This is the submitted version of a paper published in *IEEE Transactions on Information Forensics and Security*.

Citation for the original published paper (version of record):

Cao, P., Oechtering, T J. (2020)
Optimal Transmit Strategies for Gaussian MISO Wiretap Channels
*IEEE Transactions on Information Forensics and Security*, 15: 829-838
https://doi.org/10.1109/TIFS.2019.2929474

Access to the published version may require subscription.

N.B. When citing this work, cite the original published paper.

The work was supported by the Swedish Research Council (VR) project under Grant 2016-03853

Permanent link to this version:
http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-264151
Optimal Transmit Strategies for Gaussian MISO Wiretap Channels

Phuong Le Cao, Member, IEEE and Tobias J. Oechtering, Senior Member, IEEE

Abstract—This paper studies the optimal tradeoff between secrecy and non-secrecy rates of the MISO wiretap channels for different power constraint settings: sum power constraint only, per-antenna power constraints only and joint sum and per-antenna power constraints. The problem is motivated by the fact that channel capacity and secrecy capacity are generally achieved by different transmit strategies. First, a necessary and sufficient condition to ensure a positive secrecy capacity is shown. The optimal tradeoff between secrecy rate and transmission rate is characterized by a weighted rate sum maximization problem. Since this problem is not necessarily convex, equivalent problem formulations are introduced to derive the optimal transmit strategies. Under sum power constraint only, a closed-form solution is provided. Under per-antenna power constraints, necessary conditions to find the optimal power allocation are derived. Sufficient conditions are provided for the special case of two transmit antennas. For the special case of aligned channels, the optimal transmit strategies can deduced from an equivalent point-to-point channel problem. Lastly, the theoretical results are illustrated by numerical simulations.

Index Terms—Wiretap channels, per-antenna power constraints, secrecy rate, optimal transmit strategy.

I. INTRODUCTION

Security is a critical aspect in wireless communication systems due to the open nature of wireless links. To enhance the security, physical-layer secrecy methods have received much attention recently. One of the pioneer studies is the study of the secrecy capacity of the wiretap channel [1], where Wyner showed that a positive secrecy rate can be achieved when an eavesdropper’s channel is a degraded version of the main channel. The maximal secrecy rate is given by the largest difference between the mutual information to the legitimate receiver and the mutual information to the eavesdropper. Csiszár and Körner extended the result to the non-degraded case in [2]. Following these works, researchers in the physical-layer security area have studied and extended the wiretap channel in various aspects.

The secrecy capacities for Gaussian multiple-input single-output (MISO) and multiple-input multiple-output (MIMO) wiretap channels with a sum power constraint have been studied in [3]–[8]. In [3] and [4], the authors developed upper bounds that enable to characterize the secrecy capacities for MISO and MIMO wiretap channels. The key idea of the solutions is to reduce the wiretap system into a set of parallel channels based on a generalized singular value decomposition using independent Gaussian wiretap codebooks on the resulting channels. In [5], necessary conditions for the optimal input covariance matrix are derived. In particular, a closed-form expression of the MISO secrecy capacity has been shown. For the MIMO case an iterative algorithm is provided. In [7] and [8], iterative optimization algorithms to find the secrecy capacity have been proposed based on a concave-convex alternating optimization procedure. Alternatively, indirect approaches, which are based on matrix analysis tools are used to establish bounds on the secrecy capacity of MIMO Gaussian wiretap channels in [3], [4].

In practice, each antenna has its own power amplifier, which means the power allocation at the transmitter is usually done under per-antenna power constraints. The problem of finding the channel capacity with average per-antenna power constraints has been investigated in both single-user [9]–[13] and multi-user setups [14]–[16]. Recently, the capacities of point-to-point channels with joint sum and per-antenna power constraints have been considered in [17]–[20]. An interesting aspect of the joint sum and per-antenna power constraints setting is that it can be applied to systems with multiple antennas as well as to distributed systems with separated energy sources. The optimal transmit strategy problem with joint sum and per-antenna power constraints has been studied first for MISO channel with two transmit antennas in [17] and the general case in [18]. In [18], a closed-form characterization of an optimal beamforming strategy is derived. Shortly after [18], similar results have been published in [19]. In [20], the optimal transmit strategy problem for a point-to-point MIMO channel with joint sum and per-antenna power constraints has been studied.

In this work we study MISO wiretap channels with different power constraint settings including sum power constraint constraints, public message $M_p$, and secret message $M_s$. The work was supported by the Swedish Research Council (VR) project through project InfoSTOP under Grant 2016-03853.
only, per-antenna power constraints only, and joint sum and per-antenna power constraints. The optimal tradeoff between the overall transmission rate and the secrecy rate of MISO wiretap channels is motivated by the fact that the optimal coding strategy for the wiretap channel is using a two-layer codebook [21], [22]. The idea of the coding scheme is that the decoding capability of the eavesdropper is exhausted by a public message, while the legitimate receiver can decode both the public and secret messages. Therefore, instead of sending some useless random messages on the public layer, a useful message can be communicated non-securely to the legitimate receiver [21] (see Fig. 1). Since for vector-valued transmission the maximal overall transmission rate and secrecy rate are, in general, achieved by different transmit strategies, we face a tradeoff between both objectives which we will study in detail in the following. This problem is in particular interesting for the initial handshake phase in a cellular wireless downlink where no cryptographic protocols have been established. Some initial results of this paper have been presented in [23]. The contributions of the paper can be summarized as follows:

- Properties and optimal tradeoffs between the overall transmission rate and the secrecy rate of the Gaussian MISO wiretap channel under different power constraint configurations including the sum power constraint and the per-antenna power constraints are characterized and discussed.
- Parametrizations of the boundaries of the optimal rate regions of the transmission rate and the secrecy rate of the Gaussian MISO wiretap channel based on the weighted rate sum optimal rate pairs are derived.
- Closed-form solutions to compute optimal transmit strategies for general MISO wiretap channels with different power constraint settings are developed.

This paper is organized as follows: We start by briefly introducing the system model, sets of feasible transmit strategies considering different power constraint settings. After that equivalent formulations of the weighted rate sum maximization problem between the transmission rate and the secrecy rate are derived. Next, closed form solutions to find the optimal transmit strategies for different power constraint settings are derived. These solutions allow us to come up with a characterization of the boundary of the optimal region of transmission and secrecy rates. The results are then illustrated and discussed in numerical examples. Finally, we provide some remarks and conclusions.1

II. PROBLEM FORMULATION

A. System Model and Power Constraint

We consider a MISO wiretap channel with \( N_t \) antennas at the transmitter and single antenna at both legitimate receiver and eavesdropper. For each channel use, the received signals at the legitimate receiver and the eavesdropper are given as follows:

\[
y_t = h^r_{t}^H x + z_r, \tag{1}
\]

\[
y_e = h^e_{t}^H x + z_e, \tag{2}
\]

where \( x = [x_1, \ldots, x_{N_t}]^T \in \mathbb{C}^{N_t \times 1} \) is the random complex transmit signal vector, \( h^r_{t} = [h_{r1}, \ldots, h_{rN_t}]^T \in \mathbb{C}^{N_t \times 1} \), \( h_{ri} \neq 0 \forall i = 1, \ldots, N_t \), and \( h^e_{t} = [h_{e1}, \ldots, h_{eN_t}]^T \in \mathbb{C}^{N_t \times 1} \) are channel coefficient vectors between the transmitter and legitimate receiver and between the transmitter and eavesdropper, which are perfectly known at the transmitter. In practical scenarios, the perfect channel state information at the transmitter corresponds to the case when the channel remains constant for sufficiently long time. Knowledge about the eavesdropper channel can be assumed if the eavesdropper is part of the communication system, e.g. cellular downlink. The solution assuming perfect channel knowledge can be considered as an ideal case that serves as a benchmark. \( z_r \) and \( z_e \) are independent additive white complex Gaussian noise terms with \( \sigma_r^2 = \sigma_e^2 = 1 \). It will be optimal to use a zero-mean Gaussian distributed codebook generated with covariance \( Q = \mathbb{E}[x x^H] \), which also specifies the transmit strategy.

Let \( P_{tot} \) denote the maximal average sum transmit power and \( \hat{P}_k, 1 \leq k \leq N_t \), denotes the maximal average transmit power at the \( k \)-th antenna. Further, let \( S(p) \), \( p = [P_{tot}, P_1, \ldots, P_{N_t}] \), denote the set of all transmit strategies satisfying the power constraints \( p \), i.e.,

\[
S(p) := \{ Q \geq 0 : \text{tr}(Q) \leq P_{tot}, e_k^T Q e_k \leq \hat{P}_k, \forall k \in \mathcal{I} \} \tag{3}
\]

with an antenna index set \( \mathcal{I} := \{1, \ldots, N_t\} \) and where \( e_k \) is the \( k \)-th Cartesian unit vector. Depending on the per-antenna power constraints \( \hat{P}_k \) and the sum power constraint \( P_{tot} \), we can identify three different cases: (i) The sum power constraint only case is considered when the per-antenna power constraints can never be active, i.e., \( P_{tot} < \min_k(\hat{P}_k) \). (ii) The per-antenna power constraints only case is considered when the sum power constraint can never be active, i.e., \( P_{tot} > \sum_{k=1}^{N_t} \hat{P}_k \), and (iii) The joint sum and per-antenna power constraints case is considered when the power constraints relations satisfy \( \min_k(\hat{P}_k) \leq P_{tot} \leq \sum_{k=1}^{N_t} \hat{P}_k \), i.e., both sum and per-antenna power constraints can be active.

B. Tradeoff Between Transmission Rate and Secrecy Rate

A wiretap channel consists of a legitimate receiver who wishes to receive messages of high rate from a transmitter in the presence of an eavesdropper. It is known from [3], [4] that for vector-valued Gaussian channels, the secrecy capacity can be achieved with zero mean Gaussian distributed inputs. The secrecy rate is measured by the equivocation rate that describes the rate of information about the secret message in the eavesdropped signal. The MISO secrecy capacity can then be obtained from the following optimization problem

\[
C_s(p) = \max_{Q \in S(p)} R_s(Q), \tag{4}
\]

where \( R_s(Q) = \log(1 + h^r_{t}^H Q h^r_{t}) - \log(1 + h^e_{t}^H Q h^e_{t}) \).

1Notation: We use bold lower-case letters for vectors, bold capital letters for matrices. The superscripts \((\cdot)^T\), \((\cdot)^*\) and \((\cdot)^H\) stand for transpose, conjugate, and conjugate transpose. We use \( \succ \) for positive semi-definite, \( \text{tr}(\cdot) \) for trace, \( \text{rank}(\cdot) \) for rank and \( \text{diag}(\cdot) \) for generation of a diagonal matrix. The expectation operator of a random variable is given by \( \mathbb{E} [\cdot] \). \( \mathbb{R}_+ \) and \( \mathbb{C} \) are sets of non-negative real and complex numbers.
In the following proposition, we provide a condition for a positive secrecy capacity.

**Proposition 1.** A necessary and sufficient condition for a positive secrecy capacity of a Gaussian MISO wiretap channel, i.e., \( C_s(\hat{p}) > 0 \), is that \( \mathbf{h}_r^H \mathbf{h}_e^H \in \mathbb{C}^{N_t \times N_t} \) has to have at least one positive eigenvalue.

**Proof:** The proof of Proposition 1 is in Appendix A.

In [21], the authors consider a problem of simultaneously transmitting public and secret messages\(^2\). The coding schemes are designed such that the legitimate receiver can decode both the public and secret messages while the eavesdropper might be able to decode the public message only. This means the public layer can be used to transmit a useful message non-securely to the legitimate receiver (instead of broadcasting useless random messages in order to exhaust the capacity of the eavesdropper only). Accordingly, in our setting, \( M = (M_p, M_s) \), where the public message \( M_p \) and the secret message \( M_s \) are uniformly distributed over \( \{1, \ldots, 2^{nR_p}\} \) and \( \{1, \ldots, 2^{nR_s}\} \), are transmitted from the transmitter to the legitimate receiver (see Fig. 1). The secret message \( M_s \) needs to be kept secret from the eavesdropper, i.e., \( R_s \leq \frac{1}{n} H(M_s|Y_e^e) + \epsilon \) for some \( \epsilon > 0 \), while there is no secrecy constraint applied on \( M_p \). This means the eavesdropper may decode the public message \( M_p \), but does not have to. Accordingly in our setup, we do not consider a common message which has to be decoded by the eavesdropper as well.

Following [21, Theorem 1], the region of the transmission and equivocation rates of the MISO Gaussian wiretap channel under the power constraint (3) is given as follows:

\[
\mathcal{R}_{MISO}(\hat{p}) = \{(R, R_s) \in \mathbb{R}^2 : 0 \leq R_s \leq R_s(\hat{Q}), R = R_s + R_p \leq R(\hat{Q}) \text{ for some } \hat{Q} \in \mathcal{S}(\hat{p})\}
\]

(5)

with \( R(\hat{Q}) = \log(1 + \mathbf{h}_r^H \mathbf{Q} \mathbf{h}_r) \). In particular the maximal transmission rate is given by

\[
C(\hat{p}) = \max_{\hat{Q} \in \mathcal{S}(\hat{p})} R(\hat{Q}).
\]

(6)

Since the optimal transmit strategies that achieve the transmission capacity in (6) and the secrecy capacity in (4) do not have to be the same, a tradeoff between the two objectives appears. The optimal tradeoff between the overall transmission and the secrecy rates for a Gaussian MISO wiretap channel with power constraints \( \hat{p} \), is obtained by solving the following optimization problem

\[
\mathcal{R}_\Sigma(\hat{p}, w) = \max_{\hat{Q}} R_\Sigma(\hat{Q}, w), \text{ s.t. } \hat{Q} \in \mathcal{S}(\hat{p}),
\]

(7)

for a given weight \( 0 \leq w \leq 1 \), where

\[
R_\Sigma(\hat{Q}, w) = (1-w)R(\hat{Q}) + wR_s(\hat{Q}) = R(\hat{Q}) - wR_s(\hat{Q})
\]

(8)

with \( R_s(\hat{Q}) = R(\hat{Q}) - R_s(\hat{Q}), R(\hat{Q}) = \log(1 + \mathbf{h}_r^H \mathbf{Q} \mathbf{h}_r) \), and \( R_s(\hat{Q}) = \log(1 + \mathbf{h}_r^H \mathbf{Q} \mathbf{h}_s^H) \). The weight \( w \in [0,1] \) controls the optimal tradeoff between transmission rate and secrecy rate.

If the region \( \mathcal{R}_{MISO}(\hat{p}) \) is convex (see Fig. 2), then the set of weighted rate sum optimal rate pairs characterizes the boundary of the rate region. If this region is non-convex, then the set of all weighted rate sum optimal rate pairs can be used to characterize the boundary of the convex hull of the rate region, i.e., \( \mathcal{R}_{MISO}(\hat{p}) = \text{ConvexHull} (\mathcal{R}_{MISO}(\hat{p})) \). In this case, we would need to allow time-sharing between two rate pairs. Note that the secrecy rate is a fraction of the overall transmission rate, i.e., the condition \( 0 \leq R_s \leq R \) has to be satisfied. Therefore, the boundary of the rate region is also bounded by the line for which we have \( R = R_s \).

In the following, we provide solutions for the optimization problem (7). These solutions also provide us a characterization of the rate region (5) that describes the tradeoff between the overall transmission rate and the secrecy rate of the Gaussian MISO wiretap channel.

### III. Equivalent Problem Formulations and Parametrizations of the Boundary of Rate Region

Since \( \mathcal{R}_\Sigma(\hat{Q}) \) is non-convex in \( \hat{Q} \), (7) is not a convex optimization problem. In this section we provide an equivalent description of the boundary of \( \mathcal{R}_{MISO}(\hat{p}) \) so that the optimal tradeoffs can be obtained from convex problems that allow further analysis. A similar approach was taken in [16] but there the original optimization problem was already convex. For the equivalent reformulations we will use the following lemma.

**Lemma 1** ([24, Lemma 2, scalar case]). Consider the function \( f(D) = -DE + \log(D) + 1 \) where \( D, E \in \mathbb{R}, E > 0 \). Then,

\[
\max_{D > 0} f(D) = \log(E^{-1}),
\]

(9)

with the optimum value \( D^* = E^{-1} \).

By applying Lemma 1 to (7) with \( \log E_i^{-1} = \max_{D_i > 0} f_i(D_i), E_i = 1 + \mathbf{h}_r^H \mathbf{Q} \mathbf{h}_r \) and \( f_i(D_i) = -D_i E_i + \log(D_i) + 1 \) for \( i \in \{r, e\} \), the optimization problem (7) can
be expressed as
\[
R_{\Sigma}^*(\hat{p}, w) = \max_{Q \in S(\hat{p})} \left( -\max_{D_r > 0} f_r(D_r) + w \max_{D_r > 0} f_e(D_e) \right)
\]
\[
= \max_{Q \in S(\hat{p})} \min_{D_r > 0, D_e > 0} \left( -f_r(D_r) + w f_e(D_e) \right)
\]
\[
= \max_{Q \in S(\hat{p})} \min_{D_r > 0, D_e > 0} \left( D_r (1 + h^H Q h_r) - \log(D_r) \right)
\]
\[
- 1 + w(-D_e(1 + h^H Q h_e) + \log(D_e + 1))
\]
\[
+ D_r - \log(D_r) - 1 + w(-D_e + \log(D_e) + 1).
\]
For a given \(w\), let us define \(t := wD_r^2\) and \(\phi^{(1)}(Q, t) = h^H Q h_r - t e^H Q h_e = \text{tr}(AQ)\) with \(A := h h^H - t h^H h^H\), then (13) can be written as
\[
R_{\Sigma}^*(\hat{p}, w) = \max_{Q \in S(\hat{p})} \min_{D_r > 0, D_e > 0} \left( D_r \phi^{(1)}(Q, t) + D_e - \log(D_r) \right)
\]
\[
+ w(-D_e + \log(D_e) + 1) - 1.
\]

Although \(t\) is dependent on \(D_e, D_r\) and \(w\), the optimization with respect to \(Q\) depends on \(t\) only. Thus, we propose to find the optimal transmit strategy \(Q^{(1)}_{opt}(\hat{p}, t)\) by solving
\[
Q^{(1)}_{opt}(\hat{p}, t) = \arg \max_{Q \in S(\hat{p})} \phi^{(1)}(Q, t)
\]
for a given \(t\) and power constraints \(\hat{p}\). After having the optimal \(Q^{(1)}_{opt}(\hat{p}, t)\) for a given \(t\), we can obtain the corresponding optimal \(D_e^*\) and \(D_r^*\) following Lemma 1. The corresponding \(w\) is then given by \(\frac{D_r^*}{T^2}\). The following theorem shows that the previous procedure can be used to compute the optimal weighted rate sum \(R_{\Sigma}^*(\hat{p}, w)\).

**Theorem 1.** Let \(t_{max} = 2^{C_{p}(\hat{p})}\), for the optimal solution of (7) we have the following properties:

(i) For every \(w \in [0, 1]\) there exists a \(t \in [0, t_{max}]\) such that \(Q^{(1)}_{opt}(\hat{p}, t)\) is an optimal transmit strategy, i.e.,
\[
R_{\Sigma}^*(\hat{p}, w) = R_{\Sigma}^*(Q^{(1)}_{opt}(\hat{p}, t), w).
\]

(ii) For every \(t \in [0, t_{max}]\) there exists a \(w \in [0, 1]\) such that \(Q^{(1)}_{opt}(\hat{p}, t)\) is an optimal transmit strategy, i.e.,
\[
R_{\Sigma}^*(Q^{(1)}_{opt}(\hat{p}, t), w) = R_{\Sigma}^*(\hat{p}, w).
\]

**Proof:** The proof of Theorem 1 is in Appendix B.

As a result, the region that describes the optimal tradeoff between the transmission rate and the secrecy rate is equivalently described by \(R_{MISO}(\hat{p}) = \{(R, R_s) : 0 \leq R_s \leq R \leq R(Q(\hat{p}, t), R_s \leq R_s \leq R(Q(\hat{p}, t), t \in [0, t_{max}]\}.

In the following, we derive solutions to find the optimal transmit strategies and characterize the optimal tradeoff between the transmission and secrecy rates of the Gaussian MISO wiretap channels with two different power constraint cases: (i) with a sum power constraint only; (ii) per-antenna power constraints only using the reformulation above. The solutions for the optimization problem with joint sum and per-antenna power constraints is discussed in a special case of aligned channels only. The optimal solution for a specific weight is then found after a simple line search over \(t\).

**IV. Analytical Discussions and Solutions**

Since for a given \(t\) the equivalent problem in (15) is convex, optimal solutions can be also found using standard convex optimization tools [25]. However, some results can be obtained in closed-form that lead to computational efficient solutions, which are therefore interesting for practical applications.

The sufficiency of beamforming for optimality for a given set of power constraints \(\hat{p}\) is shown in the following theorem.

**Theorem 2.** For an optimal transmit strategy, it is sufficient to consider beamforming strategies, i.e., there exists always an optimal rank one solution.

**Proof:** The proof of Theorem 2 is in Appendix C.

**A. Sum Power Constraint Only**

Let \(S_{SPC}\) denote the set of all transmit strategies which satisfy the sum power constraint \(P_{tot}\) only, i.e., \(S_{SPC} = \{Q \geq 0 : \text{tr}(Q) \leq P_{tot}\}\). The equivalent problem of finding the weighted rate sum optimal transmit strategy for the MISO wiretap channel with sum power constraint only for a given \(t\) can be written as
\[
Q^{(1)}_{SPC}(t) = \arg \max_{Q \in S_{SPC}} \phi^{(1)}(Q, t),
\]
where \(\phi^{(1)}(Q, t) = h^H Q h_r - t e^H Q h_e = \text{tr}(AQ)\) with \(A = h h^H - t h^H h^H\).

**Theorem 3.** The closed-form expression for the optimal transmit strategy of (16) is given by
\[
Q^{(1)}_{SPC}(t) = P_{tot} v v^H
\]
where \(v\) is the eigenvector associated with the positive eigenvalue of \(A = h h^H - t h^H h^H\) for a given \(t\).

**Proof:** The proof of Theorem 3 is in Appendix D.

**B. Per-antenna Power Constraints Only**

Let \(S_{PAPC}\) denote the set of all transmit strategies which satisfy all per-antenna power constraints \(P_k, \forall k \in I\), i.e., \(S_{PAPC} = \{Q \geq 0 : e_k^T Q e_k \leq P_k, \forall k \in I\}\). The equivalent problem of finding the weighted rate sum optimal transmit strategy for the MISO wiretap channel with per-antenna power constraints only for a given \(t\) can be written as
\[
Q^{(1)}_{PAPC}(t) = \arg \max_{Q \in S_{PAPC}} \phi^{(1)}(Q, t),
\]
where \(\phi^{(1)}(Q, t) = \text{tr}(AQ)\) with \(A = h h^H - t h^H h^H\).

From the definition of \(A\) below (16) and (18) we know that this matrix may have a negative eigenvalue. A negative eigenvalue in the matrix \(A\) does not affect the procedure to compute the optimal solution for the sum power constraint only case. In particular, the total power is always allocated. Interestingly this does not hold for the per-antenna power constraints only and joint sum and per-antenna power constraints problems. For instance, for the MISO wiretap channels with per-antenna power constraints, when \(A\) has a negative eigenvalue, it may not be optimal to allocate full transmit power on all antennas. In this scenario, it will be good to transmit with high power in
the direction of the legitimate receiver but not in the direction of the eavesdropper. Thus, if $A$ is not positive semi-definite, then it may not be optimal to allocate full power on all antennas.

In the following, we assume that the power allocation per antenna, which is denoted by $\hat{P}_k \forall k \in \mathcal{I}$, is given. Later, we will discuss the power allocation problem. This assumption implies that $Q_{PAPC}(t)$ has diagonal elements of $q_{kk} = \hat{P}_k \forall k \in \mathcal{I}$. The remaining problem is to find the off-diagonal elements of $Q_{PAPC}(t)$ for a given $t$. The main difficulty here is the positive semi-definite constraint of $Q_{PAPC}(t)$. To overcome this, we consider a relaxed optimization problem involving the $2 \times 2$ principal minors of $Q_{PAPC}(t)$ similarly as done in [9]. Let $X_{k,l}(t)$ be a principal minor matrix which is obtained from $Q$ by removing $N_t - 2$ columns, except columns $k$ and $l$, and the corresponding $N_t - 2$ rows except rows $k$ and $l$. Then, $X_{k,l}(t)$ is given as

$$X_{k,l}(t) = \begin{bmatrix} \hat{P}_k & q_{kl}(t) \\ q_{lk}(t) & \hat{P}_l \end{bmatrix}$$  \hspace{1cm} (19)

where $k, l \in \mathcal{I}$, $k \neq l$. Therewith, we can formulate a relaxed optimization problem as follows:

$$\max_{Q} \phi^{(1)}(Q, t), \quad \text{s.t. } q_{kk} = \hat{P}_k, \forall k \in \mathcal{I}$$  \hspace{1cm} (20)

The off-diagonal elements of the covariance matrix of (20) can be obtained from the following theorem.

**Theorem 4.** The optimal transmit strategy $Q_{PAPC-R}(t)$ of the relaxed optimization problem (20) has off-diagonal elements

$$q_{kl}(t) = \frac{h_{rk}^* h_{rl} - t h_{el}^* h_{el}}{|h_{rk}^* h_{rl} - t h_{el}^* h_{el}|} \sqrt{\hat{P}_k \hat{P}_l}, \quad k, l \in \mathcal{I}, k \neq l.$$  \hspace{1cm} (21)

**Proof:** The proof of Theorem 4 is in Appendix E. \hspace{1cm} $\blacksquare$

From Theorem 4, we have the following conclusion and remarks.

**Corollary 1.** If there are only two transmit antennas, i.e., $N_t = 2$, then (21) always leads to a positive semi-definite solution with eigenvalues zero and $\hat{P}_1 + \hat{P}_2$, i.e., the optimal solution (21) of the relaxed optimization problem (20) is positive semi-definite and therefore also the optimal solution of (18).

For $n > 2$, it is not clear if (21) always results in a positive semi-definite solution. Numerical experiments suggest this conjecture, but a proof is missing. Accordingly, we have only the following remark.

**Remark 1.** If the solution (21) leads to a positive semi-definite solution, then it is also an optimal solution of (18).

Thus, it is a viable strategy to first compute the solution according to (21) and then test if it is positive semi-definite.

1) **Optimal power allocation for the per-antenna power constraints only problem:** In this section, we discuss the optimal power allocation for the per-antenna power constraints only problem. We first establish a useful observation as follows.

**Proposition 2.** For the per-antenna power constraints only problem, there is always at least one per-antenna power constraint active.

**Proof:** Assume that there exists an optimal beamforming vector which does not allocate full power on all antennas. Then we can scale it by a factor larger than one and achieve a larger rate. This implies that at least one antenna should allocate full power. \hspace{1cm} $\blacksquare$

Next, a person-to-person optimality method is used to establish necessary conditions for optimality. In more details, we characterize the optimal beamforming coefficient of the $l$-th antenna given a set of beamforming coefficients of all other antennas, $k \neq l$.

Since it is sufficient to consider beamforming strategies, i.e., $Q = qq^H$ with $q = [q_1(t), \ldots, q_{N_t}(t)]^T$, $\phi^{(1)}(Q, t)$ can be expressed as $\phi^{(1)}(Q, t) = q^T \mathbf{h}_r |^2 - t q^H \mathbf{h}_e |^2$. Then, the optimal transmit power on the $l$-th antenna, i.e., $P_l^* = |q_l|^2$, $l \in \mathcal{I}$, is then determined by solving the following optimization problem

$$\arg \max_{q_l \in \mathbb{C}} |q_l|^2 h_{rl} + \sum_{k \in \mathcal{I}, k \neq l} q_k h_{rk} |^2 - t |q_l|^2 h_{el} + \sum_{k \in \mathcal{I}, k \neq l} q_k h_{ek} |^2.$$  \hspace{1cm} (22)

The following proposition characterizes a condition when it is optimal to allocate full power on the $l$-th antenna.

**Theorem 5.** For given beamforming coefficients $q_k \forall k \in \mathcal{I}$, $k \neq l$, let $\alpha$ be the phase of $\sum_{k \in \mathcal{I}, k \neq l} q_k (h_{rk}^* h_{rl} - t h_{el}^* h_{el})$. Then the optimal beamforming coefficient $q_l$ has phase $\varphi_l = \alpha$ and absolute value $|q_l^*| = \sqrt{P_l}$ if $|h_{rl}|^2 \geq t |h_{el}|^2$, else $|q_l^*| = \min\{ |\sum_{k \in \mathcal{I}, k \neq l} q_k (h_{rk}^* h_{rl} - t h_{el}^* h_{el})| / |h_{rl}|^2 - t |h_{el}|^2, \sqrt{P_l}|\}$.

**Proof:** The proof of Theorem 5 is in Appendix F. From Theorem 5 we know that when $|h_{rl}|^2 < t |h_{el}|^2$ and $|\sum_{k \in \mathcal{I}, k \neq l} q_k (h_{rk}^* h_{rl} - t h_{el}^* h_{el})| / |h_{rl}|^2 - t |h_{el}|^2 < \sqrt{P_l}$, then it is not optimal to allocate full power on the $l$-th antenna. In this case the optimal allocation for the $l$-th antenna is given by $|\sum_{k \in \mathcal{I}, k \neq l} q_k (h_{rk}^* h_{rl} - t h_{el}^* h_{el})| / |h_{rl}|^2 - t |h_{el}|^2$. Note that this allocation depends on the assumed power allocation on all other antennas.

Theorem 5 suggests a simple algorithm to find the optimal power allocation for given $(t, \mathbf{h}_r, \mathbf{h}_e, \mathbf{P})$, which is summarized in Algorithm 1. The convergence of Algorithm 1 is guaranteed because in every step it will improve and it is bounded by the sum power constraint optimization problem with $P_{tot} = \sum_{i=1}^{N_t} \hat{P}_i$. Further, Algorithm 1 converges to the optimum since the problem is convex. Note that we can always pick one phase and therefore only $N_t - 1$ phases need to be optimized.

If the channels are aligned and the secrecy capacity is positive, then it is optimal to allocate full power on all antennas, which is discussed in more detail in Section IV-C.

2) **Optimal power allocation for two-antenna case:** In this section, we provide solutions for the special case with two transmit antennas. For the per-antenna power constraints optimization problem, the off-diagonal elements of the covariance matrix for a specific case with two transmit antennas are shown in Theorem 4. Since we have the freedom to choose the phase zero at one antenna, say $\varphi_l = 0$, then the optimal phase on the remaining antenna will be $e^{j\varphi_k} = \frac{h_{rk}^* h_{rl} - t h_{el}^* h_{el}}{|h_{rk}^* h_{rl} - t h_{el}^* h_{el}|}$.
Algorithm 1: Optimal Power Allocation

1. Set $i = 1$, $q^{(i,1)} = [q_1]_{i=1}^{N_t} = [\sqrt{P_1}, \ldots, \sqrt{P_{N_t}}]^T \in \mathbb{C}^{N_t}$.

2. for $l = 1$ to $N_t$ do

3. Compute $\alpha$,

4. if $|h_{i,l}|^2 \geq t|h_{i,s}|^2$ then

5. $|q_l^i(q^{(i,l)} \setminus q_l)| = \sqrt{P_i},$

6. else

7. $|q_l^i(q^{(i,l)} \setminus q_l)| = \min\left\{\frac{|\sum_k q_k^i(h_{i,k}^* h_{i,l} - h_{i,k}^* h_{i,s})|}{|h_{i,l}|^2 - t|h_{i,s}|^2}, \sqrt{P_i}\right\}$

8. end if

9. end if

10. if $l < N_t$ then

11. $q^{(i,l+1)} = [q_1, \ldots, q_{l-1}, q_l^*, \ldots, q_{N_t}]^T$,

12. else

13. $q^{(i+1,1)} = [q_1, \ldots, q_{N_t-1}, q_{N_t}^*]T.$

14. end if

15. end if

16. end for

17. $i \leftarrow i + 1.$

18. while $|R(q^{(i+1,1)}) - R(q^{(i,1)})| \geq \epsilon$;

The following corollary of Theorem 5 provides the optimal elements of the beamforming vector for this case.

Corollary 2. Let $k, l \in \{1, 2\}, k \neq l$. For the per-antenna power constraint only problem, if $q_l^* = \sqrt{P_l}$, then $e^{\psi^*} = \frac{h_{k,l}^* h_{i,l} - h_{k,s}^* h_{i,s}}{|h_{k,l}^* h_{i,l} - h_{k,s}^* h_{i,s}|}$ and

$$|q_k^*| = \left\{ \begin{array}{ll} \sqrt{P_k}, & |h_{r,k}|^2 \geq t|h_{r,k}|^2 \\ \frac{\sqrt{P_k(h_{s,k}^* h_{r,k} - h_{s,r}^* h_{r,k})}}{|h_{r,k}^2 - t|h_{r,k}|^2}, & |h_{r,k}|^2 < t|h_{r,k}|^2. \end{array} \right. \tag{23}$$

In the following, we discuss and provide solutions for the special case that $A$ does not have a negative eigenvalue, i.e., $A$ is positive semi-definite. This case happens when channel vectors are aligned and the secrecy capacity is positive.

C. Special case of aligned channels

In general, the function $R_\Sigma(p, w)$ is not a concave function. However, if we consider channel coefficients such that $A = h_r h_r^T - th_s h_s^T$ is a positive semi-definite matrix for a given $t$, then the secrecy rate function $R_\Sigma(p, w)$ is a concave function [7, Proposition 2.1, MISO case]. In this case, $A$ has rank one with $A = h_A h_A^H$ and $h_A = \sqrt{|h_s|^2 - t|h_r|^2} h_r$. Then the objective function in the optimization problem (15) can be rewritten as

$$\phi^{(1)}(Q, t) = h_A^H Q h_A. \tag{24}$$

It follows that the special case with $A$ to be positive semi-definite directly corresponds to a point-to-point MISO channel problem with channel $h_A$. Moreover, since the arg max does not change with $t$, there is no tradeoff between secrecy and non-secrecy rate, i.e., there is only one transmit strategy that simultaneously maximizes both rates. Thus, we have the following remark.

Remark 2. If $A$ is positive semidefinite, then the optimal transmit strategies $Q_{opt}(p, t)$ can be obtained from the solution of the point-to-point MISO channel problem:

(i) [9] for the per-antenna power constraints only problem,
(ii) [18] for the joint sum and per-antenna power constraints problem, considering the channel $h_A$.

In particular, this implies that in the case of $A$ positive semi-definite that we can always find optimal transmit strategies that allocate full power (more details can be found in [9], [18]).

V. NUMERICAL EXAMPLES

In this section, an illustrative numerical example is shown for the optimization problems with sum power constraint only and per-antenna power constraint only with two antennas at the transmitter, and one antenna at legitimate receiver and eavesdropper each. We first provide a MISO wiretap channel with two transmit antennas. The complex channel coefficients of legitimate receiver and eavesdropper are given as $h_r = [0.3737 + 0.8912i, 0.9795 + 1.2926i]^T$ and $h_s = [0.4387 + 0.7655i, 0.3816 + 0.7952i]^T$. The maximum transmit powers for transmit antennas are $P_1 = 5$ and $P_2 = 10$. The sum power constraint $P_{tot} = 15$.

Fig. 3 depicts the optimal regions of the transmission and secrecy rate pairs of the wiretap channel with two different sets of power constraints: sum power constraint only and per-antenna power constraints only. The figure shows that the regions are fully characterized by the curved sections which can be obtained from the derived optimal solutions. It also shows the optimal tradeoff between the transmission rate and the secrecy rate. For instance, we can see the difference between the strategies that maximize the secrecy rates, $t = 2C_{opt}$ with $C_{opt}^S = 5.15783$ for the case with sum power constraint only and $t = 2C_{opt}^P$ with $C_{opt}^P = 1.4182$ for the case with per-antenna power constraints only.

VI. CONCLUSIONS

In this paper, we studied the tradeoff between the transmission and secrecy rate of Gaussian MISO wiretap channels considering different power constraint settings. The original optimization problem is non-convex. However, using equivalent convex reformulations allow us to provide useful characterizations of the rate regions boundary. The optimal rate pair can be then found by a simple line search. In particular, for the optimization problem with sum power constraint only, the optimal transmit strategy is characterized by a simple closed-form solution. Next, it turns out that if channel vectors are not aligned, then it may be optimal not to allocate full power if there are per-antenna power constraints. For the general case necessary conditions for optimality have been derived that have been used in an iterative person-by-person algorithm for the per-antenna power constraints only problems.
special case of aligned channels, the optimal transmit strategies can be deduced from an equivalent point-to-point channel problem. We believe that studies on optimal transmit strategies including more advanced power constraint settings are highly relevant for future wireless networks, in particular for massive MIMO setups, as done for instance in [26], [27]. Lastly, optimal transmit strategies for the wiretap channel setup are of particular interest for the initial handshake phase in the cellular downlink where cryptographic protocols have not been established yet.

APPENDIX

A. Proof of Proposition 1

To prove the proposition, we need to show the necessity and sufficiency. For the necessary part, we need to show that for \( R_s(Q) > 0, h_i h_i^H - h_i h_i^H \) has at least one positive eigenvalue. The secrecy rate can be written as

\[
R_s(Q) = \log(1 + h_i^H Q h_i) - \log(1 + h_c^H Q h_c) = \log \left( 1 + \frac{\text{tr}(h_i h_i^H - h_i h_i^H)Q}{1 + h_c^H Q h_c} \right) > 0.
\]  

Since \( 1 + h_i^H Q h_i > 0 \), it follows that \( \text{tr}(AQ) > 0 \) with \( A = h_i h_i^H - h_i h_i^H \). Since \( \text{tr}(AQ) = \sum_{i=1}^{N_i} \lambda_i(Q) v_i^H A v_i > 0 \), there must exist an \( i \in \{1, \ldots, N_i\} \) such that \( v_i^H A v_i > 0 \). Thus, we have

\[
\lambda_{\text{max}}(A) = \max_{|v_i|=1} v_i^H A v_i \geq v_i^H A v_i > 0.
\]  

For the sufficient part, we need to show that if \( A = h_i h_i^H - h_i h_i^H \) has a positive eigenvalue, then there exists \( Q \in S(\hat{p}) \) such that \( R_s(Q) > 0 \).

If \( A \) has a positive eigenvalue, then there exist a vector \( v : ||v|| = 1 \) such that \( v^H A v > 0 \). This implies that we can construct \( Q = \xi v v^H, \xi > 0 \), such that \( Q \in S(\hat{p}) \) and \( \text{tr}(AQ) > 0 \). Then we have

\[
R_s(Q) = \log(1 + h_i^H Q h_i) - \log(1 + h_c^H Q h_c) = \log \left( 1 + \frac{\text{tr}(AQ)}{1 + h_c^H Q h_c} \right) > 0.
\]

\[
R_s(Q) > R_s(Q_{\text{opt}}(\hat{p}, t), w) \forall t \in [0, t_{\text{max}}].
\]

B. Proof of Theorem 1

First, we show that for every \( w \in [0, 1] \) there exists a \( t \in [0, t_{\text{max}}] \) with \( t_{\text{max}} = 2C_{\text{S}}(\hat{p}) \) such that \( Q_{\text{opt}}(\hat{p}, t) \) is an optimal transmit strategy, i.e., \( R_{S_{\text{opt}}}(\hat{p}, w) = R_{S_{\text{opt}}}(Q_{\text{opt}}(\hat{p}, t), w) \).

For a given \( w \in [0, 1] \) we assume that there exists no \( t \in [0, t_{\text{max}}] \) such that \( Q_{\text{opt}}(\hat{p}, t) \) is optimal. This implies that there exist a \( Q^* \) so that \( R_{S_{\text{opt}}}(\hat{p}, w) = R_{S_{\text{opt}}}(Q^*, w) \) and

\[
R_{S_{\text{opt}}}(Q^*, w) > R_{S_{\text{opt}}}(Q_{\text{opt}}(\hat{p}, t), w) \forall t \in [0, t_{\text{max}}].
\]

Following Lemma 1 we know that for an optimal \( Q^* \) the corresponding values \( D_r^* \) and \( D_c^* \) are computed as

\[
D_r^* = (1 + h_i^H Q^* h_i)^{-1}, \quad D_c^* = (1 + h_c^H Q^* h_c)^{-1}.
\]

Then for \( w \in [0, 1] \) we have:

\[
R_{S_{\text{opt}}}(Q^*, w) = D_r^*(1 + h_i^H Q^* h_i) - \log(D_r^*) - 1 + w(-D_r^*(1 + h_c^H Q^* h_c) + \log(D_r^*) + 1) \\
\leq \max_{Q \in S(\hat{p})} D_r^*(h_i^H Q h_i - w D_c^* h_c^H Q h_c) + D_r^* - \log(D_r^*) - 1 - w D_r^* - w \log(D_r^*) - w.
\]

Following (14) and (15) we know that the optimal solution \( Q^* \) for the latter of (33) is computed as

\[
Q^* = \arg \max_{Q \in S(\hat{p})} h_i^H Q h_i - w D_c^* h_c^H Q h_c
\]

\[
= Q_{\text{opt}}(\hat{p}, w) = Q_{\text{opt}}(\hat{p}, t),
\]

where \( 0 \leq t = w D_r^* \leq t_{\text{max}} \). This implies that

\[
R_{S_{\text{opt}}}(Q^*, w) \leq R_{S_{\text{opt}}}(Q_{\text{opt}}(\hat{p}, t), w),
\]

for \( t = w D_r^* \in [0, t_{\text{max}}] \). However, this contradicts with (30). Thus, it follows that for every \( w \in [0, 1] \) there exists a \( t \in [0, t_{\text{max}}] \) such that \( Q_{\text{opt}}(\hat{p}, t) \) is an optimal transmit strategy.

Next, we show that for every \( t \in [0, t_{\text{max}}] \) there exists a \( w \in [0, 1] \) such that \( Q_{\text{opt}}(\hat{p}, t) \) is an optimal transmit strategy, i.e., \( R_{S_{\text{opt}}}(\hat{p}, w) = R_{S_{\text{opt}}}(Q_{\text{opt}}(\hat{p}, t), w) \). Suppose that \( Q^* \) is an optimal solution of (15), then from Lemma 1 we know that for a given \( Q^* \) the corresponding values \( t \in [0, t_{\text{max}}] \) is given by \( t = w D_r^* \) with

\[
D_r^* = (1 + h_i^H Q^* h_i)^{-1}, \quad D_c^* = (1 + h_c^H Q^* h_c)^{-1},
\]
and $Q^*$ must satisfy the KKT condition of (15) which is given as follows.
\[
\frac{\partial}{\partial Q} \phi^{(1)}(Q, t) = D + \mu I - M
\]
\[
\text{tr}(Q) \leq P_{tot}
\]
\[
c_k^T Q e_k \leq \hat{P}_k, \forall k \in \mathcal{I} \quad Q \succeq 0
\]
\[
\mu \geq 0
\]
\[
\frac{\partial}{\partial Q} \text{tr}(Q - P_{tot}) = 0
\]
\[
\mu \geq 0
\]
(38) (39) (40) (41)

where $D = \text{diag}\{\nu_k\}$ is a diagonal matrix of Lagrangian multipliers for the per-antenna power constraints, $\mu$ is the Lagrangian multiplier for the sum power constraint, $M$ is the Lagrangian multiplier for the positive semi-definite constraint, and $\hat{P} = \text{diag}\{\hat{P}_k\}, \forall k \in \mathcal{I} = \{1, \ldots, N_t\}$, is a diagonal matrix of the per-antenna power constraints.

On the other hand, we have
\[
\frac{\partial}{\partial Q} \phi^{(1)}(Q, t) \bigg|_{Q=Q^*, t=t} = D^*_t h_r h_r^H - w D^*_t h_r h_r^H
\]
\[
= h_r(1 + h_r^H Q h_r)^{-1} h_r^H - w h_r(1 + h_r^H Q h_r)^{-1} h_r^H
\]
\[
= \frac{\partial}{\partial Q} R^*_t(Q, w) \bigg|_{Q=Q^*, w=t^* D^*_t}
\]
(42) (43) (44)

Therefore, we can conclude from (38) and (44) that the optimal transmit strategy $Q^*$ is also an optimal solution of (7) with $0 \leq w = t^* D^*_t \leq 1$.

\[\text{C. Proof of Theorem 2}\]

For the proof of Theorem 2, we make use of a second equivalent reformulation where we apply Lemma 1 to (7) with $E_e(Q) = 1 + h_r^H Q h_r$ and $f_e(D_e, Q) = -D_e E_e(Q) + \log(D_e) + 1$ only. Thus, the optimization problem (7) can be alternatively expressed as
\[
R^*_t(p, w) = \max_{Q \in S(p)} \max_{D_e > 0} \log(1 + h_r^H Q h_r)
\]
\[
+ w(-D_e(1 + h_r^H Q h_r) + \log(D_e) + 1).
\]
(45)

If we define $s = w D_e$, and $\phi^{(2)}(Q, s) = \log(1 + h_r^H Q h_r) - s h_r h_r^H Q h_r$, then (45) can be written as
\[
R^*_t(p, w) = \max_{Q \in S(p)} \max_{D_e > 0} \phi^{(2)}(Q, s) - s + w \log(D_e) + w.
\]
(46)

Then the problem of finding the optimal transmit strategy $Q^{(2)}_{opt}(p, s)$ depends on $s$ only and can be expressed as
\[
Q^{(2)}_{opt}(p, s) = \arg \max_{Q \in S(p)} \phi^{(2)}(Q, s).
\]
(47)

Although $s$ is dependent on $D_e$ and $w$, the optimization with respect to $Q$ only depends on $s$. Thus, we propose to solve first (47) for a given $s$ and power constraints $p$. Once $Q^{(2)}_{opt}(p, s)$ is obtained, the corresponding $D_e$ and $w$ can be found using Lemma 1 and formula $w = s / D_e^* = s(1 + h_r^H Q^{(2)}_{opt}(p, s) h_r) h_r$.

We are now ready to prove Theorem 2. By replacing $t \in [0, \ell_{max}]$ in Theorem 1 by $s = [0, s_{\text{max}}]$ where $s_{\text{max}} = (1 + h_r^H Q h_r)^{-1}$ with $Q^* = \arg \max_{Q \in S(p)} R^*_t(Q, w = 1) = \arg \max_{Q \in S(p)} R_e(Q)$, we obtained that every optimal transmit strategy obtained from (47) is the same as the optimal transmit strategy obtained from (15) and is the optimal transmit strategy of (7). This implies that, for a given $w$, at the optimum we have $s = w D_e^* = w D_e^*$ and
\[
Q^{(2)}_{opt}(p, s) = Q^{(1)}_{opt}(p, t) = Q^{opt}(p, w).
\]
(48)

Thus, it is sufficient to find the rank of the optimal transmit strategy by considering the following optimization problem
\[
\max_Q \phi^{(2)}(Q, s), \text{ s.t. } Q \in S(p).
\]
(49)

The Lagrangian for problem (49) is given by
\[
\mathcal{L} = \log(1 + h_r^H Q h_r) - s h_r h_r^H Q h_r - \text{tr}(D(Q - \hat{P}))
\]
\[
- \mu(\text{tr}(Q) - P_{tot}) + \text{tr}(MQ),
\]
(50)

where $D = \text{diag}\{\nu_k\}$ is a diagonal matrix of Lagrangian multipliers for the per-antenna power constraints, $\mu$ is the Lagrangian multiplier for the sum power constraint, $M$ is the Lagrangian multiplier for the positive semi-definite constraint, and $\hat{P} = \text{diag}\{\hat{P}_k\}, \forall k \in \mathcal{I} = \{1, \ldots, N_t\}$, is a diagonal matrix of the per-antenna power constraints.

Taking the first derivative of the Lagrangian above and set equal to zero, we have
\[
\frac{\partial \mathcal{L}}{\partial Q} = h_r(1 + h_r^H Q h_r)^{-1} h_r^H - s h_r h_r^H D - \mu I + M
\]
\[
= h_r(1 + h_r^H Q h_r)^{-1} h_r^H - K + \mu I = 0,
\]
(51)

where $K = s h_r h_r^H D + \mu I$.

By using the slackness condition $MQ = 0$, we obtain $h_r h_r^H Q = (1 + h_r^H Q h_r) K Q$ by multiplying (51) with $Q$ from the right. On the other hand, from the KKT condition of the convex optimization problem (49), we know that in the optimum we have either $\mu > 0$ or $D > 0$. This implies that, in the optimum, $K$ has full rank and
\[
\text{rank}(Q_{opt}(p, w)) = \text{rank}(h_r h_r^H Q) \leq \text{rank}(h_r h_r^H) = 1.
\]

Since rank$(Q_{opt}(p, w)) = 0$ is not optimal, the optimal rank of $Q_{opt}(p, w))$ is one. This proves Theorem 2.

\[\text{D. Proof of Theorem 3}\]

By using singular value decomposition, for a given $t$, we have $h_r h_r^H - t h_r h_r^H = V A V^H$. Let $Q = V^H Q V$, we obtain $Q \succeq 0$. Then
\[
\phi^{(1)}(Q, t) = \text{tr}\{(h_r h_r^H - t h_r h_r^H) Q) = \text{tr}\{A Q\}
\]
\[
= \text{tr}\{A \text{diag}(Q)\} \leq \lambda_{\text{max}} P_{tot}
\]
(52)

with $\lambda_{\text{max}}$ is the positive, which is also the largest, entry of $A$ and $\text{tr}(Q) = \text{tr}(Q) = P_{tot}$.

Equation (52) holds with equality if $Q$ is diagonal and has a unique nonzero entry equal to $P_{tot}$ corresponding to the positive entry of $A$. This implies that $Q$ and $h_r h_r^H - t h_r h_r^H$ share the same eigenvectors and $Q$ has rank one. Therefore, we have $Q^{(1)}_{SC}(t) = P_{tot} v^H v$ where $v$ is the eigenvector associated with the positive eigenvalue of $h_r h_r^H - t h_r h_r^H$ for a given $t$. This proves Theorem 3.
E. Proof of Theorem 4
Consider an optimization problem (20). The Lagrangian for problem (20) is given by
\[
\mathcal{L} = h_r^H Q_b h_r - t h_e^H Q_b e_r - \sum_{k \neq l} \lambda_{kl} (q_{kl}(t))^2 - \sum_k \mu_k (q_{kk} - \bar{P}_k), \tag{53}
\]
where \(\lambda_{kl}\) and \(\mu_k\) are the Lagrange multipliers, and \(k, l \in \mathcal{I}\). Taking the first derivative of (53) and set it equal to zero, we have
\[
\frac{\partial \mathcal{L}}{\partial q_{kl}} = h_{*kl}^r h_{rl} - t h_{e*kl}^r h_{el} - \lambda_{kl} q_{kl}(t) = 0, \tag{54}
\]
or equivalently
\[
q_{kl}(t) = \frac{h_{e*kl}^r h_{el}}{\lambda_{kl}}. \tag{55}
\]
Similar to [16], the optimal value of \(q_{kl}\) in (55) is obtained when its constraint is satisfied with equality, i.e., \(|q_{kl}(t)|^2 = \bar{P}_k \bar{P}_l\). By combining this condition with (55), we have the value of \(q_{kl}(t)\) as in (21).

F. Proof of Theorem 5
Consider the optimization problem (22). Equivalently, we can express (22) as
\[
\text{arg max}_{q_1 \in \mathbb{C}} |q_1^* h_{rl} + \sum_{k \in \mathcal{I}} q_k^* h_{rk}|^2 - t|q_1^* h_{el} + \sum_{k \neq l} q_k^* h_{ek}|^2 \tag{56}
\]
\[
= \text{arg max}_{q_1 \in \mathbb{C}} \left\{ \sum_{k \in \mathcal{I}} q_k^* h_{ek}^2 + |q_1^* h_{rl}|^2 + 2 t Re \left\{ \sum_{k \neq l} q_k^* h_{ek} h_{rl} q_1^* \right\} \right\}, \tag{57}
\]
\[
= \text{arg max}_{q_1 \in \mathbb{C}} \left( |h_{rl}|^2 - t|h_{el}|^2 \right) |q_1|^2 + 2 t Re \left\{ \sum_{k \neq l} q_k^* (h_{ek} h_{rl} - h_{*ek} h_{el}) q_1^* \right\}, \tag{58}
\]
\[
= \text{arg max}_{q_1 \in \mathbb{C}} \left( |h_{rl}|^2 - t|h_{el}|^2 \right) |q_1|^2 + 2 \sum_{k \neq l} |q_k^* (h_{ek} h_{rl} - h_{*ek} h_{el})||q_1| \cos(\alpha - \varphi_1), \tag{59}
\]
\[
\langle \varphi_1 = 0 \rangle \arg \max_{|q_1| \leq \sqrt{\bar{P}^*_l}} \left( |h_{rl}|^2 - t|h_{el}|^2 \right) |q_1|^2 + 2 \sum_{k \neq l} |q_k^* (h_{ek} h_{rl} - h_{*ek} h_{el})||q_1|. \tag{60}
\]
where \(\alpha\) and \(\varphi_1\) are phases of \(\sum_{k \in \mathcal{I}} q_k (h_{ek}^* h_{rl} - h_{*ek}^* h_{el})\) and \(q_1\). Since (60) is a quadratic function, a simple curve discussion reveals that the optimum in the interval \([0, \sqrt{\bar{P}_l}]\) is as follows: (i) If \(|h_{rl}|^2 \geq t|h_{el}|^2\) then \(q_1^* = \sqrt{\bar{P}}_l\); (ii) If \(|h_{rl}|^2 < t|h_{el}|^2\) then
\[
|q_1^*| = \min \left\{ \sqrt{\bar{P}}_l, \left| \sum_{k \neq l} q_k (h_{ek}^* h_{rl} - h_{*ek}^* h_{el}) \right| \cos(\alpha) \right\}, \tag{61}
\]
\[
|q_1^*| = \frac{\sum_{k \neq l} q_k (h_{ek}^* h_{rl} - h_{*ek}^* h_{el}) \cos(\alpha)}{|h_{rl}|^2 - t|h_{el}|^2}. \tag{62}
\]
This proves Theorem 5.

ACKNOWLEDGEMENT
We would like to thank Mats Bengtsson for his helpful and insightful comments, in particular regarding the special case of aligned channels, that helped us to greatly improve the quality of the paper. We also would like to thank the anonymous reviewers that helped us to improve our presentation.

REFERENCES


**Phuong Le Cao** (S’13-M’18) received the B.Sc degree in Electronics and Telecommunications Engineering from Danang University of Technology, Vietnam, in 2006, the M.Sc degree in Communications Engineering from YuanZe University, Taiwan, in 2012, and the Ph.D degree in Electrical Engineering from KTH Royal Institute of Technology, Sweden, in 2019. From 2009 to 2013, he was a senior telecommunication engineer at Vinaphone, Vietnam Posts and Telecommunications Group. Since 2018, he has been with Ericsson AB, Sweden. He was the recipient of Outstanding Academic Award from YuanZe University in 2012, Knut and Alice Wallenbergs Foundation Jubilee appropriation - Young Scientists Program in 2015 and 2016, and Ericsson’s Research Foundation Grant in 2017. His research interests include signal processing, wireless communications, communication theory, AI and machine learning.

**Tobias J. Oechtering** (S’01-M’08-SM’12) received his Dipl-Ing degree in Electrical Engineering and Information Technology in 2002 from RWTH Aachen University, Germany, his Dr-Ing degree in Electrical Engineering in 2007 from the Technische Universität Berlin, Germany, and his Docent degree in Communication Theory in 2012 from KTH Royal Institute of Technology. In 2008 he joined the Communication Theory Lab at KTH Royal Institute of Technology, Stockholm, Sweden and has been a Professor since Nov 2018. He is currently Associate Editor of IEEE Transactions on Information Forensic and Security since June 2016 and was editor for IEEE Communications Letters during 2012-2015. Dr. Oechtering received the “Förderpreis 2009 from the Vodafone Foundation. His research interests include communication and information theory, physical layer privacy and security, statistical signal processing, as well as communication for networked control.