The Secrecy Capacity of a Compound MIMO Gaussian Channel

Rafael F. Schaefer

Lehrstuhl für Theoretische Informationstechnik
Technische Universität München, Germany
e-mail: rafael.schaefer@tum.de

Sergey Loyka

School of Electrical Engineering and Computer Science
University of Ottawa, Ontario, Canada
e-mail: sloyka@site.uottawa.ca

***Abstract*—The compound MIMO Gaussian wiretap channel is studied, where the channel to the legitimate receiver is known and the eavesdropper channel is not known to the transmitter but is known to have a bounded spectral norm (channel gain). The compound secrecy capacity is established without the degradedness assumption and the optimal signaling is identified: the compound capacity equals the worst-case channel capacity thus establishing the saddle-point property, the optimal signaling is Gaussian and on the eigenvectors of the legitimate channel and the worst-case eavesdropper is isotropic. The eigenmode power allocation somewhat resembles the standard water-filling but is not identical to it.**

I. Introduction

The nature of the wireless medium makes wireless communication systems inherently vulnerable for eavesdropping. In this context, the concept of information theoretic security is instrumental since it solely uses the physical properties of the wireless channel in order to establish security. Information theoretic security was initiated by Shannon [1] and studied later by Wyner, who introduced the now-popular *wiretap channel* [2] modeling the simplest scenario involving security with one legitimate transmitter-receiver pair and one wiretapper (eavesdropper) to be kept secret. There is currently a growing interest in information theoretic security, see e.g. [3, 4].

Since spatial multiple-input multiple-output (MIMO) techniques can improve the performance significantly [5], MIMO architectures have been identified as indispensable for future wireless systems. Accordingly, investigation of information theoretic security for MIMO systems is becoming more and more attractive. The secrecy capacity of the MIMO Gaussian wiretap channel is established in [6–9], where it turns out that Gaussian signaling is optimal. Subsequently, the optimal transmit covariance matrix has then been found under the matrix power constraint in [10] and under the total power constraint for a number of special cases [6, 7, 11, 12].

Due to the dynamic nature of the wireless medium, but also due to implementation issues, practical systems always suffer from channel uncertainty and estimation/feedback inaccuracy. Thus, the provision of accurate channel state information (CSI) to the transmitter is a major challenge for wireless communication systems. Along with this, it is hardly possible to expect that the eavesdropper will share its channel with the transmitter to make the eavesdropping harder, which makes the perfect eavesdropper CSI model more than questionable. A reasonable and well-accepted approach is to assume that the exact realization is not known; it is only known that it remains fixed during the whole transmission and that it belongs to a known set of channels, which results in the concept of *compound channels* [13, 14]. The compound wiretap channel is studied in [15, 16] for discrete memoryless and in [15, 17, 18] for MIMO Gaussian channels. The special case where the sets of channels are finite and where further the eavesdropper channel is a degraded version of the legitimate channel is addressed in [15, 17]. Interference alignment for the compound MIMO wiretap channel is presented in [18]. The compound BC with confidential messages is studied in [19].

To accommodate the channel uncertainty issues, we study here the compound MIMO Gaussian wiretap channel model, where the legitimate channel is perfectly known and the eavesdropper channel is not known to the transmitter but is known to have a bounded spectral norm (maximum channel gain), both being fixed during the whole transmission duration. This represents a quasi-static scenario where the eavesdropper cannot approach the transmitter closer than a certain protection distance so that its channel gain is bounded (due to the propagation path loss) but is unconstrained otherwise. This automatically implies only a minimal eavesdropper CSI at the transmitter, which reflects well the natural eavesdropper desire to be confidential. We make no assumptions of degradedness and establish the secrecy capacity of this compound channel.

This is accomplished in two main steps. First, we consider the corresponding discrete memoryless compound wiretap channel in Section II. For this channel model, first results are obtained in [16], but only for the special case of finite uncertainty sets. Built on these results we establish an achievable secrecy rate for this channel for the more general case of bounded but uncountable uncertainty sets. Then, we use this to obtain the corresponding result for MIMO Gaussian channels in Section III. Here, we obtain first the worst-case capacity (i.e. the capacity of the worst-case channel in the set). Then, we establish the saddle-point property of the form $\max\min = \min\max$, where the maximization is over the transmit covariance and minimization is over the eavesdropper channel. Combining the achievable secrecy rate with the saddle-point property, we establish the secrecy capacity of the

compound channel, which equals the worst-case capacity, so that a code designed for the worst-case channel also works over the whole class of channels. The optimal signaling is Gaussian and on the eigenvectors of the legitimate channel, with power allocation somewhat similar but not identical to the regular water-filling. The worst-case eavesdropper is isotropic with the maximum allowed channel gain.

II. Compound Wiretap Channel

Let $\mathcal{X}$ and $\mathcal{Y}$, $\mathcal{Z}$ be finite input and output sets and $\mathcal{S}$, $\mathcal{T}$ be arbitrary but bounded uncertainty sets. Then the communication links to the legitimate receiver and the wiretapper are given by $W_s : \mathcal{X} \times \mathcal{S} \to \mathcal{P}(\mathcal{Y})$, $s \in \mathcal{S}$, and $V_t : \mathcal{X} \times \mathcal{T} \to \mathcal{P}(\mathcal{Z})$, $t \in \mathcal{T}$, respectively, where $\mathcal{P}(\cdot)$ denotes the set of all probability distributions. For fixed $s \in \mathcal{S}$, $t \in \mathcal{T}$, and input and output sequences $x^n \in \mathcal{X}^n$ and $y^n \in \mathcal{Y}^n$, $z^n \in \mathcal{Z}^n$ of block length n, the discrete memoryless channels are given by $W_s^n(y^n|x^n) := \prod_{i=1}^n W_s(y_i|x_i)$ and $V_t^n(z^n|x^n) := \prod_{i=1}^n V_t(z_i|x_i)$.

Definition 1: The discrete memoryless *compound wiretap channel* $\mathfrak{W}$ is given by

$$\mathfrak{W} := \big\{(W_s, V_t) : s \in \mathcal{S}, t \in \mathcal{T}\big\}.$$

Definition 2: An (n, J_n)*-code* $\mathcal{C}_n$ for the compound wiretap channel consists of a stochastic encoder at the transmitter

$$E : \mathcal{J}_n \to \mathcal{P}(\mathcal{X}^n),$$

i.e., a stochastic matrix, with a set of messages $\mathcal{J}_n := \{1, ..., J_n\}$ and a decoder at the legitimate receiver described by a collection of disjoint decoding sets

$$\{\mathcal{D}_j \subset \mathcal{Y}^n : j \in \mathcal{J}_n\big\}.$$

Then for an (n, J_n)-code $\mathcal{C}_n$, the maximum probability of decoding error at the legitimate receiver is given by

$$e_n := \max_{s\in\mathcal{S}} \max_{j\in\mathcal{J}_n} \sum_{x^n\in\mathcal{X}^n} W_s^n(\mathcal{D}_j^c|x^n)E(x^n|j). \tag{1}$$

To keep the transmitted message secret from the non-legitimate eavesdropper for all channel realizations $t \in \mathcal{T}$, we require

$$\max_{t\in\mathcal{T}} \frac{1}{n} I(J; Z_t^n) \le \epsilon_n \tag{2}$$

for some $\epsilon_n > 0$ with J the random variable uniformly distributed over the set of messages $\mathcal{J}_n$ and $Z_t^n = [Z_{t,1}, Z_{t,2}, ..., Z_{t,n}]$ the channel output at the wiretapper for channel realization $t \in \mathcal{T}$.

Definition 3: A non-negative number R_c is an *achievable secrecy rate* if for all $\delta > 0$ there is an $n(\delta) \in \mathbb{N}$ and a sequence of (n, J_n)-codes $\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ such that for all $n \ge n(\delta)$ we have

$$\frac{1}{n} \log J_n \ge R_c - \delta$$

and

$$\max_{t\in\mathcal{T}} \frac{1}{n} I(J; Z_t^n) \le \epsilon_n$$

while $e_n \to 0$ and $\epsilon_n \to 0$ as $n \to \infty$. The *secrecy capacity* C_c of the compound wiretap channel $\mathfrak{W}$ is given by the supremum of all achievable secrecy rates R_c.

A. Finite Compound Wiretap Channel

The discrete memoryless compound wiretap channel for the special case of finite uncertainty sets $\mathcal{S}$ and $\mathcal{T}$ is studied in [15, 16]. In particular, we have the following achievable secrecy rate in [16, Theorem 2].

Theorem 1 ([16]): For the secrecy capacity C_c of the compound wiretap channel $\mathfrak{W}$ we have

$$C_c \ge \max_{P_X\in\mathcal{P}(\mathcal{X})} \big(\min_{s\in\mathcal{S}} I(X; Y_s) - \max_{t\in\mathcal{T}} I(X; Z_t)\big) \tag{3}$$

where the random variables Y_s and Z_t denote the outputs of the corresponding channels W_s and V_t, $s \in \mathcal{S}$, $t \in \mathcal{T}$.

In particular, in [16, Theorem 2] it is shown that the secrecy rate given in (3) with maximum probability of error and secrecy constraint of the form

$$e_n \le |\mathcal{S}|^{1/4} 2^{-n\alpha} \tag{4}$$

and

$$\max_{t\in\mathcal{T}} \frac{1}{n} I(J; Z_t^n) \le 2^{-n\beta}, \tag{5}$$

for some $\alpha, \beta > 0$, i.e., both criteria (1) and (2) decrease *exponentially fast* for increasing block length n. Note that in [16], Equation (5) is given without the division by n, but clearly it also holds with the division. Here, $|\mathcal{S}|$ denotes the cardinality of the set $\mathcal{S}$.

To make this result usable for MIMO Gaussian channels, we have to extend this result in two ways. First, we have to carefully extend it from finite to arbitrary but bounded uncertainty sets. Second, we have to take continuous alphabets and corresponding probability density functions into account. This is done in the following subsections.

B. Arbitrary Bounded Uncertainty Sets

In the following we outline how this result can be extended to the more general case where the uncertainty sets $\mathcal{S}$ and $\mathcal{T}$ may be uncountable but bounded.

To prove the desired result, we adapt the proof idea from Blackwell, Breiman, and Thomasian [13] and approximate an arbitrary, bounded compound wiretap channel by a suitable chosen finite compound wiretap channel. To this end, we need the following lemmas which are slightly adapted from [13].

Lemma 1: Let $\mathcal{X}$ and $\mathcal{Y}$, $\mathcal{Z}$ be given. For every integer $L \ge 2|\mathcal{Y}|^2|\mathcal{Z}|^2$ there is a compound wiretap channel $\mathfrak{W}_L$ with at most $(L+1)^{|\mathcal{X}||\mathcal{Y}||\mathcal{Z}|}$ elements such that for any W_s and V_t from $\mathfrak{W}$ there are channels $\overline{W}_s$ and $\overline{V}_t$ from $\mathfrak{W}_L$ such that

(a) $|W_s(y|x) - \overline{W}_s(y|x)| \le \frac{|\mathcal{Y}||\mathcal{Z}|}{L}$ and $|V_t(z|x) - \overline{V}_t(z|x)| \le \frac{|\mathcal{Y}||\mathcal{Z}|}{L}$ for all x, y, z

(b) $W_s(y|x) \le 2^{\frac{2|\mathcal{Y}|^2|\mathcal{Z}|^2}{L}} \overline{W}_s(y|x)$ and $V_t(z|x) \le 2^{\frac{2|\mathcal{Y}|^2|\mathcal{Z}|^2}{L}} \overline{V}_t(z|x)$ for all x, y, z

(c) For any input distribution $P_X \in \mathcal{P}(\mathcal{X})$, it holds $|I(X; Y_s) - I(X; \overline{Y}_s)| \le 2|\mathcal{Y}||\mathcal{Z}|(\frac{|\mathcal{Y}||\mathcal{Z}|}{L})^{\frac{1}{2}}$ and $|I(X; Z_t) - I(X; \overline{Z}_t)| \le 2|\mathcal{Y}||\mathcal{Z}|(\frac{|\mathcal{Y}||\mathcal{Z}|}{L})^{\frac{1}{2}}$.

Proof: The proof is almost identical to [13, Lemma 4] and is omitted for brevity. ∎

Thus, we can approximate any given compound wiretap channel $\mathfrak{W}$ by a compound wiretap channel $\mathfrak{W}_L$ with finite uncertainty sets $\mathcal{S}$ and $\mathcal{T}$ such that any channel in $\mathfrak{W}$ is close in several senses to one of the new channels in $\mathfrak{W}_L$. The next lemma shows that if there is a "good" code for a channel, then this can be used for all channels in a certain neighborhood.

Lemma 2: Let W_s and $\overline{W}_s$ be two channels and A a non-negative number such that $W_s(y|x) \leq 2^A \overline{W}(y|x)$ for all x, y. Then any (n, J_n)-code for $\overline{W}_s$ is also an (n, J_n)-code for W_s with $e_n \leq 2^{nA} \bar{e}_n$.

Proof: The proof is almost identical to [13, Lemma 5] and is omitted for brevity. ∎

These two lemmas allow us to prove the desired result for an arbitrary compound wiretap channel.

Theorem 2: For the secrecy capacity C_c of the compound wiretap channel $\mathfrak{W}$ we have

$$C_c \geq \max_{P_X \in \mathcal{P}(\mathcal{X})} \big(\inf_{s \in \mathcal{S}} I(X;Y_s) - \sup_{t \in \mathcal{T}} I(X;Z_t) \big) \tag{6}$$

where the sets $\mathcal{S}$ and $\mathcal{T}$ can be arbitrary but bounded.

Proof: The proof is based on the previous Lemmas 1 and 2 and follows the idea of [13].

We start with an approximation of the arbitrary compound wiretap channel $\mathfrak{W}$. To do so, we choose $L \geq \max\{\frac{2|\mathcal{Y}|^2|\mathcal{Z}|^2}{\alpha}, 2|\mathcal{Y}|^2|\mathcal{Z}|^2\}$. For each (W_s, V_t) from $\mathfrak{W}$ we select $(\overline{W}_s, \overline{V}_t)$ according to Lemma 1 and denote the corresponding finite compound wiretap channel by $\mathfrak{W}_L$ and the corresponding uncertainty sets by $\mathcal{S}_L$ and $\mathcal{T}_L$.

Next, we check the reliability part. Since $\mathcal{S}_L$ has at most $(L+1)^{|\mathcal{X}||\mathcal{Y}||\mathcal{Z}|}$ elements, we know from Theorem 1 that if we choose for given input distribution the secrecy rate $R_c \leq \min_{s \in \mathcal{S}} I(X;\overline{Y}_s) - \max_{t \in \mathcal{T}} I(X;\overline{Z}_t) - \tau$, $\tau > 0$, then there exists an (n, J_n)-code for $\mathfrak{W}_L$ with probability of error

$$\bar{e}_n \leq |\mathcal{S}_L|^{1/4} 2^{-n\alpha} \leq (L+1)^{(|\mathcal{X}||\mathcal{Y}||\mathcal{Z}|)/4} 2^{-n\alpha}$$

since $|\mathcal{S}_L| \leq (L+1)^{|\mathcal{X}||\mathcal{Y}||\mathcal{Z}|}$, cf. (4). For each W_s from $\mathfrak{W}$ there is a $\overline{W}_s$ from $\mathfrak{W}_L$ such that $W_s(y|x) \leq 2^{\frac{2|\mathcal{Y}|^2|\mathcal{Z}|^2}{L}} \overline{W}_s(y|x)$ for all x, y. Thus, Lemma 2 implies that the code for $\mathfrak{W}_L$ is also a code for $\mathfrak{W}$ with

$$\begin{aligned} e_n &\leq 2^{n\frac{2|\mathcal{Y}|^2|\mathcal{Z}|^2}{L}} \bar{e}_n \\ &\leq |\mathcal{S}_L|^{1/4} 2^{-n(\alpha - \frac{2|\mathcal{Y}|^2|\mathcal{Z}|^2}{L})} \\ &\leq (L+1)^{(|\mathcal{X}||\mathcal{Y}||\mathcal{Z}|)/4} 2^{-n(\alpha - \frac{2|\mathcal{Y}|^2|\mathcal{Z}|^2}{L})}. \end{aligned} \tag{7}$$

Since $L > \frac{2|\mathcal{Y}|^2|\mathcal{Z}|^2}{\alpha}$, we have $e_n \to 0$ as $n \to \infty$. This means the code constructed for the approximated channel is also a good code for the original channel. It remains to show that this code also achieves the secrecy rate arbitrarily close to the desired rate. From Lemma 1 we know that

$$\begin{aligned} \big| I(X;Y_s) - I(X;Z_t) - \big(I(X;\overline{Y}_s) - I(X;\overline{Z}_t) \big) \big| \\ \leq 4|\mathcal{Y}||\mathcal{Z}| \Big(\frac{|\mathcal{Y}||\mathcal{Z}|}{L} \Big)^{1/2} \end{aligned}$$

so that the difference can be made arbitrarily small by increasing the approximation parameter L. Note that even for increasing approximation parameter L, the probability of error in (7) tends to zero for increasing block length since we have an exponentially fast decreasing behavior.

Finally, we have to check that the secrecy constraint is still satisfied. The code above for the approximated finite compound wiretap channel has $\max_{t \in \mathcal{T}_L} \frac{1}{n} I(X;\overline{Z}_L) \leq 2^{-n\beta}$, cf. Theorem 1 and (5). Again, from Lemma 1 we know that $|I(X;Z_t) - I(X;\overline{Z}_t)| \leq 2|\mathcal{Y}||\mathcal{Z}|(\frac{|\mathcal{Y}||\mathcal{Z}|}{L})^{1/2}$ so that

$$\begin{aligned} \frac{1}{n} I(X;Z_t) &\leq \frac{1}{n} \Big(I(X;\overline{Z}_t) + 2|\mathcal{Y}||\mathcal{Z}|(\frac{|\mathcal{Y}||\mathcal{Z}|}{L})^{1/2} \Big) \\ &\leq \frac{1}{n} \Big(2^{-n\beta} + 2|\mathcal{Y}||\mathcal{Z}|(\frac{|\mathcal{Y}||\mathcal{Z}|}{L})^{1/2} \Big). \end{aligned}$$

Thus, also this difference becomes arbitrarily small for increasing block length n ensuring the secrecy. ∎

Remark 1: We want to highlight that an exponentially fast decreasing behavior as given in (4) and (5) is indispensable to extend the result to non-finite uncertainty sets. In addition, the error due to the approximation can be made as small as desired by further increasing the approximation parameter L.

This shows that the desired result hold also for arbitrary, bounded, but possibly non-finite, compound wiretap channels.

C. Continuous Alphabets

Next we extend Theorem 2 to continuous alphabets $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$. We assume that the random variables can be described by probability density functions and that all mutual information terms are calculated according to continuous alphabets.

Theorem 3: For the secrecy capacity C_c of the compound wiretap channel $\mathfrak{W}$ with continuous alphabets, we have

$$C_c \geq \max_{P_X \in \mathcal{P}(\mathcal{X})} \big(\inf_{s \in \mathcal{S}} I(X;Y_s) - \sup_{t \in \mathcal{T}} I(X;Z_t) \big) \tag{8}$$

where the sets $\mathcal{S}$ and $\mathcal{T}$ can be arbitrary but bounded.

Sketch of Proof: The proof follows the lines of Theorems 1 and 2, cf. also [16]. To extend the result to continuous alphabets and channels, we follow the *discretization procedure* or *partitioning method* as outlined in [20]; see [21] or [22] respectively for a more detailed treatment.

We partition the continuous sets in such a way that we end up with mutually disjoint events which cover the entire space. Then, all mutual information terms are calculated according to this partition. With increasing partitions, these mutual information terms are non-decreasing and, thus, the terms in (6) can be interpreted as the supremum taken over all possible partitions. In more detail, for any $\epsilon_k > 0$ we find for continuous sets $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$, partitions $\{\mathcal{X}_k\}_k^{K_\mathcal{X}}$, $\{\mathcal{Y}_k\}_k^{K_\mathcal{Y}}$, and $\{\mathcal{Z}_k\}_k^{K_\mathcal{Z}}$ with $K_\mathcal{X}$, $K_\mathcal{Y}$, and $K_\mathcal{Z}$ finite such that

$$\begin{aligned} I(X;Y_s) - I(X;Z_t) - \epsilon_k \\ \leq I([X]_k;[Y_s]_k) - I([X]_k;[Z_t]_k) \\ \leq I(X;Y_s) - I(X;Z_t) \end{aligned} \tag{9}$$

where $[X]_k$, $[Y_s]_k$, and $[Z_t]_k$ denote the random variables defined on the partitions $\{\mathcal{X}_k\}_k^{K_\mathcal{X}}$, $\{\mathcal{Y}_k\}_k^{K_\mathcal{Y}}$, and $\{\mathcal{Z}_k\}_k^{K_\mathcal{Z}}$.

Then, the whole encoding and decoding procedure as used in the proofs of Theorems 1 and Theorem 2, cf. also [16],

is done according to this partition. Then, the analysis of probability of error and the analysis of the secrecy criterion for finite alphabets ensures that the rate

$$R_c \leq \max_{P_X \in \mathcal{P}(\mathcal{X})} \left(\inf_{s\in\mathcal{S}} I([X]_k;[Y_s]_k) - \sup_{s\in\mathcal{S}} I([X]_k;[Z_t]_k) \right)$$

are achievable. Since ϵ_k in (9) can be made arbitrarily small, any rate $R_c \leq \max_{P_X\in\mathcal{P}(\mathcal{X})} \left(\inf_{s\in\mathcal{S}} I(X;Y_s) - \sup_{s\in\mathcal{S}} I(X;Z_t) \right)$ is achievable for continuous alphabets as well. Note that as the uncertainty sets are assumed to be bounded, all terms are well defined also for continuous alphabets. ∎

Having established that the achievable secrecy rate (6) holds also for continuous alphabets and corresponding probability density functions, i.e., channels, we are now in the position to evaluate the expressions for MIMO Gaussian channels. This is done in the next section.

III. MIMO Gaussian Channel

Let us now consider the MIMO Gaussian wiretap channel

$$\mathbf{y}_1 = \mathbf{H}_1\mathbf{x} + \boldsymbol{\xi}_1, \quad \mathbf{y}_2 = \mathbf{H}_2\mathbf{x} + \boldsymbol{\xi}_2 \tag{10}$$

where $\mathbf{x} = [x_1, x_2, ..., x_m]^T$ is the transmitted signal of dimension $m \times 1$, $(\cdot)^T$ denotes transposition, $\mathbf{y}_{1(2)}$ are the signals at the legitimate receiver (eavesdropper), $\boldsymbol{\xi}_{1(2)}$ is the circularly-symmetric additive white Gaussian noise at the receiver (eavesdropper) (normalized to unit variance in each dimension), $\mathbf{H}_{1(2)}$ is the $n_{1(2)}\times m$ matrix of the complex channel gains between each Tx and each receive (eavesdropper) antenna, $n_{1(2)}$ and m are the numbers of Rx (eavesdropper) and Tx antennas respectively. The channels $\mathbf{H}_{1(2)}$ are assumed to be fixed (constant).

For this channel, the secrecy capacity subject to the total average transmit power constraint is [6–9]

$$C_s = \max_{\mathbf{R}\geq 0} \ln \frac{|\mathbf{I}+\mathbf{W}_1\mathbf{R}|}{|\mathbf{I}+\mathbf{W}_2\mathbf{R}|} \text{ s.t.} \quad tr\mathbf{R} \leq P_T \tag{11}$$

where P_T is the total transmit power, $\mathbf{R} = E\{\mathbf{x}\mathbf{x}^+\}$ is the transmit covariance matrix, $E\{\cdot\}$ is statistical expectation, $\mathbf{W}_i = \mathbf{H}_i^+\mathbf{H}_i$, $(\cdot)^+$ means Hermitian conjugation, and $|\mathbf{W}|$ is the determinant of $\mathbf{W}$.

It is well-known that the problem in (11) is not convex in general and explicit solutions for the optimal transmit covariance are not known for the general case, but only for some special cases (e.g. low-SNR, MISO channels, or for the full-rank case) [6–9, 11].

Let us now consider a compound MIMO Gaussian wiretap channel where $\mathbf{H}_1$ is given (known to the transmitter) and $\mathbf{H}_2$ can be any (unknown) subject to the spectral norm constraint

$$|\mathbf{H}_2|_2 = \max_{|\mathbf{x}|=1} |\mathbf{H}_2\mathbf{x}| \leq \sqrt{\epsilon} \quad \text{or} \quad |\mathbf{W}_2|_2 = \lambda_1(\mathbf{W}_2) \leq \epsilon \tag{12}$$

where $|\mathbf{x}| = \sqrt{\mathbf{x}^+\mathbf{x}}$ is the Euclidean norm of $\mathbf{x}$. Note that $|\mathbf{H}\mathbf{x}|$ represents the channel (voltage) gain in transmit direction $\mathbf{x}$ so that $|\mathbf{H}|_2$ is the largest channel gain. $|\mathbf{W}|_2$ represents the largest channel power gain. Thus, the set in (12) limits the maximum gain of the eavesdropper channel without putting any constraint on its eigenvectors. This represents the physical scenario where the eavesdropper cannot approach the transmitter beyond a certain minimum (protection) distance (so that the channel gain is bounded due to propagation path loss) being unconstrained otherwise.

The following proposition gives the capacity of the worst-case channel in this set.

Proposition 1: Consider the MIMO Gaussian wiretap channel in (10) when $\mathbf{W}_2$ is any channel from the set in (12). Then, the worst-case secrecy capacity is

$$C_w = \min_{\mathbf{W}_2} \max_{\mathbf{R}} C(\mathbf{R}, \mathbf{W}_2) = C^*(\epsilon) \tag{13}$$

where max and min are subject to the constraints $\mathbf{R}, \mathbf{W}_2 \geq \mathbf{0}$, $tr\mathbf{R} \leq P_T$, $|\mathbf{W}_2|_2 \leq \epsilon$,

$$C(\mathbf{R}, \mathbf{W}_2) = \ln \frac{|\mathbf{I}+\mathbf{W}_1\mathbf{R}|}{|\mathbf{I}+\mathbf{W}_2\mathbf{R}|} \tag{14}$$

and

$$C^*(\epsilon) = \max_{tr\mathbf{R}\leq P_T} C(\mathbf{R}, \epsilon\mathbf{I}) \tag{15}$$

is the secure capacity for the isotropic eavesdropper $\mathbf{W}_{2w} = \epsilon\mathbf{I}$, which is the worst-case eavesdropper.

Proof: Follows from (11) and the facts that $\mathbf{W}_2 \leq \epsilon\mathbf{I}$ under (12) and that $|\mathbf{I}+\mathbf{W}\mathbf{R}|$ is monotonically increasing in $\mathbf{W}$, see e.g. [23]. ∎

It follows from Proposition 1 that the isotropic eavesdropper is the worst-case one under a bounded channel gain. This is also appealing from the channel feedback perspective: it is hardly possible to expect that the eavesdropper will share its channel with the transmitter to make eavesdropping harder, so only minimal information can be expected by the transmitter about the eavesdropper channel.

The expression $C^*(\epsilon)$ has been studied in details in [24].

The following proposition demonstrates the saddle-point property for the class of channels in (12).

Proposition 2: Consider the MIMO Gaussian wiretap channel in (10) for the class of channels in (12) (and fixed $\mathbf{W}_1$). Then the following saddle-point property holds:

$$\max_{\mathbf{R}} \min_{\mathbf{W}_2} C(\mathbf{R}, \mathbf{W}_2) = \min_{\mathbf{W}_2} \max_{\mathbf{R}} C(\mathbf{R}, \mathbf{W}_2) \tag{16}$$

where max and min are subject to the constraints $\mathbf{R}, \mathbf{W}_2 \geq \mathbf{0}$, $tr\mathbf{R} \leq P_T$, $|\mathbf{W}_2|_2 \leq \epsilon$.

Proof: For the max-min part, observe that $C(\mathbf{R}, \mathbf{W}_2) \geq C(\mathbf{R}, \epsilon\mathbf{I})$ (which follows from the proof of Proposition 1), so by taking max-min of both parts, one obtains

$$\max_{\mathbf{R}} \min_{\mathbf{W}_2} C(\mathbf{R}, \mathbf{W}_2) \geq \max_{\mathbf{R}} C(\mathbf{R}, \epsilon\mathbf{I}). \tag{17}$$

On the other hand, by using $\mathbf{W}_2 = \epsilon\mathbf{I}$ instead of min, one obtains

$$\max_{\mathbf{R}} \min_{\mathbf{W}_2} C(\mathbf{R}, \mathbf{W}_2) \leq \max_{\mathbf{R}} C(\mathbf{R}, \epsilon\mathbf{I}) \tag{18}$$

so that

$$\begin{aligned} \max_{\mathbf{R}} \min_{\mathbf{W}_2} C(\mathbf{R}, \mathbf{W}_2) &= \max_{\mathbf{R}} C(\mathbf{R}, \epsilon\mathbf{I}) \\ &= \min_{\mathbf{W}_2} \max_{\mathbf{R}} C(\mathbf{R}, \mathbf{W}_2). \end{aligned} \tag{19}$$

This proves the desired saddle-point property. ∎

The saddle-point property above is instrumental in establishing the secrecy capacity of the compound MIMO Gaussian wiretap channel in (10) and (12) as the following result shows.

Theorem 4: Consider the compound MIMO Gaussian wiretap channel in (10), (12) (i.e. $\mathbf{W}_1$ is known while $\mathbf{W}_2$ is unknown to the transmitter but is known to belong to the class in (12)). The secrecy capacity C_c of this compound channel is as follows:

$$\begin{aligned} C_c &= \max_{\mathbf{R}} \min_{\mathbf{W}_2} C(\mathbf{R}, \mathbf{W}_2) \\ &= \min_{\mathbf{W}_2} \max_{\mathbf{R}} C(\mathbf{R}, \mathbf{W}_2) \\ &= C^*(\epsilon), \end{aligned} \tag{20}$$

i.e., the capacity of the worst-case channel is also the (compound) capacity of the class of channels (achievable by a single code on the whole class). The worst-case channel is that of the isotropic eavesdropper with the maximum allowed gain. The optimal signaling is on the eigenmodes of the legitimate channel,

$$\mathbf{R}^* = \mathbf{U}_1 \mathbf{\Lambda}^* \mathbf{U}_1^+, \tag{21}$$

where the columns of unitary matrix $\mathbf{U}_1$ are the eigenvectors of $\mathbf{W}_1$, diagonal matrix $\mathbf{\Lambda} = diag\{\lambda_i^*\}$ collects the eigenvalues of $\mathbf{R}^*$,

$$\lambda_i^* = \frac{\epsilon + g_i}{2\epsilon g_i} \left(\sqrt{1 + \frac{4\epsilon g_i}{(\epsilon + g_i)^2} \left(\frac{g_i - \epsilon}{\lambda} - 1 \right)_+} - 1 \right) \tag{22}$$

and $\lambda > 0$ is found from the total power constraint $\sum_i \lambda_i^* = P_T$, $g_i = \lambda_i(\mathbf{W}_1)$, $(x)_+ = \max\{x, 0\}$.

Proof: Note first that

$$C_c \leq \min_{\mathbf{W}_2} \max_{\mathbf{R}} C(\mathbf{R}, \mathbf{W}_2), \tag{23}$$

i.e., the compound capacity cannot exceed the worst-case capacity in the class. On the other hand, it follows from Theorem 3 by evaluating (8) for MIMO Gaussian channels as given in (10) that

$$C_c \geq \max_{\mathbf{R}} \min_{\mathbf{W}_2} C(\mathbf{R}, \mathbf{W}_2) \tag{24}$$

$$= \min_{\mathbf{W}_2} \max_{\mathbf{R}} C(\mathbf{R}, \mathbf{W}_2) \tag{25}$$

where the equality is from Proposition 2. Combining the lower and upper bounds, (20) follows. The optimal signaling and $C^*(\epsilon)$ are as in [24]. ∎

Note that the optimal signaling directions that achieve the compound capacity are the same as those for the regular MIMO channel (no eavesdropper) but the power allocation is somewhat different from the regular water-filling, even though it shares many of its properties (see [24] for details).

IV. Conclusion

We established the secrecy capacity of the compound MIMO Gaussian wiretap channel, where the channel to the legitimate receiver is known and the eavesdropper channel is not known but is known to have a bounded spectral norm. This is in particular practically relevant, since it corresponds to the realistic scenario, where only minimal CSI about the eavesdropper is available. It is only known that the eavesdropper's channel gain does not exceed a certain value corresponding to the scenario that the eavesdropper cannot approach the transmitter beyond a certain minimum protection distance.

References

[1] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, p. 656715, Oct. 1949.

[2] A. D. Wyner, "The Wire-Tap Channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[3] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information Theoretic Security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, 2009.

[4] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[5] E. Biglieri, R. Calderbank, A. Constantinides, A. Goldsmith, A. Paulraj, and H. V. Poor, *MIMO Wireless Communications*. Cambridge University Press, 2007.

[6] A. Khisti and G. W. Wornell, "Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[7] ——, "Secure Transmission With Multiple Antennas–Part II: The MIMOME Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[8] F. Oggier and B. Hassibi, "The Secrecy Capacity of the MIMO Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[9] T. Liu and S. Shamai (Shitz), "A Note on the Secrecy Capacity of the Multiple-Antenna Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[10] R. Bustin, R. Liu, H. V. Poor, and S. Shamai (Shitz), "An MMSE Approach to the Secrecy Capacity of the MIMO Gaussian Wiretap Channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Seoul, Korea, Jun. 2009, pp. 2602–2606.

[11] S. Loyka and C. D. Charalambous, "On Optimal Signaling over Secure MIMO Channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Boston, MA, USA, Jul. 2012, pp. 443–447.

[12] J. Li and A. Petropulu, "Transmitter Optimization for Achieving Secrecy Capacity in Gaussian MIMO Wiretap Channels," *submitted to Trans. Inf. Theory*, Sep. 2009, available at http://arxiv.org/abs/0909.2622v1.

[13] D. Blackwell, L. Breiman, and A. J. Thomasian, "The Capacity of a Class of Channels," *Ann. Math. Stat.*, vol. 30, no. 4, pp. 1229–1241, Dec. 1959.

[14] J. Wolfowitz, "Simultaneous Channels," *Arch. Rational Mech. Analysis*, vol. 4, no. 4, pp. 371–386, 1960.

[15] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound Wiretap Channels," *EURASIP J. Wireless Commun. Netw.*, vol. Article ID 142374, pp. 1–13, 2009.

[16] ——, "Secrecy Results for Compound Wiretap Channels," *Probl. Inf. Transmission*, vol. 49, no. 1, pp. 73–98, Mar. 2013.

[17] E. Ekrem and S. Ulukus, "On Gaussian MIMO Compound Wiretap Channels," in *Proc. Conf. Inf. Sciences and Systems*, Baltimore, MD, USA, Mar. 2010, pp. 1–6.

[18] A. Khisti, "Interference Alignment for the Multiantenna Compound Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2976–2993, May 2011.

[19] R. F. Wyrembelski and H. Boche, "Strong Secrecy in Compound Broadcast Channels with Confidential Messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Boston, MA, USA, Jul. 2012, pp. 76–80.

[20] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge University Press, 2011.

[21] R. M. Gray, *Entropy and Information Theory*. Springer, 1990.

[22] R. G. Gallager, *Information Theory and Reliable Communication*. Wiley & Sons, 1968.

[23] F. Zhang, *Matrix Theory: Basic Results and Techniques*. Springer, 1999.

[24] S. Loyka and C. D. Charalambous, "On Optimal Signaling over Secure MIMO Channels," *IEEE Trans. Inf. Theory*, Dec. 2012, submitted.