Closed Form Secrecy Capacity of MIMO Wiretap Channels with Two Transmit Antennas

Jiangyuan Li and Athina Petropulu
Department of Electrical and Computer Engineering
Rutgers-The State University of New Jersey, New Brunswick, NJ 08854

Abstract—A Gaussian multiple-input multiple-output (MIMO) wiretap channel model is considered. The input is a two-antenna transmitter, while the outputs are the legitimate receiver and an eavesdropper, both equipped with multiple antennas. All channels are assumed to be known. The problem of obtaining the optimal input covariance matrix that achieves secrecy capacity subject to a power constraint is addressed, and a closed-form expression for the secrecy capacity is obtained.

Index Terms—Secrecy capacity, MIMO wiretap channel, physical layer security

I. INTRODUCTION

Wireless physical layer based security approaches present an alternative to cryptographic approaches. They enhance the security of a communication system by exploiting the physical characteristics of the wireless channel. Wyner identified the secrecy capacity of the single user memoryless wiretap channel [1]. Later, the Gaussian scalar wiretap channel was studied in [2]. More recently, the secrecy capacity of the MIMO wiretap channel under power constraints was analyzed in [3] and [4], while the same problem under power-covariance constraints was studied in [5] and [6]. In [7], the case (nT, nR, nE) = (2, 2, 1) (two transmit antennas, two receive antennas and one eavesdropper antenna) was analyzed, and it was shown that under certain assumptions on the channels, beamforming is optimal. In [8], the (2, 2, 2) case was studied under equality power constraint and the positive definiteness assumption HsHs′ ⪰ 0. However, the solution was not given, and moreover, it does not show that equality power constraint is equivalent to the more common inequality power constraint.

In this letter, we study the secrecy capacity for a MIMO wiretap channel with two transmit antennas and an arbitrary number of receive and eavesdropper antennas. The main result is a closed form expression for the capacity, that is obtained based on the roots of a quadratic and a quartic equation.

Notation - Upper case and lower case bold symbols denote matrices and vectors, respectively. Superscripts *, † and T denote respectively conjugate, transposition and conjugate transposition. det(A) and Tr(A) denote the determinant and trace of the matrix A, respectively. λmax(A) denotes the largest eigenvalue of the matrix A. A ⪰ 0 denotes that the matrix A is Hermitian positive semi-definite, and A ⪰ 0 denotes that the matrix A is Hermitian positive definite. |a| denotes the absolute value of the complex number a. I_n denotes the identity matrix of order n (the subscript is dropped when the dimension is obvious).

II. SYSTEM MODEL AND PROBLEM STATEMENT

Consider a MIMO wiretap channel, where the transmitter is equipped with nT = 2 antennas, while the legitimate receiver and an eavesdropper have nR and nE antennas, respectively. The received signals at the legitimate receiver and the eavesdropper are respectively given by

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

where \( H_R \) (nR × 2), \( H_E \) (nE × 2) are respectively matrices representing the channel between transmitter and legitimate receiver, and transmitter and eavesdropper; x is the 2 × 1 transmitted signal vector with zero mean and 2 × 2 covariance matrix \( P \), where \( P \) is the power constraint, \( Q \succeq 0 \) and \( Tr(Q) \leq 1 \); nR and nE are Gaussian noise vectors with zero mean and covariance matrices \( \sigma^2 I_{nR} \) and \( \sigma^2 I_{nE} \), respectively. We consider the scenario in which the transmitter has perfect channel state information (CSI) on \( H_R \) and \( H_E \).

The secrecy capacity for this scenario is

\[ C_s \triangleq \max_{Q \succeq 0, \ Tr(Q) \leq 1} C_s(Q) \]

where \( C_s(Q) = \log \det(I + QS_R) - \log \det(I + QS_E) \) and \( S_R = \rho H_R^H H_R, \ S_E = \rho H_E^H H_E, \ \rho = P/\sigma^2 \).

Lemma 1: The sufficient and necessary condition for \( C_s > 0 \) is that \( H_R^H H_R - H_E^H H_E \) has at least a positive eigenvalue. The proof is simple. Please refer to [9] Lemma 1 for details.

In this paper, we assume that the condition in Lemma 1 holds which ensures \( C_s > 0 \) and hence \( Q^* \neq 0 \).

III. CLOSED FORM SECRECY CAPACITY

The main result of this paper is contained in Theorem 1

Theorem 1: Let \( \tau_1 \) be the largest real root (if any) of the quadratic equation

\[ -\tau_1^2 q_4 + \tau_1 p_3 - q_6 = 0. \]

Let \( \tau_2 \) be the largest real root (if any) of the quartic equation

\[ (-\tau_2^2 q_2 + \tau_2 p_2 - q_5)^2 - 4(-\tau_2^2 q_1 + \tau_2 p_1 - q_4)(-\tau_2^2 q_4 + \tau_2 p_3 - q_6) = 0 \]

such that

\[ 0 < -\tau_2^2 q_2 + \tau_2 p_2 - q_5 < \frac{2(-\tau_2^2 q_1 + \tau_2 p_1 - q_4)}{(-\tau_2^2 q_1 + \tau_2 p_1 - q_4)} < 1. \]
Then the secrecy capacity equals
\[ C_s = \log (\max\{\tau_1, \tau_2\}). \]  
(6)

The coefficients \( \{p_i\}, \{q_j\} \) are given by
\[
\begin{align*}
p_1 &= -b_1^2 b_2 - b_1 b_2^* - (1 + a_1)(a_2 c_2 - |b_2|^2) \\
&\quad - (1 + a_2)(a_1 c_1 - |b_1|^2), \\
p_2 &= 2b_1^* b_2 + 2b_2^* b_1 + (1 + a_1)(a_2 - c_2 + a_2 c_2 - |b_2|^2) \\
&\quad + (1 + a_2)(a_1 - c_1 + a_1 c_1 - |b_1|^2), \\
p_3 &= (1 + a_1)(1 + c_2) + (1 + a_2)(1 + c_1) - b_1^* b_2 - b_1 b_2^*, \\
p_1 &= -a_2 c_2 + a_2 c_2 - |b_2|^2, \\
q_1 &= a_2 c_2 + a_2 c_2 - |b_2|^2, \\
q_2 &= a_1 c_1 + a_1 c_1 - |b_1|^2, \\
q_3 &= 1 + a_2 c_2 + a_2 c_2 - |b_2|^2, \\
q_4 &= 1 + a_1 c_1 + a_1 c_1 - |b_1|^2.
\end{align*}
\]
(7)

where \( a_1, b_1, c_1, a_2, b_2, c_2 \) are entries of \( S_R \) and \( S_E \), i.e.,
\[
S_R = \begin{pmatrix}
a_1^* & b_1 \\
b_1 & c_1 
\end{pmatrix}, \quad \text{and} \quad S_E = \begin{pmatrix}
a_2 & b_2 \\
b_2^* & c_2 
\end{pmatrix}. \tag{8}
\]

Remarks: The quartic equation (4) can be solved by radicals (closed form) [11] p. 87.

Proof of Theorem [1]

For the proof we need the following two lemmas.

**Lemma 2:** Let \( e_1 = [1 0]^T \). Any \( 2 \times 2 \) matrix \( Q \neq 0 \) with \( Q \geq 0 \) and \( \text{Tr}(Q) \leq 1 \) can be expressed as
\[ Q = x e_1 e_1^* + (1 - x) u u^* \]  
(9)

where \( x \) is a real number with \( 0 \leq x < 1 \) and \( u \neq 0 \) is a \( 2 \times 1 \) vector with \( u^* u \leq 1 \).

**Proof:** One can write \( Q = x e_1 e_1^* + (Q - x e_1 e_1^*) \) where \( x \) is chosen to satisfy \( \det(Q - x e_1 e_1^*) = 0 \).

**Lemma 3:** For vectors \( c_1, c_2, c_3 \) and \( c_4 \), it holds that

\[ \det(I + c_1 c_1^* + c_2 c_2^*) = \det(1 + c_1 c_1^* + c_2 c_2^* + c_3 c_3^* + c_4 c_4^*) \]  
(10)

**Proof:** Using \( \det(I + AB) = \det(I + BA) \) [10] p. 420], it holds that \( \det(I + c_1 c_1^* + c_2 c_2^*) = \det(1 + c_1 c_1^* + c_2 c_2^* + c_3 c_3^* + c_4 c_4^*) \) which leads to the desired result.

Since \( C_s > 0 \), it holds that \( Q^* \neq 0 \). From Lemma 2, we let \( Q = x e_1 e_1^* + (1 - x) u u^* \) with \( 0 \leq x < 1 \), \( u^* u \leq 1 \) and use Lemma 3 to rewrite \( C_s(x) \) as

\[
C_s(x, u) = \log \frac{\| (1 + x e_1 S_R e_1) (1 + (1 - x) u^* S_R u) - (x - x^2) u^* S_R e_1 \|^2}{\| (1 + x e_1 S_E e_1)(1 + (1 - x) u^* S_E u) - (x - x^2) u^* S_E e_1 \|^2}
\]
(11)

where \( e_2 = [0 1]^T \). Here, to obtain (11), we have used the identity \( (e_1 S_R e_1) S_R - S_R e_1 e_1^* S_R = \det(S_R) e_2 e_2^* \). Since \( C_s > 0 \), there exists a solution \( u^* \) with \( u^* u \leq 1 \). To see why, assume any solution \( u^* \) satisfies \( u^* u^* < 1 \). It is easy to verify that \( C_s(x^*, \sqrt{t} u^*) \) is a monotonic function of \( t \in [0, 1/(u^* u^*)] \). Thus, either \( t = 0 \) or \( t = 1/(u^* u^*) \) achieves a larger objective value than \( t = 1 \). But this contradicts the optimality of \( u^* \). From this result, we write

\[
C_s(x, u) = \log \frac{u^* G_1(x) u}{u^* G_2(x) u} \]
(12)

where \( G_1(x) = (1 + x e_1 S_R e_1 I + (1 - x)(S_R + x d e_2 e_2^*) \) and \( G_2(x) = (1 + x e_1 S_E e_1 I + (1 - x)(S_E + x d e_2 e_2^*) \). For fixed \( x \), the optimal \( u \) is the unit-norm eigenvector associated with the largest eigenvalue of the matrix \( G_2(x)^{-1} G_1(x) \). The problem becomes

\[
\max \frac{C_s(x)}{x} \left[ \log \lambda_{\max}(G_2(x)^{-1} G_1(x)) \right] \quad \text{s.t.} \quad 0 \leq x < 1.
\]
(13)

By using the fact that for a \( 2 \times 2 \) matrix \( B \),

\[
\lambda_{\max}(B) = \frac{\text{Tr}(B) + \sqrt{(\text{Tr}(B))^2 - 4 \det(B)}}{2}
\]
(14)

we get (simply finding \( \text{Tr}(G_2(x)^{-1} G_1(x)) = f_1(x)/f_2(x) \) and \( \det(G_2(x)^{-1} G_1(x)) = f_3(x)/f_2(x) \))

\[
\lambda_{\max}(G_2(x)^{-1} G_1(x)) = \frac{f_1(x) + \sqrt{(f_1(x))^2 - 4 f_2(x) f_3(x)}}{2 f_2(x)}
\]
(15)

where \( f_1(x) = p_1 x^2 + p_2 x + p_3, f_2(x) = q_1 x^2 + q_2 x + q_3, \)
\( f_3(x) = q_4 x^2 + q_5 x + q_6 \), and the coefficients \( p_i \)'s and \( q_i \)'s are given in (7). Since \( G_1(x) \geq 0 \) and \( G_2(x) > 0 \), it holds that \( f_1(x) > 0 \) for \( 0 \leq x < 1, \ i = 1, 2, 3 \).

From the above result, the problem of (13) becomes

\[
\max_{x, \tau} \log \tau \quad \text{s.t.} \quad 0 \leq x < 1, \quad f_1(x) + \frac{\sqrt{(f_1(x))^2 - 4 f_2(x) f_3(x)}}{f_2(x)} \geq \tau
\]
(16)

which is equivalent to

\[
\max_{x, \tau} \log \tau \quad \text{s.t.} \quad 0 \leq x < 1, \quad -\tau^2 f_2(x) + \tau f_1(x) - f_3(x) \geq 0.
\]
(17)

The equivalence of (16) and (17) can be verified as follows. Firstly, the second constraint in (17) can be rewritten as

\[
(f_1(x))^2 - 4 f_2(x) f_3(x) \geq (2 f_2(x) \tau - f_1(x))^2.
\]
(18)

For the optimal \( \tau \) and \( x \), it holds that \( 2 f_2(x) \tau - f_1(x) \geq 0 \). Otherwise, one can choose \( \tau' = f_1(x)/f_2(x) - \tau > \tau \) such that \( (\tau', x) \) satisfies the constraint (18). But this contradicts the optimality of \( \tau \). With this fact, (18) leads to the second constraint in (16). Secondly, for the optimal \( \tau \) and \( x \), the second constraint in (16) holds with equality which leads to \( -\tau^2 f_2(x) + \tau f_1(x) - f_3(x) = 0 \). The desired result follows.

Next we solve the problem of (17). Denote \( F(x) = -\tau^2 f_2(x) + \tau f_1(x) - f_3(x) \) which can be rewritten as

\[
F(x) = A_1 x^2 + B_1 x + C_1,
\]
(19)

where \( A_1 = -\tau^2 q_1 + \tau p_1 - q_4, B_1 = -\tau^2 q_2 + \tau p_2 - q_5, \)
and \( C_1 = -\tau^2 q_3 + \tau p_3 - q_6 \). One want to find the maximal \( \tau \) (denoted as \( \tau^* \)) such that there exists at least a \( x \in [0, 1) \)
function, this fact leads to two possible situations:

1) The optimal \( x \) (denoted as \( x^* \)) satisfies \( 0 < x^* < 1 \), then \( A_1 \neq 0 \) and \( x^* \) is the repeated root of \( F(x) = 0 \), i.e.,

\[
B_1^2 - 4A_1 C_1 = 0, \quad \text{and} \quad 0 < x^* = -\frac{B_1}{2A_1} < 1. \tag{20}
\]

In fact, if \( x^* \) is not the repeated root of \( F(x) = 0 \), then one can find \( \tau = \tau^* + \epsilon \) with an enough small \( \epsilon > 0 \) such that there exists a \( x \in [0, 1) \) satisfying \( F(x) \geq 0 \).

This is because the two different real roots of a quadratic equation both depend continuously on its coefficients. But this contradicts the optimality of \( \tau^* \).

2) \( x^* = 0 \) which leads to \( C_1 = 0 \).

From the above analysis, one can find \( \tau^* \) by solving \( C_1 = 0 \) and \( B_1^2 - 4A_1 C_1 = 0 \). This completes the proof.

IV. Numerical Simulations

First, we consider a MIMO wiretap channel in which \( n_T = 2 \), \( n_R = n_E = 3 \) and

\[
H_R = \begin{pmatrix}
0.7442 + 1.4223i & 1.1740 - 1.8109i \\
-0.5172 + 0.4116i & -1.3020 + 0.2417i \\
1.9755 + 0.4169i & -0.7105 + 0.7272i
\end{pmatrix},
\]

\[
H_E = \begin{pmatrix}
-0.4503 + 0.9711i & -0.7453 + 1.1555i \\
-0.7089 + 0.1272i & -0.0506 + 0.5835i \\
-0.1313 - 0.3833i & 0.1974 + 0.1632i
\end{pmatrix}.
\]

We set \( \rho = 5 \text{ dB} \). The quadratic equation (3) has two real roots \((1.4247, 10.8607)\), and hence \( \tau_1 = 10.8607 \). The quartic equation (4) has four roots \( 19.0710, 13.2768, 3.4529 \pm 1.5230 \times 10^{-8}i \), and \( \tau_2 = 13.2768 \) with \( x = -B_1/(2A_1) = 0.3189 \). Thus, the secrecy capacity is

\[
C_s = \log(\tau_2)/\log(2) = 3.7308 \text{ (bits/s/Hz)}
\]

which is achieved at \( x^* = 0.3189 \). The optimal input covariance matrix is

\[
Q^* = \begin{pmatrix}
0.5435 & -0.3198 + 0.0164i \\
-0.3198 - 0.0164i & 0.4565
\end{pmatrix}
\]

which has rank two. Fig. 1 plots the secrecy capacity for different \( \rho \).

Second, we change the previous example to \( n_E = 1 \) and

\[
H_E = [-1.2480 - 0.2893i, 4.6312 + 0.2417i].
\]

It holds that \( H_E(H_R^H H_R)^{-1} H_E^H > 1 \) (this is exactly the condition in [7, Lemma 1]). The quadratic equation (3) has two real roots \( 0.3453, 20.5293 \) and hence \( \tau_1 = 20.5293 \). The quartic equation (4) has four roots \( 6.8179 \pm 2.258i \) and \( 3.7837 \pm 4.38 \times 10^{-8}i \). Thus, \( x^* = 0 \) and hence beamforming is optimal. This is consistent with the result in [7, Lemma 1]).

V. Conclusion

We have studied a Gaussian MIMO wiretap channel in which there exists a transmitter with two antennas, a legitimate receiver and an eavesdropper both equipped with multiple antennas. We derived the the secrecy capacity in closed form.