Fiftieth Annual Allerton Conference
Allerton House, UIUC, Illinois, USA
October 1 - 5, 2012

On Multiaccess Channel with Unidirectional Cooperation and Security Constraints

Zohaib Hassan Awan[†], Abdellatif Zaidi[‡] and Luc Vandendorpe[†]
[†]ICTEAM institute, Université catholique de Louvain, Louvain-la-Neuve 1348, Belgium.
[‡]Université Paris-Est Marne-la-Vallée, 77454 Marne-la-Vallée Cedex 2, France.
zohaib.awan@uclouvain.be, abdellatif.zaidi@univ-mlv.fr, luc.vandendorpe@uclouvain.be

***Abstract*—We study a special case of Willems's two-user multi-access channel with partially cooperating encoders from a security perspective. This model differs from Willems's setup in the following aspects — 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 (DM) case, we establish inner and outer bounds on the capacity-equivocation region. The inner bound is established by a careful combination of Willems's coding scheme, noise injection scheme and additional binning that provides randomization for security. For the memoryless Gaussian model, we establish lower and upper bounds on the secrecy capacity. We also studied some extreme cases of cooperation between the encoders and showed that, under certain conditions, these bounds coincide.**

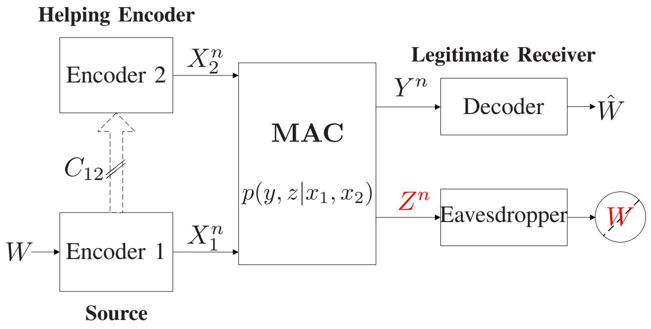

Fig. 1. Multi-access channel with partially cooperating encoders and security constraints.

I. Introduction

Wyner, in his seminal paper [1], introduced a basic wiretap model to study security from an information theoretic perspective. The wiretap model consists of three nodes, a source, a legitimate receiver and an eavesdropper. In this model for secure communication, two constraints need to be fulfilled simultaneously — transmitted information should be received reliably at the legitimate receiver and should be perfectly secured from the eavesdropper. The Wiretap model has been applied further to study the security of different multiuser channels, for instance, multi-antenna wiretap channel [2]–[4], multi-access wiretap channel [5], [6], relay-eavesdropper channel [7], [8], parallel relay channel [9] and interference channel [10], [11].

In this contribution, we study the problem of secure communication over a multi-access channel (MAC) with partially cooperating encoders. Willems studied the MAC with partially cooperating encoders model in [12], where prior to transmitting their respective messages, the two encoders are allowed to cooperate with each other over noiseless bit-pipes of finite-capacities. Willems characterizes the complete capacity region of this model for the DM case. The capacity region of the corresponding Gaussian version was characterized by Bross *et. al* in [13]. In both [12] and [13], 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.

We study a special case of Willems setup with an additional security constraint on the communication. More precisely, as depicted in Figure 1, we consider a two-user multi-access channel in which the two users can partially cooperate with each other via a unidirectional noiseless bit-pipe of finite capacity C_{12}. In addition to this, we restrict the role of Encoder 2 to only helping Encoder 1, i.e., Encoder 2 has no message of its own to transmit. We also assume that there is a passive eavesdropper who overhears the transmission and from whom the communication from Encoder 1 and Encoder 2 to the legitimate receiver should be kept secret. The eavesdropper is passive in the sense that it is not allowed to modify the transmitted information. The role of Encoder 2 is then to only help Encoder 1 communicate with the legitimate receiver while keeping the transmitted information *secret* from the eavesdropper. Practically, this model may be appropriate for example to the study of the role of backbone connections among base stations for securing transmission in cellular environments. In this work, we study the capacity-equivocation region of this model.

The MAC model that we study in this paper has some connections with a number of related works studied previously. In contrast to the orthogonal relay-eavesdropper channel studied in [14], the orthogonal link between the source and the relay is here replaced by a noiseless bit-pipe of finite capacity C_{12}. In comparison to the wiretap channel with a helper interferer (WT-HI) studied in [15], our model permits cooperation among the encoders. Finally, compared with the primitive relay channel of [16], our model imposes security

978-1-4673-4539-2/12/$31.00 ©2012 IEEE

constraints on the transmitted message.

For the DM case, we establish bounds on the capacity-equivocation region. The coding scheme that we used to construct an inner bound is based on an appropriate careful combination of Willems coding scheme [12], noise injection [7, Theorem 3] and binning for randomization. The converse proof is established by extending the converse proof of [12] by taking security constraint into account and that of [17] to account for the unidirectional noiseless bit-pipe cooperation among the encoders. In doing so, we note that one needs to re-define the involved auxiliary random variables appropriately. We note that characterizing the capacity-equivocation region of our model in the general setting is non-trivial; and, in fact, the capacity-equivocation region or secrecy-capacity of closely related models that are reported in the literature, such as [15], [18], [19], are still to be found — the model of [15] can be seen as a special case of our model obtained by taking a noiseless bit-pipe of zero capacity. From this viewpoint, the inner and outer bounds that we develop here can be seen as one step further towards a better understanding of the full capacity-equivocation region of the model that we study in this paper.

We also study the Gaussian memoryless model of the MAC model shown in Figure 1. For this setup, we only focus on the perfect secure transmission. For this model, we establish lower and upper bounds on the secrecy capacity. The coding scheme that we use to establish the lower bound uses ideas that are essentially similar to those for the DM case. The upper bound on the secrecy capacity does not involve auxiliary random variables and, so, is computable. Furthermore, it has the same expression as the secrecy capacity of the Gaussian wiretap channel with a two-antenna transmitter, single-antenna legitimate receiver and single-antenna eavesdropper [2]–[4].

We also show the optimality of our lower bound for some extreme cases of cooperation among the encoders, including when the two encoders fully cooperate, i.e., $C_{12} := \infty$. For the case in which the two encoders do not conference, i.e., $C_{12} := 0$, the studied model reduces to a wiretap channel with a helper interferer [15], [18]. In this case, our coding scheme reduces to merely injecting statistically independent noise [7, Theorem 3]; and, by comparing it to the upper bound that we develop, we show that it is optimal under certain conditions. For the case of full cooperation among the encoders, i.e., $C_{12} := \infty$, our coding scheme reduces to full two-antenna cooperation for providing secrecy in the context of multiantenna wiretap channels [2]–[4].

II. Channel Model and Definitions

Figure 1 shows the channel model. Let W denote the message to be transmitted, taken uniformly from the set $\mathcal{W} = \{1, \dots, 2^{nR}\}$. Encoder 1 is allowed to conference the message W to Encoder 2 using K communicating functions $\{\phi_{11}, \phi_{12}, \dots, \phi_{1K}\}$, over the noiseless bit-pipe. Let $G_{1k} := \phi_{1k}(W)$, defined as the output of the communication process for the k-th communication, where G_{1k} ranges over the finite alphabet $\mathcal{G}_{1k}$, $k = 1, \dots, K$. The information conferenced is bounded due to the finiteness of noiseless bit-pipe capacity between the two encoders. A conference is permissible if communication functions are such that

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

To transmit the message W, Encoder 1 sends a codeword $X_1^n \in \mathcal{X}_1^n$, where $\mathcal{X}_1$ designates the input alphabet at Encoder 1. Encoder 2 transmits a codeword $X_2^n \in \mathcal{X}_2^n$ where $\mathcal{X}_2$ designates the input alphabet at Encoder 2. Let $\mathcal{Y}$ and $\mathcal{Z}$ designate the output alphabets at the legitimate receiver and eavesdropper, respectively. The legitimate receiver gets the channel output $Y^n \in \mathcal{Y}^n$, and tries to estimate the transmitted message from it. The eavesdropper overhears the channel output $Z^n \in \mathcal{Z}^n$. The transmission over the channel is characterized by the memoryless conditional probability $p(y, z|x_1, x_2)$. The channel is memoryless in the sense that

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

A $(2^{nR}, n)$ code for the multi-access model with partially cooperating encoders shown in Figure 1 consists of encoding functions[1]

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

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

$$\psi \ : \ \mathcal{Y}^n \longrightarrow \mathcal{W}. \tag{4}$$

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

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

The eavesdropper overhears to what the encoders 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 $n \geq n(\epsilon)$

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

The secrecy capacity is defined as the maximum achievable rate at which the communication rate is equal to the equivocation rate, i.e., $(R, R_e) = (R, R)$.

[1] The source encoder, ϕ_1, is a stochastic encoder that introduces additional randomization to increase secrecy.

III. Discrete Memoryless Case

In this section we consider the MAC shown in Figure 1 and establish bounds on the capacity-equivocation region.

A. Outer Bound

The following theorem provides an outer bound on the capacity-equivocation region of the MAC with partially cooperating encoders 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 exist some random variables $U \leftrightarrow (V_1, V_2) \leftrightarrow (X_1, X_2) \leftrightarrow (Y, Z)$, such that (R, R_e) satisfies

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

Proof: The proof of Theorem 1 is provided in [20, Appendix I]. □

B. Inner Bound

Next, we establish an inner bound on the capacity-equivocation region of the MAC shown in Figure 1.

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

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

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

Outline of Proof:
We briefly outline the coding scheme that we use to prove the achievability of the inner bound of Theorem 2. The details of the proof is provided in [20, Appendix II]. The inner bound of Theorem 2 is based on a coding scheme that consists in appropriate careful combination of Willems's coding scheme [12], noise injection [7, Theorem 3] and binning for randomization to provide security. Let W denote the message to be transmitted. Using the noiseless bit-pipe of finite capacity, Encoder 1 conferences a part of the information message W to Encoder 2. After completion of the conferencing process, this part can be regarded as a common information to be transmitted by both encoders. The random variable V in Theorem 2 represents this common information. The part of the information message that is sent only by Encoder 1 can be regarded as an individual message. The random variable V_1 in Theorem 2 represents this individual information. The input of Encoder 2 is composed of the common information, which it has received through noiseless finite capacity link from Encoder 1, and a statistically independent artificial noise component. The random variable V_2 in Theorem 2 represents the input from Encoder 2. The transmission of both common information and artificial noise components at Encoder 2 in Theorem 2 is adjusted by appropriate selection of random variable V. Additional random binning is employed to secure both individual and common information from the passive eavesdropper [1]. Finally, the random variable U in Theorem 2 stands for a channel prefix. □

IV. Memoryless Gaussian Model

Now, we study the Gaussian version of the MAC channel shown in Figure 1.

A. Channel Model

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

$$\begin{aligned} Y &= h_{1d}X_1 + h_{2d}X_2 + N_1 \\ Z &= h_{1e}X_1 + h_{2e}X_2 + N_2 \quad (9) \end{aligned}$$

where h_{1d}, h_{2d}, h_{1e}, and h_{2e} are the channel gain coefficients associated with Encoder 1-to-destination (1-D), Encoder 2-to-destination (2-D), Encoder 1-to-eavesdropper (1-E), and Encoder 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 channel inputs from Encoder 1 and Encoder 2 respectively. The channel inputs are bounded by average block power constraints

$$\sum_{i=1}^{n} \mathbb{E}[X_{1,i}^2] \leq nP_1, \qquad \sum_{i=1}^{n} \mathbb{E}[X_{2,i}^2] \leq nP_2. \quad (10)$$

B. Upper Bound on the Secrecy Capacity

In this section, we establish an upper bound on the secrecy capacity on Gaussian MAC (9). We establish a computable upper bound using the techniques developed earlier to establish the secrecy capacity of a multiple-input multiple-output (MIMO) wiretap channel [2]–[4] — taking a setup with two antennas at the transmitter, one antenna at the legitimate receiver and one antenna at the eavesdropper in our case.

Corollary 1: For the Gaussian MAC with partially cooperating encoders and security constraints (9), an upper bound on the secrecy capacity is given by

$$R_e^{\text{up}} = \max_{\psi}[I(X_1, X_2; Y) - I(X_1, X_2; Z)] \quad (11)$$

where $[X_1, X_2] \sim \mathcal{N}(\mathbf{0}, \mathbf{K_P})$ with $\mathcal{K}_P = \Big\{\mathbf{K_P} : \mathbf{K_P}= \begin{bmatrix} P_1 & \psi\sqrt{P_1P_2} \\ \psi\sqrt{P_1P_2} & P_2 \end{bmatrix}, -1 \leq \psi \leq 1\Big\}$, with $\mathbb{E}[X_1^2]$, $\mathbb{E}[X_2^2]$ satisfying (10).

C. Lower Bound on the Secrecy Capacity

For the Gaussian MAC with partially cooperating encoders and security constraints (9), 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 [21, Chapter 7].

Corollary 2: For the Gaussian MAC with partially cooperating encoders and security constraints (9), a lower bound on the secrecy capacity is given by

$$\begin{aligned} R_e^{\text{low}} = \max_{\substack{0\leq\alpha\leq 1,\\ 0\leq\beta\leq 1}} \Bigg[&\min\Big\{\mathcal{C}\Big(\frac{\beta|h_{2d}|^2P_2}{\sigma_1^2+\alpha|h_{1d}|^2P_1}\Big), \mathcal{C}\Big(\frac{\beta|h_{2e}|^2P_2}{\sigma_2^2}\Big)\Big\} \\ &+ \min\Big\{\mathcal{C}\Big(\frac{\alpha|h_{1d}|^2P_1}{\sigma_1^2}\Big) + C_{12}, \\ &\mathcal{C}\Big(\frac{|h_{1d}|^2P_1+|h_{2d}|^2P_2+2\sqrt{\bar{\alpha}\bar{\beta}|h_{1d}|^2P_1|h_{2d}|^2P_2}}{{\sigma_1}^2}\Big)\Big\} \\ &-\mathcal{C}\Big(\frac{|h_{1e}|^2P_1+|h_{2e}|^2P_2+2\sqrt{\bar{\alpha}\bar{\beta}|h_{1e}|^2P_1|h_{2e}|^2P_2}}{\sigma_2^2}\Big)\Bigg]^+. \end{aligned} \tag{12}$$

Proof: The achievability follows by computing the inner bound in Theorem 2 with the choice $U :=$ constant, $V_1 := X_1$ and $V_2 := X_2$, $X_1 := \sqrt{(\alpha P_1)}\tilde{X}_1 + \sqrt{(\bar{\alpha} P_1)}V$, $X_2 := \sqrt{(\beta P_2)}\tilde{X}_2 + \sqrt{(\bar{\beta} P_2)}V$, where $\tilde{X}_1$, $\tilde{X}_2$ and V be independent random variables with $\mathcal{N}(0,1)$, and $\alpha \in [0,1]$, $\bar{\alpha} := 1-\alpha$, $\beta \in [0,1]$, and $\bar{\beta} := 1-\beta$. Straightforward algebra that is omitted for brevity gives (12). □

D. Analysis of Some Extreme Cases

In this section we consider two special cases of the Gaussian MAC (9) 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} = ∞.

The Case 1 corresponds to the wiretap channel with a helping interferer (WT-HI) studied in [15], [18]. The Case 2 corresponds to a two-antenna transmitter wiretap channel [4], [22].

1) Case $C_{12} := 0$: In this case the encoders do not cooperate. Since Encoder 2 does not know the common information to transmit, it only injects statistically independent artificial noise.

Corollary 3: For the Gaussian model (9) with $C_{12} := 0$:

1) An upper bound on the secrecy capacity is given by

$$R_e^{\text{up}} = \max_{\substack{\mathbb{E}[X_1^2]\leq P_1,\\ \mathbb{E}[X_2^2]\leq P_2}} \Big[\mathcal{C}\Big(\frac{|h_{1d}|^2\mathbb{E}[X_1^2]}{\sigma_1^2}\Big) - \mathcal{C}\Big(\frac{|h_{1e}|^2\mathbb{E}[X_1^2]}{\sigma_2^2+|h_{2e}|^2\mathbb{E}[X_2^2]}\Big)\Big]^+. \tag{13}$$

2) A lower bound on the secrecy capacity is given by

$$R_e^{\text{low}} = \max \Big[\mathcal{C}\Big(\frac{|h_{1d}|^2\mathbb{E}[X_1^2]}{\sigma_1^2}\Big) - \mathcal{C}\Big(\frac{|h_{1e}|^2\mathbb{E}[X_1^2]}{\sigma_2^2+|h_{2e}|^2\mathbb{E}[X_2^2]}\Big)\Big]^+ \tag{14}$$

where the maximization is over $\mathbb{E}[X_1^2] \leq P_1$ and $\mathbb{E}[X_2^2] \leq P_2$ such that

$$\mathcal{C}\Big(\frac{|h_{2d}|^2\mathbb{E}[X_2^2]}{|h_{1d}|^2\mathbb{E}[X_1^2]+\sigma_1^2}\Big) \geq \mathcal{C}\Big(\frac{|h_{2e}|^2\mathbb{E}[X_2^2]}{\sigma_2^2}\Big). \tag{15}$$

Proof:

Upper Bound. We bound the term in (13) as follows. The proof follows by using elements from an upper bounding technique developed in [14]. We assume that there is a noiseless link between Encoder 2 and the legitimate receiver, and the eavesdropper is *constrained* to treat Encoder 2's signal as unknown noise. The upper bound established for this alternate model, with full cooperation between Encoder 2 and the legitimate receiver and a constrained eavesdropper, also applies to the model of Corollary 3. The details of the proof is provided in [20].

Lower Bound. The proof of the lower bound follows by evaluating the equivocation rate in Theorem 2 with a specific choice of the variables. More specifically, evaluating Theorem 2 with the choice $C_{12} := 0$, $U = V = \phi$, $V_1 := X_1$ and $V_2 := X_2$, with $X_1 \sim \mathcal{N}(0, P_1)$ independent of $X_2 \sim \mathcal{N}(0, P_2)$, and such that (15) is satisfied, we obtain the rate expression in (14). The RHS of (14) then follows by maximization over $\mathbb{E}[X_1^2] \leq P_1$ and $\mathbb{E}[X_2^2] \leq P_2$ and satisfying (15). □

Remark 1: The bounds on the secrecy capacity in (13) and (14) have identical expressions but the maximization is over different sets of inputs. The bounds coincide in the case in which the inputs ($\mathbb{E}[X_1^2], \mathbb{E}[X_2^2]$) that maximize the RHS of (13) also satisfy the condition (15). In this case, the perfect secrecy of the studied model is given by

$$C_s = \max \Big[\mathcal{C}\Big(\frac{|h_{1d}|^2\mathbb{E}[X_1^2]}{\sigma_1^2}\Big) - \mathcal{C}\Big(\frac{|h_{1e}|^2\mathbb{E}[X_1^2]}{\sigma_2^2+|h_{2e}|^2\mathbb{E}[X_2^2]}\Big)\Big]^+ \tag{16}$$

where the maximization is over $\mathbb{E}[X_1^2] \leq P_1$ and $\mathbb{E}[X_2^2] \leq P_2$ satisfying

$$\mathcal{C}\Big(\frac{|h_{2d}|^2\mathbb{E}[X_2^2]}{|h_{1d}|^2\mathbb{E}[X_1^2]+\sigma_1^2}\Big) \geq \mathcal{C}\Big(\frac{|h_{2e}|^2\mathbb{E}[X_2^2]}{\sigma_2^2}\Big). \tag{17}$$

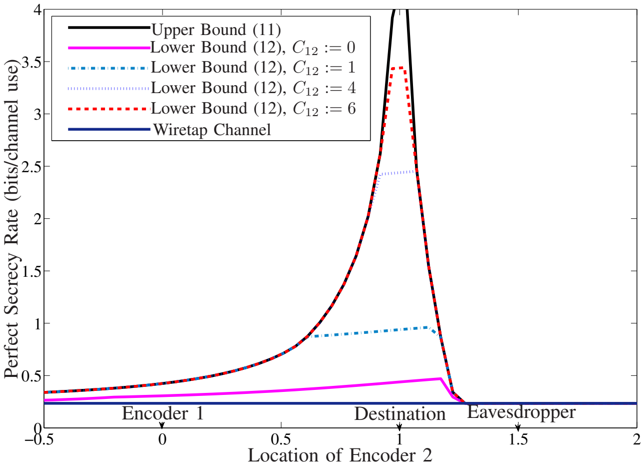

Fig. 2. Bounds on the secrecy capacity.

2) Case $C_{12} := \infty$: In this case the model (9) reduces to a wiretap channel in which the transmitter equipped with two antenna and the legitimate receiver and eavesdropper equipped with single antennas. As it will be shown below, in this case the upper bound of Corollary 1 and the lower bound of Corollary 2 coincide, thus providing a characterization of the secrecy capacity, which can also be obtained from [3], [4] in this specific case.

Corollary 4: For the Gaussian model (9) with fully cooperating encoders, the secrecy capacity is given by

$$C_s = \max_{\psi}[I(X_1, X_2; Y) - I(X_1, X_2; Z)] \tag{18}$$

where $[X_1, X_2] \sim \mathcal{N}(\mathbf{0}, \mathbf{K_P})$ 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 (10).

Proof: The upper bound follows by Corollary 1. The proof of the lower bound follows by evaluating the equivocation rate in Theorem 2 with a specific choice of the random variables. More specifically, the rate expression (18) is obtained by setting $C_{12} := \infty$, $U :=$ constant, $V_1 := X_1$, $V = V_2 = X_2$, in Theorem 2 where $[X_1, X_2] \sim \mathcal{N}(\mathbf{0}, \mathbf{K_P})$ with $\mathcal{K}_P = \left\{\mathbf{K_P} : \mathbf{K_P}= \begin{bmatrix} P_1 & \psi\sqrt{P_1P_2} \\ \psi\sqrt{P_1P_2} & P_2 \end{bmatrix}, -1 \leq \psi \leq 1\right\}$ and $\mathbb{E}[X_1^2]$ and $\mathbb{E}[X_2^2]$ satisfying (10).
With straightforward algebra, it can be checked that this corresponds also to the special case $C_{12} = \infty$ in Corollary 2. □

V. Numerical results

We consider the Gaussian MAC (9) 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, $h_{i,j} = d_{i,j}^{-\gamma/2}$, where γ is the path loss exponent. We assume that both users have an average power constraint of 1 watt each and the path loss exponent γ:=2. We consider a network geometry in which Encoder 1 is located at the point (0,0), Encoder 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 Encoders 1 and 2. The upper (11) and the lower (12) bounds are optimized numerically for Gaussian inputs. Figure 2 shows the upper and lower bounds on the secrecy capacity for different values of finite capacity link. As a reference we consider the case in which there is no helping Encoder, i.e., a basic wiretap channel. If we set $C_{12} := 0$, Encoder 1 does not conference to Encoder 2, for this setup the MAC (9) reduces to the classic WT-HI [15], [18]. In this case Encoder 2 can help Encoder 1 by injecting confusion codewords to confuse the eavesdropper [7, Theorem 3]. If we increase the capacity of noiseless bit-pipe, the achievable secrecy rate increases, this follows because Encoder 2 is more informed about the information message from Encoder 1 and can cooperate with each other. For instance, if we consider a very large value of noiseless bit-pipe capacity, the upper and lower bounds will eventually coincide. This is due to the fact that a large value of C_{12} results in full cooperation between the encoders, due to which the channel reduces to a two-antenna transmitter wiretap channel for which secrecy capacity is established (Corollary 4).

VI. Conclusion

In this contribution, we studied a special case of Willems's multi-access channel with partially cooperating encoders [12] from security perspective. We established outer and inner bounds on the capacity-equivocation region, for the DM case. The inner bound is established by an appropriate careful combination of Willems's coding scheme, noise injection [7, Theorem 3] and additional random binning for security. The converse proof is obtained by using the techniques developed earlier in the context of broadcast channels with confidential messages and Willems's MAC to the considered setup. We note that the outer and inner bounds which we have established do not agree in general, but can be seen as a step ahead towards characterizing the capacity-equivocation region. For the Gaussian setup, we establish lower and upper bounds on the secrecy capacity. We also study some extreme cases of cooperation between the encoders. For the setup in which the encoders do not cooperate, we show that under certain conditions, our lower and upper bounds agree. For the case of full cooperation between the encoders, the studied setup reduces to a multi-antenna wiretap channel and the developed bounds coincide.

VII. Acknowledgment

This work has been supported in part by the European Commission in the framework of the Network of Excellence in Wireless Communications (NEWCOM#), and the Concerted Research Action, SCOOP. The authors would also like to thank BELSPO for the support of the IAP BESTCOM network.

References

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

[2] 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.

[3] 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.

[4] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[5] 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.

[6] Y. Liang and H. V. Poor, "Multiple access channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[7] 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.

[8] M. Yuksel and E. Erkip, "The relay channel with a wire-tapper," in *41st Annual Conference on Information Sciences and Systems*, Baltimore, MD, USA, Mar. 2007, pp. 13–18.

[9] Z. H. Awan, A. Zaidi, and L. Vandendorpe, "Secure communication over parallel relay channel," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 359–371, Apr. 2012.

[10] O. Koyluoglu and H. El Gamal, "Cooperative encoding for secrecy in interference channels," *IEEE Transactions on Information Theory*, vol. 57, no. 9, pp. 5682 –5694, Sept. 2011.

[11] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2493 –2507, June 2008.

[12] 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.

[13] 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.

[14] 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*, 2009.

[15] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secret communication," *IEEE Transactions on Information Theory*, vol. 57, no. 5, pp. 3153–3167, May. 2011.

[16] 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.

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

[18] X. He and A. Yener, "Providing secrecy with structured codes: Tools and applications to two-user gaussian channels," *available online http://arxiv.org/abs/0907.5388*, 2009.

[19] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of a class of one-sided interference channel," in *IEEE Int. Symp. on Information Theory*, Jul. 2008, pp. 379–383.

[20] Z. H. Awan, A. Zaidi, and L. Vandendorpe, "Multiaccess channel with partially cooperating encoders and security constraints," *available online http://arxiv.org/pdf/1205.6852.pdf*, 2012.

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

[22] 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.