The Individual Secrecy Capacity of the Gaussian SISO and Degraded Gaussian MIMO Multi-Receiver Wiretap Channel

Ahmed S. Mansour*, Rafael F. Schaefer†, and Holger Boche*

* Lehrstuhl für Theoretische Informationstechnik
Technische Universität München
Munich 80290, Germany
Email:{ahmed.mansour, boche}@tum.de

† Department of Electrical Engineering
Princeton University
Princeton, NJ 08544, USA
Email: rafaelfs@princeton.edu

***Abstract*—We study secure communication in which a transmitter wants to send confidential messages to an arbitrary number of receivers in the presence of an external eavesdropper. We consider two classes of Gaussian channels: the Gaussian single-input single-output (SISO) multi-receiver wiretap channel and the degraded Gaussian multiple-input multiple-output (MIMO) multi-receiver wiretap channel. These two channels belong to the class of degraded multi-receiver wiretap channels. In previous literature the secrecy capacity regions of these two channels were established under the conservative joint secrecy constraint. Thus, we focus our work on the less conservative individual secrecy constraint, which is characterized by a higher throughput. We establish the individual secrecy capacity region for these two cases. The achievability follows from the individual secrecy capacity established for the discrete memoryless degraded wiretap channels where coding is performed using Gaussian signals. On the other hand, the converse is established by adapting the techniques used for formulating the joint secrecy capacity region to the individual secrecy constraint.**

I. Introduction

The wireless medium is characterized by an open nature that allows transmitted signals to be received not only by legitimate receivers but eavesdroppers as well. To overcome this problem, physical or higher layer secrecy techniques are used. Recently, physical layer security, also known as *information theoretic security*, is becoming more attractive because it is not based on any assumptions regarding the computational power of the eavesdroppers. Information theoretic security was first introduced by Shannon in [1], where secure communication was achieved using a secret key shared between the transmitter and the receiver. In [2], Wyner studied the degraded wiretap channel and proved that secure transmission is still achievable in the absence of a secret key by exploiting the noisiness of the channel. In [3], this result was extended to the Gaussian scalar wiretap channel.

Recently, the problem of secure communication in wiretap channels with more than one legitimate receiver has captured a lot of attention. Researchers found it very challenging to establish the secrecy capacity for the general multi-receiver wiretap channel, but they managed to solve different special cases. In [4], the degraded two-receiver wiretap channel was investigated, where the authors succeeded in establishing the secrecy capacity. This result played an important role in establishing the secrecy capacity for the Gaussian SISO two-receiver wiretap channel [5] and the degraded Gaussian MIMO two-receiver wiretap channel [6]. In [7], the secrecy capacity of the degraded wiretap channel with arbitrary number of receivers was established. Finally, in [5], the secrecy capacities for both Gaussian SISO and MIMO (not necessarily degraded) multi-receiver wiretap channel were formulated. However, all these works only considered the conservative *joint secrecy* criterion.

In [8], the degraded multi-receiver wiretap BC was investigated under the less conservative secrecy constraint known as the *individual secrecy*. This criterion was addressed by the wiretap multiple access channels in [9] and the wiretap broadcast channel with receiver side information in [10, 11], where it was shown that under the individual secrecy constraint, we have a larger secrecy capacity region by using the available side information to apply secret key encoding. In [8], the individual secrecy capacity region of the degraded multi-receiver wiretap channel was established. This result was also extended to the two-receiver Gaussian SISO wiretap channel. In this paper, we will use this result to formulate the individual secrecy capacity region of the Gaussian SISO and degraded MIMO multi-receiver wiretap channels.

This paper is organized as follows: In Section II, we describe the model of the degraded multi-receiver wiretap channel and explain the differences between joint and individual secrecy. In Section III, we present a detailed proof for the individual secrecy capacity of the Gaussian SISO multi-receiver wiretap channel. In Section IV, we establish the individual secrecy capacity of the degraded Gaussian MIMO multi-receiver wiretap channel by adapting the technique used for the SISO case to the vector nature of the MIMO channel.

II. Degraded Multi-Receiver Wiretap Channel

The degraded multi-receiver wiretap channel consists of a transmitter with an input alphabet $\mathcal{X}$, k legitimate receivers with output alphabets $\mathcal{Y}_j$,[1] and an external eavesdropper with output alphabet $\mathcal{Z}$, such that the following Markov chain holds

$$\mathrm{X} - \mathrm{Y}_1 - \mathrm{Y}_2 - \cdots - \mathrm{Y}_k - \mathrm{Z}. \tag{1}$$

This work of R. F. Schaefer was supported by the German Research Foundation (DFG) under Grant WY 151/2-1.

[1] Through the whole paper j is taken to be in $[\![1, k]\!]$, unless stated otherwise.

We consider the standard model of a block code of arbitrary but fixed length n with input and output sequences x^n, y_j^n and z^n.

Definition 1. *A $(2^{nR_1}, \ldots, 2^{nR_k}, n)$ code $\mathcal{C}_n$ for the degraded multi-receiver wiretap channel consists of: k independent message sets $\mathcal{M}_j = [\![1, 2^{nR_j}]\!]$, a source of local randomness $\mathcal{R}$, an encoding function at the transmitter*

$$E : \mathcal{M}_1 \times \cdots \times \mathcal{M}_k \times \mathcal{R} \to \mathcal{X}^n,$$

which maps the k confidential messages $(m_1, \ldots, m_k) \in \mathcal{M}_1 \times \cdots \times \mathcal{M}_k$ and a realization of the local randomness $r \in \mathcal{R}$ to a codeword $x^n(m_1, \ldots, m_k, r)$, and k decoders

$$\varphi_j : \mathcal{Y}_j^n \to \mathcal{M}_j \cup \{?\},$$

that maps each channel observation at the respective receiver to the corresponding required message or an error message.

We assume that the messages $\mathrm{M}_1, \ldots, \mathrm{M}_k$ are chosen uniformly at random. The reliability performance of $\mathcal{C}_n$ is measured in terms of its average probability of error

$$P_e(\mathcal{C}_n) \triangleq \mathbb{P}\big[\hat{\mathrm{M}}_1 \neq \mathrm{M}_1 \text{ or } \ldots \text{ or } \hat{\mathrm{M}}_k \neq \mathrm{M}_k\big], \tag{2}$$

where $\hat{\mathrm{M}}_j$ is the estimated message at the j^{th} legitimate receiver. One of the main properties of the degraded multi-receiver wiretap channel is that each legitimate receiver is not only capable of decoding its own message, but it can also decode the messages of the receivers degraded from it. This property is one of the consequences of the Markov chain in (1), which indicates that the channel of Y_j is better than that of Y_{j+1}.

The secrecy performance of the code that assures the ignorance of the eavesdropper about the confidential messages, can be measured with respect to two different secrecy criteria.

1. Joint Secrecy: This criterion requires the mutual leakage of the confidential messages to the eavesdropper to be small. This condition can be formulated as follows:

$$L_J(\mathcal{C}_n) \triangleq \mathbb{I}(\mathrm{M}_1, \ldots, \mathrm{M}_k; \mathrm{Z}^n) \leq \tau_n \tag{3}$$

This definition also implies that:

$$\sum_{j=1}^{k} \mathbb{I}(\mathrm{M}_j; \mathrm{Z}^n | \mathrm{M}_{j+1}, \ldots, \mathrm{M}_k) \leq \tau_n. \tag{4}$$

2. Individual Secrecy: This criterion requires the sum of individual leakages of each confidential message to the eavesdropper to be small. This requirement can be expressed as follows:

$$L_I(\mathcal{C}_n) \triangleq \sum_{j=1}^{k} \mathbb{I}(\mathrm{M}_j; \mathrm{Z}^n) \leq \tau_n. \tag{5}$$

The selection among the previous two secrecy criteria is a trade-off between the degree of secrecy and the maximum achievable rate region. The joint secrecy criterion is a conservative secrecy constraint, where the legitimate receivers do not trust each other, so it guarantees that the confidential message of each receiver is secure, even if the confidential messages of the other receivers were revealed to the eavesdropper. On the other hand, the individual secrecy criterion is a relaxed secrecy constraint that is based on the mutual trust between the legitimate receivers. This implies that the individual secrecy achievable rate region is bigger than the joint one [8].

Definition 2. *A rate tuple $(R_1, \ldots, R_k) \in \mathbb{R}_+^k$ is achievable for the multi-receiver wiretap channel, if there exists a sequence of $(2^{nR_1}, \ldots, 2^{nR_k}, n)$ codes $\mathcal{C}_n$ and two sequences ϵ_n and τ_n, where $\lim_{n\to\infty} \epsilon_n, \tau_n = 0$ such that, for n is large enough, the following holds:*

$$P_e(\mathcal{C}_n) \leq \epsilon_n \qquad \textit{and} \qquad L(\mathcal{C}_n) \leq \tau_n. \tag{6}$$

Depending on the selected secrecy criteria, $L(\mathcal{C}_n)$ is given by (3) *or* (5).

Theorem 1. *[8] The individual secrecy capacity region of the degraded multi-receiver wiretap channel is given by the union of all rate tuples $(R_1, \ldots, R_k) \in \mathbb{R}_+^k$ that satisfy*

$$R_j \leq \mathbb{I}(\mathrm{U}_j; \mathrm{Y}_j | \mathrm{U}_{j+1}) - \mathbb{I}(\mathrm{U}_j; \mathrm{Z} | \mathrm{U}_{j+1}) + \sum_{l=j+1}^{k} R_l \tag{7a}$$

$$R_j \leq \mathbb{I}(\mathrm{U}_j; \mathrm{Y}_j | \mathrm{U}_{j+1}) + \mathbb{I}(\mathrm{U}_{j+1}; \mathrm{Z}) \tag{7b}$$

$$\sum_{l=j}^{k} R_l \leq \sum_{l=j}^{k} \mathbb{I}(\mathrm{U}_l; \mathrm{Y}_l | \mathrm{U}_{l+1}) \tag{7c}$$

where $\mathrm{U}_1 = \mathrm{X}$, $\mathrm{U}_{k+1} = \emptyset$ and the union runs over all random variables $(\mathrm{U}_k, \ldots, \mathrm{U}_2, \mathrm{X})$ such that, $\mathrm{U}_k - \cdots - \mathrm{U}_2 - \mathrm{X} - \mathrm{Y}_1 - \mathrm{Y}_2 - \cdots - \mathrm{Y}_k - \mathrm{Z}$ forms a Markov chain.

Evaluating the capacity for a certain degraded multi-receiver wiretap channel is equivalent to finding the optimal joint distribution of $(\mathrm{X}, \mathrm{U}_2, \ldots, \mathrm{U}_k)$ for this channel that satisfy the Markov chain in (1) and trace the boundary of the region in (7).

III. Gaussian SISO Multi-Receiver Wiretap Channel

In this section, we will establish the individual secrecy capacity region of the Gaussian SISO multi-receiver wiretap channel. This result generalizes the one in [8], where the individual secrecy capacity region of the Gaussian SISO two-receiver wiretap channel was established. We define the Gaussian SISO multi-receiver wiretap channel as:

$$\mathrm{Y}_j = \mathrm{X} + \mathrm{N}_j \tag{8a}$$

$$\mathrm{Z} = \mathrm{X} + \mathrm{N}_Z, \tag{8b}$$

where the channel input X is subject to a power constraint $\mathbb{E}[\mathrm{X}^2] \leq P$. The N_j and N_Z are zero-mean Gaussian random variables, whose variances are given by σ_j^2 and σ_Z^2 respectively.

The Gaussian SISO multi-receiver wiretap channel belongs to the class of degraded wiretap channels, where the variances (power) of the Gaussian noises N_j and N_Z define the degradedness order of the channel. In [8], it was showed that the capacity region in (7) establishes the individual secrecy capacity of any degraded wiretap channel regardless of the degradedness order of the eavesdropper. This implies that Theorem 1 can be used to derive the individual secrecy capacity of the Gaussian SISO multi-receiver wiretap channel. However, we will assume without loss of generality that the variances of the Gaussian noises satisfy the following order:

$$\sigma_1^2 \leq \sigma_2^2 \leq \cdots \leq \sigma_k^2 \leq \sigma_Z^2. \tag{9}$$

Theorem 2. *The individual secrecy capacity region of the Gaussian SISO multi-receiver wiretap channel is given by the union of all rate tuples* $(R_1,\dots,R_k)\in\mathbb{R}_+^k$ *that satisfy*

$$R_j \le f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P+\sigma_j^2}\right)-f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P+\sigma_Z^2}\right)+\sum_{l=j+1}^{k}R_l \tag{10a}$$

$$R_j \le f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P+\sigma_j^2}\right)+f\left(\frac{\sum_{i=j+1}^{k}\alpha_i P}{\sum_{i=1}^{j}\alpha_i P+\sigma_Z^2}\right) \tag{10b}$$

$$\sum_{l=j}^{k}R_l \le \sum_{l=j}^{k} f\left(\frac{\alpha_l P}{\sum_{i=1}^{l-1}\alpha_i P+\sigma_l^2}\right) \tag{10c}$$

where $f(x)=\frac{1}{2}\log(1+x)$ *and the union is taken over all values of* $\alpha_j\in[0,1]$ *such that* $\sum_{i=1}^{k}\alpha_i\le 1$.

Proof: The previous region is achieved by choosing $\mathrm{U}_j=\mathrm{U}_{j+1}+\mathrm{V}_j$, where the V_j are independent Gaussian random variables with variance α_j and $\mathrm{U}_{k+1}=0$. This means that each V_j contains information about the confidential message M_j and a part of the local randomness R_j that is used to confuse the eavesdropper in this layer. The decoder at a certain receiver Y_i, where $i\in[\![1,k]\!]$, can decode all V_j for $j\ge i$ because of the order of the variances of the Gaussian noises in (9), while handling the remaining V_j for $j<i$ as an interference noise. The previous coding structure implies that, $(\mathrm{U}_k,\dots,\mathrm{U}_2,\mathrm{X})$ are characterized by a joint Gaussian distribution.
Before we jump to the converse part of the theorem, we need to highlight the following proposition.

Proposition 1. *For the Gaussian SISO multi-receiver wiretap channel defined in* (8)*, where* $\mathbb{E}[\mathrm{X}^2]\le P$ *and the variances of the Gaussian noises satisfy the order in* (9)*, if*

$$\mathbb{I}(\mathrm{U}_j;\mathrm{Y}_j|\mathrm{U}_{j+1})-\mathbb{I}(\mathrm{U}_j;\mathrm{Z}|\mathrm{U}_{j+1})\le f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P+\sigma_j^2}\right)-f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P+\sigma_Z^2}\right), \tag{11}$$

where $\mathrm{U}_{k+1}=\emptyset$, $\mathrm{U}_k-\cdots-\mathrm{U}_2-\mathrm{X}-\mathrm{Y}_1-\mathrm{Y}_2-\cdots-\mathrm{Y}_k-\mathrm{Z}$ *forms a Markov chain and* $\sum_{i=1}^{k}\alpha_i=1$*, then* $\mathbb{E}[\mathrm{U}_j^2]\le\sum_{i=j}^{k}\alpha_i P$.

Proof of Proposition 1: We start by U_k and assume that U_k is a Gaussian random variable such that, $\mathbb{E}[\mathrm{U}_k^2]=(\alpha_k+\gamma)P$. If we let $\mathrm{X}=\mathrm{U}_k+\bar{\mathrm{V}}_k$, where $\bar{\mathrm{V}}_k$ is a Gaussian random vector independent from U_k, we have

$$\mathbb{I}(\mathrm{U}_k;\mathrm{Y}_k)-\mathbb{I}(\mathrm{U}_k;\mathrm{Z})=f\left(\frac{(\alpha_k+\gamma)P}{(\sum_{i=1}^{k-1}\alpha_i-\gamma)P+\sigma_k^2}\right)-f\left(\frac{(\alpha_k+\gamma)P}{(\sum_{i=1}^{k-1}\alpha_i-\gamma)P+\sigma_Z^2}\right). \tag{12}$$

This conditions contradicts the one in (11) at $j=k$, unless $\gamma\le 0$ which consequently implies that $\mathbb{E}[\mathrm{U}_k^2]\le\alpha_k P$. Now, following the same steps, we can show that $\mathbb{E}[\mathrm{U}_j^2]\le\sum_{i=j}^{k}\alpha_i P$. ∎

Now, we are ready to present our converse. We start with the bound in (7a) and consider the k^{th} user first. We have

$$\begin{aligned}
R_k &\le \mathbb{I}(\mathrm{U}_k;\mathrm{Y}_k)-\mathbb{I}(\mathrm{U}_k;\mathrm{Z})\\
&\overset{(a)}{=}\Big[\mathbb{I}(\mathrm{X};\mathrm{Y}_k)-\mathbb{I}(\mathrm{X};\mathrm{Z})\Big]-\Big[\mathbb{I}(\mathrm{X};\mathrm{Y}_k|\mathrm{U}_k)-\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_k)\Big]\\
&\overset{(b)}{\le}\left[f\left(\frac{P}{\sigma_k^2}\right)-f\left(\frac{P}{\sigma_Z^2}\right)\right]-\Big[\mathbb{I}(\mathrm{X};\mathrm{Y}_k|\mathrm{U}_k)-\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_k\Big]\\
&\overset{(c)}{=}\left[f\left(\frac{P}{\sigma_k^2}\right)-f\left(\frac{P}{\sigma_Z^2}\right)\right]-\left[f\left(\frac{\bar{\alpha}_k P}{\sigma_k^2}\right)-f\left(\frac{\bar{\alpha}_k P}{\sigma_Z^2}\right)\right]\\
&\overset{(d)}{=} f\left(\frac{\alpha_k P}{\sum_{i=1}^{k-1}\alpha_i P+\sigma_k^2}\right)-f\left(\frac{\alpha_k P}{\sum_{i=1}^{k-1}\alpha_i P+\sigma_Z^2}\right),
\end{aligned} \tag{13}$$

where (a) follows by using the chain rule and the Markov chain $\mathrm{U}_k-\mathrm{X}-(\mathrm{Y}_k,\mathrm{Z})$; (b) follows because $\mathbb{I}(\mathrm{X};\mathrm{Y}_k)-\mathbb{I}(\mathrm{X};\mathrm{Z})$ is maximized by a Gaussian X [3]; (c) follows because $0\le\mathbb{I}(\mathrm{X};\mathrm{Y}_k|\mathrm{U}_k)-\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_k)\le f(P/\sigma_k^2)-f(P/\sigma_Z^2)$, which implies that for any pair $(\mathrm{U}_k,\mathrm{X})$, there exists an $\bar{\alpha}_k\in[0,1]$ such that, $\mathbb{I}(\mathrm{X};\mathrm{Y}_k|\mathrm{U}_k)-\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_k)=f(\bar{\alpha}_k P/\sigma_k^2)-f(\bar{\alpha}_k P/\sigma_Z^2)$; and (d) follows by letting $\alpha_k=1-\bar{\alpha}_k$ and $\bar{\alpha}_k=\sum_{i=1}^{k-1}\alpha_i$. Now, we consider the $(k-1)^{th}$ user under the same bound, we have

$$\begin{aligned}
R_{k-1} &\le \mathbb{I}(\mathrm{U}_{k-1};\mathrm{Y}_{k-1}|\mathrm{U}_k)-\mathbb{I}(\mathrm{U}_{k-1};\mathrm{Z}|\mathrm{U}_k)+R_k\\
&\overset{(a)}{=}\Big[\mathbb{I}(\mathrm{X};\mathrm{Y}_{k-1}|\mathrm{U}_k)-\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_k)\Big]\\
&\quad-\Big[\mathbb{I}(\mathrm{X};\mathrm{Y}_{k-1}|\mathrm{U}_{k-1})-\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_{k-1})\Big]+R_k\\
&\overset{(b)}{\le}\left[f\left(\frac{\bar{\alpha}_k P}{\sigma_{k-1}^2}\right)-f\left(\frac{\bar{\alpha}_k P}{\sigma_Z^2}\right)\right]\\
&\quad-\Big[\mathbb{I}(\mathrm{X};\mathrm{Y}_{k-1}|\mathrm{U}_{k-1})-\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_{k-1}\Big]+R_k\\
&\overset{(c)}{=}\left[f\left(\frac{\bar{\alpha}_k P}{\sigma_{k-1}^2}\right)-f\left(\frac{\bar{\alpha}_k P}{\sigma_Z^2}\right)\right]\\
&\quad-\left[f\left(\frac{\bar{\alpha}_{k-1} P}{\sigma_k^2}\right)-f\left(\frac{\bar{\alpha}_{k-1} P}{\sigma_Z^2}\right)\right]+R_k\\
&\overset{(d)}{=} f\left(\frac{\alpha_{k-1} P}{\sum_{i=1}^{k-2}\alpha_i P+\sigma_k^2}\right)-f\left(\frac{\alpha_{k-1} P}{\sum_{i=1}^{k-2}\alpha_i P+\sigma_Z^2}\right)+R_k,
\end{aligned} \tag{14}$$

where (a) follows by using the chain rule and the Markov chain $\mathrm{U}_k-\mathrm{U}_{k-1}-\mathrm{X}-(\mathrm{Y}_{k-1},\mathrm{Z})$; (b) follows because under the constraint $\mathbb{I}(\mathrm{X};\mathrm{Y}_k|\mathrm{U}_k)-\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_k)=f(\bar{\alpha}_k P/\sigma_k^2)-f(\bar{\alpha}_k P/\sigma_Z^2)$, the expression $\mathbb{I}(\mathrm{X};\mathrm{Y}_{k-1}|\mathrm{U}_k)-\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_k)$ is maximized by a joint Gaussian distribution on the pair $(\mathrm{U}_k,\mathrm{X})$ [5]; (c) follows because $0\le\mathbb{I}(\mathrm{X};\mathrm{Y}_{k-1}|\mathrm{U}_{k-1})-\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_{k-1})\le f(\bar{\alpha}_k P/\sigma_{k-1}^2)-f(\bar{\alpha}_k P/\sigma_Z^2)$, which implies that for any triple $(\mathrm{U}_k,\mathrm{U}_{k-1},\mathrm{X})$, there exists an $\bar{\alpha}_{k-1}\in[0,\bar{\alpha}_k]$ such that, $\mathbb{I}(\mathrm{X};\mathrm{Y}_{k-1}|\mathrm{U}_{k-1})-\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_{k-1})=f(\bar{\alpha}_{k-1}P/\sigma_{k-1}^2)-f(\bar{\alpha}_{k-1}P/\sigma_Z^2)$; and (d) follows by letting $\alpha_{k-1}=\bar{\alpha}_k-\bar{\alpha}_{k-1}$ and $\bar{\alpha}_{k-1}=\sum_{i=1}^{k-2}\alpha_i$.
Now, if we apply the same steps in (14) to the remaining users, we can show that the bound in (10a) holds. These calculations establish two additional constraints: the first is $\sum_{i=1}^{k}\alpha_i=1$, while the second is the bound in (11), which implies that $\mathbb{E}[\mathrm{U}_j^2]\le\sum_{i=j}^{k}\alpha_i P$. We now consider the bound in (7b) as

follows:

$$\begin{aligned}
R_j &\le \mathbb{I}(\mathrm{U}_j;\mathrm{Y}_j|\mathrm{U}_{j+1}) + \mathbb{I}(\mathrm{U}_{j+1};\mathrm{Z}) \\
&\overset{(a)}{=} \mathbb{I}(\mathrm{U}_j;\mathrm{Y}_j|\mathrm{U}_{j+1}) - \mathbb{I}(\mathrm{U}_j;\mathrm{Z}|\mathrm{U}_{j+1}) + \mathbb{I}(\mathrm{U}_j;\mathrm{Z}) \\
&\overset{(b)}{\le} f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P+\sigma_j^2}\right) - f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P+\sigma_Z^2}\right) \\
&\quad + \mathbb{I}(\mathrm{U}_j;\mathrm{Z}) \\
&\overset{(c)}{\le} f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P+\sigma_j^2}\right) - f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P+\sigma_Z^2}\right) \\
&\quad + f\left(\frac{\sum_{i=j}^{k}\alpha_i P}{\sum_{i=1}^{j-1}\alpha_i P+\sigma_Z^2}\right) \\
&= f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P+\sigma_j^2}\right) + f\left(\frac{\sum_{i=j+1}^{k}\alpha_i P}{\sum_{i=1}^{j}\alpha_i P+\sigma_Z^2}\right), \qquad (15)
\end{aligned}$$

where (a) follows by using the chain rule and the Markov chain $\mathrm{U}_{j+1} - \mathrm{U}_j - \mathrm{Z}$; (b) follows by the same steps used to establish (10a) and (c) follows because under the power constraint on U_j and X, in addition to the Markov chain $\mathrm{U}_j - \mathrm{X} - \mathrm{Z}$, $\mathbb{I}(\mathrm{U}_j;\mathrm{Z})$ is maximized by a joint Gaussian distribution on the pair $(\mathrm{U}_j,\mathrm{X})$. Finally, we consider the bound in (7c), for which we have

$$\begin{aligned}
\sum_{l=j}^{k} R_l &\le \sum_{l=j}^{k} \mathbb{I}(\mathrm{U}_l;\mathrm{Y}_l|\mathrm{U}_{l+1}) \\
&\overset{(a)}{=} \sum_{l=j}^{k} \left[\mathbb{I}(\mathrm{U}_l;\mathrm{Y}_l|\mathrm{U}_{l+1}) - \mathbb{I}(\mathrm{U}_l;\mathrm{Z}|\mathrm{U}_{l+1})\right] + \mathbb{I}(\mathrm{U}_j;\mathrm{Z}) \\
&\overset{(b)}{\le} \sum_{l=j}^{k} \left[f\left(\frac{\alpha_l P}{\sum_{i=1}^{l-1}\alpha_i P+\sigma_l^2}\right) - f\left(\frac{\alpha_l P}{\sum_{i=1}^{l-1}\alpha_i P+\sigma_Z^2}\right)\right] \\
&\quad + \mathbb{I}(\mathrm{U}_j;\mathrm{Z}) \\
&\overset{(c)}{\le} \sum_{l=j}^{k} \left[f\left(\frac{\alpha_l P}{\sum_{i=1}^{l-1}\alpha_i P+\sigma_l^2}\right) - f\left(\frac{\alpha_l P}{\sum_{i=1}^{l-1}\alpha_i P+\sigma_Z^2}\right)\right] \\
&\quad + f\left(\frac{\sum_{i=j}^{k}\alpha_i P}{\sum_{i=1}^{j-1}\alpha_i P+\sigma_Z^2}\right) \\
&= \sum_{l=j}^{k} f\left(\frac{\alpha_l P}{\sum_{i=1}^{l-1}\alpha_i P+\sigma_l^2}\right), \qquad (16)
\end{aligned}$$

where (a) follows by using the chain rule and the Markov chain $\mathrm{U}_k - \mathrm{U}_{k-1} - \cdots - \mathrm{U}_j - \mathrm{Z}$; while (b) and (c) follows as in (15). Now, our converse is complete. ■

IV. Degraded Gaussian MIMO Multi-Reciever Wiretap Channel

In this section, we will establish the individual secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel by adapting the converse techniques used in [5] to Theorem 1. We define the degraded Gaussian MIMO multi-receiver wiretap channel as:

$$\mathbf{Y}_j = \mathbf{X} + \mathbf{N}_j \qquad (17a)$$

$$\mathbf{Z} = \mathbf{X} + \mathbf{N}_Z, \qquad (17b)$$

where $\mathbf{X}$, $\mathbf{Y}_j$, $\mathbf{N}_j$, $\mathbf{Z}$ and $\mathbf{N}_Z$ are column vectors of length m, where m is the number of antennas available at the transmitter and each receiver. The channel input $\mathbf{X}$ is subject to a covariance constraint $\mathbb{E}[\mathbf{X}\mathbf{X}^\top] \preceq \mathbf{S}$, where $\mathbf{S} \succ \mathbf{0}$. $\mathbf{N}_j$ and $\mathbf{N}_Z$ are zero-mean Gaussian random vectors, whose covariance matrices are given by $\mathbf{\Sigma}_j$ and $\mathbf{\Sigma}_Z$, such that

$$\mathbf{0} \prec \mathbf{\Sigma}_1 \preceq \mathbf{\Sigma}_2 \preceq \cdots \preceq \mathbf{\Sigma}_k \preceq \mathbf{\Sigma}_Z. \qquad (18)$$

The semi-definite ordering of the noise covariance matrices in (18) implies that $\mathbf{X} - \mathbf{Y}_1 - \cdots - \mathbf{Y}_k - \mathbf{Z}$ forms a Markov chain, where changing the order of the covariance matrix will change the position of the receiver in the Markov chain. This implies that, the degraded Gaussian MIMO wiretap channel belongs to the class of degraded wiretap channels and its individual secrecy capacity region can be computed by finding the optimal joint distribution on $(\mathrm{U}_k,\ldots,\mathrm{U}_2,\mathbf{X})$ that traces the boundary of the capacity region in (7).

Theorem 3. *The individual secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel is given by the union of all rate tuples $(R_1,\ldots,R_k) \in \mathbb{R}_+^k$ that satisfy*

$$\begin{aligned}
R_j &\le \frac{1}{2}\log\frac{\left|\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_j\right|}{\left|\sum_{i=1}^{j-1}\mathbf{K}_i+\mathbf{\Sigma}_j\right|} - \frac{1}{2}\log\frac{\left|\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{j-1}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|} \\
&\quad + \sum_{l=j+1}^{k} R_l \qquad (19a) \\
R_j &\le \frac{1}{2}\log\frac{\left|\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_j\right|}{\left|\sum_{i=1}^{j-1}\mathbf{K}_i+\mathbf{\Sigma}_j\right|} + \frac{1}{2}\log\frac{\left|\sum_{i=1}^{k}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|} \qquad (19b) \\
\sum_{l=j}^{k} R_l &\le \sum_{l=j}^{k}\frac{1}{2}\log\frac{\left|\sum_{i=1}^{l}\mathbf{K}_i+\mathbf{\Sigma}_l\right|}{\left|\sum_{i=1}^{l-1}\mathbf{K}_i+\mathbf{\Sigma}_l\right|} \qquad (19c)
\end{aligned}$$

where the union is taken over all positive semi-definite matrices $\mathbf{K}_j \succeq \mathbf{0}$, such that $\sum_{i=1}^{k}\mathbf{K}_i \preceq \mathbf{S}$.

Remark 1. *Although it is more common in literature and practically meaningful to consider a sum power constraint, we used a covariance constraint instead for convenience. Moreover, it was shown in [12], that once the capacity region is obtained under a covariance constraint, the capacity region under the sum power constraint follows easily.*

Proof: The region in (19) can be achieved by using a Gaussian random vector realization for the auxiliary random variables in Theorem 1, where the random vector $\mathbf{U}_j$ is used as a realization for the auxiliary random variable U_j. The vectors are constructed recursively as follows: $\mathbf{U}_j = \mathbf{U}_{j+1} + \mathbf{V}_j$, where $\mathbf{V}_j$ are independent Gaussian random vectors with covariance matrices $\mathbf{K}_j$ and $\mathbf{U}_{k+1}$ is a zero vector. This means that each $\mathbf{V}_j$ contains information about the confidential message M_j and a part of the local randomness R_j that is used to confuse the eavesdropper in this layer. The decoder at a certain receiver $\mathbf{Y}_i$, where $i \in [\![1,k]\!]$, can decode all $\mathbf{V}_j$ for $j \ge i$ because of the order of the covariance matrices of the noise vectors in (18), while handling the remaining $\mathbf{V}_j$ for $j < i$ as noise.

Before we present the converse part of the theorem, we need to highlight the bound established in [5] for the degraded Gaussian MIMO wiretap channel.

$$\mathbb{I}(\mathrm{U}_j;\mathbf{Y}_j|\mathrm{U}_{j+1})-\mathbb{I}(\mathrm{U}_j;\mathbf{Z}|\mathrm{U}_{j+1})\leq \frac{1}{2}\log\frac{\left|\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_j\right|}{\left|\sum_{i=1}^{j-1}\mathbf{K}_i+\mathbf{\Sigma}_j\right|}-\frac{1}{2}\log\frac{\left|\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{j-1}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}, \quad (20)$$

where $\mathrm{U}_k-\cdots-\mathrm{U}_2-\mathbf{X}-\mathbf{Y}_1-\cdots-\mathbf{Y}_k-\mathbf{Z}$ forms a Markov chain and $\mathbf{K}_j\succeq\mathbf{0}$ are positive semi-definite matrices, such that $\sum_{i=1}^{k}\mathbf{K}_i=\mathbf{S}$, where $\mathbb{E}[\mathbf{X}\mathbf{X}^\top]\preceq\mathbf{S}$. The establishment of the previous bound uses similar steps to the one used to establish the bound in (11) for the Gaussian SISO case, along with the properties of Fisher information matrix. One of the consequences of the bound in (20) is the extension of Proposition 1 to the degraded Gaussian MIMO wiretap channel as follows:

Proposition 2. *For the degraded Gaussian MIMO multi-receiver wiretap channel defined in* (17)*, where covariance matrices of the Gaussian noise vectors satisfy the semi-definite order in* (18)*, if the bound in* (20) *holds with all its constraints, then the vector realizations* $\mathbf{U}_j$ *of the auxiliary random variables* U_j *in* (20) *must satisfy the following covariance constraint:* $\mathbb{E}[\mathbf{U}_j\mathbf{U}_j^\top]\preceq\sum_{i=j}^{k}\mathbf{K}_i$.

Proof: The proof follows by adapting the same techniques used to prove Proposition 1 to the vector nature of the degraded Gaussian MIMO multi-receiver wiretap channel and is omitted due to space constraints. ∎

Now, we can formulate our converse. We start with the first bound in Theorem 1. If we apply the bound in (20) to Eq. (7a), we reach the first bound in Theorem 3. We then move to the second bound in (7b), we have

$$\begin{aligned}
R_j &\overset{(a)}{\leq} \mathbb{I}(\mathrm{U}_j;\mathbf{Y}_j|\mathrm{U}_{j+1})-\mathbb{I}(\mathrm{U}_j;\mathbf{Z}|\mathrm{U}_{j+1})+\mathbb{I}(\mathrm{U}_j;\mathbf{Z})\\
&\overset{(b)}{\leq} \frac{1}{2}\log\frac{\left|\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_j\right|}{\left|\sum_{i=1}^{j-1}\mathbf{K}_i+\mathbf{\Sigma}_j\right|}-\frac{1}{2}\log\frac{\left|\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{j-1}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}\\
&\quad+\mathbb{I}(\mathbf{U}_j;\mathbf{Z})\\
&\overset{(c)}{\leq} \frac{1}{2}\log\frac{\left|\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_j\right|}{\left|\sum_{i=1}^{j-1}\mathbf{K}_i+\mathbf{\Sigma}_j\right|}-\frac{1}{2}\log\frac{\left|\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{j-1}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}\\
&\quad+\frac{1}{2}\log\frac{\left|\sum_{i=1}^{k}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{j-1}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}\\
&= \frac{1}{2}\log\frac{\left|\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_j\right|}{\left|\sum_{i=1}^{j-1}\mathbf{K}_i+\mathbf{\Sigma}_j\right|}+\frac{1}{2}\log\frac{\left|\sum_{i=1}^{k}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}, \quad (21)
\end{aligned}$$

where (a) follows as in (15); (b) follows from (20) and the fact that for a Gaussian MIMO channel and under the Markov chain $\mathrm{U}_j-\mathbf{X}-\mathbf{Z}$, $\mathbb{I}(\mathrm{U}_j;\mathbf{Z})$ is maximized by a vector realization $\mathbf{U}_j$ for the auxiliary random variable U_j, such that $\mathbf{U}_j$ and $\mathbf{X}$ are jointly Gaussian; (c) follows from the covariance constraint on $\mathbf{U}_j$ in Proposition 2. Finally, we consider the bound in (7c), we have

$$\begin{aligned}
\sum_{l=j}^{k}R_l &\overset{(a)}{\leq} \sum_{l=j}^{k}\left[\mathbb{I}(\mathrm{U}_l;\mathbf{Y}_l|\mathrm{U}_{l+1})-\mathbb{I}(\mathrm{U}_l;\mathbf{Z}|\mathrm{U}_{l+1})\right]+\mathbb{I}(\mathrm{U}_j;\mathbf{Z})\\
&\overset{(b)}{\leq} \sum_{l=j}^{k}\left[\frac{1}{2}\log\frac{\left|\sum_{i=1}^{l}\mathbf{K}_i+\mathbf{\Sigma}_l\right|}{\left|\sum_{i=1}^{l-1}\mathbf{K}_i+\mathbf{\Sigma}_l\right|}\right.\\
&\quad\left.-\frac{1}{2}\log\frac{\left|\sum_{i=1}^{l}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{l-1}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}\right]+\frac{1}{2}\log\frac{\left|\sum_{i=1}^{k}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{j-1}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}\\
&= \sum_{l=j}^{k}\frac{1}{2}\log\frac{\left|\sum_{i=1}^{l}\mathbf{K}_i+\mathbf{\Sigma}_l\right|}{\left|\sum_{i=1}^{l-1}\mathbf{K}_i+\mathbf{\Sigma}_l\right|}, \quad (22)
\end{aligned}$$

where (a) follows as in (16), while (b) follows as in (21). This completes our converse. ∎

V. Conclusion

We studied secure communication over two classes of Gaussian channels: the Gaussian SISO and the degraded Gaussian MIMO multi-receiver wiretap channel. We established the individual secrecy capacity region for both channels, where coding with Gaussian signals is used to prove the acheivability, while the converse follows using the techniques in [5].

References

[1] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

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

[4] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "Secrecy rate region of the broadcast channel with an eavesdropper," in *Forty-Sixth Annual Allerton Conference*, Sep. 2009, pp. 834–841.

[5] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, 2011.

[6] R. Liu, T. Liu, H. V. Poor, and S. S. (Shitz), "A vector generalization of Costa's entropy-power inequality with applications," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1865–1879, April 2010.

[7] E. Ekrem and S. Ulukus, "Secrecy capacity of a class of broadcast channels with an eavesdropper," *EURASIP J. Wirel. Commun. Netw.*, pp. 1–29, March 2009.

[8] A. S. Mansour, R. F. Schaefer, and H. Boche, "The individual secrecy capacity of degraded multi-receiver wiretap broadcast channels," in *Communications (ICC), 2015 IEEE International Conference on*, London, United Kingdom, June 2015.

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

[10] A. S. Mansour, R. F. Schaefer, and H. Boche, "Secrecy measures for broadcast channels with receiver side information: Joint vs individual," in *IEEE Inf. Theory Workshop*, Hobart, Tasmania, Australia, November 2014, pp. 426–430.

[11] ——, "Joint and individual secrecy in broadcast channels with receiver side information," in *Signal Processing Advances in Wireless Communications (SPAWC), 2014 IEEE 15th International Workshop*, Toronto, Canada, June 2014, pp. 369 – 373.

[12] H. Weingarten, Y. Steinberg, and S. S. (Shitz), "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3936–3964, Sept 2006.