MAC with Partially Cooperating Encoders and Security Constraints

Zohaib Hassan Awan
ICTEAM institute
Université Catholique de Louvain
Louvain La Neuve 1348, Belgium
zohaib.awan@uclouvain.be

Abdellatif Zaidi
Université Paris-Est Marne-la-Vallée
77454 Marne-la-Vallée Cedex 2,
France
abdellatif.zaidi@univ-mlv.fr

Luc Vandendorpe
ICTEAM institute
Université Catholique de Louvain
Louvain La Neuve 1348, Belgium
luc.vandendorpe@uclouvain.be

ABSTRACT

We study a special case of Willems's two-user multiaccess channel with partially cooperating encoders from security perspective. This model differs from Willems's setup in that only one encoder, Encoder 1, is allowed to conference, Encoder 2 does not transmit any message, and there is an additional passive eavesdropper from whom the communication should be kept secret. For the discrete memoryless case, we establish inner and outer bounds on the rate-equivocation region. Furthermore, we show that these bounds coincide in the case of perfect secrecy, and so we characterize fully the secrecy capacity. For the Gaussian model, we establish lower and upper bounds on the perfect secrecy rate. We also show that these bounds agree in some extreme cases of cooperation between encoders. We illustrate our results through some numerical examples.

General Terms

Multiple access channel, conferencing, security.

1. INTRODUCTION

We investigate the problem of secure communication over a multiple access channel (MAC) with partially cooperating encoders. The MAC with partially cooperating encoders and no security constraints was studied by Willems in [1]. In this model, prior to sending their messages, two encoders communicate with each other over noiseless bit-pipes of finite-capacities. Willems characterizes the complete capacity region of this model in the discrete memoryless case. In [2], Bross *et al.* establish the capacity region of the corresponding Gaussian model [2]. In both [1] and [2], among other observations, it is shown in particular that holding a conference prior to the transmission enlarges the capacity region relative to the standard MAC with independent inputs.

In this work, we study a special case of Willem's setup by adding security constraints on the communication. More specifically, we restrict the role of Encoder 2 to only helping Encoder 1, i.e., Encoder 2 has no message to transmit. Also, we consider that there is a passive eavesdropper who overhears the transmission from the encoders to a legitimate receiver and tries to capture the communication. The role of Encoder 2 is then to help Encoder 1 communicate with the legitimate receiver while keeping the transmitted information *secret* from the eavesdropper. The two encoders are connected via a unidirectional bit-pipe of finite capacity C_{12} which permits the Encoder 1 to share information about the transmitted message with Encoder 2. Figure 1 shows the model that we study. From a practical viewpoint, this model may be useful for the study of cooperation among base stations over a backbone links in order to hide information from a potential adversary. In this contribution, we study the secrecy capacity region of this model.

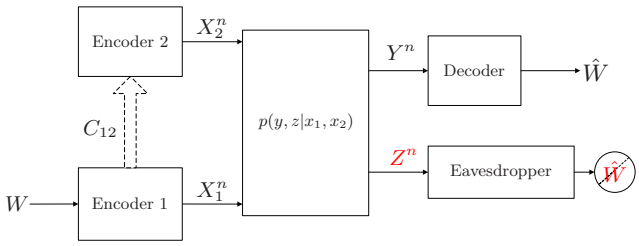

Figure 1: Multiaccess channel with partially cooperating encoders and security constraints.

For the DM case, we establish outer and inner bounds on the secrecy-capacity region. We obtain the inner bound by generalizing the coding scheme of [1] to incorporate binning accounting for security. We obtain the converse proof by using bounding techniques similar to in [3, 4], and redefining the auxiliary random variables taking into account the specific channel structure. Furthermore, we show that the bounds coincide in the case of perfect secrecy; and, so, we characterize the secrecy capacity of this model.

Next, we study a Gaussian model. We focus only on perfect secure transmission in this case. For this model, we also establish lower and upper bounds on the secrecy capacity. The lower bound uses a coding scheme that is similar to the one that we use for the achievability result in the DM case. The upper bound has the same expression as the secrecy capacity of the Gaussian two-antenna transmitter one-antenna receiver wiretap channel [5–7]; but is obtained here using an alternative proof that follows by reasoning from the outer

SECURENETS 2011, May 16, Paris, France

DOI 10.4108/icst.valuetools.2011.245784

bound that we establish for the DM case, in a way similar to our previous work [8].

We show that our lower bound performs well in general and is optimal in some extreme cases, including when the two encoders do not conference (i.e., $C_{12} = 0$) or fully cooperate (i.e., $C_{12} = \infty$). Our coding schemes reduces to merely injecting independent noise [4, Theorem 3] in the first case, and to full two-antenna cooperation [5–7] in the second case.

The MAC model that we study in this paper has connections with a number of related works. Compared to the orthogonal relay-eavesdropper channel studied in [9], the orthogonal link between the source and relay is replaced here by a bit-pipe of finite capacity C_{12}. Compared to the wiretap channel with a helping interferer studied in [10], our model incorporates cooperation between the users. Finally, compared to the primitive relay channel in [11], our model here adds security constraints on the transmitted message.

Notation:

In this paper, the notation X^n is used as a shorthand for $(X_1, X_2, \ldots, X_n)$, $\mathbb{E}\{.\}$ denotes the expectation operator, $|\mathcal{X}|$ denotes the cardinality of set $\mathcal{X}$, the boldface letter $\mathbf{X}$ denotes the covariance matrix, $H(.)$, $h(.)$ denote the entropy of the discrete and continuous random variables respectively. We define the functions $\mathcal{C}(x) = \frac{1}{2}\log_2(1+x)$ and $[x]^+ = \max\{0, x\}$. Throughout the paper the logarithm function is taken to the base 2.

2. DISCRETE MEMORYLESS MODEL

In this section we establish outer and inner bounds on the rate-equivocation region for the MAC with partially cooperating encoders shown in Figure 1.

2.1 Channel Model

We consider a two-encoder discrete memoryless channel $p(y, z|x_1, x_2)$ with input alphabets $\mathcal{X}_1$ at Encoder 1 and $\mathcal{X}_2$ at Encoder 2 and output alphabets $\mathcal{Y}$ at a legitimate receiver and $\mathcal{Z}$ at a passive eavesdropper. The channel is memoryless in the sense that

$$p(y^n, z^n|x_1^n, x_2^n) = \prod_{i=1}^{n} p(y_i, z_i|x_{1,i}, x_{2,i}). \tag{1}$$

Encoder 1 wants to transmit a message $W \in \mathcal{W} = \{1, \ldots, 2^{nR}\}$ to the legitimate receiver while keeping it secret from the eavesdropper. Encoder 1 can get help from Encoder 2 to whom it is connected via a bit-pipe of finite capacity C_{12}. Encoder 1 conferences the message W to Encoder 2 using K functions $\{\phi_{11}, \phi_{12}, \ldots, \phi_{1K}\}$, over the noiseless pipe. We define $Q_{1k} := \phi_{1k}(W)$ as the output of the communication process for the k-*th* communication, where Q_{1k} ranges over the finite alphabet $\mathcal{Q}_{1k}$, for $k = 1, \ldots, K$. The information conferenced is bounded due to the finiteness of noiseless pipe capacity between the encoders of user 1 and 2, given by C_{12}. A conference is permissible if communication functions are such that

$$\sum_{k=1}^{K} \log|\mathcal{Q}_{1k}| \leq nC_{12}. \tag{2}$$

Definition 1. A $(2^{nR}, n)$ code with one way cooperating encoder as shown in Figure 1 consists of encoding functions

$$\begin{aligned} \phi_1 &: \{1, \ldots, 2^{nR}\} \longrightarrow \mathcal{X}_1^n, \\ \phi_{1k} &: \{1, \ldots, 2^{nR}\} \longrightarrow \{1, \ldots, \mathcal{Q}_{1k}\} \ k = 1, ..., K, \\ \phi_2 &: \{1, \ldots, 2^{nC_{12}}\} \longrightarrow \mathcal{X}_2^n, \end{aligned} \tag{3}$$

and a decoding function $\psi(\cdot)$ at the legitimate receiver

$$\psi : \mathcal{Y}^n \longrightarrow \{1, \ldots, 2^{nR}\}. \tag{4}$$

The average error probability for the $(2^{nR}, n)$ code is defined as

$$P_e^n = \frac{1}{2^{nR}} \sum_{W \in \mathcal{W}} p\{\hat{W} \neq W|W\}. \tag{5}$$

The eavesdropper overhears to what the user 1 and 2 transmit and tries to guess the information from it. The equivocation rate per channel use is defined as $R_e = H(W|Z^n)/n$. A rate-equivocation pair (R, R_e) is said to be achievable if for any $\epsilon > 0$ there exists a sequence of codes $(2^{nR}, n)$ such that for any $n \geq n(\epsilon)$

$$\begin{aligned} \frac{H(W)}{n} &\geq R - \epsilon, \\ \frac{H(W|Z^n)}{n} &\geq R_e - \epsilon, \\ P_e^n &\leq \epsilon. \end{aligned} \tag{6}$$

2.2 Outer Bound

The following theorem provides an outer bound on the secrecy-capacity region of the MAC with one-way cooperating encoder and security constraints shown in Figure 1.

Theorem 1. For the MAC with partially cooperating encoders and security constraints shown in Figure 1, and for any achievable rate-equivocation pair (R, R_e), there exists random variables $U \leftrightarrow (V_1, V_2) \leftrightarrow (X_1, X_2) \leftrightarrow (Y, Z)$, such that (R, R_e) satisfies

$$\begin{aligned} R &\leq \min\{I(V_1, V_2; Y), I(V_1; Y|V_2) + C_{12}\} \\ R_e &\leq R \\ R_e &\leq \min\{I(V_1, V_2; Y|U) - I(V_1, V_2; Z|U), \\ &\qquad I(V_1; Y|V_2, U) + C_{12} - I(V_1, V_2; Z|U)\}. \end{aligned} \tag{7}$$

Proof: The proof of Theorem 1 appears in [12].

Remark 1. The proof of Theorem 1 uses techniques that are similar to in [3, 4]; but, in addition, we need to redefine the involved auxiliary random variables.

Remark 2. The bound on the equivocation rate in Theorem 1 reduces to the secrecy capacity of Wyner's wiretap channel [13] by removing the helping Encoder 2, i.e, by setting $C_{12} := 0$ and $V_2 = X_2 = \phi$.

2.3 Inner Bounds

We now turn to establish an inner bound on the secrecy-capacity region of the MAC with one-way cooperating encoder and security constraints shown in Figure 1. The following theorem states the result.

Theorem 2. For the MAC with partially cooperating encoders and security constraints shown in Figure 1, the rate

pairs in the closure of the convex hull of all (R, R_e) satisfying

$$\begin{aligned} R &\le \min\{I(V_1,V_2;Y|U), I(V_1;Y|V_2,U)+C_{12}\} \\ R_e &\le R \\ R_e &\le \min\{I(V_1,V_2;Y|U) - I(V_1,V_2;Z|U), \\ &\qquad I(V_1;Y|V_2,U)+C_{12}-I(V_1,V_2;Z|U)\} \end{aligned} \quad (8)$$

for some measure $p(u,v_1,v_2,x_1,x_2,y,z) = p(u)p(v_1,v_2|u)$ $p(x_1,x_2|v_1,v_2)p(y,z|x_1,x_2)$, are achievable.

Proof: The proof of Theorem 2 appears in Appendix A.

Considering the bounds on the equivocation rate in Theorem 1 and Theorem 2, it easy to see that these coincide, and so characterize fully the secrecy capacity.

***Theorem** 3.* For the MAC with partially cooperating encoders and security constraints shown in Figure 1, the perfect secrecy capacity is given by

$$\begin{aligned} C_s = \max \min\{&I(V_1,V_2;Y|U) - I(V_1,V_2;Z|U), \\ &I(V_1;Y|V_2,U)+C_{12}-I(V_1,V_2;Z|U)\} \end{aligned} \quad (9)$$

where the maximization is all measures of the form

$$\begin{aligned} &p(u,v_1,v_2,x_1,x_2,y,z) = \\ &\qquad p(u)p(v_1,v_2|u)p(x_1,x_2|v_1,v_2)p(y,z|x_1,x_2). \end{aligned} \quad (10)$$

3. MEMORYLESS GAUSSIAN MODEL

In this section, we study the Gaussian version of the MAC with partially cooperating encoders and security constraints shown in Figure 1. We only focus on the case of perfect secrecy, i.e., $(R, R_e) = (R, R)$.

3.1 Channel Model

For the Gaussian model, the outputs of the MAC at the legitimate receiver and eavesdropper are given by

$$\begin{aligned} Y_i &= h_{1d}X_{1,i} + h_{2d}X_{2,i} + N_{1,i} \\ Z_i &= h_{1e}X_{1,i} + h_{2e}X_{2,i} + N_{2,i} \end{aligned} \quad (11)$$

where i is the time index, h_{1d}, h_{2d}, h_{1e}, h_{2e} are the fading gain coefficients associated with the user 1-to-destination (1-D), user 2-to-destination (2-D), user 1-to-eavesdropper (1-E), and user 2-to-eavesdropper (2-E) links respectively. The noise processes $\{N_{1,i}\}$ and $\{N_{2,i}\}$ are independent and identically distributed (i.i.d) with the components being zero mean Gaussian random variables with variances σ_1^2 and σ_2^2, respectively; and $X_{1,i}$ and $X_{2,i}$ are the inputs from the Encoder 1 and Encoder 2, respectively. The channel inputs are bounded by average block power constraints,

$$\sum_{i=1}^{n} \mathbb{E}[X_{1,i}^2] \le nP_1, \qquad \sum_{i=1}^{n} \mathbb{E}[X_{2,i}^2] \le nP_2. \quad (12)$$

3.2 Upper Bound on the Perfect Secrecy Rate

A trivial upper bound on the Gaussian MAC with partially cooperating encoders and security constraints (11) follows from the secrecy capacity of a multiple-input multiple-output (MIMO) wiretap channel [5,6] — taking a setup with two antennas at the transmitter, one antenna at the legitimate receiver and one antenna at the eavesdropper in our case. That is,

$$C_{\rm s} \le \max_{\mathbf{K_P}\in\mathcal{K}_P} [I(X_1,X_2;Y) - I(X_1,X_2;Z)] \quad (13)$$

where the maximization is over $[X_1,X_2] \sim \mathcal{N}(\mathbf{0},\mathbf{K_P})$ with $\mathcal{K}_P = \left\{\mathbf{K_P} : \mathbf{K_P} = \begin{bmatrix} P_1 & \psi\sqrt{P_1P_2} \\ \psi\sqrt{P_1P_2} & P_2 \end{bmatrix},\ -1 \le \psi \le 1\right\}$, with $\mathbb{E}[X_1^2]$, $\mathbb{E}[X_2^2]$ satisfying (12).

Alternatively, we can also establish the upper bound (13) from the rate-equivocation region established for the DM case in Theorem 1, as follows. Taking the first term of minimization in the bound on the equivocation rate in Theorem 1, we get

$$C_{\rm s} \le \max\ [I(V_1,V_2;Y \mid U) - I(V_1,V_2;Z \mid U)] \quad (14)$$

where $U \leftrightarrow (V_1,V_2) \leftrightarrow (X_1,X_2) \leftrightarrow (Y,Z)$. The rest of the proof closely follows the bounding technique established in [8], in the context of a parallel relay-eavesdropper channel. More specifically, continuing from (14) we get

$$\begin{aligned} C_{\rm s} &\le I(V_1,V_2;Y \mid U) - I(V_1,V_2;Z \mid U) \\ &\overset{(a)}{\le} I(V_1,V_2;Y) - I(V_1,V_2;Z) \\ &\le I(V_1,V_2;Y,Z) - I(V_1,V_2;Z) \\ &\overset{(b)}{=} [I(X_1,X_2;Y,Z) - I(X_1,X_2;Y,Z \mid V_1,V_2)] \\ &\quad -[I(X_1,X_2;Z) - I(X_1,X_2;Z \mid V_1,V_2)] \\ &= [I(X_1,X_2;Y,Z) - I(X_1,X_2;Z)] \\ &\quad -[I(X_1,X_2;Y,Z \mid V_1,V_2) - I(X_1,X_2;Z \mid V_1,V_2)] \\ &\le I(X_1,X_2;Y,Z) - I(X_1,X_2;Z) \\ &= I(X_1,X_2;Y \mid Z) \end{aligned} \quad (15)$$

where (a) follows from the fact that the conditional mutual information difference $I(V_1,V_2;Y \mid U) - I(V_1,V_2;Z \mid U)$ is maximized by $U :=$ constant and (b) holds since $(V_1,V_2) \leftrightarrow (X_1,X_2) \leftrightarrow (Y,Z)$ is a Markov chain.

Now, the upper bound in (15) can be tightened by using an argument previously used in [5,6] in the context of multi-antenna wiretap channel. Noticing that the upper bound (14) depends on $p(y,z|x_1,x_2)$ only through its marginals $p(y|x_1,x_2)$ and $p(z|x_1,x_2)$, the upper bound (15) can be further tightened as

$$R_e^{\rm up} \le \max_{p(x_1,x_2)} \min_{p(y',z'|x_1,x_2)} I(X_1,X_2;Y' \mid Z') \quad (16)$$

where the joint conditional $p(y',z'|x_1,x_2)$ has the same marginals as $p(y,z|x_1,x_2)$, i.e., $p(y'|x_1,x_2) = p(y|x_1,x_2)$ and $p(z'|x_1,x_2) = p(z|x_1,x_2)$.

Following [5,6], it can be shown that the bound in (16) is maximized with the jointly Gaussian inputs $[X_1,X_2] \sim \mathcal{N}(\mathbf{0},\mathbf{K_P})$, with $\mathbb{E}[X_1^2]$ and $\mathbb{E}[X_2^2]$ satisfying (12).

Finally, the evaluation of the upper bound (16) with these jointly Gaussian inputs and then the minimization over all possible correlations between Y' and Z' yield the desired result.

3.3 Lower Bound on the Perfect Secrecy Rate

For the Gaussian MAC with partially cooperating encoders and security constraints (11), we obtain a lower bound on the secrecy capacity by using our result for the DM model in Theorem 2. The results established for the DM case can be readily extended to memoryless channels with discrete time and continuous alphabets using standard techniques [14, Chapter 7].

$$R_e^{\text{low}} = \max_{\substack{P_1,P_2,\\ 0\le\alpha\le 1}} \min\left\{\mathcal{C}\left(\frac{|h_{1d}|^2P_1+|h_{2d}|^2P_2+2\sqrt{\bar{\alpha}|h_{1d}|^2P_1|h_{2d}|^2P_2}}{{\sigma_1}^2}\right)-\mathcal{C}\left(\frac{|h_{1e}|^2P_1+|h_{2e}|^2P_2+2\sqrt{\bar{\alpha}|h_{1e}|^2P_1|h_{2e}|^2P_2}}{\sigma_2^2}\right)\right]^+,$$
$$\left[\mathcal{C}\left(\frac{\alpha|h_{1d}|^2P_1}{\sigma_1^2}\right)+C_{12}-\mathcal{C}\left(\frac{|h_{1e}|^2P_1+|h_{2e}|^2P_2+2\sqrt{\bar{\alpha}|h_{1e}|^2P_1|h_{2e}|^2P_2}}{\sigma_2^2}\right)\right]^+\Big\}. \quad (17)$$

Corollary 1. For the Gaussian MAC with partially cooperating encoders and security constraints (11), a lower bound on the secrecy capacity is given by (17).

Proof: The achievability follows by evaluating the inner bound in Theorem 2 with the choice $V_1 = X_1$ and $U = V_2 = X_2$, $X_1 := \tilde{X}_1 + \sqrt{\frac{\bar{\alpha}P_1}{P_2}}X_2$, $\tilde{X}_1 \sim \mathcal{N}(0, \alpha P_1)$ independent of $X_2 \sim \mathcal{N}(0, P_2)$, with $\alpha \in [0,1]$ and $\bar{\alpha} := 1-\alpha$. This gives

$$R_e^{\text{low}} \le \min\{I(X_1,X_2;Y) - I(X_1,X_2;Z), \quad I(X_1;Y|X_2) + C_{12} - I(X_1,X_2;Z)\}. \quad (18)$$

The computation of the terms involved in (18) with the aforementioned jointly Gaussian distribution is as follows.

$$\begin{aligned} &I(X_1,X_2;Y)\\ &=h(Y)-h(Y|X_1,X_2)\\ &=h(h_{1d}X_1+h_{2d}X_2+N_1)-h(N_1)\\ &=\frac{1}{2}\log 2\pi e(|h_{1d}|^2P_1+|h_{2d}|^2P_2+2\sqrt{\bar{\alpha}|h_{1d}|^2|h_{2d}|^2P_1P_2}+\sigma_1^2)\\ &\quad-\frac{1}{2}\log 2\pi e\sigma_1^2\\ &=\frac{1}{2}\log\left(1+\frac{|h_{1d}|^2P_1+|h_{2d}|^2P_2+2\sqrt{\bar{\alpha}|h_{1d}|^2|h_{2d}|^2P_1P_2}}{\sigma_1^2}\right), \end{aligned} \quad (19)$$

$$\begin{aligned} &I(X_1,X_2;Z)\\ &=h(Z)-h(Z|X_1,X_2)\\ &=h(h_{1e}X_1+h_{2e}X_2+N_2)-h(N_2)\\ &=\frac{1}{2}\log 2\pi e(|h_{1e}|^2P_1+|h_{2e}|^2P_2+2\sqrt{\bar{\alpha}|h_{1e}|^2|h_{2e}|^2P_1P_2}+\sigma_2^2)\\ &\quad-\frac{1}{2}\log 2\pi e\sigma_2^2\\ &=\frac{1}{2}\log\left(1+\frac{|h_{1e}|^2P_1+|h_{2e}|^2P_2+2\sqrt{\bar{\alpha}|h_{1e}|^2|h_{2e}|^2P_1P_2}}{\sigma_2^2}\right), \end{aligned} \quad (20)$$

$$\begin{aligned} I(X_1;Y|X_2) &= h(Y|X_2)-h(Y|X_1,X_2)\\ &= h(h_{1d}X_1+h_{2d}X_2+N_1|X_2)-h(N_1)\\ &= h(h_{1d}X_1+N_1|X_2)-h(N_1)\\ &\overset{(a)}{=} h(h_{1d}\tilde{X}_1+h_{1d}\sqrt{\frac{\bar{\alpha}P_1}{P_2}}X_2+N_1|X_2)-h(N_1)\\ &\overset{(b)}{=} h(h_{1d}\tilde{X}_1+N_1)-h(N_1)\\ &= \frac{1}{2}\log 2\pi e(\alpha|h_{1d}|^2P_1+\sigma_1^2)-\frac{1}{2}\log 2\pi e\sigma_1^2\\ &= \frac{1}{2}\log\left(1+\frac{\alpha|h_{1d}|^2P_1}{\sigma_1^2}\right) \end{aligned} \quad (21)$$

where (a) follows because $X_1 := \tilde{X}_1 + \sqrt{\frac{\bar{\alpha}P_1}{P_2}}X_2$, (b) follows because $\tilde{X}_1$ and X_2 are independent. Substituting (19)-(21) in (18) gives (17). This completes the proof. □

3.4 Analysis of Some Extreme Cases

In this section we study two special cases of the Gaussian MAC (11) with partially cooperating encoders shown in Figure 1, where the capacity of the bit-pipe is either,

1. $C_{12} = 0$, or
2. $C_{12} = \infty$.

The first case corresponds to the classical MAC wiretap channel [15] in which the encoders of user 1 and 2 do not cooperate. The second case corresponds to the MAC with totally cooperating encoders. This channel can be viewed as a two-antenna transmitter wiretap channel [6, 16].

Case 1: $C_{12} = 0$

In this case the encoders do not cooperate, and our model reduces to a special case of the classical multiaccess wiretap channel with independent inputs (since encoder 2 does not send any message).

Corollary 2. For the Gaussian MAC (11) with independent inputs, the perfect secrecy capacity is given by

$$C_s = \max_{P_1,P_2} \min\left\{\left[\mathcal{C}\left(\frac{|h_{1d}|^2P_1+|h_{2d}|^2P_2}{\sigma_1^2}\right)-\mathcal{C}\left(\frac{|h_{1e}|^2P_1+|h_{2e}|^2P_2}{\sigma_2^2}\right)\right]^+, \left[\mathcal{C}\left(\frac{|h_{1d}|^2P_1}{\sigma_1^2}\right)-\mathcal{C}\left(\frac{|h_{1e}|^2P_1}{|h_{2e}|^2P_2+\sigma_2^2}\right)\right]^+\right\}. \quad (22)$$

Proof. ***Upper Bound.*** The bound given by the first term of the minimization in (22) follows straightforwardly from (13) — taking independent inputs as $C_{12} = 0$.

We bound the second term of the minimization in (22) by using elements from an upper bounding technique developed in [9]. We assume that there is a noiseless link between user 2 and the legitimate receiver, and the eavesdropper is constrained to treat the user 2's signal as unknown noise. The upper bound established for this model, with full cooperation between the user 2 and the legitimate receiver and a constrained eavesdropper, also applies to the general model.

With full cooperation between user 2–legitimate receiver link, the legitimate receiver can remove the effect of user 2 transmission from the output Y_i of the MAC (11). The equivalent channel model is given by

$$Y_i' = h_{1,d}X_{1,i} + N_{1,i}. \quad (23)$$

For the constrained eavesdropper the user 2's transmission acts as an interference, the worst case is obtained with the X_2 being Gaussian distributed [9]. The equivalent channel

model at the eavesdropper is given by

$$Z_i' = h_{1,e}X_{1,i} + \underbrace{h_{2,e}\mathbb{E}[X_{2,i}^2]}_{\text{interference}} + N_{2,i}. \quad (24)$$

The equivalent channel model, with full cooperation between user 2–legitimate receiver link and worst case user 2 to eavesdropper transmission, reduces to a Gaussian wiretap channel, the secrecy capacity of which is established in [17], i.e,

$$C_s \leq \max[I(X_1;Y') - I(X_1;Z')] \quad (25)$$

where the maximization is over $X_1 \sim \mathcal{N}(0,P_1), X_2 \sim \mathcal{N}(0,P_2)$.

Straightforward algebra which is omitted for brevity shows that the computation of (25) gives the second term of the minimization in (22).

Lower Bound. The proof follows by straightforward application of NF scheme [4, Theorem 3] to the considered setup, where the encoders send independent codewords. The achievability follows by evaluating the achievable equivocation rate in [4, Theorem 3] with the choice $V_1 := X_1$, $V_2 := X_2$, and $X_1 \sim \mathcal{N}(0,P_1)$ independent of $X_2 \sim \mathcal{N}(0,P_2)$. □

Case 2: $C_{12} = \infty$

In the case in which $C_{12} = \infty$, the model reduces to the classical two-antenna transmitter wiretap channel.

***Corollary** 3.* For the Gaussian MAC (11) with fully cooperating encoders, the secrecy capacity is given by

$$C_s = \max_{\mathbf{K_P} \in \mathcal{K}_P} I(X_1,X_2;Y) - I(X_1,X_2;Z) \quad (26)$$

where the maximization is over $[X_1,X_2] \sim \mathcal{N}(\mathbf{0},\mathbf{K_P})$ with $\mathcal{K}_P = \left\{\mathbf{K_P} : \mathbf{K_P} = \begin{bmatrix} P_1 & \psi\sqrt{P_1P_2} \\ \psi\sqrt{P_1P_2} & P_2 \end{bmatrix}, -1 \leq \psi \leq 1\right\}$, with $\mathbb{E}[X_1^2]$ and $\mathbb{E}[X_2^2]$ satisfying (12).

4. NUMERICAL RESULTS

In this section we provide some numerical examples to illustrate our results. We consider the Gaussian MAC (11) in which the outputs at the legitimate receiver and eavesdropper are corrupted by additive white Gaussian noise (AWGN) of zero mean and unit variance each. We model channel gains between node $i \in \{1,2\}$ and $j \in \{d,e\}$ as distance dependent path loss, $h_{i,j} = d_{i,j}^{-\alpha/2}$, where α is the path loss exponent. We assume that both users have an average power constraint of 1 watt each. We consider a network geometry in which user 1 is located at the point (0,0), user 2 is located at the point (d,0), the legitimate receiver is located at the point (1,0) and the eavesdropper is located at the point (1.5,0), where d is the distance between user 1 and 2. In all examples path loss exponent α:=2 and the perfect secrecy rate is given in bits per channels use.

Figure 2 shows the upper and lower bounds on the perfect secrecy rates for different capacities of noiseless pipe. The upper bound (13) and the lower bound (17) are optimized numerically for Gaussian inputs. In the lower bound (17) if we set $C_{12} = 0$, user 1 does not conference to user 2, for this case the channel reduces to the classical wiretap channel [13]. Therefore the achievable secrecy rate remains constant. If we increase the capacity of noiseless pipe, the achievable secrecy rate increases, this follows because the user 2 is more informed about user 1 and can cooperate with each other. It is interesting to know that, if we consider a very large value of noiseless pipe capacity, the upper and lower bounds will eventually coincide. This follows because a large value of C_{12} results in total cooperation between the users, due to which the channel reduces to a two-antenna transmitter wiretap channel for which secrecy capacity is established (Corollary 3).

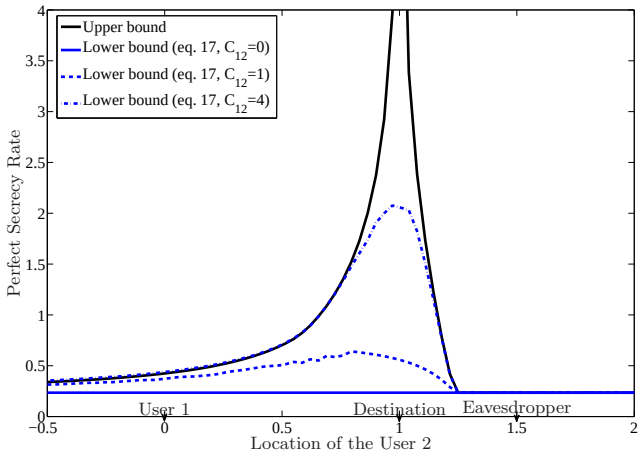

Figure 2: Bounds on the secrecy capacity.

5. ACKNOWLEDGMENTS

This work has been supported by the European Commission in the framework of the FP7 Network of Excellence in Wireless Communications (NEWCOM++), and by the Concerted Research Action SCOOP.

APPENDIX

A. PROOF OF THEOREM 2

The proof is a combination of Willem's coding scheme [1], with additional binning for security [3]. We begin the proof by first setting $V_1 := X_1$, $V_2 := X_2$ in Theorem 2. After proving Theorem 2 with X_1, X_2, we prefix a memoryless channel $p(x_1,x_2|v_1,v_2)$ as reasoned in [3, Lemma 4] to finish the proof.

Random Coding.

1. Randomly generate a typical sequence u^n with probability $p(u^n) = \prod_{i=1}^n p(u_i)$. We assume that all terminals know u^n.

2. Randomly generate $2^{n(R_{12}-\epsilon)}$ independent and identically distributed (i.i.d) x_2^n codewords, each with probability $p(x_2^n|u^n) = \prod_{i=1}^n p(x_{2i}|u_i)$ and index them as $x_2^n(w_0)$, $w_0 \in [1, 2^{n(R_{12}-\epsilon)}]$.

3. For each $x_2^n(w_0)$ generate $2^{n(R_1-\epsilon)}$ conditionally i.i.d x_1^n sequence, each with probability $p(x_1^n|x_2^n(w_0),u^n) = \prod_{i=1}^n p(x_{1i}|x_{2i}(w_0),u_i)$, and index them as $x_1^n(w_0,w_1)$, $w_1 \in [1, 2^{n(R_1-\epsilon)}]$.

4. We define $\mathcal{W}' = \{1,\dots 2^{n(R'-I(X_1,X_2;Z|U))}\}, \mathcal{L} = \{1,\dots, 2^{n(I(X_1,X_2;Z|U))}\}$ and $\mathcal{K} = \mathcal{W}' \times \mathcal{L}$, where $R' = R_1 + R_{12}$.

In the following we assume that $R' - I(X_1, X_2; Z|U) \geq 0$, otherwise this coding scheme does not achieve any security level.

Encoding.

For a given rate pair (R, R_e) with $R \leq R'$ and $R_e \leq R$, we propose the following random coding scheme. Let $w \in \mathcal{W} = \{1, \ldots 2^{nR}\}$ be the message, where $w = (w_0, w_1)$. The stochastic encoder performs the mapping similar to [4, Theorem 2] as follows.

- If $R \geq R' - I(X_1, X_2; Z|U)$, then let $\mathcal{W} = \mathcal{W}' \times \mathcal{J}$ where $\mathcal{J} = \{1, \ldots, 2^{n(R-[R'-I(X_1,X_2;Z|U)])}\}$. We define g be the mapping that partitions $\mathcal{L}$ into $\mathcal{J}$ subsets of nearly equal size. The stochastic encoder then maps $w = (w', j) \leftrightarrow (w', l)$, where l is uniformly chosen from $g^{-1}(j) \subset \mathcal{L}$.
- If $R \leq R' - I(X_1, X_2; Z|U)$, the stochastic encoder maps $w \leftrightarrow (w, l)$, where l is uniformly chosen from $\mathcal{L}$.

The encoder of user 1 sends $x_1^n(w_0, w_1, l)$ on the main channel and the encoder of user 2 sends $x_2^n(w_0)$.

Decoding.

1. The encoder of user 2 knows w_0, if $R_{12} \leq C_{12}$.
2. The legitimate receiver declares that $\hat{w}_0 = w_0$ was sent, by looking at jointly ϵ-typical $(x_2^n(w_0), y^n, u^n)$. We obtain $\hat{w}_0 = w_0$ with high probability and for a sufficiently large values of n, if $R_{12} \leq I(X_2; Y|U)$.
3. The legitimate receiver then declares that $(\hat{w}_0, \hat{w}_1, \hat{l})$ was sent, if $(x_1(\hat{w}_0, w_1, l), x_2(\hat{w}_0), y^n, u^n)$ are jointly ϵ-typical. It is easy to see that for sufficiently large values of n, this follows with high probability, if $R_1 \leq I(X_1; Y|X_2, U)$.

Thus, we obtain,

$$\begin{aligned} R_{12} &\leq I(X_2; Y|U) \\ R_{12} &\leq C_{12} \\ R_1 &\leq I(X_1; Y|X_2, U). \end{aligned} \tag{27}$$

Therefore rate R' is given by

$$\begin{aligned} R' &= R_1 + R_{12} \\ &= \min\{I(X_1; Y|X_2, U) + C_{12}, I(X_1, X_2; Y|U)\}. \end{aligned} \tag{28}$$

Equivocation computation.

The computation of equivocation is similar to the one established in [4] and is included for completeness.

From [4, Theorem 2, eq.(41)] we obtain

$$\begin{aligned} H(W|Z^n) \geq\ & H(X_1^n, X_2^n|U^n) + H(Z^n|X_1^n, X_2^n, U^n) \\ & - H(Z^n|U^n) - H(X_1^n, X_2^n|W, Z^n, U^n) \end{aligned} \tag{29}$$

where $W = (W_0, W_1)$. We first consider $H(X_1^n, X_2^n|W, Z^n, U^n)$. Given (w_0, w_1) the eavesdropper needs to decode only l, which can be decoded from Z^n with arbitrary small error probability because $l \in \mathcal{L} = \{1, \ldots, 2^{n(I(X_1,X_2;Z|U))}\}$. Therefore

$$H(X_1^n, X_2^n|W, Z^n, U^n) \leq n\epsilon_1. \tag{30}$$

Since the channel is memoryless we can write

$$H(Z^n|U^n) - H(Z^n|X_1^n, X_2^n, U^n) \leq nI(X_1, X_2; Z|U) + n\epsilon_n$$

where $\epsilon_n \to 0$, as $n \to \infty$ [13]. If $R \geq R' - I(X_1, X_2; Z|U)$ then $H(X_1^n, X_2^n|U^n) = n(R_1 + R_{12})$ follows from codebook construction. The secrecy rate is given by

$$nR_e \geq n(R_1 + R_{12} - I(X_1, X_2; Z|U) - \epsilon_2). \tag{31}$$

If $R \leq R' - I(X_1, X_2; Z|U)$, $H(X_1^n, X_2^n|U^n) = n(R + I(X_1, X_2; Z|U))$ then

$$\begin{aligned} nR_e &\geq n(R + I(X_1, X_2; Z|U) - I(X_1, X_2; Z|U) - \epsilon_2) \\ &= n(R - \epsilon_2). \end{aligned} \tag{32}$$

Therefore, perfect secrecy is obtained.

Now, we can introduce additional randomization by prefixing a memoryless channel with the conditional distribution $p(x_1, x_2|v_1, v_2)$ in the above coding scheme to obtain Theorem 2 [3, Lemma 4].

This completes the proof.

B. REFERENCES

[1] F. M. J. Willems, "The discrete memoryless multiple access channel with partially cooperating encoders," *IEEE Transactions on Information Theory*, vol. 29, no. 3, pp. 441–445, May. 1983.

[2] S. I. Bross, A. Lapidoth, and M. Wigger, "The Gaussian Mac with conferencing encoders," in *IEEE International Symposium on Information Theory*, Toronto, ON, Jul. 2008, pp. 2702–2706.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May. 1978.

[4] L. Lai and H. E. Gamal, "The relay eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *Available: http://arxiv.org/abs/0710.1920.*

[7] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multi-antenna wiretap channel," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[8] Z. H. Awan, A. Zaidi, and L. Vandendorpe, "Secure communication over parallel relay channel," *submitted to IEEE Transactions on Information Forensics and Security.*

[9] V. Aggarwal, L. Sankar, A. R. Calderbank, and H. V. Poor, "Secrecy capacity of a class of orthogonal relay eavesdropper channels," *EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security*, vol. 2009.

[10] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secret communication," *Available: http://arxiv.org/abs/0908.2397.*

[11] Y.-H. Kim, "Coding techniques for primitive relay channels," in *45th Annual Allerton Conference Communication, Control and Computing*, Monticello, IL, USA, Sept. 2007, pp. 129–135.

[12] Z. H. Awan, A. Zaidi, and L. Vandendorpe, "MAC with partially cooperating encoders and security constraints," *in preparation for submission to IEEE Transactions on Information Forensics and Security.*

[13] A. D. Wyner, "The wiretap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, Oct. 1975.

[14] R. G. Gallager, *Information theory and reliable communication*. New York:Wiley, 1968.

[15] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Transactions on Information Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[16] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[17] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.