

Constrained Colluding Eavesdroppers: An Information-Theoretic Model

Mahtab Mirmohseni and Panagiotis Papadimitratos
 KTH Royal Institute of Technology, Stockholm, Sweden
 Email: {mahtabmi,papadim}@kth.se

Abstract

We study the secrecy capacity in the vicinity of colluding eavesdroppers. Contrary to the *perfect collusion* assumption in previous works, our new information-theoretic model considers *constraints* in collusion. We derive the achievable secure rates (lower bounds on the perfect secrecy capacity), both for the discrete memoryless and Gaussian channels. We also compare the proposed rates to the non-colluding and perfect colluding cases.

Index Terms

Colluding eavesdroppers; Secrecy capacity; Information-theoretic security; Wiretap channel

I. INTRODUCTION

Wyner [1] introduced the information-theoretic model for confidentiality in noisy communications, called *wiretap channel*, where a legitimate transmitter wishes to transmit a confidential message to a legitimate receiver while keeping it hidden from an eavesdropper (wiretapper). The eavesdropper is assumed to have unlimited computation power, know the coding scheme of the legitimate user, and it only listens to the channel. When the channel to the eavesdropper is a degraded version of the channel to the legitimate receiver, Wyner [1] proposed the secrecy capacity achieving scheme, known also as *Wyner's wiretap channel coding*, which constitutes of multicoding and randomized encoding [2, Section 22.1.1]. This result is extended to the broadcast channel with confidential message and to the general wiretap channel (not necessarily degraded) by Csiszár and Körner [3].

Recently, different legitimate-wiretapper user combinations were studied [4]–[8]. In this line of works, scenarios with multiple eavesdroppers considered only *non-colluding* ones. This implies that information

leakage of a certain message to all eavesdropper is computed as the maximum of the leakage to each of them. In some applications, this assumption may underestimate the eavesdroppers' power: eavesdroppers can collude, i.e., share their channel outputs (observations), and make the attack more effective [9]. Hence, combating colluding eavesdroppers, especially in wireless networks, has been a significant challenge [9]–[14]. To the best of our knowledge, all previous works modeled k colluding eavesdroppers as one eavesdropper with k antennas; we term this *perfect colluding* eavesdroppers. Using the equivalent Single-Input Multiple-Output (SIMO) Gaussian wiretap channel, the information leakage is determined by the aggregate Signal to Noise Ratio (SNR) of all eavesdroppers; compared to the maximum SNR in the non-colluding case [9]. This assumption significantly overestimates eavesdropping capability, forcing a legitimate user to increase its power linearly with the number of eavesdroppers to achieve a positive secure rate. However, collusion (esp. in the wireless networks) necessitates communication resources and power consumption. This, in fact, restricts the collusion channel capacity and thus improves the achievable secure rate by the legitimate user. Hence, here the problem is to find an appropriate model and to analyze the effect of these constraints on the secrecy capacity based on this model.

A. Our Contributions

In this paper, we consider the potential constraints in collusion, by modeling *constrained collusion* with an equivalent wiretap channel, called *Wiretap Channel with Constrained Colluding Eavesdroppers* (WTC-CCE). For our *general* WTC-CCE, we assume that colluding eavesdroppers communicate (by defining their channel inputs) over a virtual *collusion channel*, in addition to the main channel. The higher the collusion channel capacity, the more leaked information can be exchanged. Our model captures previously studied models as special cases: non-colluding with zero collusion rates and perfect collusion with infinite collusion rates. We also propose a special case, the *orthogonal* WTC-CCE: the collusion channel is orthogonal to the main one (unlike the general WTC-CCE where eavesdroppers shares the same channel with the legitimate transmitter). First, we derive an achievable secure rate (a lower bound on the perfect secrecy capacity) for the general discrete memoryless WTC-CCE. The idea is to let the eavesdroppers do their best in colluding. Hence, the information leakage rate is derived by considering the outer bound on the capacity region of the collusion channel; this resembles the cut-set upper bound for the relay channel [2]. Next, we extend our result to the general Gaussian WTC-CCE and its orthogonal version. The main difference is that in the general model, the eavesdroppers may use jamming techniques to confuse the legitimate receiver but they could be exposed to the legitimate user. In the orthogonal model, beyond increased required resources, the eavesdroppers may loose some information leakage rate due to

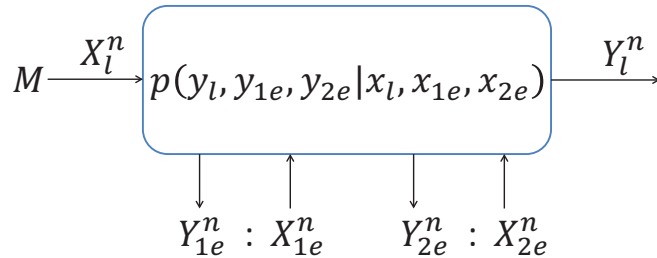


Fig. 1. General Wiretap Channel with Constrained Colluding Eavesdroppers (WTC-CCE).

not sending jamming signals. However, the orthogonality may serve eavesdroppers in hiding themselves. We provide numerical examples to analyze the achievable secure rate and evaluate the overestimation amount (by comparing to perfect colluding case) in different scenarios.

The rest of the paper is organized as follows. Section II introduces the channel model and the notations. In Section III, our main results for the general discrete-memoryless channel are presented, while in Section IV, the Gaussian channel results are stated. Finally, Section V concludes the paper.

II. CHANNEL MODEL AND PRELIMINARIES

Upper-case letters (e.g., X) denote Random Variables (RVs) and lower-case letters (e.g., x) their realizations. The probability mass function (p.m.f) of a RV X with alphabet set \mathcal{X} is denoted by $p_X(x)$; occasionally, the subscript X is omitted. X_i^j indicates a sequence of RVs $(X_i, X_{i+1}, \dots, X_j)$; we use X^j instead of X_1^j for brevity. $\mathcal{N}(0, \sigma^2)$ denotes a zero-mean Gaussian distribution with variance σ^2 .

Consider the WTC-CCE in Fig. 1: a four terminal discrete channel (one transmitter, one legitimate receiver and two eavesdroppers), denoted by $(\mathcal{X}_l \times \mathcal{X}_{1e} \times \mathcal{X}_{2e}, p(y_l, y_{1e}, y_{2e} | x_l, x_{1e}, x_{2e}), \mathcal{Y}_l \times \mathcal{Y}_{1e} \times \mathcal{Y}_{2e})$. $X_l \in \mathcal{X}_l$ and $X_{je} \in \mathcal{X}_{je}$ are the channel inputs of the legitimate transmitter and eavesdropper j and $Y_l \in \mathcal{Y}_l$ and $Y_{je} \in \mathcal{Y}_{je}$ are the channel outputs at the legitimate receiver and eavesdropper j , for $j \in \{1, 2\}$. $p(y_l, y_{1e}, y_{2e} | x_l, x_{1e}, x_{2e})$ is the channel transition probability distribution. We also assume that the channel is memoryless. In n channel uses, the legitimate transmitter desires to send the message M to the legitimate receiver using the following code.

Definition 1: A $(2^{nR}, n, P_e^{(n)})$ code for WTC-CCE consists of:

- (i) A message set $\mathcal{M} = [1 : 2^{nR}]$, where m is uniformly distributed over \mathcal{M} .
- (ii) A *randomized* encoding function, f_n , at the legitimate transmitter that maps a message m to a codeword $x_l^n \in \mathcal{X}_l^n$.

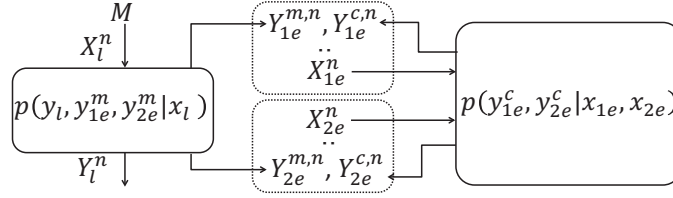


Fig. 2. Orthogonal WTC-CCE.

- (iii) Two sets of encoding functions at the eavesdroppers: $\{f_{j_e,t}\}_{t=1}^n : \mathbb{R}^{t-1} \rightarrow \mathbb{R}$ such that $x_{j_e,t} = f_{j_e,t}(y_{j_e}^{t-1})$, for $j \in \{1, 2\}$ and $1 \leq t \leq n$.
- (iv) A decoding function at the legitimate receiver $g : \mathcal{Y}_l^n \mapsto \mathcal{M}$.
- (v) Probability of error for this code is defined as:

$$P_e^{(n)} = \frac{1}{2^{nR}} \sum_{m \in \mathcal{M}} Pr(g(y_l^n) \neq m | m \text{ sent}). \quad (1)$$

- (vi) The information leakage rate at eavesdropper $j \in \{1, 2\}$ is defined as:

$$R_{L,j}^{(n)} = \frac{1}{n} I(M; Y_{j_e}^n). \quad (2)$$

All codewords are revealed to the eavesdroppers. However, eavesdroppers' mapping are not known to the legitimate user.

Remark 1: The mutual information term in (2) is same as the non-colluding case, compared to $I(M; Y_{1e}^n, Y_{2e}^n)$ in the perfect colluding scenario. The difference here comes from the channel distribution and the fact that Y_{1e}^n and Y_{2e}^n given X_l are not independent (due to X_{1e} and X_{2e}).

Definition 2: A rate-leakage tuple $(R, R_{L,1}, R_{L,2})$ is achievable if there exists a sequence of $(2^{nR}, n, P_e^{(n)})$ codes such that $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$ and $\limsup_{n \rightarrow \infty} R_{L,j}^{(n)} \leq R_{L,j}$ for $j \in \{1, 2\}$. The secrecy capacity \mathcal{C}_s is the supremum of all achievable rates R such that perfect secrecy is achieved, i.e., $R_{L,j} = 0$ for $j \in \{1, 2\}$.

Motivated by the fact that the eavesdroppers prefer to avoid exposure, we also consider a special case of the WTC-CCE. We assume that the collusion channel (used by the eavesdroppers) is decoupled from the main channel and consider the orthogonal WTC-CCE in Fig. 2. Here, $Y_{j_e} = (Y_{j_e}^m, Y_{j_e}^c)$ for $j \in \{1, 2\}$ and $p(y_l, y_{1e}, y_{2e} | x_l, x_{1e}, x_{2e}) = p(y_l, y_{1e}^m, y_{2e}^m | x_l) p(y_{1e}^c, y_{2e}^c | x_{1e}, x_{2e})$, where the variables related to the main and the collusion channels are indicated with the superscripts m and c , respectively. Substituting $X_{1e} = X_{2e} = \emptyset$ results in the non-colluding case; $Y_{1e}^c = Y_{2e}^m, Y_{2e}^c = Y_{1e}^m$ results in the perfect colluding case. To simplify notation let \bar{j} be the complement of j in $\{1, 2\}$. Now, consider the general Gaussian

WTC-CCE at time $t = 1, \dots, n$ for $j \in \{1, 2\}$, modeled as:

$$\begin{aligned} Y_{l,t} &= h_l X_{l,t} + h_{1e}^l X_{1e,t} + h_{2e}^l X_{2e,t} + Z_{l,t} \\ Y_{je,t} &= h_l^{je} X_{l,t} + h_{\bar{j}e}^{je} X_{\bar{j}e,t} + Z_{je,t} \end{aligned} \quad (3)$$

where h_i^k is a known channel gain from transmitter i to receiver k . We assume perfect echo cancellation at eavesdroppers ($h_{1e}^{1e} = h_{2e}^{2e} = 0$). $X_{u,t}$ is an input signal with average power constraint

$$\frac{1}{n} \sum_{t=1}^n |x_{u,t}|^2 \leq P_u \quad (4)$$

and $Z_{u,t}$ is an independent and identically distributed (i.i.d) zero-mean Gaussian noise component with power N_u , for $u \in \{l, 1e, 2e\}$. In practice, h_{1e}^l and h_{2e}^l may be small. The Gaussian counterpart of orthogonal WTC-CCE for $j \in \{1, 2\}$ can be shown as:

$$\begin{aligned} Y_{l,t} &= h_l X_{l,t} + Z_{l,t} \\ Y_{je,t}^m &= h_{jm} X_{l,t} + Z_{je,t}^m \quad , \quad Y_{je,t}^c = h_{jc} X_{\bar{j}e,t} + Z_{je,t}^c \end{aligned} \quad (5)$$

where h_{jm} and h_{jc} are known channel gains received at eavesdropper j from the main channel and the collusion channel, respectively; power constraints of P_l, P_{1e}, P_{2e} apply for input signals; $Z_{je,t}^m$ and $Z_{je,t}^c$ are i.i.d zero-mean Gaussian noise components with powers N_{je}^m and N_{je}^c at eavesdropper j from the main channel and the collusion channel, respectively.

III. DISCRETE MEMORYLESS CHANNEL

Our first result establishes an achievable secure rate for the general discrete memoryless WTC-CCE.

Theorem 1: For the general discrete memoryless WTC-CCE, the secrecy capacity is lower-bounded by:

$$\begin{aligned} \mathcal{R}_s^{DM} &= \sup \inf I(X_l; Y_l) - \min\{I(X_l; Y_{1e}, Y_{2e} | X_{1e}, X_{2e}), \\ &\quad \max\{I(X_l, X_{1e}, X_{2e}; Y_{1e}), I(X_l, X_{1e}, X_{2e}; Y_{2e})\}\} \end{aligned} \quad (6)$$

where the supremum and infimum are taken over all joint p.m.fs of the form $p(x_l | x_{1e}, x_{2e})p(y_l, y_{1e}, y_{2e} | x_l, x_{1e}, x_{2e})$ and $p(x_{1e}, x_{2e})$, respectively.

Proof: The proof is based on the random coding scheme, which uses Wyner wiretap coding at the legitimate user. At the eavesdroppers, the idea is to let them do their best in colluding. Hence, the coding strategy of the eavesdroppers is not determined in the scheme. As a result, the information leakage rate

is derived by considering the outer bound on the capacity region of the collusion channel and looks like the cut-set upper bound for the relay channel [2].

Codebook Generation: Generate $2^{n(R+R_s)}$ i.i.d x_l^n sequences, each with probability $\prod_{t=1}^n p(x_{l,t})$. Index them as $x_l^n(m, s)$ where $m \in [1 : 2^{nR}]$ and $s \in [1 : 2^{nR_s}]$.

Encoding: To send message $m \in [1 : 2^{nR}]$, the stochastic encoder at the legitimate transmitter uniformly randomly chooses s and transmits $x_l^n(m, s)$.

Decoding: The decoder at the legitimate receiver wants to correctly recover m, s and seeks a unique message \tilde{m} and some \tilde{s} such that $(x_l^n(\tilde{m}, \tilde{s}), y_l^n)$ are jointly typical. Applying the packing lemma [2], with arbitrary high probability $\tilde{m} = m$, if n is large enough and

$$R + R_s \leq I(X_l; Y_l). \quad (7)$$

Analysis of information leakage rate: To simplify the notation, let $X_e = (X_{1e}, X_{2e})$ and $Y_e = (Y_{1e}, Y_{2e})$. We derive two bounds for the randomness index rate, R_s . First, we obtain the second term of information leakage rates in the min term in (6), i.e., $R_{L2} = \max\{I(X_l, X_{1e}, X_{2e}; Y_{1e}), I(X_l, X_{1e}, X_{2e}; Y_{2e})\}$.

Now, consider the leaked information to Y_{1e}^n averaged over the random codebook \mathcal{C} .

$$\begin{aligned} I(M; Y_{1e}^n | \mathcal{C}) &= H(M | \mathcal{C}) - H(M | Y_{1e}^n, \mathcal{C}) \\ &= nR - H(M, Y_{1e}^n, X_l^n, X_e^n | \mathcal{C}) + H(X_l^n, X_e^n | M, Y_{1e}^n, \mathcal{C}) + H(Y_{1e}^n | \mathcal{C}) \\ &= nR - H(X_l^n, X_e^n | \mathcal{C}) - H(M, Y_{1e}^n | X_l^n, X_e^n, \mathcal{C}) + H(X_l^n, X_e^n | M, Y_{1e}^n, \mathcal{C}) + H(Y_{1e}^n | \mathcal{C}) \\ &\leq nR - H(X_l^n | \mathcal{C}) - H(Y_{1e}^n | X_l^n, X_e^n, \mathcal{C}) + H(X_l^n, X_e^n | M, Y_{1e}^n, \mathcal{C}) + H(Y_{1e}^n | \mathcal{C}) \\ &= nR - n(R + R_s) + I(X_l^n, X_e^n; Y_{1e}^n | \mathcal{C}) + H(X_l^n, X_e^n | M, Y_{1e}^n, \mathcal{C}) \\ &\stackrel{(a)}{\leq} -nR_s + nI(X_l, X_e; Y_{1e}) + H(X_l^n, X_e^n | M, Y_{1e}^n, \mathcal{C}) \stackrel{(b)}{\leq} n\delta_1 \end{aligned}$$

(a) holds since the channel is memoryless; (b) follows by using [2, Lemma 22.1]: if $R_s \geq I(X_l, X_{1e}, X_{2e}; Y_{1e})$, then $H(X_l^n, X_{1e}^n, X_{2e}^n | M, Y_{1e}^n, \mathcal{C}) \leq nR_s - nI(X_l, X_{1e}, X_{2e}; Y_{1e}) + n\delta_1$. Following similar steps, one can show that if $R_s \geq I(X_l, X_{1e}, X_{2e}; Y_{2e})$, then $I(M; Y_{2e}^n | \mathcal{C}) \leq \delta_2$. Considering (2), combining (7) and these constraints on R_s gives \mathcal{R}_s^{DM} with R_{L2} .

Now, to derive the first term of information leakage rates in min in (6), i.e., $R_{L1} = I(X_l; Y_{1e}, Y_{2e} | X_{1e}, X_{2e})$, and evaluate the leaked information to both Y_{1e}^n and Y_{2e}^n , averaged over the random codebook \mathcal{C} .

$$\begin{aligned} I(M; Y_e^n | \mathcal{C}) &= H(M | \mathcal{C}) - H(M | Y_e^n, \mathcal{C}) \\ &= nR - H(M, Y_e^n, X_l^n | \mathcal{C}) + H(X_l^n | M, Y_e^n, \mathcal{C}) + H(Y_e^n | \mathcal{C}) \end{aligned}$$

$$\begin{aligned}
&\stackrel{(a)}{=} nR - H(X_l^n | \mathcal{C}) - H(M, Y_e^n | X_l^n, \mathcal{C}) + H(X_l^n | M, Y_e^n, X_e^n, \mathcal{C}) + H(Y_e^n | \mathcal{C}) \\
&\stackrel{(b)}{\leq} nR - n(R + R_s) + I(X_l^n; Y_e^n | \mathcal{C}) + H(X_l^n | M, Y_e^n, X_e^n, \mathcal{C}) \\
&\stackrel{(c)}{=} -nR_s + \sum_{i=1}^n I(X_l^n; Y_{e,i} | Y_e^{i-1}, X_{e,i}, \mathcal{C}) + H(X_l^n | M, Y_e^n, X_e^n, \mathcal{C}) \\
&\stackrel{(d)}{\leq} -nR_s + nI(X_l; Y_e | X_e) + H(X_l^n | M, Y_e^n, X_e^n, \mathcal{C}) \stackrel{(e)}{\leq} n\delta_3 \tag{8}
\end{aligned}$$

(a) and (c) follow since $x_{j_e,t} = f_{j_e,t}(y_{j_e}^{t-1})$, for $j \in \{1, 2\}$ and $1 \leq t \leq n$; (b) is due to the fact that conditioning does not increase the entropy; (d) holds due to the memoryless property of the channel; (e) follows by using [2, Lemma 22.1]: if $R_s \geq I(X_l; Y_{1e}, Y_{2e} | X_{1e}, X_{2e})$, then $H(X_l^n | M, Y_{1e}^n, Y_{2e}^n, X_{1e}^n, X_{2e}^n, \mathcal{C}) \leq nR_s - nI(X_l; Y_{1e}, Y_{2e} | X_{1e}, X_{2e}) + n\delta_3$. Note that (8) implies the individual leakage rates as $I(M; Y_{j_e}^n | \mathcal{C}) \leq n\delta_3$ for $j \in \{1, 2\}$. Now, combining (7) and this constraint on R_s gives \mathcal{R}_s^{DM} with R_{L1} . This completes the proof. \blacksquare

Remark 2: Substituting $Y_{j_e} = (Y_{j_e}^m, Y_{j_e}^c)$ for $j \in \{1, 2\}$ in (6) results in an achievable secure rate (\mathcal{R}_s^{ODM}) for the orthogonal discrete memoryless WTC-CCE, where the supremum is taken over all joint p.m.fs of the form $p(x_l | x_{1e}, x_{2e})p(y_l, y_{1e}^m, y_{2e}^m | x_l)p(y_{1e}^c, y_{2e}^c | x_{1e}, x_{2e})$.

Remark 3: By setting $X_{1e} = X_{2e} = \emptyset$ in (6), \mathcal{R}_s^{DM} reduces to $\sup I(X_l; Y_l) - \max\{I(X_l; Y_{1e}), I(X_l; Y_{2e})\}$ for the non-colluding case. Furthermore, redefining $Y_{1e}^c = Y_{2e}^m, Y_{2e}^c = Y_{1e}^m$ in \mathcal{R}_s^{ODM} results in the achievable secure rate for the perfect colluding case, i.e., $\sup I(X_l; Y_l) - I(X_l; Y_{1e}, Y_{2e})$.

IV. GAUSSIAN CHANNEL

We study the Gaussian WTC-CCE. First, we consider the orthogonal Gaussian WTC-CCE. Let $\theta(x) \doteq \frac{1}{2} \log(1 + x)$.

Theorem 2: The following is an achievable secure rate for orthogonal Gaussian WTC-CCE (defined in (5)).

$$\begin{aligned}
\mathcal{R}_s^{OG} = \theta\left(\frac{h_l^2 P_l}{N_l}\right) - \min \left\{ \theta\left(P_l \left(\frac{h_{1m}^2}{N_{1e}^m} + \frac{h_{2m}^2}{N_{2e}^m}\right)\right), \right. \\
\left. \max \left\{ \theta\left(\frac{h_{1m}^2 P_l}{N_{1e}^m} + \frac{h_{1c}^2 P_{2e}}{N_{1e}^c} + \frac{h_{1m}^2 h_{1c}^2 P_l P_{2e}}{N_{1e}^c N_{1e}^m}\right), \theta\left(\frac{h_{2m}^2 P_l}{N_{2e}^m} + \frac{h_{2c}^2 P_{1e}}{N_{2e}^c} + \frac{h_{2m}^2 h_{2c}^2 P_l P_{1e}}{N_{2e}^c N_{2e}^m}\right) \right\} \right\}. \tag{9}
\end{aligned}$$

Proof: We can extend the achievable secrecy rate in Theorem 1 (after applying Remark 2) to the Gaussian case with continuous alphabets with standard arguments [15]. As we do not know the optimal distribution $p(x_l | x_{1e}, x_{2e})$ that maximizes \mathcal{R}_s^{ODM} , we use a Gaussian input distribution (at the legitimate transmitter) to achieve a lower bound. Let $X_l \sim \mathcal{N}(0, P_l)$. Note that the leakage rates in \mathcal{R}_s^{ODM} (i.e.,

R_{L1} and R_{L2}) are Multiple Access Channel (MAC) type bounds. From the maximum-entropy theorem [15] (or [2, P. 21]), these bounds are largest (or equivalently \mathcal{R}_s^{ODM} is minimized over $p(x_{1e}, x_{2e})$) for the Gaussian inputs at the eavesdroppers. Hence, set $X_{j_e} \sim \mathcal{N}(0, P_{j_e})$ for $j \in \{1, 2\}$ and define $-1 \leq \rho_j \leq 1$ as the correlation coefficient between X_{j_e} and X_l , i.e., $E(X_{j_e}X_l) = \rho_j \sqrt{P_{j_e}P_l}$ for $j \in \{1, 2\}$ and $\rho_{12} = \frac{E(X_{1e}X_{2e})}{\sqrt{P_{1e}P_{2e}}}$. After, calculating the mutual information terms in (6), one can easily show that the leakage rate is maximized (or secure rate is minimized) for $\rho_{12} = \rho_1 = \rho_2 = 0$. This means that in the orthogonal setup, the best strategy for the eavesdroppers is using the independent codewords. This achieves \mathcal{R}_s^{OG} in (9). \blacksquare

Remark 4: To achieve the non-colluding rate, i.e., $\theta(\frac{h_l^2 P_l}{N_l}) - \max\{\theta(\frac{h_{1m}^2 P_l}{N_{1m}^m}), \theta(\frac{h_{2m}^2 P_l}{N_{2m}^m})\}$, set $P_{1e} = P_{2e} = 0$ in \mathcal{R}_s^{OG} . Moreover, it is enough to set $P_{1e}, P_{2e} \rightarrow \infty$ in \mathcal{R}_s^{OG} to derive the perfect colluding rate: $\theta(\frac{h_l^2 P_l}{N_l}) - \theta(P_l(\frac{h_{1m}^2}{N_{1m}^m} + \frac{h_{2m}^2}{N_{2m}^m}))$.

In the following, we obtain a secure rate for the general Gaussian WTC-CCE. The proof is similar to Theorem 2.

Theorem 3: The following is an achievable secure rate for Gaussian WTC-CCE (in (3)).

$$\mathcal{R}_s^G = \min_{\rho_1, \rho_2, \rho_{12}} \theta \left(\frac{h_l^2 P_l + \rho_1^2 (h_{1e}^l)^2 P_{1e} + \rho_2^2 (h_{2e}^l)^2 P_{2e} + 2h_l h_{1e}^l \rho_1 \sqrt{P_l P_{1e}} + 2h_l h_{2e}^l \rho_2 \sqrt{P_l P_{2e}}}{(h_{1e}^l)^2 P_{1e} (1 - \rho_1^2) + (h_{2e}^l)^2 P_{2e} (1 - \rho_2^2) + 2h_{1e}^l h_{2e}^l \rho_{12} \sqrt{P_{1e} P_{2e}} + N_l} \right) \quad (10)$$

$$- \min \left\{ \max\{A(1), A(2)\}, \theta \left(P_l \left(1 - \frac{\rho_1^2 P_{1e}^2 + \rho_2^2 P_{2e}^2 + 2\rho_1 \rho_2 \rho_{12} P_{1e} P_{2e}}{P_{1e} P_{2e} (1 - \rho_{12}^2)} \right) \left(\frac{(h_{1e}^l)^2}{N_{1e}} + \frac{(h_{2e}^l)^2}{N_{2e}} \right) \right) \right\}.$$

where for $j \in \{1, 2\}$:

$$A(j) = \theta \left(\frac{(h_l^{j_e})^2 P_l + (h_{j_e}^{j_e})^2 P_{j_e} + 2h_l^{j_e} h_{j_e}^{j_e} \rho_2 \sqrt{P_l P_{j_e}}}{N_{j_e}} \right).$$

Remark 5: Channel gains h_{1e}^l and h_{2e}^l make the jamming possible for the eavesdroppers. However, they also increase the probability of exposure. In order to compare the two strategies (through numerical examples), we define the non-jamming rate \mathcal{R}_s^{NJG} by setting $h_{1e}^l = h_{2e}^l = 0$ in \mathcal{R}_s^G . In addition, by setting $P_{1e}, P_{2e} \rightarrow \infty$ in \mathcal{R}_s^G , the secure rate is zero, which is less than (or equal to) the perfect colluding rate. This is due to the jamming possibility and is achieved by $\rho_{12} = \rho_1 = \rho_2 = 0$.

Fig. 3 compares the secure rates for the Gaussian WTC-CCE, i.e., $\mathcal{R}_s^G, \mathcal{R}_s^{OG}, \mathcal{R}_s^{NJG}$, to the non-colluding and perfect colluding scenarios in two different collusion channel conditions. It can be seen that the perfect colluding assumption significantly overestimates the eavesdroppers. Recall that the WTC-CCE rates consider the best possible strategy for the eavesdroppers; which may not be achievable for them. Thus, even the constrained colluding rates consider the worst case scenarios for the eavesdroppers' ability to collude.

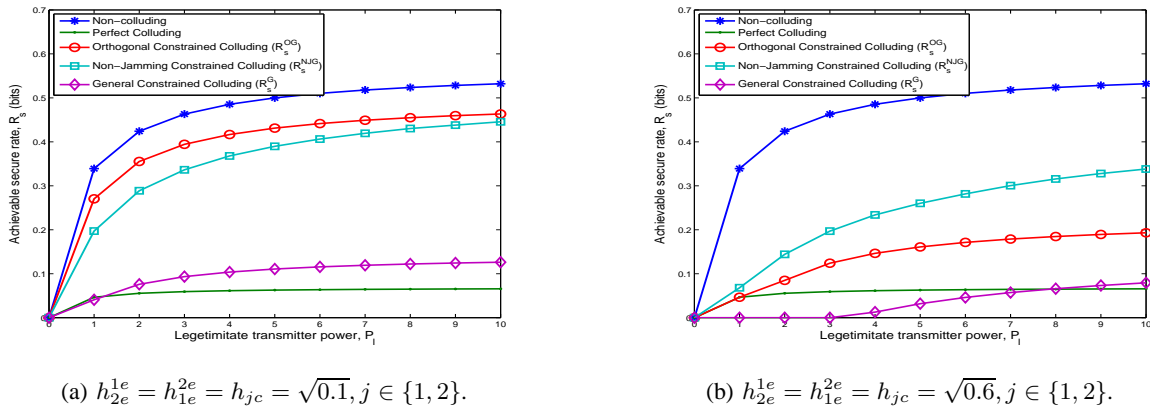


Fig. 3. Achievable secure rates \mathcal{R}_s for $P_{j_e} = 1$, $h_{j_e}^l = \sqrt{0.2}$, $h_i^{j_e} = h_{jm} = 1$, $N_l = N_{j_e} = N_{j_e}^m = N_{j_e}^c = 1, j \in \{1, 2\}$.

In Fig. 3a (weak collusion channel), using the orthogonal collusion channel for eavesdroppers is worse than using the non-orthogonal one (because $\mathcal{R}_s^{OG} \geq \mathcal{R}_s^{NJG}$). In fact, with weak direct collusion links, eavesdroppers may benefit of the main channel by relaying (transmitting correlated codewords). Hence, the optimal ρ_1, ρ_2 for \mathcal{R}_s^{NJG} are not zero; while they are zero for \mathcal{R}_s^{OG} . However, for improved collusion channel (in Fig. 3b), using an orthogonal collusion channel is better (from the eavesdroppers point of view) if one cannot use jamming (or does not want to use jamming to avoid exposure), i.e., $\mathcal{R}_s^{OG} \leq \mathcal{R}_s^{NJG}$. To evaluate the general rate \mathcal{R}_s^G , one should note the effect of jamming in addition to collusion, which even enables the eavesdroppers (or now jammers) to make the secure rate zero for some range of legitimate power P_l .

V. CONCLUSION

We proposed WTC-CCE, a wiretap-based channel model to capture collusion constraints and derived the achievable secure rates. Our results showed that indeed the perfect collision model overestimates the eavesdroppers if they choose to be unexposed. With no exposure constraint, they can jam to further reduce the secure rate in some cases.

REFERENCES

- [1] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, Oct. 1975.
- [2] A. El Gamal and Y.-H. Kim, *Network information theory*. Cambridge Univ. Press, 2011.
- [3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, May 1978.
- [4] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, Jun. 2008.

- [5] E. Ekrem and S. Ulukus, "Multi-receiver wiretap channel with public and confidential messages," *IEEE Trans. Inf. Theory*, vol. 59, no. 4, April 2013.
- [6] Y. K. Chia and A. El Gamal, "Three-receiver broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, May 2012.
- [7] Y. Oohama, "Capacity theorems for relay channels with confidential messages," *Proc. IEEE ISIT*, Nice, France, June 2007
- [8] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, Sep. 2008.
- [9] P. C. Pinto, J. Barros, and M. Z. Win, "Wireless physical-layer security: the case of colluding eavesdroppers," *Proc. IEEE ISIT*, Jun. 2009
- [10] O. O. Koyluoglu, C. E. Koksall, and H. A. El Gamal, "On Secrecy Capacity Scaling in Wireless Networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, May 2012.
- [11] J. Zhang, L. Pu, X. Wang, "Impact of secrecy on capacity in large-scale wireless networks," *Proc. IEEE INFOCOM, Mini-Conference*, 2012.
- [12] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks part II: maximum rate and collusion," *IEEE Trans. Inf. Forensics and Security*, vol. 7, no. 1, Feb. 2012.
- [13] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," *Proc. IEEE MILCOM*, Oct. 2005.
- [14] J. Wang, P. Huang, and X. Wang, "Cross-layer scheduling in multi-user system with delay and secrecy constraints," <http://arxiv.org/abs/1210.1139v2>, Aug. 2013.
- [15] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed., Wiley, 2006.