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), for the discrete memoryless channel and the Gaussian channel. We also compare the proposed rates to the non-colluding and perfect colluding cases.

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, to know the coding scheme of the legitimate user, and to only listen 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 comprises multico ding 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 an eavesdropper (wiretapper) is defined as the maximum of the leakages (to each one). In some applications, this assumption may underestimate the eavesdroppers’ power: they can collude, i.e., share their channel outputs (observations), and render 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 these 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 the 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, the problem at hand is to find an appropriate model and to analyze the effect of these constraints on the secrecy capacity.

In this paper, we model constrained collusion with an equivalent wiretap channel, called WTC-CCE: the collusion channel is orthogonal to the main one (unlike the general WTC-CCE where the eavesdroppers share 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 this way they could be exposed (to the legitimate user). In the orthogonal model, beyond the increased required resources, the eavesdroppers may loose some information leakage rate because they cannot send 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.

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 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}, ..., X_j); we use
$X^j$ instead of $X^j_l$ for brevity. $N(0, \sigma^2)$ denotes a zero-mean Gaussian distribution with variance $\sigma^2$.

Consider the WTC-CCE in Fig. 1: a four terminal discrete channel (one transmitter, one legitimate receiver and two eavesdroppers), denoted by $(X_l \times X_{l,e} \times X_{e,t}, p(y_n^m, y_{e,t}^m, y_{e}^m|x_n^m, x_{e,t}^m, x_{e}^m), X_l \times Y_{l,e} \times Y_{e,t})$. $X_l$ and $X_{l,e}$ are the channel inputs of the legitimate transmitter and eavesdropper $j$ and $Y_l \in Y$ and $Y_{l,e} \in Y_{l,e}$ are the channel outputs at the legitimate receiver and eavesdropper $j$, for $j \in \{1, 2\}$, $p(y_n^m, y_{e,t}^m, y_{e}^m|x_n^m, x_{e,t}^m, x_{e}^m)$ is the channel transition probability distribution. We also assume that the channel is memoryless. In $n$ channel uses, the legitimate transmitter uses the following code 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 $M = [1, 2^nR]$, where each $M$ is uniformly distributed over $M$. (ii) A Randomized encoding function, $f_n$, at the legitimate transmitter that maps a message $m$ to a codeword $x_n^m \in X_n^m$. (iii) Two sets of encoding functions at the eavesdroppers: $\{f_{j,e,t}^{m,n}: \mathbb{R}^{r-1} \rightarrow \mathbb{R}\}$ such that $x_{j,e,t}^m = f_{j,e,t}(y_{j,e,t}^{m,n})$, for $j \in \{1, 2\}$ and $1 \leq t \leq n$. (iv) A Decoding function at the legitimate receiver $g : \mathcal{Y}_n^m \rightarrow \mathbb{R}$. (v) Probability of error for this code is defined as: $P_{e}^{(n)} = \frac{1}{2^n} \sum_{m \in M} P_{\epsilon}(g(x_n^m) \neq m | m \text{ sent})$. (vi) The information leakage rate at eavesdropper $j \in \{1, 2\}$ is defined as:

$$R_{l,j}^{(n)} = \frac{1}{n} I(M; Y_{l,j}^m).$$

All codewords are revealed to the eavesdroppers. However, the eavesdroppers’ mappings are not known to the legitimate user.

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

Definition 2: A rate-leakage tuple $(R, R_{l,e}, R_{l,j})$ 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 $\lim \sup_{n \rightarrow \infty} R_{l,j}^{(n)} \leq R_{l,j}$ for $j \in \{1, 2\}$. The secrecy capacity $C_s$ 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 we consider the orthogonal WTC-CCE in Fig. 2. Here, $Y_{j,e} = (Y_{j,e}^m, Y_{j,e}^{m,n})$ for $j \in \{1, 2\}$ and $p(y_{j,e}, y_{e}^m|x_{l,e}, x_{e}^m) = p(y_{j,e}, y_{e}^m|x_{l,e})p(y_{j,e}, y_{e}^m|x_{e}^m)$, where the variables relating to the main and the collusion channels are indicated with the superscripts $m$ and $e$ respectively. Substituting $X_{l,e} = X_{e} = 0$ results in the non-colluding case; $Y_{l,e} = Y_{e}^{m,n}$ results in the perfect colluding case. To simplify notation, let $j$ be the complement of $j$ in $\{1, 2\}$.

Proof: The proof is based on the random coding scheme, which uses Wyner wiretap coding at the legitimate user. For the eavesdroppers, the idea is to let them do their best in colluding. Hence, the coding strategy of the eavesdroppers is

$$Y_{l,t} = h_l X_{l,t} + Z_{l,t}$$

$$Y_{j,e,t} = h_{je} X_{j,e,t} + Z_{je,t}$$

$$\begin{align*}
Y_{l,t} &= h_l X_{l,t} + Z_{l,t} \\
Y_{j,e,t} &= h_{je} X_{j,e,t} + Z_{je,t}
\end{align*}$$

where $h_l$ is a known channel gain from transmitter $l$ to receiver $k$. We assume perfect echo cancellation at eavesdroppers ($h_{l,e} = h_{e} = 0$). $X_{j,e}$ is an input signal with average power constraint $\frac{1}{n} \sum_{t=1}^{n} |x_{j,e,t}|^2 \leq P_n$ and $Z_{j,e,t}$ is an independent and identically distributed (i.i.d) zero-mean Gaussian noise component with power $N_0$, for $u \in \{1, 2\}$. In practice, $h_{l,e}$ and $h_{e}$ may be small. The Gaussian counterpart of the orthogonal WTC-CCE for $j \in \{1, 2\}$ can be shown as:

$$Y_{l,t} = h_l X_{l,t} + Z_{l,t}$$

$$Y_{j,e,t} = h_{je} X_{j,e,t} + Z_{je,t}$$

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 $P_l, P_{l,e}, P_{e}$ apply for input signals; $Z_{jm}^{m,n}$ and $Z_{jm}^{m,n}$ are i.i.d zero-mean Gaussian noise components with powers $N_{jm}^{m,n}$ and $N_{jm}^{m,n}$ 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:

$$R_{s}^{DM} = \sup_{R_1, R_2, n} \inf \left(I(X_1; Y_1) - \min \left(I(X_1; Y_{1,e}, Y_{2,e}|X_{1,e}, X_{2,e}), \max \left(I(X_1, X_{1,e}, X_{2,e}; Y_1), I(X_1, X_{1,e}, X_{2,e}; Y_{2,e}) \right)\right) \right)$$

where the supremum and infimum are taken over all joint p.m.f.s of the form $p(x_{l,e}, x_{e})p(y_{l,e}, y_{e}^m|x_{l,e})p(y_{l,e}, y_{e}^m|x_{e}^m)$ and $p(x_{l,e}, x_{e})$ respectively.
\[ R_{s}^{OG} = \theta\left(\frac{h_{2}^{2}P_{l}}{N_{l}}\right) - \min\left(\theta\left(\frac{h_{1}^{2}P_{l}}{N_{l}}\right), \max\left(\theta\left(\frac{h_{2}^{2}P_{l}}{N_{l}}\right), \theta\left(\frac{h_{2}^{2}P_{l}}{N_{2e}}\right)\right)\right) \]

\[ R_{s}^{\Omega} = \min_{\rho_{1}, \rho_{2} \geq 1} \theta\left(\frac{h_{2}^{2}P_{l} + \rho_{1}^{2}h_{1}^{2}P_{2e} + \rho_{2}^{2}h_{2}^{2}P_{2e} + 2\rho_{1}\rho_{2}h_{1}^{2}P_{l}h_{2}^{2}P_{2e} + 2h_{1}^{2}h_{2}^{2}P_{l}h_{2}^{2}P_{2e}}{P_{l} + P_{2e} \left(1 - \rho_{1}^{2}\right) + \rho_{2}^{2}}\right) \min\left\{ \max\left(\lambda_{1}(A, 1)\right), \theta\left(1 - \frac{\rho_{1}^{2}P_{l}^{2} + \rho_{2}^{2}P_{2e}^{2} + 2\rho_{1}\rho_{2}P_{l}P_{2e}}{P_{l} + P_{2e} \left(1 - \rho_{1}^{2}\right)}\right)\right\} \}

\[ R_{s}^{\Omega} \leq nR - n\left(\frac{R_{s}^{OG}}{C_{OG}}\right) + I(X^{n}_{e}; Y^{n}_{e}) - I(X^{n}_{c}; Y^{n}_{c}) + H\left(\frac{R_{s}^{OG}}{C_{OG}}\right) \]

\[ R_{s}^{\Omega} \leq nR - n\left(\frac{R_{s}^{OG}}{C_{OG}}\right) + I\left(X^{n}_{e}; Y^{n}_{e}\right) - I\left(X^{n}_{e}; Y^{n}_{e}\right) + H\left(\frac{R_{s}^{OG}}{C_{OG}}\right) \]

\[ R_{s}^{\Omega} \leq nR - n\left(\frac{R_{s}^{OG}}{C_{OG}}\right) + I\left(X^{n}_{e}; Y^{n}_{e}\right) - I\left(X^{n}_{e}; Y^{n}_{e}\right) + H\left(\frac{R_{s}^{OG}}{C_{OG}}\right) \]

\[ R_{s}^{\Omega} \leq nR - n\left(\frac{R_{s}^{OG}}{C_{OG}}\right) + I\left(X^{n}_{e}; Y^{n}_{e}\right) - I\left(X^{n}_{e}; Y^{n}_{e}\right) + H\left(\frac{R_{s}^{OG}}{C_{OG}}\right) \]

The theorem states that the achievable secrecy rate for the Gaussian WTC-CCE is

\[ R_{s}^{OG} \leq \frac{1}{2} \log(1 + x) \]

\[ \text{Proof:} \text{ We can extend the achievable secrecy rate in Theorem 1 (after applying Remark 2) to the Gaussian case with continuous alphabets using standard arguments [15]. As we do not know the optimal distribution } p(x_{1}, x_{2}) \text{ that maximizes } R_{s}^{OG} \text{, we use a Gaussian input distribution (i.e., } R_{s}^{OG} \text{ is minimized over } p(x_{1}, x_{2}) \text{ for Gaussian inputs at the eavesdroppers. Hence, set } X_{je} \sim \mathcal{N}(0, P_{e}) \text{ for } j \in \{1, 2\} \text{ and define } -1 \leq \rho_{j} \leq 1 \text{ as the correlation coefficient between}\]
Achievable secure rates $\mathcal{R}_s$ for $P_{1e} = 1$, $h_{1e} = \sqrt{\Omega l}$, $h_{jm} = 1$, $N_l = N_{1e} = N_{jm}^l = N_{jm}^e = 1, j \in \{1, 2\}$.

Fig. 3.

Remark 4: To achieve the non-colluding rate, i.e., $\theta(h_{1e}^2 P_{1e})\max\{\theta(h_{jm}^2 P_{jm}), \theta(h_{jm}^2 P_{jm})\}$, set $P_{1e} = P_{2e} = 0$ in $\mathcal{R}_s^{GOG}$. Moreover, it is enough to set $P_{1e}, P_{2e} \to \infty$ in $\mathcal{R}_s^{GOG}$ to derive the perfect colluding rate: $\theta(h_{1e}^2 P_{1e}) - \theta(P_1(\frac{h_{1e}^2 P_{1e}}{N_{1e}} + \frac{h_{jm}^2 P_{jm}}{N_{jm}^l})))$.

Remark 5: Channel gains $h_{1e}$ and $h_{jm}^e$ make 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 $\mathcal{R}_s^{UOG}$ by setting $h_{1e} = h_{jm}^e = 0$ in $\mathcal{R}_s^{GOG}$. In addition, by setting $P_{1e}, P_{2e} \to \infty$ in $\mathcal{R}_s^{GOG}$, the secure rate is zero, which is less than (or equal to) the perfect colluding rate. This is due to jamming and it is achieved by $p_{12} = p_{11} = 0$.

Fig. 3 compares the secure rates for the Gaussian WTC-CCE, i.e., $\mathcal{R}_s^{G}, \mathcal{R}_s^{GOG}, \mathcal{R}_s^{NJG}$, to the non-colluding and perfect colluding scenarios in two different collusion channel conditions. It can be seen that the perfect collusion 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.

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 collusion 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