ABSTRACT

We consider a multiple-input multiple-output (MIMO) Gaussian wiretap channel model, where there exists a transmitter, a legitimate receiver and an eavesdropper, each node equipped with multiple antennas. We study the problem of finding the optimal input covariance that achieves secrecy capacity subject to a power constraint, which in general leads to a difficult non-convex optimization problem. For the Gaussian multiple-input single-output (MISO) wiretap channel where there exists a transmitter equipped with multiple antennas, a legitimate receiver and an eavesdropper each equipped with one antenna, the optimal input covariance is obtained in closed form. For the general case, we derive the necessary conditions for the optimal input covariance in the form of a set of equations. We show that for MISO case, the derived conditions guarantee the optimal input covariance. Numerical results are presented to illustrate the proposed theoretical findings.

Index Terms— Physical layer based security, secrecy capacity, Gaussian MIMO wiretap channel.

1. INTRODUCTION

Wireless physical (PHY) layer based security from an information theoretic point of view has received considerable attention recently [1]. Wireless PHY layer based security approaches exploit the physical characteristics of the wireless channel to enhance the security of communication systems. The wiretap channel, first introduced and studied by Wyner [2], is the most basic physical layer model that captures the problem of communication security. Wyner showed that when an eavesdropper’s channel is a degraded version of the main channel, the source and destination can achieve a positive secrecy rate. The maximum secrecy rate from the source to the destination is defined as the secrecy capacity. The Gaussian wiretap channel, in which the outputs at the legitimate receiver and at the eavesdropper are respectively given by

\[ y_R = H_R x + n_R, \quad y_E = H_E x + n_E \]  

(1)

where \( H_R, H_E \) are respectively channel matrices between the transmitter and legitimate receiver, and between the transmitter and eavesdropper; \( x \sim \mathcal{CN}(0, R_x) \) is the input vector; \( n_R \) and \( n_E \) are circular Gaussian noise vectors with zero mean and covariance matrices \( R_R \) and \( R_E \), respectively. \( y_R \) and \( y_E \) are the observed signals at the legitimate receiver and eavesdropper, respectively. The received signals at the legitimate receiver and the eavesdropper are respectively given by

MIMO wiretap channel subject to power constraints was established in terms of an optimization problem over all possible input covariances in [4], [5]. An alternative expression of secrecy capacity for another type of Gaussian MIMO wiretap channel subject to power covariance constraint was derived in closed form rather than as a solution to an optimization problem in [6], [7].

For the Gaussian MIMO wiretap channel model in [5], finding the optimal input covariance that achieves secrecy capacity subject to power constraint leads to a non-convex optimization problem which is in general difficult to solve. The solution of a special case in which the transmitter and the legitimate receiver have two antennas and the eavesdropper has one antenna was given in [8].

In this paper, we investigate the aforementioned non-convex optimization problem. In particular, for the Gaussian multiple-input single-output (MISO) wiretap channel where there exists a transmitter equipped with multiple antennas, a legitimate receiver and an eavesdropper each equipped with a single antenna, we obtain the optimal input covariance in closed form. For the general MIMO case, we derive the necessary conditions for the optimal solution consisting of a set of equations. We also show that for the MISO case, the derived conditions guarantee the optimal solution consisting of a set of equations.

For more detailed results please refer to [9]. The proposed secrecy capacity results are different from those of [6], [7] as we here consider a power constraint instead of the power covariance constraint used in [6], [7].

2. SYSTEM MODEL AND FORMULATIONS

Consider a Gaussian MIMO wiretap channel where the transmitter is equipped with \( n_T \) antennas, while the legitimate receiver and an eavesdropper have \( n_R \) and \( n_E \) antennas, respectively. The received signals at the legitimate receiver and the eavesdropper are respectively given by

\[ y_R = H_R x + n_R, \quad y_E = H_E x + n_E \]  

(1)
mean and covariances $\sigma^2 I_n R$ and $\sigma^2 I_n E$, respectively. We assume the channel matrices $H_R$ and $H_E$ have been normalized so that $\text{Tr}(H_E H_R^\dagger) = nP$ and the power constraint is $P$, namely, $\text{Tr}(R_x) = P$. We represent $R_x$ in terms of $P$ and the normalized input covariance $Q$, so that $R_x = PQ$ and $\text{Tr}(Q) = 1$. We denote the signal-to-noise ratio (SNR) as $\rho \triangleq P/\sigma^2$. We assume that global channel state information (CSI) is available, including the eavesdroppers’ channels. This corresponds to the cases where the eavesdroppers are active in the network and their transmissions can be monitored [11].

The secrecy capacity is defined as [5]

$$C_s \triangleq \max_{Q \geq 0, \text{Tr}(Q) = 1} C_s(Q) \tag{2}$$

where $C_s(Q) = \log \det(I_{nR} + \rho H_R Q H_R^\dagger) - \log \det(I_{nE} + \rho H_E Q H_E^\dagger)$ is the secrecy rate.

The transmitter optimization problem is to determine the optimal $Q$ that maximizes the secrecy rate, i.e., achieves secrecy capacity. We denote the feasible set of (2) as $\Omega = \{Q|Q \succeq 0, \text{Tr}(Q) = 1\}$ which is a convex set.

3. CLOSED FORM SECRECY CAPACITY OF THE GAUSSIAN MISO WIRETAP CHANNEL

We first provide a lemma that will be used later.

**Lemma 1** Let $r$ and $s$ be two known non-zero vectors.

(i) If $r = \xi s$ for a certain scalar $\xi$, $r r^\dagger - s s^\dagger$ has only one nonzero eigenvalue equal to $(|\xi|^2 - 1)|s|^2$ with the associated eigenvector $s/|s|$.

(ii) If $r^\dagger s = 0$, $r r^\dagger - s s^\dagger$ has only two nonzero eigenvalues $\eta_1 = |r|^2 s/|s|$, $\eta_2 = -|s|^2 r/|r|$, with associated eigenvectors $r/|r|$, $s/|s|$, respectively.

(iii) If neither $r = \xi s$ nor $r^\dagger s = 0$, $r r^\dagger - s s^\dagger$ has only two nonzero eigenvalues $\eta_1 = |r|^2 - c_4 |r|^2 s/|s|^2 > 0$, $\eta_2 = c_1 |r|^2 - c_4 |r|^2 < 0$ with the associated eigenvectors $e_1 = c_1^{1/2} (r + c_2 e^{i(\pi - \varphi)} s)/c_2$, $e_2 = c_3^{1/2} (r + c_4 e^{i(\pi - \varphi)} s)/c_2$, where $c_1 = |r|^2 + c_2^2 |s|^2 - c_4 |r|^2 |s|^2$, $c_2 = (|r|^2 + |s|^2 - \sqrt{(|r|^2 + |s|^2)^2 - 4 |r|^2 |s|^2})/2 |r|^2 s^2)$, $c_3 = |r|^2 + c_4 |s|^2 > 2 c_4 |r|^2 s/|s|^2$, $c_4 = (|r|^2 + |s|^2 + \sqrt{(|r|^2 + |s|^2)^2 - 4 |r|^2 |s|^2})/2 |r|^2 s^2)$.

The proof is simple, therefore, omitted for the sake of brevity.

Since in this section we analyze the Gaussian MISO wiretap channel, the channel matrices become vectors, denoted by $h_R$ and $h_E$.

**Theorem 1** The secrecy capacity of Gaussian MISO wiretap channel equals

$$C_s = \log \frac{b + \sqrt{b^2 - 4ac}}{2a} \tag{3}$$

where $a = 1 + \rho \|h_E\|^2$, $b = 2 + \rho \|h_R\|^2 + \rho \|h_E\|^2 + \rho^2 (\|h_R\|^2 \|h_E\|^2 - \|h_R h_E\|^2)$ and $c = 1 + \rho \|h_R\|^2$.

**Proof:** The secrecy rate maximization problem can be written as

$$\max_{Q \in \Omega} \log[(1 + \rho h_R^\dagger Q h_R)/(1 + \rho h_E^\dagger Q h_E)] \tag{4}$$

which is a fractional program associated with the following parametric problem [14]

$$F(\alpha) = \max_{Q \in \Omega} [1 + \rho (h_R Q h_R - \alpha h_E h_E^\dagger)] \tag{5}$$

where $\alpha > 0$. Let $\alpha^0$ be the unique root of $F(\alpha)$, according to [14], the optimal $Q$ corresponding to $F(\alpha^0)$ also optimizes (4). Based on the fact that $h^\dagger Q h = \text{Tr}(Q h h^\dagger)$ for any vector $h$, we rewrite the optimization problem (5) as

$$F(\alpha) = \max_{Q \in \Omega} [1 - \alpha + \rho \text{Tr}(Q (h_R h_R - \alpha h_E h_E^\dagger))]. \tag{6}$$

By eigen-decomposition $h_R h_R^\dagger - \alpha h_E h_E^\dagger = U_a D_a U_a^\dagger$ and letting $Q_a = U_a^\dagger Q U_a$, we know that $Q_a \in \Omega$. It holds

$$\text{Tr}(Q (h_R h_R^\dagger - \alpha h_E h_E^\dagger)) = \text{Tr}(Q_a D_a) \leq \lambda_{\max}(h_R h_R^\dagger - \alpha h_E h_E^\dagger) \tag{7}$$

Equation (7) holds with equality if $Q_a$ is diagonal and has a unique nonzero entry (equal to one) corresponding to the position of the largest entry in $D_a$. In other words, $Q$ and $h_R h_R^\dagger - \alpha h_E h_E^\dagger$ have the same eigenvectors, and $Q$ has rank one. Thus, it holds $Q = u_{a,\max} u_{a,\max}^\dagger$ where $u_{a,\max}$ is the eigenvector associated with the largest eigenvalue of $h_R h_R^\dagger - \alpha h_E h_E^\dagger$. The largest eigenvalue and the associated eigenvector of $h_R h_R^\dagger - \alpha h_E h_E^\dagger$ can be expressed in closed form based on Lemma 1. In our problem, $r = h_R$, $s = \sqrt{\alpha} h_E$. By using Lemma 1, we obtain

$$F(\alpha) = 1 + (\rho/2) \|h_E\|^2 - [1 + (\rho/2) \|h_E\|^2] \alpha + \frac{\rho}{2} \sqrt{(\|h_R\|^2 + \alpha \|h_E\|^2)^2 - 4 \alpha \|h_R h_E\|^2}. \tag{8}$$

$F(\alpha) = 0$ has a unique root $\alpha^0 = (b + \sqrt{b^2 - 4ac})/(2a)$, thus, the secrecy capacity is given by $C_s = \log \alpha^0$.

Based on Theorem 1, if $h_R = \xi h_E$ and $|\xi| < 1$, then $b = a + c$, $a - c > 0$ and further $C_s = 0$. If $h_R = \xi h_E$ and $|\xi| > 1$, then $b = a + c$, $a - c < 0$ and $C_s = \log((1 + \rho |\xi|^2 \|h_E\|^2)/(1 + \rho \|h_E\|^2)) > 0$. This is consistent with the fact that when the eavesdropper channel is a degraded version of the legitimate receiver channel the secrecy capacity is positive. If $h_R \neq \xi h_E$, then $b > a + c$ and it always holds that $C_s > 0$. Thus, if $h_R \neq \xi h_E$, the Gaussian MISO wiretap channel always has positive secrecy capacity independent of the channel.

To gain more insight into the secrecy capacity, we consider the rate at which the secrecy capacity scales with $\log \rho$.
as in [10]. If \( h_R \neq \xi h_E \), then under high SNR, it follows from (3) that
\[
C_s(\rho) = \log \rho + \log(\|h_R\|^2 - |h_R^\dagger h_E|^2/\|h_E\|^2 + O(1/\rho))
\]
where \( O(\cdot) \) is the big-O notation. The secrecy degree of freedom (s.d.o.f.) of the Gaussian MISO wiretap channel is
\[
s.d.o.f \triangleq \lim_{\rho \to \infty} \frac{C_s(\rho)}{\log \rho} = 1. \quad (10)
\]

Before ending this section, we discuss the properties when the channel gain by expressing \( h_E = \beta h_{E,0} \) where \( h_{E,0} \) is a fixed vector and \( \beta \) varies from 0 to \( \infty \). From Theorem 1, when \( \beta \to 0 \), \( C_s \to \log(1 + \rho \|h_R\|^2) \); when \( \beta \to \infty \), \( C_s \to \log(1 + \rho (\|h_R\|^2 - |h_R^\dagger h_E|^2/\|h_E\|^2)^2)). \)

4. CONDITIONS FOR OPTIMAL INPUT COVARIANCE OF THE GAUSSIAN MIMO WIRETAP CHANNEL

In this section, we analyze a general Gaussian MIMO wiretap channel. First, we obtain the necessary conditions for the optimal \( Q \) by using Karush-Kuhn-Tucker (KKT) conditions. Let us construct the cost function
\[
L(\Theta, Q, \Psi) = C_s(Q) - \theta(\text{Tr}(Q) - 1) + \text{Tr}(\Psi Q) \quad (11)
\]
where \( \theta \) is the Lagrange multiplier associated with the constraint \( \text{Tr}(Q) = 1 \), \( \Psi \) is the Lagrange multiplier associated with the constraint \( Q \succeq 0 \). The KKT conditions enable us to write [15]
\[
\Theta - \theta I_{n_t} + \Psi = 0, \quad (12)
\]
\[
\Psi \succeq 0, \text{Tr}(\Psi Q) = 0, Q \succeq 0, \text{Tr}(Q) = 1, \quad (13)
\]
where
\[
\Theta = \rho H_R^\dagger(I_{n_t} + \rho H_R Q H_R^\dagger)^{-1}H_R^\dagger - \rho H_E^\dagger(I_{n_t} + \rho H_E Q H_E^\dagger)^{-1}H_E. \quad (14)
\]

Here we use the facts: \( \frac{\partial}{\partial Q} \text{Tr}(\Psi Q) = \Psi^T \) and
\[
\frac{\partial \log \det(I + \rho H Q H^\dagger)}{\partial Q} = [\rho H^\dagger(I + \rho H Q H^\dagger)^{-1}H^\dagger]. \quad (15)
\]

\( \Theta \) is an important variable for the transmitter optimization problem. From the KKT conditions (12) and (13), we obtain the equivalent (but without containing the Lagrange multipliers) conditions for optimal \( Q \) consisting of a set of equations given in the following theorem.

**Theorem 2** The optimal \( Q \succeq 0 \) satisfies
\[
\Theta = \text{Tr}(Q \Theta) \quad (16)
\]
\[
\lambda_{\max}(\Theta) = \text{Tr}(Q \Theta), \quad (17)
\]

**Proof:** It follows from (13) that \( \Psi Q = Q \Psi = 0 \), that is, \( \Psi \) and \( Q \) commute and have the same eigenvectors [16, p.239] and their eigenvalue patterns are complementary in the sense that if \( \lambda_i(Q) > 0 \), then \( \lambda_i(\Psi) = 0 \), and vice versa [12].

This result, when combined with (12), implies that \( \Theta \) and \( Q \) commute and have the same eigenvectors, i.e., they have the eigen-decompositions \( Q = U_q D_q U_q^\dagger \) and \( \Theta = U_q D_q U_q^\dagger \).

Further, we get \( \Theta = Q \Theta = \theta \Theta \), which, when combined with \( \text{Tr}(\Theta) = 1 \) and the fact \( \text{Tr}(\Theta Q) = \text{Tr}(Q^{1/2} \Theta Q^{1/2}) \) is always real, leads to \( \theta = \text{Tr}(Q \Theta) \) and (16) (also see [13]).

The condition (16) reveals that for the optimal \( Q \), \( Q \Theta \) is a scaled version of \( Q \). Further the eigenvalues of \( \Theta \) corresponding to the positive eigenvalues of \( Q \) are all equal to \( \text{Tr}(Q \Theta) \), while the remaining eigenvalues of \( \Theta \) are all less than or equal to \( \text{Tr}(Q \Theta) \), which follows from (12), (16) and \( \Psi \succeq 0 \). Based on the above, it holds the second condition (17). Here we complete the proof.

Equations (16) and (17) provide two elementary conditions that characterize the optimal \( Q \). At this point we do not have a proof that any \( Q \) satisfying the conditions of Theorem 2 is the optimal input covariance. However, for some special cases, e.g., the Gaussian MISO wiretap channel analyzed in §3, this is true. In particular, for this case we provide the following theorem.

**Theorem 3** For Gaussian MISO wiretap channel, any \( Q \) satisfying the conditions of Theorem 2 is the optimal input covariance.

**Proof:** By using the matrix inverse formula for two vectors \( x \) and \( y \): \((I + xy^T)^{-1} = I - xy^T/(1 + y^T x)\), we write
\[
\Theta = \frac{\rho h_R h_R^\dagger}{1 + \rho h_R^\dagger Q h_R} - \frac{\rho h_E h_E^\dagger}{1 + \rho h_E^\dagger Q h_E}. \quad (18)
\]

That is to say, \( \Theta \) has the form of \( \alpha_1 h_R h_R^\dagger - \alpha_2 h_E h_E^\dagger \), \( \alpha_1 > 0, \alpha_2 > 0 \). According to Lemma 1, we know that: if \( h_R = \xi h_E \), then \( \Theta \) has only one nonzero eigenvalue; if \( h_R \neq \xi h_E \), then \( \Theta \) has only two nonzero eigenvalues, one is positive and the other is negative. With these, since \( Q \) satisfies (16) and (17), it is easy to verify \( Q \) has rank one (also see the proof of Theorem 2). Let \( Q = uu^T \) and we have
\[
\Theta = \frac{\rho h_R h_R^\dagger}{1 + \rho h_R^\dagger uu^T h_R} - \frac{\rho h_E h_E^\dagger}{1 + \rho h_E^\dagger uu^T h_E}. \quad (19)
\]
\[
\text{Tr}(Q \Theta) = \frac{1}{1 + \rho h_R^\dagger uu^T h_R} - \frac{1}{1 + \rho h_E^\dagger uu^T h_E}. \quad (20)
\]

Let \( \omega_1 = 1 + \rho h_R^\dagger uu^T h_R, \omega_2 = 1 + \rho h_E^\dagger uu^T h_E \). According to Lemma 1, the largest eigenvalue of \( \Theta \) is given by
\[
\lambda_{\max}(\Theta) = \frac{\rho |h_R|^2}{2\omega_1} - \frac{\rho |h_E|^2}{2\omega_2} + \frac{1}{2} \sqrt{\left(\frac{\rho |h_R|^2}{\omega_1} + \frac{\rho |h_E|^2}{\omega_2}\right)^2 - 4\rho^2 |h_R|^2 |h_E|^2}. \quad (21)
\]
Since $Q$ satisfies (17), it follows from (20) and (21) that
\[
1 + (\rho/2)\|h_R\|^2 - \left[ (1 + (\rho/2)\|h_E\|^2) (\omega_1/\omega_2) + \frac{\rho}{2} \sqrt{(\|h_R\|^2 + \|h_E\|^2\omega_1/\omega_2)^2 - 4(h_R^* h_E)^2 \omega_1/\omega_2} \right] = 0.
\]
(22)
This equation (22) is exactly (8), i.e., $F(\alpha) = 0$ where $\alpha = \omega_1/\omega_2$. On the other hand, we know
\[
\omega_1/\omega_2 = \frac{(1 + \rho h_R^* uu^* h_R)/(1 + \rho h_E^* uu^* h_E)}{(1 + (\rho/2)\|h_E\|^2) (\omega_1/\omega_2) + \frac{\rho}{2} \sqrt{(\|h_R\|^2 + \|h_E\|^2\omega_1/\omega_2)^2 - 4(h_R^* h_E)^2 \omega_1/\omega_2}}.
\]
(23)
According to the result in §3, the root of $F(\alpha) = 0$ corresponds to the maximization of the right hand side (RHS) of (23) (see also (4)). Thus, the conditions of Theorem 2 guarantee the optimal input covariance.

The further study of the Theorem 2 will be our future work.

5. NUMERICAL SIMULATIONS

For illustration purposes, we consider a Gaussian MISO wiretap channel where $n_T = 4$, $n_R = 1$, $n_F = 1$. We set the channels gain vectors $h_R = [-1.37 + 0.32i, -0.04 + 1.07i, -0.64 + 0.37i, 0.39 - 0.41i]^T$, $h_E = G[0.24 + 0.00i, -0.64 - 0.20i, -0.01 + 0.69i, -0.03 - 1.19i]^T$, where $G$ is a constant for simulation purposes.

Fig. 1 depicts the secrecy capacity for $G = 1$ under different SNRs. It can be seen from Fig. 1 that for high SNR, the secrecy capacity varies linearly with $\log(\rho)$. Fig. 2 plots the secrecy capacity for $G$ varying from 0 to 10, where SNR = 10 dB. It can be seen from Fig. 2 that the secrecy capacity is positive even when the $\|h_E\|^2$ is much larger than $\|h_R\|^2$.

6. CONCLUSION

We have investigated the problem of finding the optimal input covariance that achieves secrecy capacity of the Gaussian MIMO wiretap channel subject to a power constraint. In particular, for the Gaussian MISO wiretap channel, the optimal input covariance is obtained in closed form. For general cases, we derive the necessary conditions for the optimal solution consisting of a set of equations. We also show that for MISO case, the derived conditions guarantee the optimal input covariance.

7. REFERENCES