Time and Power Allocation for the Gaussian Wiretap Channel with Feedback of Secret Keys

Javier Vía
University of Cantabria. Spain
jvia@gtas.dicom.unican.es

***Abstract*—This paper solves the time and power allocation problem for the simplest feedback scheme for the Gaussian wiretap channel, which is based on the transmission of random secret keys to be used in a one time pad manner. Specifically, the optimal transmission powers at Alice and Bob, as well as the time sharing factor between the feedback and feedforward channels, are given by the solution of a non-convex optimization problem, which is found by means of the golden section algorithm and the sequential solution of several convex optimization problems. Additionally, an specific and highly efficient procedure for the solution of the inner convex optimization problems is provided, which avoids the need for general purpose optimization packages. Finally, several simulation results illustrate the potential secrecy gains achievable with a feedback scheme as simple as the one considered in this paper.**

***Keywords*—Physical Layer Secrecy, Wiretap Channel, One-Time Pad, Feedback, Resource Allocation.**

I. Introduction

During the last years, physical layer security [1], [2] has received increasing interest of the information theory, signal processing, and communications communities, which has already provided many important results [3]–[5]. As an example, one of the fundamental and best understood problems in physical layer security consists in the classical wiretap channel [3], in which an eavesdropper (Eve) aims at intercepting a secret communication between two legitimate parties, the transmitter (Alice) and the receiver (Bob). However, the practical case in which feedback is allowed still presents several difficulties, and only partial information-theoretic results are available [6]–[8]. On the other hand, although the signal processing community has generated many interesting works on the wiretap channel, specially focusing on the case of multiantenna nodes [9]–[11], the gains offered by simple feedback schemes have been underexplored [12], [13].

This paper focuses on the two-way Gaussian wiretap channel with single-antenna nodes, and in a very simple feedback scheme based on the transmission of random secret keys by means of Wyner coding. Specifically, the secret random keys are transmitted over the feedback wiretap channel at a rate not higher than its secrecy capacity. Thus, these secret keys are later used to protect, by means of the one time pad [14], the otherwise insecure messages in the forward wiretap channel [6]. Despite its simplicity, this feedback scheme raises a far from trivial question related to the optimal time and power allocation. In particular, we address the problem of finding the optimal time sharing factor and power allocation between Alice and Bob with the goal of maximizing the overall secrecy rate. As will be seen, the non-convex time and power allocation problem can be solved by means of the golden section algorithm [15] and a sequence of convex optimization problems, which admit a simple solution based on a specific algorithm, thus avoiding the use of general purpose numerical optimization packages [16].

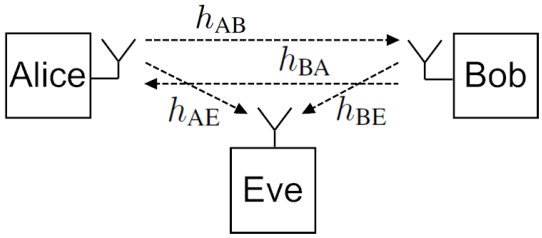

Fig. 1. Wiretap channel with feedback.

II. Preliminaries and Problem Formulation

Consider a wiretap channel [1], [3] as the one illustrated in Fig. 1, with two legitimate single-antenna nodes Alice and Bob, and one single-antenna eavesdropper Eve. When Alice transmits, the signals received by Bob and Eve can be written as

$$x_{\mathrm{B}} = h_{\mathrm{AB}} s_{\mathrm{A}} + n_{\mathrm{B}}, \qquad x_{\mathrm{AE}} = h_{\mathrm{AE}} s_{\mathrm{A}} + n_{\mathrm{AE}}, \tag{1}$$

where n_{B} and n_{AE} are independent circularly symmetric complex Gaussian noise with zero mean and unit variance, s_{A} is the signal transmitted by Alice, and h_{AB} and h_{AE} represent the complex channel from Alice, to Bob and Eve respectively. Analogously, the received signals in the feedback channel (from Bob to Alice) are

$$x_{\mathrm{A}} = h_{\mathrm{BA}} s_{\mathrm{B}} + n_{\mathrm{A}}, \qquad x_{\mathrm{BE}} = h_{\mathrm{BE}} s_{\mathrm{B}} + n_{\mathrm{BE}}, \tag{2}$$

with similar definitions for h_{BA}, h_{BE}, n_{A}, n_{BE} and s_{B}.

This paper addresses the problem of transmitting secret information from Alice to Bob, and is well known that when feedback is not allowed, Alice can transmit secret information at a rate [1]

$$R_{\mathrm{AB}}^{\mathrm{S}} = \left[C(g_{\mathrm{AB}} P_{\mathrm{A}}) - C(g_{\mathrm{AE}} P_{\mathrm{A}}) \right]_+, \tag{3}$$

where $[\cdot]_+ = \max(\cdot, 0)$, $g_{\mathrm{AB}} = |h_{\mathrm{AB}}|^2$, $g_{\mathrm{AE}} = |h_{\mathrm{AE}}|^2$, P_{A} is the transmission power, and $C(p) = \log(1+p)$ is the classical Shannon's capacity. Moreover, Alice can simultaneously transmit a stream of public data, with no guaranteed secrecy, at a rate [6]

$$R_{\mathrm{AB}}^{\mathrm{P}} = C(g_{\mathrm{AB}} P_{\mathrm{A}}) - R_{\mathrm{AB}}^{\mathrm{S}}. \tag{4}$$

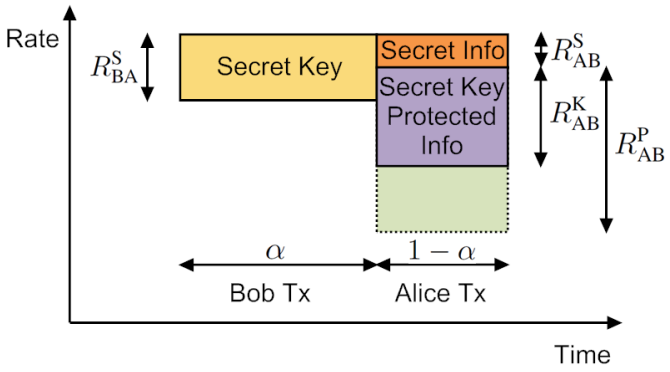

Fig. 2. Proposed secret-key based feedback scheme. During the first stage, Bob sends a secret random message to Alice. In the second stage, this information is used as a secret key in order to protect the message transmitted in an insecure manner.

A. Proposed Scheme

What this paper proposes is a very simple feedback scheme for improving the secrecy rate, which is illustrated in Fig. 2. In particular, the proposed scheme divides the transmission time into the following two stages:

- Stage I: During the first stage, which takes a fraction α of the transmission time, Bob transmits (with power P_{B}) random secret information to Alice at a rate $R^{\mathrm{S}}_{\mathrm{BA}} = [C(g_{\mathrm{BA}}P_{\mathrm{B}}) - C(g_{\mathrm{BE}}P_{\mathrm{B}})]_+$.
- Stage II: During the remaining fraction $(1-\alpha)$ of time, Alice transmits secret information at a rate $R^{\mathrm{S}}_{\mathrm{AB}}$ as well as key-protected public information with rate $R^{\mathrm{K}}_{\mathrm{AB}}$. That is, the secret information transmitted by Bob is used in the second stage as a shared key to protect, by means of the one-time pad [14], the otherwise insecure transmission over the public *channel*.

With the previous description, it is clear that the overall secrecy rate is

$$\overline{R}^{\mathrm{S}}_{\mathrm{AB}} = (1-\alpha)\left(R^{\mathrm{S}}_{\mathrm{AB}} + R^{\mathrm{K}}_{\mathrm{AB}}\right), \tag{5}$$

and obviously, the secret key protected rate is bounded by

$$(1-\alpha)R^{\mathrm{K}}_{\mathrm{AB}} \leq \min\left((1-\alpha)R^{\mathrm{P}}_{\mathrm{AB}}, \alpha R^{\mathrm{S}}_{\mathrm{BA}}\right). \tag{6}$$

That is, the number of secret key protected bits can not exceed the number of key bits, nor the number of bits in the public stream. Finally, we must point out that the proposed scheme can be seen as an adaptation of the technique proposed in [6] for the case of wiretap channels with secure rate-limited feedback. Moreover, although the technique in [6] is information theoretically optimal in the case with secure rate-limited feedback, it is clearly suboptimal in the general setting of wiretap channels with feedback [7], [8], [13]. Therefore, the proposed technique, which from a coding point of view allows us to consider the forward and backward links in an independent manner, can be considered as a benchmark for more sophisticated feedback schemes.

B. Optimization Problem

Considering peak, average and total power constraints, the resource (powers and time sharing factor α) allocation problem to be solved can be written as

$$\begin{aligned}
\underset{P_{\mathrm{A}},P_{\mathrm{B}},\alpha,R^{\mathrm{K}}_{\mathrm{AB}}}{\text{maximize}} \quad & (1-\alpha)R^{\mathrm{S}}_{\mathrm{AB}}(g_{\mathrm{AB}}P_{\mathrm{A}}, g_{\mathrm{AE}}P_{\mathrm{A}}) + (1-\alpha)R^{\mathrm{K}}_{\mathrm{AB}} \\
\text{subject to} \quad & (1-\alpha)R^{\mathrm{K}}_{\mathrm{AB}} \leq \alpha R^{\mathrm{S}}_{\mathrm{BA}}(g_{\mathrm{BA}}P_{\mathrm{B}}, g_{\mathrm{BE}}P_{\mathrm{B}}), \\
& R^{\mathrm{K}}_{\mathrm{AB}} \leq R^{\mathrm{P}}_{\mathrm{AB}}(g_{\mathrm{AB}}P_{\mathrm{A}}, g_{\mathrm{AE}}P_{\mathrm{A}}), \\
& 0 \leq P_{\mathrm{A}} \leq P^{\mathrm{P}}_{\mathrm{A}}, \\
& 0 \leq P_{\mathrm{B}} \leq P^{\mathrm{P}}_{\mathrm{B}}, \\
& (1-\alpha)P_{\mathrm{A}} \leq P^{\mathrm{Av}}_{\mathrm{A}}, \\
& \alpha P_{\mathrm{B}} \leq P^{\mathrm{Av}}_{\mathrm{B}}, \\
& \alpha P_{\mathrm{B}} + (1-\alpha)P_{\mathrm{A}} \leq P^{\mathrm{T}}, \\
& 0 \leq \alpha \leq 1,
\end{aligned} \tag{7}$$

where the dependence of the rates with the powers and channel gains has been made explicit, and where $P^{\mathrm{P}}_{\mathrm{A}}, P^{\mathrm{P}}_{\mathrm{B}}, P^{\mathrm{Av}}_{\mathrm{A}}, P^{\mathrm{Av}}_{\mathrm{B}}$ and P^{T} represent the peak, average and total power constraints, which are fixed parameters.

Despite the non-convexity of problem (7), we will see that it can be efficiently solved by means of the algorithm presented in the next section. However, before presenting the solution of the resource allocation problem, we need to point out some important facts.

Remark 1: It is easy to see that one of the global solutions of (7) satisfies $(1-\alpha)R^{\mathrm{K}}_{\mathrm{AB}} = \alpha R^{\mathrm{S}}_{\mathrm{BA}}$ and accordingly $\overline{R}^{\mathrm{S}}_{\mathrm{AB}} = (1-\alpha)R^{\mathrm{S}}_{\mathrm{AB}} + \alpha R^{\mathrm{S}}_{\mathrm{BA}}$. That is, all the secret key bits will be used in the second stage. This can be directly corroborated by noting that, given a solution of (7) with $(1-\alpha)R^{\mathrm{K}}_{\mathrm{AB}} < \alpha R^{\mathrm{S}}_{\mathrm{BA}}$, one can decrease P_{B} without modifying the objective function nor violating the constraints until $(1-\alpha)R^{\mathrm{K}}_{\mathrm{AB}} = \alpha R^{\mathrm{S}}_{\mathrm{BA}}$. From now on, we will focus on this particular solution (that with the lowest P_{B}), which allows us to rewrite (7) as

$$\begin{aligned}
\underset{P_{\mathrm{A}},P_{\mathrm{B}},\alpha}{\text{maximize}} \quad & (1-\alpha)R^{\mathrm{S}}_{\mathrm{AB}} + \alpha R^{\mathrm{S}}_{\mathrm{BA}} \\
\text{subject to} \quad & \alpha R^{\mathrm{S}}_{\mathrm{BA}} \leq (1-\alpha)R^{\mathrm{P}}_{\mathrm{AB}}, \\
& 0 \leq P_{\mathrm{A}} \leq P^{\mathrm{P}}_{\mathrm{A}}, \\
& 0 \leq P_{\mathrm{B}} \leq P^{\mathrm{P}}_{\mathrm{B}}, \\
& (1-\alpha)P_{\mathrm{A}} \leq P^{\mathrm{Av}}_{\mathrm{A}}, \\
& \alpha P_{\mathrm{B}} \leq P^{\mathrm{Av}}_{\mathrm{B}}, \\
& \alpha P_{\mathrm{B}} + (1-\alpha)P_{\mathrm{A}} \leq P^{\mathrm{T}}, \\
& 0 \leq \alpha \leq 1,
\end{aligned} \tag{8}$$

where, for notational simplicity, we have omitted the dependence of the different rates with the transmission powers.

Remark 2: Since all the rate functions $R^{\mathrm{S}}_{\mathrm{BA}}, R^{\mathrm{S}}_{\mathrm{AB}}, R^{\mathrm{P}}_{\mathrm{AB}}$ are concave on the powers $P_{\mathrm{A}}, P_{\mathrm{B}}$, time sharing does not offer any advantage. That is, it does not make sense to alternate between two (or more) implementations of the proposed scheme with different values of the parameters $P_{\mathrm{A}}, P_{\mathrm{B}}, \alpha$.

Remark 3: The case with $R^{\mathrm{S}}_{\mathrm{BA}} = 0$ ($g_{\mathrm{BA}} \leq g_{\mathrm{BE}}$) results in the trivial solution $\alpha = 0$. Therefore, we can consider without loss of generality $g_{\mathrm{BA}} > g_{\mathrm{BE}}$.

Remark 4: In the case with $R^{\mathrm{S}}_{\mathrm{AB}} = 0$ ($g_{\mathrm{AB}} \leq g_{\mathrm{AE}}$) we have $\alpha R^{\mathrm{S}}_{\mathrm{BA}} = (1-\alpha)R^{\mathrm{P}}_{\mathrm{AB}} = (1-\alpha)C(g_{\mathrm{AB}}P_{\mathrm{A}})$. Moreover, this case can be treated without loss of generality by assuming $g_{\mathrm{AE}} = g_{\mathrm{AB}}$. Thus, from now on we will assume $g_{\mathrm{AE}} \leq g_{\mathrm{AB}}$.

Remark 5: Finally, it is important to note that, in general, the solution of (8) does not necessarily satisfies $\alpha R^{\mathrm{S}}_{\mathrm{BA}} = (1-\alpha)R^{\mathrm{P}}_{\mathrm{AB}}$ (see the example in Fig. 3). Analogously, it is not true that $\alpha = 0$ or $R^{\mathrm{S}}_{\mathrm{BA}} > R^{\mathrm{S}}_{\mathrm{AB}}$ at the solution. These conditions are only satisfied in some particular scenarios, two of which deserve special attention.

1) Scenario 1: Only Peak Power Constraints: In the case with only peak power constraints, the secret and public rates do not depend on α, which makes easy to prove that, if[1] $R^{\mathrm{S}}_{\mathrm{BA}}(g_{\mathrm{BA}}P^{\mathrm{P}}_{\mathrm{B}}, g_{\mathrm{BE}}P^{\mathrm{P}}_{\mathrm{B}}) > R^{\mathrm{S}}_{\mathrm{AB}}(g_{\mathrm{AB}}P^{\mathrm{P}}_{\mathrm{A}}, g_{\mathrm{AE}}P^{\mathrm{P}}_{\mathrm{A}})$, the solution must satisfy $P_{\mathrm{A}} = P^{\mathrm{P}}_{\mathrm{A}}$, $P_{\mathrm{B}} = P^{\mathrm{P}}_{\mathrm{B}}$ and

$$\alpha R^{\mathrm{S}}_{\mathrm{BA}} = (1-\alpha)R^{\mathrm{P}}_{\mathrm{AB}}, \tag{9}$$

which yields

$$\alpha = \frac{R^{\mathrm{P}}_{\mathrm{AB}}}{R^{\mathrm{P}}_{\mathrm{AB}} + R^{\mathrm{S}}_{\mathrm{BA}}}, \tag{10}$$

and

$$\overline{R}^{\mathrm{S}}_{\mathrm{AB}} = R^{\mathrm{S}}_{\mathrm{AB}} + R^{\mathrm{P}}_{\mathrm{AB}}\frac{R^{\mathrm{S}}_{\mathrm{BA}} - R^{\mathrm{S}}_{\mathrm{AB}}}{R^{\mathrm{S}}_{\mathrm{BA}} + R^{\mathrm{P}}_{\mathrm{AB}}}, \tag{11}$$

or equivalently

$$\overline{R}^{\mathrm{S}}_{\mathrm{AB}} = C(g_{\mathrm{AB}}P^{\mathrm{P}}_{\mathrm{A}})\left[\frac{R^{\mathrm{S}}_{\mathrm{BA}}}{R^{\mathrm{S}}_{\mathrm{BA}} + R^{\mathrm{P}}_{\mathrm{AB}}}\right]. \tag{12}$$

Thus, the second term in the right hand side of (11) can be seen as the secrecy rate gain provided by the use of the proposed feedback scheme, whereas the term in brackets in (12) can be interpreted as the penalization on the (conventional) channel capacity due to the presence of an eavesdropper.

2) Scenario 2: Reciprocal Channels with Only a Total Power Constraint: The same conclusion can be reached in the case with reciprocal channels ($g_{\mathrm{AB}} = g_{\mathrm{BA}}$) and only a total power constraint. Basically, the fact of having reciprocal channels implies the monotonicity (with P) of

$$R^{\mathrm{S}}_{\mathrm{BA}}(g_{\mathrm{BA}}P, g_{\mathrm{BE}}P) - R^{\mathrm{S}}_{\mathrm{AB}}(g_{\mathrm{AB}}P, g_{\mathrm{BE}}P). \tag{13}$$

In other words, one of the two links (forward or backward) provides a higher secrecy rate than the other for any power level P. Thus, we can easily conclude that, for $g_{\mathrm{BE}} \leq g_{\mathrm{AE}}$, the global solution satisfies[2]

$$\alpha = \frac{R^{\mathrm{P}}_{\mathrm{AB}}}{R^{\mathrm{P}}_{\mathrm{AB}} + R^{\mathrm{S}}_{\mathrm{BA}}}, \tag{14}$$

and

$$\overline{R}^{\mathrm{S}}_{\mathrm{AB}} = R^{\mathrm{S}}_{\mathrm{AB}} + R^{\mathrm{P}}_{\mathrm{AB}}\frac{R^{\mathrm{S}}_{\mathrm{BA}} - R^{\mathrm{S}}_{\mathrm{AB}}}{R^{\mathrm{S}}_{\mathrm{BA}} + R^{\mathrm{P}}_{\mathrm{AB}}} = C(g_{\mathrm{AB}}P_{\mathrm{A}})\left[\frac{R^{\mathrm{S}}_{\mathrm{BA}}}{R^{\mathrm{S}}_{\mathrm{BA}} + R^{\mathrm{P}}_{\mathrm{AB}}}\right]. \tag{15}$$

[1]The case with $R^{\mathrm{S}}_{\mathrm{BA}}(g_{\mathrm{BA}}P^{\mathrm{P}}_{\mathrm{B}}, g_{\mathrm{BE}}P^{\mathrm{P}}_{\mathrm{B}}) \leq R^{\mathrm{S}}_{\mathrm{AB}}(g_{\mathrm{AB}}P^{\mathrm{P}}_{\mathrm{A}}, g_{\mathrm{AE}}P^{\mathrm{P}}_{\mathrm{A}})$ results in the trivial solution $\alpha = P_{\mathrm{B}} = 0$, $P_{\mathrm{A}} = P^{\mathrm{P}}_{\mathrm{A}}$

[2]Note that unlike the case with only peak power constraints, eqs. (14) and (15) are based on rates depending on the final power allocation. Note also that the trivial case with $g_{\mathrm{BE}} \geq g_{\mathrm{AE}}$, or equivalently $R^{\mathrm{S}}_{\mathrm{BA}}(g_{\mathrm{BA}}P, g_{\mathrm{BE}}P) \leq R^{\mathrm{S}}_{\mathrm{AB}}(g_{\mathrm{AB}}P, g_{\mathrm{AE}}P)$, again results in $\alpha = 0$ and $P_{\mathrm{A}} = P^{\mathrm{T}}$.

Algorithm 1 Golden Section Algorithm for the solution of the time and power allocation problem.

Input: Channel gains $g_{\mathrm{AB}}, g_{\mathrm{BA}}, g_{\mathrm{AE}}, g_{\mathrm{BE}}$, power constraints $P^{\mathrm{P}}_{\mathrm{A}}, P^{\mathrm{P}}_{\mathrm{B}}, P^{\mathrm{Av}}_{\mathrm{A}}, P^{\mathrm{Av}}_{\mathrm{B}}, P^{\mathrm{T}}$, and precision γ.
Output: Optimal time sharing factor α and powers P_{A}, P_{B}.
Initialize: $\phi = 1 + \frac{1-\sqrt{5}}{2}$, and $M = \frac{\log\gamma}{\log(1-\phi)}$.
Evaluate (by solving (17)) $\overline{R}^{\mathrm{S}}_{\mathrm{AB}}(\alpha)$ at $\alpha_{\min} = 0$, $\alpha_1 = \phi$, $\alpha_2 = 1-\phi$, and $\alpha_{\max} = 1$.
for $t = 1, \ldots, M$ **do**
  if the maximum evaluated $\overline{R}^{\mathrm{S}}_{\mathrm{AB}}(\alpha)$ is at α_2 or $\alpha_{\max}$ **then**
    Set $\alpha_{\min} = \alpha_1$, and update $\alpha_1 = \alpha_2$.
    Update $\alpha_2 = \phi\alpha_{\min} + (1-\phi)\alpha_{\max}$.
  else
    Set $\alpha_{\max} = \alpha_2$, and update $\alpha_2 = \alpha_1$.
    Update $\alpha_1 = (1-\phi)\alpha_{\min} + \phi\alpha_{\max}$.
  end if
  Evaluate $\overline{R}^{\mathrm{S}}_{\mathrm{AB}}(\alpha)$ at the new evaluation point, and obtain P_{A} and P_{B} by solving (17).
end for

III. Solution of the General Time and Power Allocation Problem

This section presents the general solution to problem (8). In particular, let us start by noting that, although (7) is not jointly convex on $P_{\mathrm{A}}, P_{\mathrm{B}}, \alpha, R^{\mathrm{K}}_{\mathrm{AB}}$, it is convex on $P_{\mathrm{A}}, P_{\mathrm{B}}, R^{\mathrm{K}}_{\mathrm{AB}}$ for a fixed α. Therefore, problem (7) can be reformulated as

$$\begin{aligned} \underset{\alpha}{\text{maximize}} \quad & \overline{R}^{\mathrm{S}}_{\mathrm{AB}}(\alpha) \\ \text{subject to} \quad & 0 \leq \alpha \leq 1, \end{aligned} \tag{16}$$

where $\overline{R}^{\mathrm{S}}_{\mathrm{AB}}(\alpha)$ is the optimal value of the convex optimization problem

$$\begin{aligned} \underset{P_{\mathrm{A}}, P_{\mathrm{B}}, R^{\mathrm{K}}_{\mathrm{AB}}}{\text{maximize}} \quad & (1-\alpha)R^{\mathrm{S}}_{\mathrm{AB}}(g_{\mathrm{AB}}P_{\mathrm{A}}, g_{\mathrm{AE}}P_{\mathrm{A}}) + (1-\alpha)R^{\mathrm{K}}_{\mathrm{AB}} \\ \text{subject to} \quad & (1-\alpha)R^{\mathrm{K}}_{\mathrm{AB}} \leq \alpha R^{\mathrm{S}}_{\mathrm{BA}}(g_{\mathrm{BA}}P_{\mathrm{B}}, g_{\mathrm{BE}}P_{\mathrm{B}}), \\ & R^{\mathrm{K}}_{\mathrm{AB}} \leq R^{\mathrm{P}}_{\mathrm{AB}}(g_{\mathrm{AB}}P_{\mathrm{A}}, g_{\mathrm{AE}}P_{\mathrm{A}}), \\ & 0 \leq P_{\mathrm{A}} \leq \bar{P}_{\mathrm{A}}, \\ & 0 \leq P_{\mathrm{B}} \leq \bar{P}_{\mathrm{B}}, \\ & \alpha P_{\mathrm{B}} + (1-\alpha)P_{\mathrm{A}} \leq P^{\mathrm{T}}, \end{aligned} \tag{17}$$

with $\bar{P}_{\mathrm{A}} = \min\left(P^{\mathrm{P}}_{\mathrm{A}}, P^{\mathrm{Av}}_{\mathrm{A}}/(1-\alpha)\right)$ and $\bar{P}_{\mathrm{B}} = \min\left(P^{\mathrm{P}}_{\mathrm{B}}, P^{\mathrm{Av}}_{\mathrm{B}}/\alpha\right)$. Furthermore, taking into account the second remark in Subsection II-B, and invoking standard convexity results, it is easy to show that $\overline{R}^{\mathrm{S}}_{\mathrm{AB}}(\alpha)$ is concave in $\alpha \in [0,1]$. Therefore, the solution of (16) can be obtained by means of the Golden Section Algorithm [15], which is summarized in Algorithm 1.

A. Solution for Fixed α (Inner Optimization Problem)

As previously pointed out, problem (17) is convex, and can be solved by standard convex optimization tools [16], [17]. However, further insight can be obtained by carefully analyzing the optimization problem. In particular, taking into account the first remark in Subsection II-B, we can rewrite

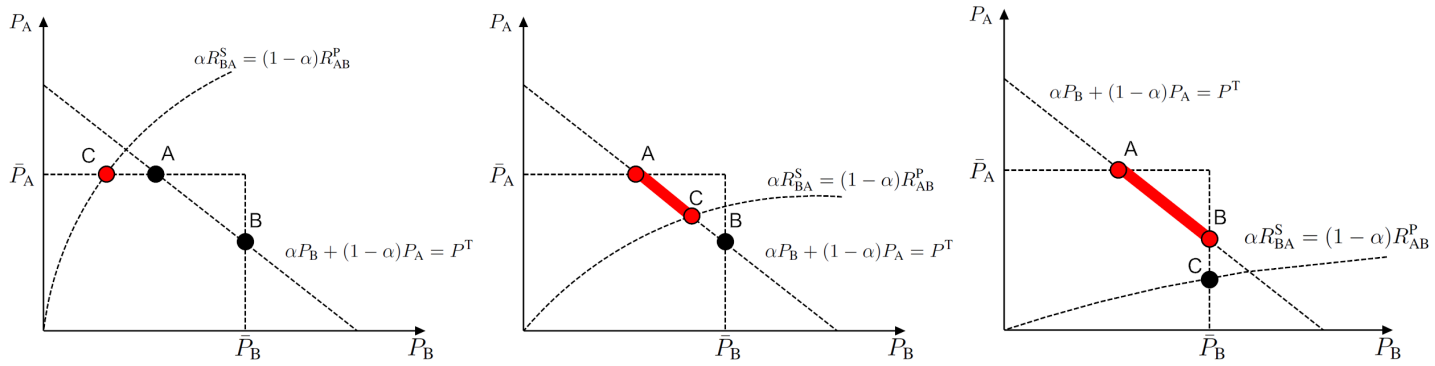

Fig. 3. Geometrical interpretation for the solution of problem (18). Dashed lines represents each one of the four constraints and the objective function is nondecreasing and concave in $P_{\rm A}$ and $P_{\rm B}$. Left: When point C is to the left of point A, C is the solution. Center: When point C is in the segment AB, the solution belongs to the segment AC. Right: If C is below B, the solution belongs to segment AB. Note that in this last scenario, the solution does not satisfy $\alpha R^{\rm S}_{\rm BA} = (1-\alpha) R^{\rm P}_{\rm AB}$.

(17) as

$$\begin{aligned} \underset{P_{\rm A}, P_{\rm B}}{\text{maximize}} \quad & (1-\alpha) R^{\rm S}_{\rm AB} + \alpha R^{\rm S}_{\rm BA} \\ \text{subject to} \quad & \alpha R^{\rm S}_{\rm BA} \leq (1-\alpha) R^{\rm P}_{\rm AB}, \\ & 0 \leq P_{\rm A} \leq \bar{P}_{\rm A}, \\ & 0 \leq P_{\rm B} \leq \bar{P}_{\rm B}, \\ & \alpha P_{\rm B} + (1-\alpha) P_{\rm A} \leq P^{\rm T}. \end{aligned} \tag{18}$$

Fortunately, problem (18) admits a simple geometrical interpretation, which is illustrated in Figure 3 and allows us to solve the optimization problem in a very simple manner. In particular, taking into account that the objective function is nondecreasing and concave in $P_{\rm A}$ and $P_{\rm B}$, the problem practically reduces to find the set of active constraints, which can be easily done by means of the following steps:

1) Let us start by checking whether the first two constraints are active. In order to do so, we just need to set $P_{\rm A} = \bar{P}_{\rm A}$ and $P_{\rm B} = \frac{P^{\rm T} - (1-\alpha)\bar{P}_{\rm A}}{\alpha}$, which is represented by point A in Fig. 3, and check whether $\alpha R^{\rm S}_{\rm BA} \geq (1-\alpha) R^{\rm P}_{\rm AB}$, i.e.

$$(1-\alpha)\log(1+g_{\rm AE}P_{\rm A}) \leq \alpha \log\left(\frac{1+g_{\rm BA}P_{\rm B}}{1+g_{\rm BE}P_{\rm B}}\right). \tag{19}$$

If the previous condition is satisfied, the two first constraints of (18) are active at the solution (point C in Fig. 3), which is given by

$$P_{\rm A} = \bar{P}_{\rm A}, \qquad P_{\rm B} = \frac{x-1}{g_{\rm BA} - g_{\rm BE}x}, \tag{20}$$

with $x = (1+g_{\rm AE}\bar{P}_{\rm A})^{(\alpha^{-1}-1)}$.

2) If condition (19) is not satisfied, the total power constraint is active at the solution. Therefore, $P_{\rm B}$ can be rewritten as $P_{\rm B} = \frac{P^{\rm T} - (1-\alpha)P_{\rm A}}{\alpha}$, which reduces (18) to the following one-dimensional convex optimization problem

$$\begin{aligned} \underset{P_{\rm A}}{\text{maximize}} \quad & (1-\alpha) R^{\rm S}_{\rm AB}(P_{\rm A}) + \alpha R^{\rm S}_{\rm BA}(P_{\rm A}) \\ \text{subject to} \quad & \tilde{P}_{\rm A} \leq P_{\rm A} \leq \bar{P}_{\rm A}, \end{aligned} \tag{21}$$

where the dependence of the objective function with $P_{\rm A}$ has been pointed out, and where $\tilde{P}_{\rm A}$ (which establishes the lower-right extreme of the red segment in Fig. 3) is the minimum value of $P_{\rm A}$ satisfying the first and third constraints in (18). Obviously, the previous problem can be easily solved, for instance, by means of bisection on the derivative of the concave objective function.

IV. Numerical Results

In this section, some numerical results illustrate the performance of the proposed key-based feedback scheme for secrecy. All the results are based on the averaged secrecy rates obtained from 10^5 independent simulations of a scenario with reciprocal standard Rayleigh channels ($h_{\rm AB} = h_{\rm BA}$), and where the eavesdropper channels are independent Rayleigh channels with variances $\beta\phi$ for $h_{\rm AE}$ and $\beta(1-\phi)$ for $h_{\rm BE}$. In this manner, parameter β controls the average quality of the eavesdropper channels, whereas ϕ controls the relative quality between the wiretap channel to Alice and Bob, i.e., a value of ϕ close to zero can represent a scenario with an eavesdropper much closer to Bob, whereas $\phi \simeq 1$ represents a scenario with an eavesdropper closer to Alice. The power constraint parameters have been defined as $P^{\rm P}_{\rm A} = P^{\rm P}_{\rm B} = 2P^{\rm T}$, $P^{\rm Av}_{\rm A} = P^{\rm Av}_{\rm B} = 0.7P^{\rm T}$, and $P^{\rm T}$ is used to control the overall SNR.

The first experiment evaluates the averaged secrecy rate for $\beta = 0.5$ and different SNRs and ϕ values. The results are shown in Fig. 4, where we can see that, excluding the case in which the eavesdropper channel to Bob is very good, the use of feedback provides a significative gain in the averaged secrecy rates. As expected, the gap between the schemes with and without feedback increases with ϕ.

The second experiment evaluates the averaged secrecy rate for a constant $\phi = 0.5$ and different values of the overall eavesdropper channel quality factor β. As can be seen in Fig. 5, the feedback based scheme clearly provides an important increase of the averaged secrecy rates for different values of β.

Finally, the impact of the parameter ϕ is again illustrated in Fig. 6, where we can see that the worst value of ϕ for the feedback scheme is around 0.5, whereas the worst performance of the scheme without feedback is obtained for $\phi = 1$. In a practical setting with feedback, this suggests that an

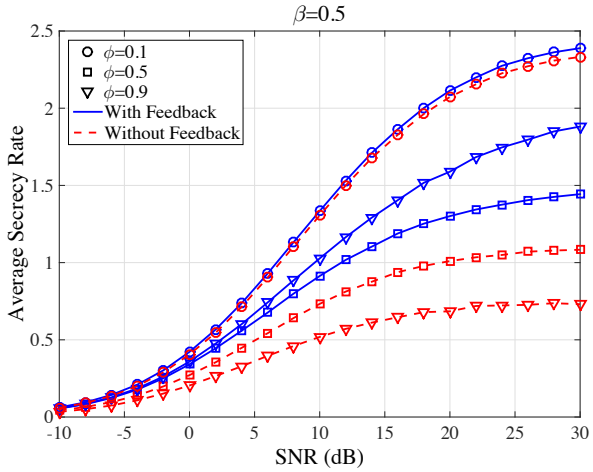

Fig. 4. Averaged secrecy rates for $\beta = 0.5$ and different values of ϕ.

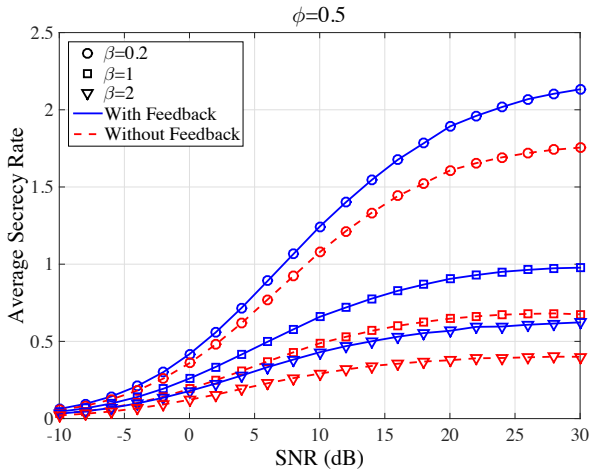

Fig. 5. Averaged secrecy rates for $\phi = 0.5$ and different values of β.

eavesdropper can not gain anything by getting closer to the information transmitting node.

V. Conclusions

In a wiretap channel with feedback, a simple and practical feedback scheme is based on the preliminary transmission of a secret key, to be used in a one time pad manner for the transmission of secret information. This paper has addressed the problem of time and power allocation in a general single antenna scenario with peak, average, and total power constraints. The solution of the non-convex optimization problem can be efficiently found by solving a sequence of convex optimization problems and applying the Golden Section algorithm. Furthermore, a specific algorithm for the inner convex optimization problem is presented, and several simulation results illustrate the secrecy gains achievable with a feedback scheme as simple as the one proposed in this paper.

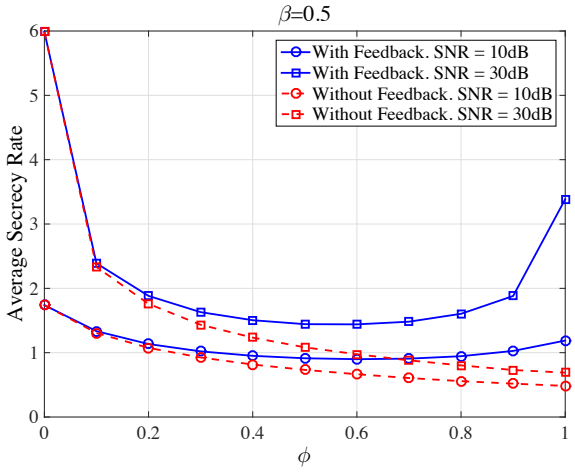

Fig. 6. Averaged secrecy rate as a function of ϕ for $\beta = 0.5$.

References

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

[2] L. Sankar, W. Trappe, H. Poor, and M. Debbah, "Signal processing for cybersecurity and privacy [from the guest editors]," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 14–15, 2013.

[3] A. Wyner, "The wire-tap channel," *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[4] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas - part I: The MISOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, 2010.

[5] ——, "Secure transmission with multiple antennas - part II: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[6] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, "Wiretap channel with secure rate-limited feedback," *IEEE Transactions on Information Theory*, vol. 55, no. 12, pp. 5353–5361, Dec 2009.

[7] X. He and A. Yener, "The role of feedback in two-way secure communications," *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 8115–8130, Dec 2013.

[8] A. El Gamal, O. Koyluoglu, M. Youssef, and H. El Gamal, "Achievable secrecy rate regions for the two-way wiretap channel," *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 8099–8114, Dec 2013.

[9] Q. Li and W. K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Transactions on Signal Processing*, vol. 59, no. 8, pp. 3799–3812, 2011.

[10] A. Mukherjee and A. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 351–361, 2011.

[11] S. Fakoorian and A. Swindlehurst, "Full rank solutions for the MIMO Gaussian wiretap channel with an average power constraint," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2620–2631, 2013.

[12] G. Zheng, I. Krikidis, J. Li, A. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4962–4974, Oct 2013.

[13] B. Yang, W. Wang, Q. Yin, and J. Fan, "Secret wireless communication with public feedback by common randomness," *IEEE Wireless Communications Letters*, vol. 3, no. 3, pp. 269–272, June 2014.

[14] C. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct 1949.

[15] J. Kiefer, "Sequential minimax search for a maximum," *Proceedings of the American Mathematical Society*, vol. 4, no. 3, pp. pp. 502–506, 1953. [Online]. Available: http://www.jstor.org/stable/2032161

[16] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 1.21," http://cvxr.com/cvx, Dec. 2010.

[17] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, March 2004.