On the Ergodic Secrecy Capacity of the Wiretap Channel under Imperfect Main Channel Estimation

Zouheir Rezki
Electrical Engineering Program
Physical Science and Engineering Division
King Abdullah University of Science and Technology (KAUST)
Thuwal, Mekkah Province, Saudi Arabia
zouheir.rezki@kaust.edu.sa

Ashish Khisti
Electrical and Computer Engineering Department
University of Toronto
Toronto, ON, Canada
akhisti@comm.utoronto.ca

Mohamed-Slim Alouini
Electrical Engineering Program
Physical Science and Engineering (PSE) Division
King Abdullah University of Science and Technology (KAUST)
Thuwal, Mekkah Province, Saudi Arabia
slim.alouini@kaust.edu.sa

***Abstract*—The ergodic secrecy capacity of the wiretap channel is known when the main channel (between the transmitter and the legitimate receiver) state information (CSI) is perfect at the transmitter and the coherence period is sufficiently large to enable random coding arguments in each block. In a fast fading scenario, when the codeword length spans many coherence periods, the secrecy capacity is still not known. In this paper, we present a framework that characterizes this secrecy capacity under imperfect main channel estimation at the transmitter. Inner and outer bounds on the ergodic secrecy capacity are derived for a class of independent identically distributed (i.i.d.) fading channels. The achievable rate is a simple on-off scheme using a Gaussian input. The upper bound is obtained using an appropriate correlation scheme of the main and the eavesdropper channels. The upper and the lower bounds coincide with recently derived ones in the perfect main CSI extreme. Furthermore, the lower bound matches the upper bound in no main CSI extreme, where the secrecy capacity is equal to zero. Numerical results are provided for independent identically distributed (i.i.d.) Rayleigh fading channels.**

***Index Terms*—Secrecy capacity, imperfect channel estimation, on-off signaling.**

I. Introduction

The wire-tap channel, in which a source communicates with a receiver through a discrete, memoryless channel (DMC) and a wire-taper observes the output of this channel via another DMC, has been introduced by Wyner [1]. In this seminal work, it has been shown that if the capacity of the main channel is greater than the capacity of the wire-tapper one, then there exists a encoding-decoding scheme such that reliable communication with perfect-secrecy is possible (without the use of any encryption key). In a slightly similar framework, Leung-Yan-Cheong and Hellman have characterized the secrecy-capacity and the achievable rate-equivocation region for the Gaussian Wire-tap channel with additive noise [2]. Later on, Csiszar generalized Wyner's wire-tap channel by considering a non-degraded broadcast channel with confidential messages [3]. In a more practical purpose, secrecy-capacity-achieving codes have been proposed for some specific wire-tap channels in [4]. Several other papers have discussed practical and theoretical aspects of perfectly secure communication in cryptographic and/or information-theoretic point of views over Gaussian wire-tap, broadcast and multiple access channels, e.g., [5]–[11].

Motivated by these positive previous results, many other authors have recently addressed the impact of fading on secure communications. Intuitively, fading generally increases the randomness of the channel input and it is therefore not surprising that fading may help improve communication security. Indeed, it has been shown in, e.g., [12]–[14] that in a quasi-static fading channel and in contrast to the Gaussian channel, secure communication is possible even if the average signal-to-noise ratio (SNR) of the main channel is less than that of the wire-tapper (or one of the wire-tappers in a multiple eavesdroppers case as discussed in [15]). Moreover, if a high level of outage is to be tolerated, then the outage secrecy rate of the fading channel can even be higher than the secrecy capacity of the Gaussian wire-tap channel for similar average SNR levels. The effect of fading on secure communication for single-antenna wire-tap and broadcast channels has also been studied in [16]–[18] where the secrecy-capacity along with the optimal power allocation and/or rate-adaptation strategies at the source have been derived under different channel state information (CSI) assumptions. The secrecy-capacity of a deterministic multiple-antenna wire-tap channel has been studied recently in [19], [20]. The effect of multiple antennas in enhancing the security capability of a wireless link has also been addressed in [21] in terms of low probability of intercept and low probability of detection constraints. Finally, the secret diversity-multiplexing tradeoff of a multiple-antenna wire-tap channel has been investigated in [22].

To the best of our knowledge, the secrecy capacity in a fast fading scenario, when the codeword length spans many coherence periods, is still not known, even with perfect main CSI at the transmitter. However, upper and lower bounds have been reported in [23]. In this paper, we study the secrecy capacity of fast fading channels under imperfect main channel estimation at the transmitter. More precisely, we assume that the main and the eavesdropper channels are independent identically distributed (i.i.d.), ergodic and stationary processes, with continuous and bounded probability density functions (PDF), and that the transmitter, in addition to the statistics of both channels, is also provided an estimated value of the instantaneous main channel gain, whereas the legitimate and the wiretap receivers are perfectly aware of their respective

This work was conducted when Zouheir Rezki was visiting University of Toronto and was supported by KAUST Collaboration Travel Fund (CTF).

$$\underset{|\mathbf{h}|^2,|\mathbf{g}|^2,|\hat{\mathbf{h}}|^2\geq\tau_0}{\mathbf{E}}\left[\log\left(\frac{1+P_0(\tau_0)\,|\mathbf{h}|^2}{1+P_0(\tau_0)\,|\mathbf{g}|^2}\right)\right]\leq C_s\leq\max_{P(\hat{\mathbf{h}})}\underset{\hat{\mathbf{h}},\tilde{\mathbf{h}}}{\mathbf{E}}\left[\log\left(\frac{1+P(\hat{\mathbf{h}})|\sqrt{1-\alpha}\,\hat{\mathbf{h}}+\sqrt{\alpha}\,\tilde{\mathbf{h}}|^2}{1+P(\hat{\mathbf{h}})|\tilde{\mathbf{h}}|^2}\right)\right]^{+} \tag{3}$$

$$\underset{|\mathbf{h}|^2,|\hat{\mathbf{h}}|^2\geq\tau}{\mathbf{E}}\left[\frac{P_0^{'}(\tau_0)\,|\mathbf{h}|^2}{1+P_0(\tau_0)\,|\mathbf{h}|^2}\right]-\underset{|\mathbf{g}|^2}{\mathbf{E}}\left[\frac{P_0^{'}(\tau_0)\,|\mathbf{g}|^2}{1+P_0(\tau_0)\,|\mathbf{g}|^2}\right]\left(1-F_{|\hat{\mathbf{h}}|^2}(\tau_0)\right)-f_{|\hat{\mathbf{h}}|^2}(\tau_0)\left(\underset{|\mathbf{h}|^2||\hat{\mathbf{h}}|^2}{\mathbf{E}}\left[\log\left(1+P_0(\tau_0)\,|\mathbf{h}|^2\right)\mid|\hat{\mathbf{h}}|^2=\tau_0\right]-\underset{|\mathbf{g}|^2}{\mathbf{E}}\left[\log\left(1+P_0(\tau_0)\,|\mathbf{g}|^2\right)\right]\right)= \tag{4}$$

channel gains. In the previous setting, we present:

- Upper and lower bounds on the secrecy capacity;
- Asymptotic analysis at high-SNR regime, together with the perfect and no main CSI extremes.

The organization of this paper is as follows. Section II introduces our system model, followed by our main result along with its proof in section III. In section IV, asymptotic analysis is presented. Section V contains a summary of our results when applied to Rayleigh fading channels which we use in order to provide numerical results in section VI. Finally, section VII concludes the paper.

II. System Model

We consider a discrete-time memoryless wire-tap channel consisting of a transmitter, a legitimate receiver and an eavesdropper. Each terminal is equipped with a single antenna, i.e., a single-input single-output single-eavesdropper (SISOSE) case. The outputs at both the legitimate destination and the eavesdropper, at time coherence period i, $i=1,\ldots,L$, are expressed, respectively by:

$$\begin{cases}\mathbf{y}(i)=\mathbf{h}(i)\mathbf{x}(i)+\mathbf{v}(i)\\ \mathbf{z}(i)=\mathbf{g}(i)\mathbf{x}(i)+\mathbf{w}(i),\end{cases} \tag{1}$$

where $\mathbf{x}(i)\in\mathbb{C}$ is the transmitted signal, and $\mathbf{h}(i)\in\mathbb{C}$, $\mathbf{g}(i)\in\mathbb{C}$ are zero-mean and unit-variance channel gains that represent the main channel and the eavesdropper channel, respectively; and $\mathbf{v}(i)\in\mathbb{C}$, $\mathbf{w}(i)\in\mathbb{C}$ are zero-mean, unite-variance circularly symmetric white Gaussian noises. The channel gains $\mathbf{h}$ and $\mathbf{g}$ are assumed to be i.i.d., ergodic and stationary with bounded and continuous PDF's. We assume perfect CSI at the receiver sides. That is, the legitimate and the eavesdropper receivers knows the instantaneous channel realizations h(i) and g(i). However, the transmitter is not aware about the channel realization g(i) and is only provided a noisy version of $\mathbf{h}(i)$, say $\check{\mathbf{h}}(i)$, obtained via a band manager that coordinates the main channel, or through a feedback link, such that $f_{\mathbf{h}|\check{\mathbf{h}}}(h|\check{h})$ is also known. In order to improve its instantaneous estimate of $\mathbf{h}(l)$, the secondary transmitter further performs minimum mean square error (MMSE) estimation to obtain $\hat{\mathbf{h}}(l)=\mathbf{E}\left[\mathbf{h}(l)\mid\check{\mathbf{h}}(l)=\check{h}(l)\right]$. Note that to compute the MMSE estimate, the secondary transmitter needs to know the conditional PDF of $\mathbf{h}(l)$ given $\check{\mathbf{h}}(l)$, which it does. Therefore, the main channel estimation model can be written as:

$$\mathbf{h}(l)=\sqrt{1-\alpha}\,\hat{\mathbf{h}}(l)+\sqrt{\alpha}\,\tilde{\mathbf{h}}(l), \tag{2}$$

where $\tilde{\mathbf{h}}(l)$ is the zero-mean unit-variance MMSE channel estimation error and α is the MMSE error variance ($\alpha\in(0,1)$). By well-known properties of the conditional mean, $\hat{\mathbf{h}}(l)$ and $\tilde{\mathbf{h}}(l)$ are uncorrelated. For simplicity, we also assume that $\hat{\mathbf{h}}(l)$ and $\tilde{\mathbf{h}}(l)$ are identically distributed as $\mathbf{h}(l)$. Furthermore, since the channel and the estimation models defined in (1) and (2), respectively, are stationary and memoryless, the statistics of the capacity achieving input $x(l)$ are also memoryless and i.i.d.. Therefore, for simplicity we may drop the time index l in (1) and (2). Finally, the source is constrained according to an average power constraint:

$$\mathbf{E}[|\mathbf{x}|^2]\leq P_{avg},$$

where the expectation is over the input distribution.

III. Ergodic Capacity

In this section, our main result is presented in Theorem 1, followed by the proof.

Theorem 1: An inner and an outer bounds on the secrecy capacity of the discrete-time memoryless channel described by (1), under imperfect main channel estimation (2), are given by (3) at the top of the page, where $P_0(\tau)=\frac{P_{avg}}{1-F_{|\hat{\mathbf{h}}|^2}(\tau)}$ and where τ_0 is a solution of (4) also at the top of the page, where $P_0^{'}(\tau)$ is the derivative of $P_0(\tau)$ with respect to τ .

Proof:

- Achievability:

To achieve the left hand side (LHS) in (3), the encoder uses a fixed rate Gaussian codebook, and then the power is instantaneously adapted according to the channel estimation value. For simplicity, an on-off power scheme is adopted, i.e.,

$$P(\hat{\mathbf{h}})=\begin{cases}P_0(\tau) & \left|\hat{\mathbf{h}}\right|^2\geq\tau\\ 0 & \text{otherwise}\end{cases}$$

Details of the achievability are described below. For convenience, let R_s be the LHS in (3) and $R_e=\underset{|\mathbf{g}|^2,|\hat{\mathbf{h}}|^2\geq\tau_0}{\mathbf{E}}\left[\log\left(1+P_0(\tau_0)\,|\mathbf{g}|^2\right)\right]$. Then, to achieve R_s, the encoder forms $2^{L(R_s-\epsilon_1)}$ sub-codebooks, C_w, each sub-codebook C_w is associated to a secret message w, $w=1,\ldots,2^{LR_s}$, and consists of $2^{L(R_e-\epsilon_2)}$ Gaussian codewords of length L symbols drawn from $\mathcal{CN}\left(0,P_{avg}\right)$, for small ϵ_1 and small ϵ_2. To encode a message w, a codeword $x^{(L)}$ is chosen uniformly at random from C_w and is transmitted through the channel, during L time coherence periods. By a random coding argument, it can be shown that there exists at least one such a codebook with an arbitrary small error probability P_e and with the equivocation rate R_e arbitrary close to R_s, as $L\to\infty$ [1], [24, Section II.B]. To complete the proof, the LHS of (3), a differentiable function in τ, is maximized over all positive τ values, and the optimum

τ_0 is a obtained by solving (4), a differentiation of the LHS of (3) with respect to τ.

- Outer bound

The following upper bound on the secrecy capacity has been established, e.g., [20], [23]:

$$C_s \le \min_{p_{\mathbf{y}',\mathbf{z}',\mathbf{h}',\mathbf{g}'|\mathbf{x}}} \max_{p_{\mathbf{x}}} I\left(\mathbf{x};\mathbf{y}' \mid \mathbf{z}',\mathbf{g}',\mathbf{h}'\right), \tag{5}$$

for any joint conditional $p_{\mathbf{y}',\mathbf{z}',\mathbf{h}',\mathbf{g}'|\mathbf{x}}$ that satisfies: $p_{\mathbf{y}',\mathbf{h}'|\mathbf{x}} = p_{\mathbf{y},\mathbf{h}|\mathbf{x}}$ and $p_{\mathbf{z}',\mathbf{g}'|\mathbf{x}} = p_{\mathbf{z},\mathbf{g}|\mathbf{x}}$. Since $p_{\mathbf{y}',\mathbf{z}',\mathbf{h}',\mathbf{g}'|\mathbf{x}} = p\left(\mathbf{v}',\mathbf{w}'\right)p\left(\mathbf{h}',\mathbf{g}' \mid \mathbf{x}\right)$, where $\mathbf{v}'$ and $\mathbf{w}'$ are identically distributed as $\mathbf{v}$ and $\mathbf{w}$, respectively; then correlating $\mathbf{v}'$ and $\mathbf{w}'$ such that $\mathbf{E}\left[\mathbf{v}'^{*}\mathbf{w}'\right] = argmin(|h|,|g|)/argmax(|h|,|g|)$[1] and using the fact that a Gaussian input achieves the inner maximum in (5), the following upper bound on the RHS of (5) holds:

$$C_s \le \min_{p(\mathbf{h}',\mathbf{g}'|\mathbf{x})} \max_{P(\hat{\mathbf{h}}')} \mathop{\mathbf{E}}_{\mathbf{h}',\mathbf{g}',\hat{\mathbf{h}}'} \left[\log\left(\frac{1+P\left(\hat{\mathbf{h}}'\right)|\mathbf{h}'|^2}{\left(1+P\left(\hat{\mathbf{h}}'\right)|\mathbf{g}'|^2\right)}\right)\right]^{+}. \tag{6}$$

Finally, since $\tilde{\mathbf{h}}$ is identically distributed as $\mathbf{g}$, and since the transmitter is only aware of $\hat{\mathbf{h}}$, then $\tilde{\mathbf{h}}$ is independent of the $\mathbf{x}$ and thus $\left(\mathbf{h}',\mathbf{g}'\right) = \left(\mathbf{h},\tilde{\mathbf{h}}\right)$ is a valid choice that provides an upper bound on (6) which yields the outer bound in (3). ■

It is worth mentioning that in our proof of the upper bound, the choice $\left(\mathbf{h}',\mathbf{g}'\right) = \left(\mathbf{h},\tilde{\mathbf{h}}\right)$ has the following interpretation. In order to reduce its equivocation, the eavesdropper "sticks" to the component of the main channel that is unknown to the transmitter. When specialized to the case of perfect main CSI, our upper bound coincides with the tightest known upper bound [16], [23]. However our lower bound is not the best possible one when specialized to the perfect CSI case. Developing better lower bounds remains an interesting open problem in our proposed setup. Although the inner and the outer bounds do not generally coincide, they provide, to the best of our knowledge, the best available characterization of the secrecy capacity over i.i.d. fading channels that accounts for imperfect main channel estimation at the transmitter. Note also that since the right hand side (RHS) of (3) is concave, the maximum can be found by deriving the optimum power profile $P(\hat{h})$ using the Lagrange approach. That is, the optimal power profile is the solution of the following optimality condition:

$$\mathop{\mathbf{E}}_{\tilde{\mathbf{h}}\in D_{\hat{h}}}\left[\frac{|\sqrt{1-\alpha}\,\hat{h}+\sqrt{\alpha}\,\tilde{\mathbf{h}}|^2}{1+P(\hat{h})|\sqrt{1-\alpha}\,\hat{h}+\sqrt{\alpha}\,\tilde{\mathbf{h}}|^2} - \frac{|\tilde{\mathbf{h}}|^2}{1+P(\hat{h})|\tilde{\mathbf{h}}|^2}\right] - \lambda = 0, \tag{7}$$

where $D_{\hat{h}}$ is the set defined by: $D_{\hat{h}} = \left\{\tilde{h} = \tilde{\rho}e^{i\tilde{\theta}} \;\middle|\; \tilde{\rho} \le \frac{\hat{\rho}}{\rho_0(\hat{\theta}-\tilde{\theta})}\right\}$, where $\hat{h} = \hat{\rho}e^{i\hat{\theta}}$, $\rho_0(t) = \frac{\sqrt{(1-\alpha)(\alpha\cos(t)^2-\alpha+1)}-\sqrt{\alpha(1-\alpha)}\cos(t)}{1-\alpha}$, and where λ is the Lagrange multiplier corresponding to the average power constraint. If for a particular value of $\hat{h}$, there is no positive solution $P\left(\hat{h}\right)$ for (7), then the instantaneous power is set to zero, i.e., $P\left(\hat{h}\right) = 0$.

[1]The function $argmin(|a|,|b|)$ is defined as follows: $argmin(|a|,|b|) = a$ if $|a| \ge |b|$, otherwise $argmin(|a|,|b|) = b$. Analogously is defined $argmax(|a|,|b|)$.

IV. Asymptotic Analysis

It is of interest to use Theorem 1 in order to obtain useful insights in some interesting asymptotic cases. Below, we analyze the secrecy capacity at high-SNR (SNR $\to \infty$), together with the perfect main CSI ($\alpha \to 0$) and no main CSI ($\alpha \to 1$).

A. High-SNR Regime

Our result is summarized in Corollary 1.

Corollary 1: At high-SNR, the secrecy capacity C_s^{∞} is bounded by:

$$\mathop{\mathbf{E}}_{|\mathbf{h}|^2,|\mathbf{g}|^2,|\hat{\mathbf{h}}|^2\ge\tau_0}\left[\log\left(\left|\frac{\mathbf{h}}{\mathbf{g}}\right|^2\right)\right] \le C_s^{\infty} \le \mathop{\mathbf{E}}_{\tilde{\mathbf{h}},\hat{\mathbf{h}}}\left[\log\left(\frac{\left|\sqrt{1-\alpha}\hat{\mathbf{h}}+\sqrt{\alpha}\tilde{\mathbf{h}}\right|^2}{\left|\tilde{\mathbf{h}}\right|^2}\right)\right]^{+}, \tag{8}$$

where τ_0 is a solution of:

$$\mathop{\mathbf{E}}_{|\mathbf{h}|^2|\hat{\mathbf{h}}|^2}\left[\log\left(|\mathbf{h}|^2\right) \mid |\hat{\mathbf{h}}|^2 = \tau_0\right] - \mathop{\mathbf{E}}_{|\mathbf{g}|^2}\left[\log\left(|\mathbf{g}|^2\right)\right] = 0 \tag{9}$$

Proof:

- Asymptotic achievable rate

By Theorem 1, the rate $R_s(\tau) = \mathop{\mathbf{E}}_{|\mathbf{h}|^2,|\mathbf{g}|^2,|\hat{\mathbf{h}}|^2\ge\tau}\left[\log\left(\frac{1+P_0(\tau)|\mathbf{h}|^2}{1+P_0(\tau)|\mathbf{g}|^2}\right)\right]$ is achievable, for any $\tau \ge 0$. As $P \to \infty$, we have:

$$\begin{aligned}
\lim_{P\to\infty} R_s(\tau) &= \lim_{P\to\infty} \mathop{\mathbf{E}}_{|\mathbf{h}|^2\ge|\mathbf{g}|^2,|\hat{\mathbf{h}}|^2\ge\tau}\left[\log\left(\frac{1+P_0(\tau)|\mathbf{h}|^2}{1+P_0(\tau)|\mathbf{g}|^2}\right)\right] \\
&\quad + \lim_{P\to\infty} \mathop{\mathbf{E}}_{|\mathbf{h}|^2<|\mathbf{g}|^2,|\hat{\mathbf{h}}|^2\ge\tau}\left[\log\left(\frac{1+P_0(\tau)|\mathbf{h}|^2}{1+P_0(\tau)|\mathbf{g}|^2}\right)\right] \qquad (10) \\
&= \mathop{\mathbf{E}}_{|\mathbf{h}|^2\ge|\mathbf{g}|^2,|\hat{\mathbf{h}}|^2\ge\tau}\left[\lim_{P\to\infty}\log\left(\frac{1+P_0(\tau)|\mathbf{h}|^2}{1+P_0(\tau)|\mathbf{g}|^2}\right)\right] \\
&\quad + \mathop{\mathbf{E}}_{|\mathbf{h}|^2<|\mathbf{g}|^2,|\hat{\mathbf{h}}|^2\ge\tau}\left[\lim_{P\to\infty}\log\left(\frac{1+P_0(\tau)|\mathbf{h}|^2}{1+P_0(\tau)|\mathbf{g}|^2}\right)\right] \qquad (11) \\
&= \mathop{\mathbf{E}}_{|\mathbf{h}|^2,|\mathbf{g}|^2,|\hat{\mathbf{h}}|^2\ge\tau}\left[\log\left(\frac{|\mathbf{h}|^2}{|\mathbf{g}|^2}\right)\right],
\end{aligned}$$

where (11) follows from the Dominant Convergence Theorem, since for any P_{avg} value,

$$\left|\log\left(\frac{1+P_0(\tau)|\mathbf{h}|^2}{1+P_0(\tau)|\mathbf{g}|^2}\right)\right| \le \left|\log\left(\frac{|\mathbf{h}|^2}{|\mathbf{g}|^2}\right)\right|,$$

for all $|\mathbf{h}|^2 \ge |\mathbf{g}|^2$, and

$$\left|\log\left(\frac{|\mathbf{h}|^2}{|\mathbf{g}|^2}\right)\right| < \infty;$$

since $f_{\mathbf{g}}$ is continuous and bounded; and since $\left|\int_0^1 \log(x)\,dx\right| = 1$ and $\mathop{\mathbf{E}}_{|\mathbf{h}|^2,|\hat{\mathbf{h}}|^2\ge\tau}\left[|\mathbf{h}|^2\right] \le \mathop{\mathbf{E}}_{|\mathbf{h}|^2,|\hat{\mathbf{h}}|^2}\left[|\mathbf{h}|^2\right] < \infty$; then the limits in (10) exist and we can insert the limits inside the expectations in (10). To complete this part of the proof, $R_s(\tau)$ is maximized over all $\tau \ge 0$ and the optimum value is achieved at τ_0 that satisfies the necessary optimality condition (9).

- Asymptotic upper bound

For convenience, let UB be the right hand side (RHS) of (3) and let UB^{cst} be the RHS of (3) where $P\left(\hat{\mathbf{h}}\right) = P_{avg}$, a uniform

$$\underset{|\mathbf{h}|^2\geq\tau_0,|\mathbf{g}|^2}{\mathbf{E}}\left[\log\left(\frac{1+P_{avg}e^{\tau}|\mathbf{h}|^2}{1+P_{avg}e^{\tau}|\mathbf{g}|^2}\right)\right]\leq C_s\leq\max_{P(\mathbf{h})}\underset{|\mathbf{h}|^2,|\mathbf{g}|^2}{\mathbf{E}}\left[\log\left(\frac{1+P(\mathbf{h})|\mathbf{h}|^2}{1+P(\mathbf{h})|\mathbf{g}|^2}\right)\right]^+, \tag{14}$$

$$\underset{|\mathbf{h}|^2\geq\tau}{\mathbf{E}}\left[\frac{P_{avg}e^{\tau}|\mathbf{h}|^2}{1+P_{avg}e^{\tau}|\mathbf{h}|^2}\right]-\underset{|\mathbf{g}|^2}{\mathbf{E}}\left[\frac{P_{avg}e^{\tau}|\mathbf{g}|^2}{1+P_{avg}e^{\tau}|\mathbf{g}|^2}\right]\left(1-F_{|\hat{\mathbf{h}}|^2}(\tau)\right)-f_{|\hat{\mathbf{h}}|^2}(\tau)\left(\log(1+P\tau e^{\tau})-\underset{|\mathbf{g}|^2}{\mathbf{E}}\left[\log\left(1+Pe^{\tau}|\mathbf{g}|^2\right)\right]\right)=0 \tag{15}$$

power policy independently of $\hat{\mathbf{h}}$. The later particular choice provides a lower bound on UB and thus:

$$\begin{aligned}\lim_{P_{avg}\to\infty}UB&\geq\lim_{P_{avg}\to\infty}UB^{cst}\\&=\lim_{P_{avg}\to\infty}\underset{\hat{\mathbf{h}},\tilde{\mathbf{h}}}{\mathbf{E}}\left[\log\left(\frac{1+P_{avg}|\sqrt{1-\alpha}\,\hat{\mathbf{h}}+\sqrt{\alpha}\,\tilde{\mathbf{h}}|^2}{1+P_{avg}|\tilde{\mathbf{h}}|^2}\right)\right]^+\\&=\underset{\hat{\mathbf{h}},\tilde{\mathbf{h}}}{\mathbf{E}}\left[\log\left(\frac{|\sqrt{1-\alpha}\,\hat{\mathbf{h}}+\sqrt{\alpha}\,\tilde{\mathbf{h}}|^2}{|\tilde{\mathbf{h}}|^2}\right)\right]^+,\end{aligned} \tag{12}$$

where (12) holds by a similar reasoning than the one used to obtain (11). On the other hand, for any $P\left(\hat{\mathbf{h}}\right)\geq 0$, the following upper bound on UB holds true:

$$\begin{aligned}UB&\leq\max_{P(\hat{\mathbf{h}})}\underset{\hat{\mathbf{h}},\tilde{\mathbf{h}}}{\mathbf{E}}\left[\log\left(\frac{|\sqrt{1-\alpha}\,\hat{\mathbf{h}}+\sqrt{\alpha}\,\tilde{\mathbf{h}}|^2}{|\tilde{\mathbf{h}}|^2}\right)\right]^+\\&=\underset{\hat{\mathbf{h}},\tilde{\mathbf{h}}}{\mathbf{E}}\left[\log\left(\frac{|\sqrt{1-\alpha}\,\hat{\mathbf{h}}+\sqrt{\alpha}\,\tilde{\mathbf{h}}|^2}{|\tilde{\mathbf{h}}|^2}\right)\right]^+.\end{aligned} \tag{13}$$

Applying the limit on both sides of (13) completes the proof of our asymptotic upper bound. ■

Clearly, Corollary 1 states that the secrecy capacity is bounded at high-SNR confirming that the secret multiplexing gain is equal to zero, regardless of the main channel estimation quality.

B. Perfect And No Main CSI Extremes

When specialized to the no main CSI extreme, the inner and the outer bounds in Theorem 1 coincide, providing a trivial secrecy capacity. On the other hand, in the perfect main CSI extreme, the upper bound coincides with the secrecy capacity of a wiretap fading channel under the assumption of asymptotically long coherence intervals derived in [16, Theorem 2]. Our result is formalized in Corollary 2.

Corollary 2: In no main CSI extreme, the secrecy capacity C_s is equal to zero: $C_s = 0$; whereas, in perfect main CSI extreme, the inner and the outer bounds in (3) reduce to (14) at the top of the page, where τ_0 is the solution of (15) also at the top of the page.

Proof:

- No Main CSI

In this case, we have $\alpha = 1$, i.e., $\mathbf{h} = \tilde{\mathbf{h}}$ and $P\left(\hat{\mathbf{h}}\right) = P$. The upper bound in (3) is equal to zero, and so is the secrecy capacity.

- Perfect Main CSI

In this case, we have $\alpha = 0$, i.e., $\mathbf{h} = \hat{\mathbf{h}}$ and $P\left(\hat{\mathbf{h}}\right) = P(\mathbf{h})$. Since $\mathbf{g}$ is independent of $\mathbf{x}$, then $\left(\mathbf{h}', \mathbf{g}'\right) = (\mathbf{h}, \mathbf{g})$ is a valid choice that is when applied to (6), provides the upper bound in Corollary 2. ■

V. Application: i.i.d. Rayleigh Fading Channels

In this section, we apply the results derived in the previous sections to i.i.d. Rayleigh fading channels. That is, the main channel $\mathbf{h}$ and the eavesdropper channel $\mathbf{g}$ are circularly symmetric complex Gaussian with mean zero and variance one, and so are $\hat{\mathbf{h}}$ and $\tilde{\mathbf{h}}$. In our derivations summarized in Table I, we have used the PDF's:

$$f_{|\mathbf{h}|^2|\hat{\mathbf{h}}}(|h|^2\mid\hat{h})=\frac{1}{\alpha}e^{-\frac{|h|^2+(1-\alpha)|\hat{h}|^2}{\alpha}}I_0\left(2\sqrt{\frac{(1-\alpha)|\hat{h}|^2|h|^2}{\alpha^2}}\right), \tag{16}$$

where $I_0(\cdot)$ is the modified Bessel function of the first kind. Also, if $\hat{\boldsymbol{\theta}}$ and $\tilde{\boldsymbol{\theta}}$ are uniformly distributed between $[-\pi, \pi]$, then the PDF of $\boldsymbol{\theta} = \left(\hat{\boldsymbol{\theta}} - \tilde{\boldsymbol{\theta}}\right)$ is:

$$f_{\boldsymbol{\theta}}(\theta)=\begin{cases}\frac{1}{(2\pi)^2}(2\pi+\theta) & -2\pi\leq\theta<0\\ \frac{1}{(2\pi)^2}(2\pi-\theta) & 0\leq\theta<2\pi\\ 0 & \text{elsewhere.}\end{cases} \tag{17}$$

Similarly, if $\hat{\boldsymbol{\rho}}$ and $\tilde{\boldsymbol{\rho}}$ are Rayleigh distributed, with distribution $f_{\hat{\boldsymbol{\rho}}}(\hat{\rho}) = 2\hat{\rho}e^{-\hat{\rho}^2} = f_{\tilde{\boldsymbol{\rho}}}(\hat{\rho})$, then their ratio $\boldsymbol{\rho} = \hat{\boldsymbol{\rho}}/\tilde{\boldsymbol{\rho}}$ has the PDF:

$$f_{\boldsymbol{\rho}}(\rho)=\frac{2\rho}{(1+\rho^2)^2}, \tag{18}$$

for $\rho \geq 0$. Finally, for a Rayleigh fading channel, we have: $P_0(\tau) = P_0'(\tau) = P_{avg}e^{\tau}$. In Tab. I, $\mathrm{E_i}(x) = \int_x^{\infty}\frac{e^{-t}}{t}\mathrm{d}t$ is the exponential integral function and $\gamma \approx 0.577216$ is the Euler's constant.

VI. Numerical Results

In this section, numerical results are provided for i.i.d. Rayleigh fading channels. Figure 1 depicts the inner and the outer bounds in Theorem 1 in nats per channel use (npcu) for different main channel estimation error variances α. Also shown in Fig. 1 are the high-SNR bounds given by (8) along with the corresponding bounds to perfect and no-main CSI extremes given by (14). As can be seen in Fig. 1, the secrecy rate is strictly positive even for a poor main channel estimation quality ($\alpha = 0.9$). Although there is a gap between the inner and the outer bounds for all $\alpha \in [0, 1[$, this gap is bounded for all SNR values. Figure 2 depicts the bounds versus α for different SNR values. The bounds match for $\alpha = 1$, confirming that the secrecy capacity in no main CSI extreme is equal to zero. In Fig. 3, the optimal values of τ_0 versus SNR is displayed. The curves in Fig. 3 have been obtained by solving the necessary condition (4) or (15). Interestingly, at high-SNR, and for a given channel estimation error α, τ_0 converges to a fixed value, say $\tau_0^{\infty}(\alpha)$, which suggests that at high-SNR regime, if the transmitter is provided this value, it would be

Table I
SUMMARY OF THE DERIVED RESULTS FOR I.I.D. RAYLEIGH FADING CHANNELS.

General i.i.d.	i.i.d. Rayleigh
(3)	$\int_{\hat{h}=\tau_0}^{\infty}\int_{h=0}^{\infty}\int_{g=0}^{\infty}\log\left(\frac{1+P_0(\tau_0)h}{1+P_0(\tau_0)g}\right)e^{-g}f_{\lvert\mathbf{h}\rvert^2\lvert\hat{\mathbf{h}}}\left(h\mid\sqrt{\hat{h}}\right)e^{-\hat{h}}\,\mathrm{d}g\,\mathrm{d}h\,\mathrm{d}\hat{h}\le C_s\le\int_{\tilde{\rho}=0}^{\infty}\int_{\tilde{\theta}=-\pi}^{\pi}\int_{\tilde{\rho}=0}^{\frac{\hat{\rho}}{\rho_0(\tilde{\theta})}}\log\left(\frac{1+P(\hat{\rho})\left((1-\alpha)\hat{\rho}^2+\alpha\tilde{\rho}^2+2\sqrt{\alpha(1-\alpha)}\hat{\rho}\tilde{\rho}\cos(u)\right)}{1+P(\hat{\rho})\tilde{\rho}^2}\right)f_{\hat{\rho}}(\tilde{\rho})\,\frac{1}{2\pi}f_{\hat{\rho}}(\hat{\rho})\,\mathrm{d}\tilde{\rho}\,\mathrm{d}\tilde{\theta}\,\mathrm{d}\hat{\rho}$
(4)	$\int_{\hat{h}=\tau_0}^{\infty}\int_{h=0}^{\infty}\frac{P_0(\tau_0)h}{(1+P_0(\tau_0)h)}f_{\lvert\mathbf{h}\rvert^2\lvert\hat{\mathbf{h}}}\left(h\mid\sqrt{\hat{h}}\right)e^{-\hat{h}}\,\mathrm{d}h\,\mathrm{d}\hat{h}=e^{-\tau_0}\left(1-\frac{1+P_0(\tau_0)}{P_0(\tau_0)}e^{\frac{1}{P_0(\tau_0)}}\mathrm{E_i}\left(\frac{1}{P_0(\tau_0)}\right)+\int_{h=0}^{\infty}\log\left(1+P_0(\tau_0)h\right)f_{\lvert\mathbf{h}\rvert^2\lvert\hat{\mathbf{h}}}\left(h\mid\sqrt{\tau_0}\right)\mathrm{d}h\right)$
(7)	$\int_{\tilde{\theta}=-\pi}^{\pi}\int_{\tilde{\rho}=0}^{\frac{\hat{\rho}}{\rho_0(\tilde{\theta})}}\left(\frac{(1-\alpha)\hat{\rho}^2+\alpha\tilde{\rho}^2+2\sqrt{\alpha(1-\alpha)}\hat{\rho}\tilde{\rho}\cos(u)}{1+P(\hat{\rho})\left((1-\alpha)\hat{\rho}^2+\alpha\tilde{\rho}^2+2\sqrt{\alpha(1-\alpha)}\hat{\rho}\tilde{\rho}\cos(u)\right)}-\frac{\tilde{\rho}^2}{1+P(\hat{\rho})\tilde{\rho}^2}\right)f_{\tilde{\rho}}(\tilde{\rho})\,\frac{1}{2\pi}\mathrm{d}\tilde{\rho}\,\mathrm{d}u-\lambda=0$
(8)	$e^{-\tau_0}\left(\gamma+e^{\tau_0}\mathrm{E_i}(\tau_0)-e^{\tau_0}\mathrm{E_i}\left(\frac{\tau_0}{\alpha}\right)+\mathrm{E_i}\left(\frac{1-\alpha}{\alpha}\tau_0\right)+\log\left((1-\alpha)\tau_0\right)\right)\le C_s^{\infty}\le\int_{-2\pi}^{2\pi}\int_{\frac{\hat{\rho}}{\rho_0(\theta)}}^{\infty}\log\left((1-\alpha)\rho^2+\alpha+2\sqrt{\alpha(1-\alpha)}\rho\cos(\theta)\right)f_{\boldsymbol{\rho}}(\rho)\,f_{\boldsymbol{\theta}}(\theta)$
(9)	$\mathrm{E_i}\left(\frac{1-\alpha}{\alpha}\tau_0\right)+\log(\tau_0)+\log(1-\alpha)+\gamma=0$
(14)	$e^{-\tau_0}\left(e^{\frac{e^{-\tau_0}}{P_{avg}}}\left(e^{\tau_0}\mathrm{E_i}\left(\frac{e^{-\tau_0}}{P_{avg}}+\tau_0\right)-\mathrm{E_i}\left(\frac{e^{-\tau_0}}{P_{avg}}\right)\right)+\log\left(1+\tau_0e^{\tau_0}P_{avg}\right)\right)\le C_s\le\max_{P(h)}\int_0^{\infty}\left(\log\left(1+h\,P(h)\right)-e^{\frac{1}{P(h)}}\left(\mathrm{E_i}\left(\frac{1}{P(h)}\right)-\mathrm{E_i}\left(h+\frac{1}{P(h)}\right)\right)\right)e^{-h}\,\mathrm{d}h$
(15)	$\frac{e^{-2\tau}}{P_{avg}}\left(e^{\frac{e^{-\tau}}{P_{avg}}}\left(\left(1+e^{\tau}P_{avg}\right)\mathrm{E_i}\left(\frac{e^{-\tau}}{P_{avg}}\right)-e^{\tau}\mathrm{E_i}\left(\frac{e^{-\tau}}{P_{avg}}+\tau\right)\right)-e^{\tau}P_{avg}\log\left(1+e^{\tau}P_{avg}\tau\right)\right)=0$

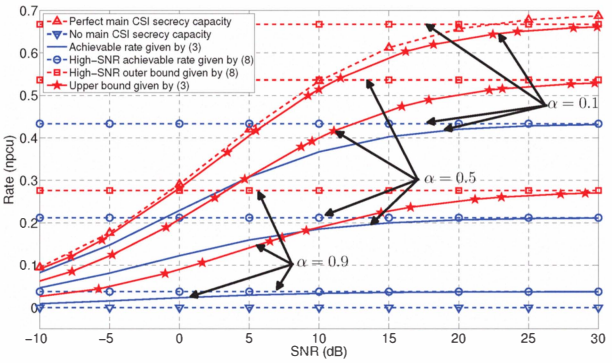

Figure 1. Achievable rate and upper bound for i.i.d. Rayleigh fading channels, with various main channel estimation errors α.

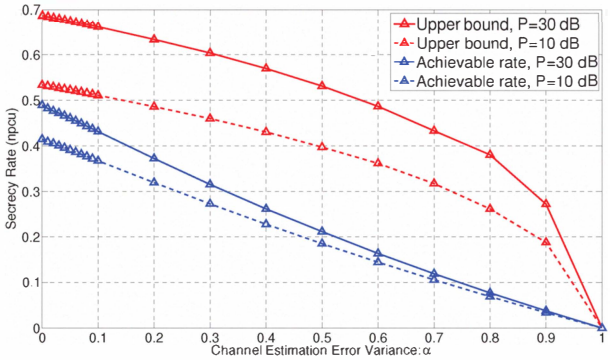

Figure 2. Achievable rate and upper bound for i.i.d. Rayleigh fading channels in function of α.

able to achieve the same secrecy rate without the need of $\hat{\mathbf{h}}$. Note also that for a given SNR value, τ_0 decreases with the channel estimation quality.

VII. Conclusion

The secrecy capacity of i.i.d. fast fading channels, under imperfect main channel estimation at the transmitter, has been addressed. Inner and outer bounds have been derived for a given channel estimation quality, and the gap between these bound has been characterized numerically. In addition to insightful asymptotic analysis at high-SNR regime, we have also addressed the perfect and no main CSI at the transmitter extremes as special cases, where we have shown that our bounds coincide with recently derived bounds for the i.i.d. fading channels. Our framework shows, for instance, that even a poor main channel estimator at the transmitter can help establishing secure communication. Furthermore, a simple constant rate on-off power scheme is enough to achieve

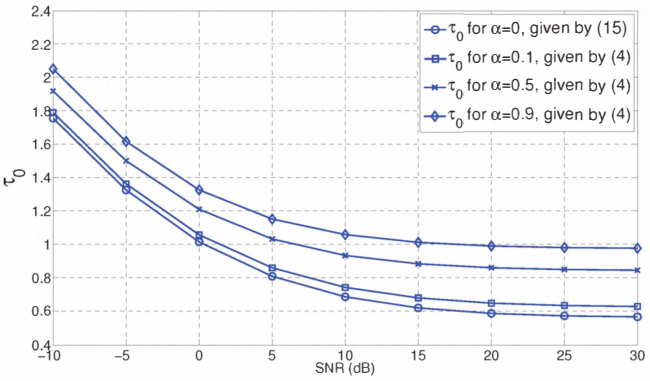

Figure 3. Optimal on-off power parameter τ_0 versus SNR for i.i.d. Rayleigh fading channels and for various values of α.

a positive secrecy rate. It is to reminded that one can enhance the later achievable secrecy rate by optimizing the transmit power with respect to the main channel estimation, at the expense of increasing the system complexity.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[4] A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[5] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, November 1976.

[6] U. Maurer and S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information," *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 499–514, Mar 1999.

[7] H. Imai, G. Hanaoka, J. Shikata, A. Otsuka, and A. Nascimento, "Cryptography with information theoretic security," in *Proc. of the 2002 IEEE Information Theory Workshop (ITW'2002)*, Bangalore, India, Oct. 2002, pp. 73–.

[8] Y. Watanabe, Y. Zheng, and H. Imai, "Traitor traceable signature scheme," in *Proc. International Symposium on Information Theory (ISIT'2000)*, Sorrento, Italy, 2000, pp. 462–.

[9] I. Csiszar and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.

[10] M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1562–1575, April 2006.

[11] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Transactions on Information Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[12] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. International Symposium on Information Theory (ISIT'2005)*, Adelaide, Australia, Sept. 2005, pp. 2152–2155.

[13] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. International Symposium on Information Theory (ISIT'2006)*, Seattle, Washington, USA, July 2006, pp. 356–360.

[14] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[15] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *Proc. International Symposium on Information Theory (ISIT'2007)*, Nice, France, June 2007, pp. 1301–1305.

[16] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[17] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[18] A. Khisti, A. Tchamkerten, and G. Wornell, "Secure broadcasting over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2453 –2469, Jun. 2008.

[19] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 41st Annual Conference on Information Sciences and Systems (CISS'2007)*, The John Hopkins University, Baltimore, Maryland, USA, March 2007, pp. 905–910.

[20] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. International Symposium on Information Theory (ISIT'2008)*, Nice, France, July 2008, pp. 524–528.

[21] I. Hero, A.O., "Secure space-time communication," *IEEE Transactions on Information Theory*, vol. 49, no. 12, pp. 3235–3249, December 2003.

[22] M. Yuksel and E. Erkip, "Diversity-multiplexing tradeoff for the multiple-antenna wire-tap channel," *IEEE Transactions on Wireless Communications*, vol. PP, no. 99, pp. 1 –10, Jan. 2011.

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

[24] X. Tang, R. Liu, P. Spasojevic, and H. Poor, "On the throughput of secure Hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inform. Theory*, vol. 55, no. 4, pp. 1575 –1591, Apr. 2009.