the capacity region is given by

$$\bigcup \{(R_1, R_2) : R_1, R_2 \geq 0$$

$$R_1 \leq I(X_1; Y|X_2) \tag{10a}$$

$$R_1 + R_2 \leq (I(X_1, X_2; Y) - I(X_1, X_2; Z))^+\}, \tag{10b}$$

where the union is taken over all joint distributions that factorize as $p(x_1, x_2)p(y, z|x_1, x_2)$. Moreover, for the degraded Gaussian cMAC-WT ($h_1 = h_2 = h \leq 1$), the capacity region is given by

$$\bigcup \{(R_1, R_2) : R_1, R_2 \geq 0$$

$$R_1 \leq \frac{1}{2} \log \left(1 + P_1(1 - \rho^2)\right)^+ \tag{11a}$$

$$R_1 + R_2 \leq \frac{1}{2} \log \left(\frac{1 + P_1 + P_2 + 2\rho\sqrt{P_1 P_2}}{1 + h_1 P_1 + h_2 P_2 + 2\rho\sqrt{h_1 h_2 P_1 P_2}} \right)^+ \}, \tag{11b}$$

where the union is taken over all possible $-1 \leq \rho \leq 1$.

Proof: Achievability follows immediately from Proposition 2 by setting $V_j = X_j$ and Q constant. For the converse, the upper bound (10a) is a direct consequence of Proposition 3, whereas the upper bound (10b) follows from Proposition 3 by using Theorem 3 in [1]. The capacity region for the Gaussian model follows similarly by noting that, for fixed correlation ρ between the inputs and under the power constraints, the two bounds (10a)-(10b) are both maximized by a Gaussian distribution. In particular, for the sum-rate bound (10b), it is sufficient to use the entropy power inequality similarly to [15] to prove the claim. ■

For the Gaussian cMAC-WT with any h_1 and h_2 we can also identify the sum-rate capacity as follows.

Proposition 5 (Sum-rate capacity for the Gaussian cMAC-WT) The sum-rate capacity region of the Gaussian cMAC-WT is given by

$$C_{sum} = \max_{\substack{0 \leq P'_j \leq P_j \\ -1 \leq \rho \leq 1}} \frac{1}{2} \log \left(\frac{1 + P'_1 + P'_2 + 2\rho\sqrt{P'_1 P'_2}}{1 + h_1 P'_1 + h_2 P'_2 + 2\rho\sqrt{h_1 h_2 P'_1 P'_2}} \right)^+ . \tag{12}$$

Proof: Achievability is given by Proposition 2 with an appropriate choice of the parameters (see Remark 5 below). The converse instead follows by a cut-set argument. Specifically, assume that the two transmitters can perfectly cooperate. The model then reduces to a multiantenna wire-tap channel, whose capacity upper bounds the sum-rate of the cMAC-WT and is given by (12) as found in [8]. ■

Remark 5: The results of Proposition 5 shows that, unlike the MAC-WT [3] [4], for the sum-rate of the cMAC-WT cooperative jamming is not useful, that is, it is optimal to set $a_{1i} = a_{2i} = 1$ (and $N = 1$) in Proposition 2 (see also Remark 4). This may be interpreted in light of the results of [7] [8], where it is shown that for a Gaussian wire-tap channel with a multi-antenna transmitter (and possibly receivers [8]), it is optimal to use Gaussian signalling with optimized covariance matrix. In the cMAC-WT, due to the cooperation between the two transmitters afforded by cognition, a similar behavior is observed.

Remark 6 (*Secrecy capacity region for the degraded orthogonal-component Gaussian cMAC-WT*) Following [10], we can also consider the alternative Gaussian model in which each user has an orthogonal link to the legitimate receiver, as $Y = (Y_1, Y_2)$ with

$$Y_1 = X_1 + N_{y1},\ Y_2 = X_2 + N_{y2}, \tag{13}$$

with independent unit-power Gaussian noises N_{y1} and N_{y2}, while the wire-tapper still receives (4b). From Proposition 2, the following secrecy rate region is achievable

$$R_1 \leq \frac{1}{2}\log(1+P_1) \tag{14a}$$

$$R_1 + R_2 \leq \frac{1}{2}\log\left(\frac{(1+P_1)(1+P_2)}{1+h_1P_1+h_2P_2}\right)^+. \tag{14b}$$

Now, assume that $h_1 + h_2 \leq 1$. It can be seen that, under this assumption, the signal received by the eavesdropper is (stochastically) degraded with respect to Y, since we can equivalently write $Z = \sqrt{h_1}Y_1 + \sqrt{h_2}Y_2 + \sqrt{1-(h_1+h_2)}\tilde{N}_z$, where $\tilde{N}_z$ is unit-power Gaussian, independent of X_1 and X_2. Therefore, we can exploit the capacity result of Proposition 4 to establish that (14) is the secrecy capacity region for the model at hand when $h_1 + h_2 \leq 1$. This result is the counterpart of the sum-capacity result in [10], where the sum-capacity of an orthogonal-component MAC-WT is derived as (14b). In other words, in terms of the sum-rate, cognition does not provide any gain in this model due to the impossibility of coherent power combining at the destination (though it may do so for the individual rates).

V. Concluding Remarks

"Cognition", in an information-theoretic sense, can be seen as a simple model that enables the study of the impact of cooperation in communication networks. In this paper, we extended the model of [3] [4], i.e., the multiple access channel with an eavesdropper, to a scenario where cooperation between the two sources is possible via cognition. Achievable secrecy rates, outer bounds and secrecy capacity results for some special cases have been derived focusing on a model in which one of the two source knows the message of the second in advance. Our conclusions shed light into scenarios where cooperation is more or less effective in improving the secrecy rates. Possible extensions of this work include studying generalized-feedback multiple access channels with an eavesdropper and fully assessing the impact of cooperative jamming.

VI. Appendix

A. Appendix A: Proof of Proposition 2

We prove Proposition 2 for Q constant to simplify the discussion and notation. The general result follows as discussed in the proof of Proposition 1 by conditioning on a (typical) time-sharing sequence q^n [5]. Moreover, we prove the result for $X_j = V_j$, $j = 1, 2$, since the general result follows similarly to, e.g., [6] [5], by substituting in the proof below V_j to X_j and then prefixing channels $p(x_1|x_2, v_1, v_2, q)$ and $p(x_2|v_2, q)$ (i.e., randomization). We proceed similarly to [5] by first showing the existence of a codebook satisfying certain properties (by using random coding techniques) and then calculating the equivocation for a specific code in the class. Specifically, we are at first interested in showing that there exists at least a code that: (*i*) satisfies (2); (*ii*) guarantees at the same time that the probability of error at the eavesdropper in detecting x_1^n and x_2^n, given W_1, W_2 vanishes as $n \to \infty$. In other words, condition (*ii*) requires that there exists a decoding function $\tilde{g}_n$ for the eavesdropper such that $\Pr[\tilde{g}_n(Z^n, W_1, W_2) \neq (S_{12}, S_1, S_2)] \to 0$, where we recall that the codewords are generated as (1). The reason for enforcing condition (*ii*) will be clear when we will evaluate the equivocation at the eavesdropper. To prove the existence of such a codebook, we use the following random generation.

Codebook generation: Generate $2^{n(R_2+R_2')}$ codewords $x_2^n(a, b)$ with $a \in [1, 2^{nR_2}]$, $b \in [1, 2^{nR_2'}]$ by choosing uniformly within the set of strongly typical sequences $T_\epsilon^{(n)}(X_2)$. For each such sequence $x_2^n(a, b)$, generate $2^{n(R_1+R_1')}$ codewords $x_1^n(a, b, c, d)$ with $c \in [1, 2^{nR_1}]$, $d \in [1, 2^{nR_1'}]$ by choosing uniformly from the set of conditionally typical sequences $T_\epsilon^{(n)}(X_1|x_2^n(a, b))$.

Encoding: Given messages $W_1 \in [1, 2^{nR_1}]$ and $W_2 \in [1, 2^{nR_2}]$ and random variables $S_1 \in [1, 2^{nR_1'}]$, $S_{12} \in [1, 2^{nR_2'}]$, user 2 transmits $x_2^n(W_2, S_{12})$ and user 1 sends $x_1^n(W_2, S_{12}, W_1, S_1)$. Notice that private randomness at user 2, i.e., S_2, is not used, and is therefore set to $S_2 = \emptyset$. We will see that it will be optimal to choose also $R_1' = 0$.

Check of conditions (*i*) *and* (*ii*): In order for condition (*i*) to be satisfied, the following rate constraints are sufficient (and necessary) [13]

$$R_1 + R_1' \leq I(X_1; Y|X_2) \tag{15a}$$

$$R_1 + R_1' + R_2 + R_2' \leq I(X_1, X_2; Y). \tag{15b}$$

Moreover, in order for (*ii*) to be guaranteed as well, it is sufficient (and necessary) that

$$R_1' \leq I(X_1; Z|X_2) \tag{16a}$$

$$R_1' + R_2' \leq I(X_1, X_2; Z). \tag{16b}$$

For reasons that will be clear below, we specifically impose

$$R_1' + R_2' = I(X_1, X_2; Z). \tag{17}$$

Notice that (17), due to (15b), requires $I(X_1, X_2; Z) \leq I(X_1, X_2; Y)$, which is assumed hereafter. Having proved that under conditions (15) and (16), a codebook that satisfies conditions (*i*) and (*ii*) exists, we now turn to the calculation of the equivocation for any given code, say $\mathcal{C}$, in the class identified above (with (17)).

Equivocation: We have

$$\begin{aligned} H(W_1, W_2|Z^n) &= H(W_1, W_2) - I(W_1, W_2; Z^n) = \\ &= H(W_1, W_2) - I(X_1^n, X_2^n; Z^n) \qquad (18) \\ &+ I(X_1^n, X_2^n; Z^n|W_1, W_2), \end{aligned}$$

where we have exploited the Markov chain $(W_1, W_2) - (X_1^n, X_2^n) - Z^n$. Now, we consider the terms in (18) separately. We start with

$$\begin{aligned} I(X_1^n, X_2^n; Z^n|W_1, W_2) &= H(X_1^n, X_2^n|W_1, W_2) \\ &- H(X_1^n, X_2^n|Z^n, W_1, W_2) \\ &\geq n(R_1' + R_2') - n\epsilon_n, \end{aligned}$$

where $H(X_1^n, X_2^n|W_1, W_2) = n(R_1' + R_2')$ follows from the definition of the code given above, inequality $H(X_1^n, X_2^n|Z^n, W_1, W_2) \leq n\epsilon_n$ with $\epsilon_n \to 0$ for $n \to \infty$ is due to Fano's inequality and the condition (*ii*) satisfied by the code. We then focus on the remaining term in (18):

$$I(X_1^n, X_2^n; Z^n) = H(Z^n) - H(Z^n|X_1^n, X_2^n). \qquad (19)$$

To treat the second term in (19), we observe that $H(Z^n|X_1^n, X_2^n)$ equals

$$2^{-n(R_1+R_1'+R_2+R_2')} \sum_{(x_1^n, x_2^n) \in \mathcal{C}} H(Z^n|X_1^n = x_1^n, X_2^n = x_2^n),$$

which is in turn equal to (see also [5]):

$$\begin{aligned} &\sum_{(x_1^n, x_2^n) \in \mathcal{C}} \sum_{\substack{x_1 \in \mathcal{X}_1, \\ x_2 \in \mathcal{X}_2}} N(x_1, x_2|x_1^n, x_2^n) \cdot H(Z|X_1 = x_1, X_2 = x_2) \geq \\ &\sum_{(x_1^n, x_2^n) \in \mathcal{C}} \sum_{\substack{x_1 \in \mathcal{X}_1, \\ x_2 \in \mathcal{X}_2}} (p(x_1, x_2) - \epsilon_1) \cdot H(Z|X_1 = x_1, X_2 = x_2) = \\ &\qquad\qquad H(Z|X_1, X_2) - \epsilon_2, \end{aligned}$$

where the first equality follows from the definition of $N(a, b|x_1^n, x_2^n)$ as the joint type of sequences (x_1^n, x_2^n), and the inequality in the second line follows from the code construction and the definition of jointly typical sequences. We look now at the first term in (19). We have (see also [5])

$$\begin{aligned} H(Z^n) &= H(Z^n) + H(\hat{Z}^n|Z^n) \\ &= H(\hat{Z}^n) + H(Z^n|\hat{Z}^n), \end{aligned}$$

having defined the sequence $\hat{Z}^n$ as the function of Z^n: $\hat{z}^n = z^n$ if $z^n \in T_\epsilon^{(n)}(Z)$ and $\hat{z}^n$ arbitrary otherwise. It follows that $H(Z^n) \leq \log|T_\epsilon^{(n)}(Z)| + n\epsilon_n' \leq H(Z) + \epsilon + n\epsilon_n'$, where we have used Fano's inequality $H(Z^n|\hat{Z}^n) \leq 1 + n \log|\mathcal{Z}| \Pr[\hat{Z}^n \neq Z^n] = n\epsilon_n'$, with $\epsilon_n' \to 0$ for $n \to \infty$, since we have $\Pr[\hat{Z}^n \neq Z^n] \to 0$ by the conditional Asymptotic Equipartition Property (AEP). As a result of the inequalities derived above, recalling (17) and neglecting the $o(n)$ and of the order of ϵ terms, we have from (18)

$$\begin{aligned} H(W_1, W_2|Z^n) &\geq H(W_1, W_2) - nI(X_1, X_2; Z) + n(R_1' + R_2') \\ &= H(W_1, W_2), \end{aligned}$$

which shows that the desired equivocation condition (3) is satisfied.

The proof is concluded by noting that the rate region from (15), (16a) and (17) is given by (eliminating R_2')

$$R_1 \leq I(X_1; Y|X_2) - R_1' \qquad (20a)$$

$$R_1 + R_2 \leq I(X_1, X_2; Y) - I(X_1, X_2; Z) \qquad (20b)$$

with $R_1' \leq I(X_1; Z|X_2)$, which is maximized for $R_1' = 0$.

For the Gaussian case, we evaluate (7) with $\Pr[Q = i] = \lambda_i$, $p(v_1, v_2|Q = i) = \mathcal{N}\left(\mathbf{0}, \begin{bmatrix} P_{1i} & \rho_i\sqrt{P_{1i}P_{2i}} \\ \rho_i\sqrt{P_{1i}P_{2i}} & P_{1i} \end{bmatrix}\right)$ and $X_{ji} = a_{ji}V_{ji} + \bar{a}_{ji}X_{ji}'$ with X_{ji}' being a Gaussian variable independent of all other variables and with power P_{ji}. The constraint on N follows from Theorem 2 in [12].

References

[1] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory,* vol. IT-24, no. 3, pp. 339-348, May 1978.

[2] R. Liu, I. Maric, P. Spasojevic and R.D Yates, "Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions," *IEEE Inform. Theory,* vol. 54, no. 6, pp. 2493-2507, Jun. 2008.

[3] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inform. Theory,* vol. 54, no. 12, pp. 5747-5755, Dec. 2008.

[4] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inform. Theory,* vol. 54, no. 6, pp. 2735-2751, June 2008.

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

[6] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inform. Theory*, vol. 54, no. 9, pp. 4005-4019, Sept. 2008.

[7] A. Khisti and G. Wornell, "Secure transmission with multiple antennas: the MISOME wiretap channel," submitted [arXiv:0708.4219v1].

[8] T. Liu and S. Shamai, "A note on the secrecy capacity of the multi-antenna wiretap channel," submitted [arXiv:0710.4105v1].

[9] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdu, "Cognitive interference channels with confidential messages," in *Proc. Annual Allerton Conf. on Communication, Control and Computing,* Monticello, IL, Sept. 26-28, 2007.

[10] E. Ekrem and S. Ulukus, "On the secrecy of multiple access wiretap channel," in *Proc. Annual Allerton Conf. on Communications, Control and Computing,* Monticello, IL, Sept. 2008.

[11] V. Aggarwal, L. Sankar, R. Calderbank, H. V. Poor, "Secrecy capacity of a class of orthogonal relay eavesdropper channels," submitted [arXiv:0812.2275].

[12] A. S. Motahari, A. K. Khandani, "Capacity bounds for the Gaussian interference channel," submitted [arXiv:0801.1306v1].

[13] V.V. Prelov, "Transmission over a multiple-access channel with a special source hierarchy," *Probl. Peredach. Inform.,* vol. 20, pp. 3-10, Oct.-Dec. 1984.

[14] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.,* vol. 54, pp. 1355–1387, 1975.

[15] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inform. Theory,* vol. IT-24, no. 4, pp. 451-456, Jul. 1978.