Secure Broadcasting with Imperfect Channel State Information at the Transmitter

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2500563, IEEE Transactions on Wireless Communications

Secure Broadcasting with Imperfect Channel State Information at the Transmitter

Amal Hyadi, *Student Member, IEEE*, Zouheir Rezki, *Senior Member, IEEE*, Ashish Khisti, *Senior Member, IEEE*, and Mohamed-Slim Alouini, *Fellow, IEEE*

***Abstract*—We investigate the problem of secure broadcasting over fast fading channels with imperfect main channel state information (CSI) at the transmitter. In particular, we analyze the effect of the noisy estimation of the main CSI on the throughput of a broadcast channel where the transmission is intended for multiple legitimate receivers in the presence of an eavesdropper. Besides, we consider the realistic case where the transmitter is only aware of the statistics of the eavesdropper's CSI and not of its channel's realizations. First, we discuss the common message transmission case where the source broadcasts the same information to all the receivers, and we provide an upper and a lower bounds on the ergodic secrecy capacity. For this case, we show that the secrecy rate is limited by the legitimate receiver having, on average, the worst main channel link and we prove that a non-zero secrecy rate can still be achieved even when the CSI at the transmitter is noisy. Then, we look at the independent messages case where the transmitter broadcasts multiple messages to the receivers, and each intended user is interested in an independent message. For this case, we present an expression for the achievable secrecy sum-rate and an upper bound on the secrecy sum-capacity and we show that, in the limit of large number of legitimate receivers K, our achievable secrecy sum-rate follows the scaling law $\log((1-\alpha)\log(K))$, where α is the estimation error variance of the main CSI. The special cases of high SNR, perfect and no-main CSI are also analyzed. Analytical derivations and numerical results are presented to illustrate the obtained expressions for the case of independent and identically distributed Rayleigh fading channels.**

***Index Terms*—Secure broadcasting, imperfect channel state information, ergodic secrecy capacity, common message broadcast, independent messages broadcast.**

I. Introduction

Ensuring the confidentiality of the users is one of the key challenges of wireless communication systems. To date, securing a communication is mainly performed at the application layer using cryptographic protocols. From a research perspective, it has been shown that securing a transmission can be enhanced at the physical layer without the use of cryptography. The first important results in this research area were presented in [1] and [2]. In [1], Wyner introduced the degraded wiretap channel where a source communicates with one receiver over a discrete, memoryless channel in the presence of an eavesdropper observing the legitimate channel's output. Wyner has proved that, for such a system, there exists a coding scheme that ensures the reliability of the communication with perfect secrecy. In [2], Csiszár and Körner reconsidered Wyner's wiretap channel for the case of a non-degraded communication, i.e., the main and the eavesdropper's channels are supposed to be independent from each other. This model is considered to be more suitable to analyze secrecy in mobile communication systems [3].

More recently, the impact of fading on secure communication was investigated in a number of works. Unlike the traditional additive white Gaussian noise (AWGN) scenario, fading generally increases the randomness of the channel input and hence improves the communication security. Indeed, it has been shown, in [4]–[8], that achieving a secure communication over quasistatic fading channels is feasible even when the average signal-to-noise ratio (SNR) of the main channel is less than the one of the eavesdropper. In [9], the secrecy capacity of a slow-fading channel with an eavesdropper was investigated for the cases of full channel state information (CSI) and only main CSI at the transmitter. In [10], an upper and a lower bounds on the secrecy capacity were presented for fast-fading channels with perfect main CSI at the transmitter. The case of imperfect CSI was studied in [11], [12] where an upper and a lower bounds on the secrecy capacity were presented for single user transmission. Works in this area generally assume that at least the statistics of the eavesdropper's fading channel are known to the transmitter.

Recent research interest has been given to analysing the secrecy capacity of multi-antenna and multi-users systems. In [13], [14], the secrecy capacity of a deterministic multi-antenna wiretap channel was studied and the positive impact of deploying multiple antennas on secrecy has been highlighted. The authors in [8] analysed a degraded single-input-multiple-output (SIMO) wiretap channel and showed that the secrecy diversity gain is proportional to the number of receiver antennas. The corresponding multiple-input-single-output (MISO) case was studied in [15] and [16], while the multiple-input-multiple-output (MIMO) case was considered in [13], [17]–[19]. For the broadcast multi-users scenario, Csiszár and Körner extended the original wiretap channel, proposed by Wyner, to the case where the source sends common information to both the destination and the eavesdropper while the confidential messages are sent only to the destination. The secrecy capacity of this scenario, for

Part of this work has been presented at the 2014 IEEE Global Communications Conference (GLOBECOM'2014), Austin, TX, USA.

This work was supported by the Qatar National Research Fund (a member of Qatar Foundation) under NPRP Grant NPRP 5-603-2-243. The statements made herein are solely the responsibility of the authors.

A. Hyadi, Z. Rezki and M.-S. Alouini are with the Division of Computer, Electrical, and Mathematical Sciences & Engineering (CEMSE), King Abdullah University of Science and Technology (KAUST), Thuwal, Makkah Province, Saudi Arabia. [e-mail: {amal.hyadi, zouheir.rezki, slim.alouini}@kaust.edu.sa].

A. Khisti is with the Electrical and Computer Engineering Department, University of Toronto, Toronto, ON, Canada. [e-mail: akhisti@comm.utoronto.ca].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2500563, IEEE Transactions on Wireless Communications

the case of a broadcast wiretap channel with parallel and fading channels assuming perfect main CSI at the transmitter, was considered in [20]. For the multiple access scenario, the authors in [21] investigated the secrecy capacity of a degraded channel where the eavesdropper obtains a degraded version of the receiver's signal.

The great majority of works in the literature examine the secrecy performances of wireless systems under the assumption of perfect CSI at the transmitter. In this paper, we consider the more realistic scenario where only partial CSI is available. In particular, we investigate the impact on the ergodic secrecy capacity of a broadcast wiretap channel where a source transmits to multiple legitimate receivers in the presence of one eavesdropper. Assuming imperfect main CSI at the transmitter, we present an upper and a lower bounds on the secrecy capacity and we study the special cases of high-SNR, perfect main CSI and no CSI transmissions. Both the common message case, where a unique information is broadcasted to all the legitimate receivers, and the independent messages case, where the source transmits multiple independent messages, are considered.

The present paper builds on the results in [11], [12], obtained for single user transmission, and generalizes them to the broadcast multiuser channel. Assuming imperfect channel estimation at the transmitter, the work in [11], [12] provides a lower and an upper bounds on the ergodic secrecy capacity of the single user wiretap channel. The proposed achievable rate follows from a standard wiretap code with a Gaussian input and a simple on-off power control, while the upper bound is obtained using an appropriate correlation scheme of the main and the eavesdropper channels. In this paper, we expand these results to the broadcast wiretap channel. We consider that transmitter is aware of the statistics of the eavesdropper's CSI but not of its channel's realizations. Also, we assume that the transmitter is only provided with an imperfect estimation of the main channel gain. It is worth mentioning that, on one hand, when a common message is broadcasted to all the legitimate receivers, the secrecy capacity performance is limited by the user with the worst channel quality. Also, the transmission scheme, achieving the proposed secrecy rate, is elaborated in such a way to avoid any extra leakage of information to the eavesdropper. On the other hand, when multiple independent messages are broadcasted, a genie-aided channel must be carefully selected to obtain the proposed upper bound. This upper bound is shown to be tight in the very noisy CSI extreme.

The paper is organized as follows. Section II describes the system model. The main results along with the corresponding proofs are introduced in section III for the common message transmission and section IV for the independent messages case. Section V considers the case of Rayleigh fading channels. Finally, selected numerical results are presented in section VI, while section VII concludes the paper.

Notations: Throughout the paper, we use the following notational conventions. The expectation operation is denoted by $\mathbb{E}[.]$, the modulus of a scalar x is expressed as $|x|$, and we define $\{\nu\}^+ = \max(0,\nu)$. The function $P(.)$ is used to describe the power profile adopted at the transmitter. The argument of this function can be a scalar or a vector. The entropy of a discrete random variable X is denoted by $H(X)$, and the mutual information between random variables X and Y is denoted by $I(X;Y)$. In addition, we use $f_X(.)$ and $F_X(.)$ to denote the probability density function (PDF) and the cumulative distribution function (CDF) of the random variable X.

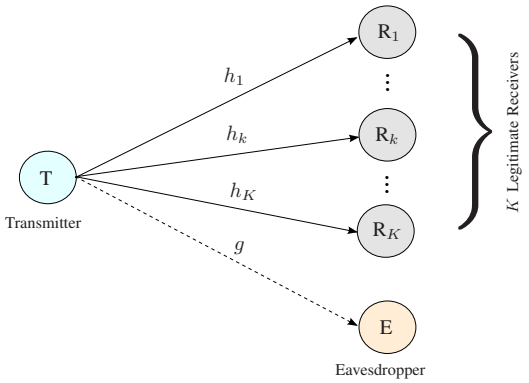

Fig. 1. The fading wiretap channel with multiple receivers and one eavesdropper.

II. System Model

We consider a broadcast wiretap channel where a transmitter T communicates with K legitimate receivers $(\mathrm{R}_1, \cdots, \mathrm{R}_K)$ in the presence of an eavesdropper E as depicted in Fig. 1. Each terminal is equipped with a single antenna for transmission and reception. During every coherence interval $i \in \{1, \cdots, n\}$, the received signals by each legitimate receiver $\mathrm{R}_k, k \in \{1, \cdots, K\}$, and the eavesdropper are, respectively, given by

$$\begin{cases} Y_k(i) = h_k(i)X(i) + v_k(i) \\ Z(i) = g(i)X(i) + w(i), \end{cases} \tag{1}$$

where $h_k(i) \in \mathbb{C}$, $g(i) \in \mathbb{C}$ are zero-mean, unit-variance complex Gaussian channel gains corresponding to each legitimate channel and the eavesdropper's channel, respectively; and $v_k(i) \in \mathbb{C}$, $w(i) \in \mathbb{C}$ represent zero-mean, unit-variance circularly symmetric white Gaussian noises at R_k and E, respectively; and $X(i)$ is the transmitted message to all the receivers. An average transmit power constraint is imposed at the transmitter such that $\mathbb{E}[|X(i)|^2] \leq P_{\text{avg}}$, where the expectation is over the input distribution.

The channel gains h_k and g are independent, ergodic and stationary. We consider that the transmitter is only aware of the statistics of the eavesdropper's CSI and not of its channel's realizations $g(i)$. Also, we assume that the transmitter is only provided with a noisy version of each $h_k(i)$, say $\hat{h}_k(i) \sim \mathcal{CN}(0,1)$, such that the main channel estimation model can be written as

$$h_k(i) = \sqrt{1-\alpha}\hat{h}_k(i) + \sqrt{\alpha}\tilde{h}_k(i),$$

where α is the estimation error variance ($\alpha \in [0,1]$) and $\tilde{h}_k(i) \sim \mathcal{CN}(0,1)$ is the zero-mean unit-variance channel estimation error. We assume that $\hat{h}_k(i)$ and $\tilde{h}_k(i)$ are uncorrelated

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2500563, IEEE Transactions on Wireless Communications

and hence independent. To ensure correct decoding with high probability at the legitimate receivers' side, we assume that each receiver R_k has a perfect knowledge of its channel gain $h_k(i)$. Also, we assume that the eavesdropper is aware of its channel gain $g(i)$, and of all the legitimate receivers' channel gains $h_k(i), k \in \{1, \cdots, K\}$. The estimated channel gains $\hat{h}_k(i), k \in \{1, \cdots, K\}$, are known globally. Giving that the channel gains are ergodic and stationary with bounded and continuous PDFs, the index time i can be omitted. In the rest of this paper, we denote $|h_k|^2$, $|\hat{h}_k|^2$, $|\tilde{h}_k|^2$ and $|g|^2$ by γ_k, $\hat{\gamma}_k$, $\tilde{\gamma}_k$ and γ_e, respectively.

We are interested in the broadcast secrecy capacity of such a channel when the block length of the transmitted message is large, i.e., $n \to \infty$. In accordance with Wyner's weak secrecy, we consider that a secret transmission is achieved when the normalized leakage of information obtained by the eavesdropper while observing its channel output, vanishes in the limit of long block lengths.

III. Broadcasting a Common Message

In this section, we consider the common message transmission case when a unique confidential information is broadcasted to all the legitimate receivers. Taking into account the adopted system model, we present the upper and the lower bounds on the secrecy capacity. The asymptotic analyses, for the high-SNR regime and the perfect CSI case, are also investigated.

A. Main Results

In this subsection, we present the main results obtained for the ergodic secrecy capacity of the considered system model when broadcasting a common message.

1) Lower and Upper Bounds:

Theorem 1: The common message secrecy capacity, $\mathcal{C}_\mathrm{s}$, of the fast fading broadcast channel under imperfect main channels estimation at the transmitter is bounded by

$$\mathcal{C}_\mathrm{s}^- \leq \mathcal{C}_\mathrm{s} \leq \mathcal{C}_\mathrm{s}^+, \tag{2}$$

such as
$$\mathcal{C}_\mathrm{s}^- = \max_{P(\tau)} \min_{1\leq k\leq K} \mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma_k,\\ \hat{\gamma}_k\geq\tau}} \left[\log\left(\frac{1+\gamma_k P(\tau)}{1+\gamma_e P(\tau)}\right)\right], \tag{3a}$$

and
$$\mathcal{C}_\mathrm{s}^+ = \min_{1\leq k\leq K} \max_{P(\hat{h}_k)} \mathop{\mathbb{E}}_{\hat{h}_k,\tilde{h}_k} \left[\left\{\log\left(\frac{1+|\sqrt{1-\alpha}\hat{h}_k+\sqrt{\alpha}\tilde{h}_k|^2 P(\hat{h}_k)}{1+|\tilde{h}_k|^2 P(\hat{h}_k)}\right)\right\}^+\right], \tag{3b}$$

with $P(\tau)=P_\mathrm{avg}/\left(1-F_{\hat{\gamma}_k}(\tau)\right)$ and $\mathbb{E}[P(\hat{h}_k)]\leq P_\mathrm{avg}$.

2) High-SNR Regime:

Corollary 1: At high-SNR regime, the secrecy capacity for the common message case is bounded by

$$\mathcal{C}_\text{H-SNR}^- \leq \mathcal{C}_\mathrm{s} \leq \mathcal{C}_\text{H-SNR}^+, \tag{4}$$

such as $\mathcal{C}_\text{H-SNR}^- = \min_{1\leq k\leq K} \mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma_k,\\ \hat{\gamma}_k\geq\tau}} \left[\log\left(\frac{\gamma_k}{\gamma_e}\right)\right]$, where τ satisfies $\mathop{\mathbb{E}}_{\gamma_k|\hat{\gamma}_k}\left[\log(\gamma_k)\,\middle|\,\hat{\gamma}_k=\tau\right] - \mathop{\mathbb{E}}_{\gamma_e}\left[\log(\gamma_e)\right]=0$, and

$$\mathcal{C}_\text{H-SNR}^+ = \min_{1\leq k\leq K} \mathop{\mathbb{E}}_{\hat{h}_k,\tilde{h}_k} \left[\left\{\log\left(\frac{|\sqrt{1-\alpha}\hat{h}_k+\sqrt{\alpha}\tilde{h}_k|^2}{|\tilde{h}_k|^2}\right)\right\}^+\right].$$

3) Perfect Main CSI case:

Corollary 2: When the transmitter has perfect knowledge of the legitimate receivers' CSI, the secrecy capacity is bounded as

$$\mathcal{C}_\text{P-CSI}^- \leq \mathcal{C}_\mathrm{s} \leq \mathcal{C}_\text{P-CSI}^+, \tag{5}$$

such as $\mathcal{C}_\text{P-CSI}^- = \max_{P(\tau)} \min_{1\leq k\leq K} \mathop{\mathbb{E}}_{\gamma_e,\gamma_k\geq\tau} \left[\log\left(\frac{1+\gamma_k P(\tau)}{1+\gamma_e P(\tau)}\right)\right]$,

and $\mathcal{C}_\text{P-CSI}^+ = \min_{1\leq k\leq K} \max_{P(\gamma_k)} \mathop{\mathbb{E}}_{\gamma_k,\gamma_e} \left[\left\{\log\left(\frac{1+\gamma_k P(\gamma_k)}{1+\gamma_e P(\gamma_k)}\right)\right\}^+\right]$,

with $P(\tau) = P_\mathrm{avg}/\left(1-F_{\gamma_k}(\tau)\right)$ and $\mathbb{E}[P(\gamma_k)] \leq P_\mathrm{avg}$.

B. Ergodic Capacity Analysis

In this subsection, we establish the obtained results for the ergodic secrecy capacity presented in the previous subsection.

1) Proof of Achievability in Theorem 1:

A detailed proof of achievability is provided in Appendix A. Here, we outline the adopted transmission scheme. We consider a probabilistic model where the transmission is constrained by the quality of the legitimate channels. Considering the case $K=2$, we define the following parameters:

- τ is a prefixed transmission threshold,
- $\mathcal{R}_w=\mathbb{E}\left[\log(1+\gamma_e P(\hat{\gamma}_k))\right]$, with $P(\hat{\gamma}_k)$ is chosen to satisfy the average power constraint,
- $\mathcal{R}_k=\mathbb{E}\left[\log(1+\gamma_k P(\hat{\gamma}_k))\,|\hat{\gamma}_k \geq \tau\right] - \mathcal{R}_w$,
- $p_k=\Pr\left[\hat{\gamma}_k \geq \tau\right]$,
- $n_0=p_k p_j n$, and $n_1=p_k(1-p_j)n$, with $k, j \in \{1, 2\}/k\neq j$.

We use two independent Gaussian codebooks C_0 and C_1 constructed similarly to the standard wiretap codes. Codebook C_0 is a $(n_0, 2^{n_0\mathcal{R}_k})$ code, with $2^{n_0(\mathcal{R}_k+\mathcal{R}_w)}$ codewords randomly partitioned into $2^{n_0\mathcal{R}_k}$ bins, and codebook C_1 is a $(n_1, 2^{n_1\mathcal{R}_k})$ code, with $2^{n_1(\mathcal{R}_k+\mathcal{R}_w)}$ codewords randomly partitioned into $2^{n_1\mathcal{R}_k}$ bins. The transmitted common message is given in the form $W=(W_0, W_1)$, where W_0 and W_1 are uniformly distributed over the indices $\left\{1, 2, \cdots, 2^{n_0\mathcal{R}_k}\right\}$ and $\left\{1, 2, \cdots, 2^{n_1\mathcal{R}_k}\right\}$, respectively.

Next, we define the events: $S_1 = \{\hat{\gamma}_1\geq\tau\,,\, \hat{\gamma}_2\geq\tau\}$, $S_2 = \{\hat{\gamma}_1\geq\tau\,,\, \hat{\gamma}_2<\tau\}$, $S_3 = \{\hat{\gamma}_1<\tau\,,\, \hat{\gamma}_2\geq\tau\}$ and $S_4 = \{\hat{\gamma}_1<\tau\,,\, \hat{\gamma}_2<\tau\}$. That is, the transmitter selects randomly a codeword $U_0^{n_0}$ associated with message W_0 and broadcasts it when he experiences event S_1. For message W_1, the transmitter selects two codewords uniformly and independently of one another; one codeword $U_1^{n_1}$ to be sent in state S_2 and the other one $U_2^{n_1}$ to be sent in state S_3. The source remains idle when experiencing event S_4. The randomness and the independence in the choice of the two codewords for message W_1 ensures that the eavesdropper does not take advantage of this repetition.

Since message W_0 is transmitted over channel state S_1 with $\Pr[S_1] = \Pr[\hat{\gamma}_1\geq\tau\,,\, \hat{\gamma}_2\geq\tau]$, state S_1 occurs n_0/n times and the size of codebook $\mathcal{C}_0$ is therefore n_0. Similarly, message W_1 is transmitted over channel state S_2 and S_3 with $\Pr[S_2] = \Pr[S_3] = \Pr[\hat{\gamma}_k\geq\tau\,,\, \hat{\gamma}_j<\tau]$, $k, j \in \{1, 2\}, k \neq j$. Thus, state S_2 and S_3 each occurs n_1/n times and the size of codebook $\mathcal{C}_1$ is n_1. The transmission stops when we have transmitted exactly n_0 symbols of $U_0^{n_0}$ and n_1 symbols each of $U_1^{n_1}$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2500563, IEEE Transactions on Wireless Communications

and $U_2^{n_1}$. Given that the estimated channel gains are known globally, the receivers know the current state of the system and accordingly know which codeword the transmitted symbol belongs to. Decoder 1 uses the observations corresponding to the codewords $U_0^{n_0}$ and $U_1^{n_1}$ to recover message (W_0, W_1) while decoder 2 uses the ones corresponding to the codewords $U_0^{n_0}$ and $U_2^{n_1}$ to recover the message (W_0, W_1). Details on the codebook generation, the coding and the decoding schemes, and the secrecy analysis of this probabilistic transmission model are similar to the perfect CSI case presented in [22]. The overall achievable rate can then be written as

$$\mathcal{R} = \min_k \left\{ \frac{n_0}{n} R_k + \frac{n_1}{n} R_k \right\} = \min_k p_k R_k, \tag{6}$$

which reduces to $\mathcal{R} = \min_k \mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma_k,\\ \hat{\gamma}_k \geq \tau}} \left[\log \left(\frac{1+\gamma_k P(\hat{\gamma}_k)}{1+\gamma_e P(\hat{\gamma}_k)} \right) \right]$. The extension to the case $K \geq 2$ follows along similar lines as [22]. To finish the proof, we consider a transmission power that is instantaneously adapted according to the following on-off power scheme

$$P(\hat{\gamma}_k) = \begin{cases} P(\tau) = \dfrac{P_{\text{avg}}}{1 - F_{\hat{\gamma}_k}(\tau)} & \hat{\gamma}_k \geq \tau \\ 0 & \text{otherwise,} \end{cases} \tag{7}$$

then, we maximize the achievable rate $\mathcal{R}$ over $P(\tau)$ yielding the lower bound on the secrecy capacity presented in (3a). The threshold τ should then be chosen to satisfy

$$\mathop{\mathbb{E}}_{\gamma_k,\hat{\gamma}_k \geq \tau} \left[\frac{\gamma_k P'(\tau)}{1+\gamma_k P(\tau)} \right] - \mathop{\mathbb{E}}_{\gamma_e} \left[\frac{\gamma_e P'(\tau)}{1+\gamma_e P(\tau)} \right] (1 - F_{\hat{\gamma}_k}(\tau)) = f_{\hat{\gamma}_k}(\tau) \left(\mathop{\mathbb{E}}_{\gamma_k|\hat{\gamma}_k} \left[\log\left(1+\gamma_k P(\tau)\right) \middle| \hat{\gamma}_k = \tau \right] - \mathop{\mathbb{E}}_{\gamma_e} \left[\log\left(1+\gamma_e P(\tau)\right) \right] \right). \tag{8}$$

Remark 1: We opted for the use of the On-Off power scheme, for the achievable rate, because it is near optimal and less complex. Clearly, the achievable secrecy rate can be directly improved by optimizing over all power policies satisfying the average power constraint. Indeed, one expects a better rate by solving

$$\mathcal{C}_{\text{s}}^{-} = \max_{P(\hat{\gamma}_k)} \mathop{\mathbb{E}}_{\gamma_e,\gamma_k,\hat{\gamma}_k} \left[\log \left(\frac{1+\gamma_k P(\hat{\gamma}_k)}{1+\gamma_e P(\hat{\gamma}_k)} \right) \right], k \in \{1, \cdots, K\}. \tag{9}$$

The objective function in (9) is not convex. Using the Lagrange approach, it is possible to obtain the necessary optimality condition via the Karush-Kuhn-Tucker (KKT) condition. The corresponding Lagrangian, to the optimization problem in (9), with the average power constraint $\mathbb{E}[P(\hat{\gamma}_k)] \leq P_{\text{avg}}$, can be written as

$$\mathcal{L}(P(\hat{\gamma}_k), \mu_k) = \mathop{\mathbb{E}}_{\gamma_e,\gamma_k|\hat{\gamma}_k} \left[\log \left(\frac{1+\gamma_k P(\hat{\gamma}_k)}{1+\gamma_e P(\hat{\gamma}_k)} \right) \right] - \mu_k \left(\mathbb{E}[P(\hat{\gamma}_k)] - P_{\text{avg}} \right), \tag{10}$$

with μ_k being the Lagrange multiplier. Differentiating $\mathcal{L}(P(\hat{\gamma}_k), \mu_k)$ with respect to $P(\hat{\gamma}_k)$ yields the following necessary condition for optimality

$$\mathop{\mathbb{E}}_{\gamma_e,\gamma_k|\hat{\gamma}_k} \left[\frac{\gamma_k - \gamma_e}{(1+\gamma_k P(\hat{\gamma}_k))(1+\gamma_e P(\hat{\gamma}_k))} \middle| \hat{\gamma}_k \right] = \mu_k.$$

We define the function

$$f_{\hat{\gamma}_k}(P) = \mathop{\mathbb{E}}_{\gamma_e,\gamma_k|\hat{\gamma}_k} \left[\frac{\gamma_k - \gamma_e}{(1+\gamma_k P(\hat{\gamma}_k))(1+\gamma_e P(\hat{\gamma}_k))} \middle| \hat{\gamma}_k \right].$$

Then, following similar lines as [R5, Lemma 5], it can be shown that if there exists $\hat{\gamma}_{k_0}$, such that $\mathbb{E}[\gamma_k - \gamma_e | \hat{\gamma}_{k_0}] > 0$, i.e., such that $(1-\alpha)(\hat{\gamma}_{k_0} - 1) > 0$, then using the entire available power is optimal, and the power allocation scheme is given by

$$P(\hat{\gamma}_k) = \begin{cases} f_{\hat{\gamma}_k}^{-1}(\mu_k) & \text{if} \quad 0 \leq \mu_k \leq (1-\alpha)(\hat{\gamma}_k - 1) \\ 0 & \text{otherwise,} \end{cases} \tag{11}$$

under the power constraint $P(\mu_k) = \mathop{\mathbb{E}}_{\hat{\gamma}_k} [P(\hat{\gamma}_k)]$, i.e. each value of μ_k corresponds to an average power constraint $P_{\text{avg}} = P(\mu_k)$. This optimal procedure, although complex and time-consuming, does not provide a substantial gain. Indeed, the rate achieved by the proposed On-Off power scheme and the one resulting from the Karush-Kuhn-Tucker (KKT) condition are very close.

2) Proof of the Upper Bound in Theorem 1:

To establish the upper bound on the capacity in (2), we start by supposing that the transmitter sends message X to only one legitimate receiver R_k. Using a similar approach, as in [11], we have

$$\mathcal{C}_{\text{s}} \leq \max_{P(\hat{h}_k)} \mathop{\mathbb{E}}_{\hat{h}_k,\tilde{h}_k} \left[\left\{ \log \left(\frac{1+|\sqrt{1-\alpha}\hat{h}_k + \sqrt{\alpha}\tilde{h}_k|^2 P(\hat{h}_k)}{1+|\tilde{h}_k|^2 P(\hat{h}_k)} \right) \right\}^+ \right]. \tag{12}$$

The choice of the receiver to transmit to is arbitrary. In order to tighten this upper bound, we can then choose receiver R_k that minimizes this quantity, yielding the result in (3b).

By setting $\hat{h}_k = \hat{\rho}_k e^{i\hat{\theta}_k}$, $\tilde{h}_k = \tilde{\rho}_k e^{i\tilde{\theta}_k}$ and $u_k = \hat{\theta}_k - \tilde{\theta}_k$, the upper bound on the secrecy capacity can be expressed as

$$\mathcal{C}_{\text{s}}^{+} = \min_{1 \leq k \leq K} \max_{P(\hat{\rho}_k)} \mathop{\mathbb{E}}_{\hat{\rho}_k \tilde{\rho}_k u_k} \left[\left\{ \log \left(\frac{1+\left((1-\alpha)\hat{\rho}_k^2 + \alpha\tilde{\rho}_k^2 + 2\sqrt{\alpha(1-\alpha)}\hat{\rho}_k\tilde{\rho}_k \cos(u_k) \right) P(\hat{\rho}_k)}{1+\tilde{\rho}_k^2 P(\hat{\rho}_k)} \right) \right\}^+ \right]. \tag{13}$$

The optimal power profile, in this case, is the solution of the optimality condition

$$\mathop{\mathbb{E}}_{\tilde{\rho}_k \leq \frac{\hat{\rho}_k}{\rho_0(u_k)}} \left[\frac{\xi(\hat{\rho}_k, \tilde{\rho}_k, u_k)}{1+\xi(\hat{\rho}_k, \tilde{\rho}_k, u_k) P(\hat{\rho}_k)} - \frac{\tilde{\rho}_k^2}{1+\tilde{\rho}_k^2 P(\hat{\rho}_k)} \right] - \mu_k = 0. \tag{14}$$

with μ_k is the Lagrange multiplier obtained by setting $\mathbb{E}[P(\hat{\rho}_k)] = P_{\text{avg}}$,

$$\xi(\hat{\rho}_k, \tilde{\rho}_k, u_k) = (1-\alpha)\hat{\rho}_k^2 + \alpha\tilde{\rho}_k^2 + 2\sqrt{\alpha(1-\alpha)}\hat{\rho}_k\tilde{\rho}_k \cos(u_k),$$

and

$$\rho_0(u_k) = \frac{\sqrt{(1-\alpha)(\alpha\cos(u_k)^2 - \alpha + 1)} - \sqrt{\alpha(1-\alpha)}\cos(u_k)}{1-\alpha}.$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2500563, IEEE Transactions on Wireless Communications

3) Proof of the High-SNR Results in Corollary 1:

- *Asymptotic Lower Bound:* From Theorem 1, the rate

$$\mathcal{R}_{\rm s}(\tau) = \min_{1\le k\le K} \mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma_k,\\ \hat{\gamma}_k\ge\tau}} \left[\log\left(\frac{1+\gamma_k P(\tau)}{1+\gamma_e P(\tau)}\right)\right]$$

is achievable for any $\tau \ge 0$.

At high-SNR regime, i.e., $P_{\rm avg}\to\infty$, we have

$$\lim_{P_{\rm avg}\to\infty} R_{\rm s}(\tau) = \min_{1\le k\le K} \lim_{P_{\rm avg}\to\infty} \mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma_k,\\ \hat{\gamma}_k\ge\tau}} \left[\log\left(\frac{1+\gamma_k P(\tau)}{1+\gamma_e P(\tau)}\right)\right], \quad (15)$$

since $\left|\log\left(\frac{1+\gamma_k P(\tau)}{1+\gamma_e P(\tau)}\right)\right| \le \left|\log\left(\frac{\gamma_k}{\gamma_e}\right)\right|$, f_{γ_e} is continuous and bounded, $\mathop{\mathbb{E}}_{\gamma_k,\hat{\gamma}_k\ge\tau}[\gamma_e] \le \mathop{\mathbb{E}}_{\gamma_k,\hat{\gamma}_k}[\gamma_e] < \infty$ and $\left|\log\left(\frac{\gamma_k}{\gamma_e}\right)\right| < \infty$, then using the Dominant Convergence Theorem we can interchange the order of the limit and the expectation. We can then write

$$\lim_{P_{\rm avg}\to\infty} R_{\rm s}(\tau) = \min_{1\le k\le K} \mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma_k,\\ \hat{\gamma}_k\ge\tau}} \lim_{P_{\rm avg}\to\infty} \left[\log\left(\frac{1+\gamma_k P(\tau)}{1+\gamma_e P(\tau)}\right)\right] \quad (16)$$

$$= \min_{1\le k\le K} \mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma_k,\\ \hat{\gamma}_k\ge\tau}} \left[\log\left(\frac{\gamma_k}{\gamma_e}\right)\right]. \quad (17)$$

To complete the proof, we choose τ that maximizes (17), yielding the result in Corollary 1.

- *Asymptotic Upper Bound:* On one hand, we have

$$\lim_{P_{\rm avg}\to\infty} \mathcal{C}^{+}_{\text{H-SNR}}$$

$$= \lim_{P_{\rm avg}\to\infty} \min_{1\le k\le K} \max_{P(\hat{h}_k)} \mathop{\mathbb{E}}_{\hat{h}_k,\tilde{h}_k} \left[\left\{\log\left(\frac{1+|\sqrt{1-\alpha}\hat{h}_k+\sqrt{\alpha}\tilde{h}_k|^2 P(\hat{h}_k)}{1+|\tilde{h}_k|^2 P(\hat{h}_k)}\right)\right\}^{+}\right] \quad (18)$$

$$\ge \lim_{P_{\rm avg}\to\infty} \min_{1\le k\le K} \mathop{\mathbb{E}}_{\hat{h}_k,\tilde{h}_k} \left[\left\{\log\left(\frac{1+|\sqrt{1-\alpha}\hat{h}_k+\sqrt{\alpha}\tilde{h}_k|^2 P_{\rm avg}}{1+|\tilde{h}_k|^2 P_{\rm avg}}\right)\right\}^{+}\right] \quad (19)$$

$$= \min_{1\le k\le K} \mathop{\mathbb{E}}_{\hat{h}_k,\tilde{h}_k} \left[\left\{\lim_{P_{\rm avg}\to\infty} \log\left(\frac{1+|\sqrt{1-\alpha}\hat{h}_k+\sqrt{\alpha}\tilde{h}_k|^2 P_{\rm avg}}{1+|\tilde{h}_k|^2 P_{\rm avg}}\right)\right\}^{+}\right] \quad (20)$$

$$= \min_{1\le k\le K} \mathop{\mathbb{E}}_{\hat{h}_k,\tilde{h}_k} \left[\left\{\log\left(\frac{|\sqrt{1-\alpha}\hat{h}_k+\sqrt{\alpha}\tilde{h}_k|^2}{|\tilde{h}_k|^2}\right)\right\}^{+}\right], \quad (21)$$

where (20) is obtained using a similar reasoning as for the asymptotic lower bound case. On the other hand, for any $P(\hat{h}_k) \ge 0$, we have

$$\mathcal{C}^{+}_{\text{H-SNR}} \le \min_{1\le k\le K} \max_{P(\hat{h}_k)} \mathop{\mathbb{E}}_{\hat{h}_k,\tilde{h}_k} \left[\left\{\log\left(\frac{|\sqrt{1-\alpha}\hat{h}_k+\sqrt{\alpha}\tilde{h}_k|^2}{|\tilde{h}_k|^2}\right)\right\}^{+}\right] \quad (22)$$

$$= \min_{1\le k\le K} \mathop{\mathbb{E}}_{\hat{h}_k,\tilde{h}_k} \left[\left\{\log\left(\frac{|\sqrt{1-\alpha}\hat{h}_k+\sqrt{\alpha}\tilde{h}_k|^2}{|\tilde{h}_k|^2}\right)\right\}^{+}\right]. \quad (23)$$

Taking the limit on both sides of (22) completes the proof.

4) Proof of the Perfect CSI Results in Corollary 2:

When the transmitter has perfect knowledge of the legitimate receivers' CSI, i.e., α=0, we have $\hat{\gamma}_k$=γ_k, yielding the result in (5). This case captures the result in [20] with the difference that in our lower bound, we have chosen an on-off power scheme.

Remark 2: When no main CSI is available at the transmitter, the secrecy capacity of the broadcast wiretap channel is equal to zero: $\mathcal{C}_{\rm s}$=0. Indeed, when the transmitter has no main CSI, i.e., α=1, each legitimate channel is statistically equivalent to $\tilde{h}$, and no power adaptation can be performed, i.e., $P(\hat{\gamma}_k)$=$P_{\rm avg}$. The eavesdropper channel is, then, equivalent to the legitimate channels, implying

$$\mathop{\mathbb{E}}_{\gamma_k,\gamma_e}\left[\log\left(1+\gamma_k P_{\rm avg}\right)\right] = \mathop{\mathbb{E}}_{\gamma_k,\gamma_e}\left[\log\left(1+\gamma_e P_{\rm avg}\right)\right]. \quad (24)$$

Thus, the upper bound vanishes, yielding $\mathcal{C}_{\rm s} = 0$.

IV. Broadcasting Independent Messages

In this section, we consider the independent messages case when multiple confidential messages are transmitted to the legitimate receivers. Taking into account the adopted system model, we present the upper and the lower bounds on the secrecy sum-capacity. The asymptotic analyses, for the high-SNR regime and the perfect CSI case, are also investigated.

A. Main Results

In this subsection, we present the main results obtained for the ergodic secrecy sum-capacity of the considered system model when broadcasting independent messages.

1) Lower and Upper Bounds:

Theorem 2: The secrecy sum-capacity, $\widetilde{\mathcal{C}}_{\rm s}$, of the fast fading broadcast channel with imperfect main CSI is bounded by

$$\widetilde{\mathcal{C}}^{-}_{\rm s} \le \widetilde{\mathcal{C}}_{\rm s} \le \widetilde{\mathcal{C}}^{+}_{\rm s}, \quad (25)$$

$$\text{such as} \quad \widetilde{\mathcal{C}}^{-}_{\rm s} = \max_{P(\tau)} \mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma^{\rm est}_{\max},\\ \hat{\gamma}_{\max}\ge\tau}} \left[\log\left(\frac{1+\gamma^{\rm est}_{\max} P(\tau)}{1+\gamma_e P(\tau)}\right)\right], \quad (26a)$$

with $\gamma^{\rm est}_{\max}$=$|\sqrt{1-\alpha}\hat{h}_{\max}+\sqrt{\alpha}\tilde{h}|^2$ and $P(\tau)$=$\frac{P_{\rm avg}}{1-F_{\hat{\gamma}_{\max}}(\tau)}$,

$$\text{and} \quad \widetilde{\mathcal{C}}^{+}_{\rm s} = \min\left\{\max_{P(\hat{\Gamma})} \mathop{\mathbb{E}}_{\gamma_{\max},\hat{\Gamma},\tilde{\gamma}} \left[\left\{\log\left(\frac{1+\gamma_{\max} P(\hat{\Gamma})}{1+\tilde{\gamma} P(\hat{\Gamma})}\right)\right\}^{+}\right], \right.$$
$$\left. K \max_{P(\hat{\gamma})} \mathop{\mathbb{E}}_{\gamma,\hat{\gamma},\tilde{\gamma}} \left[\left\{\log\left(\frac{1+\gamma P(\hat{\gamma})}{1+\tilde{\gamma} P(\hat{\gamma})}\right)\right\}^{+}\right]\right\}, \quad (26b)$$

with $\hat{\Gamma} = (\hat{\gamma}_1, \hat{\gamma}_2, \cdots, \hat{\gamma}_K)$, $\mathbb{E}[P(\hat{\Gamma})] \le P_{\rm avg}$ and $\mathbb{E}[P(\hat{\gamma})] \le P_{\rm avg}$.

2) High-SNR Regime:

Corollary 3: At high-SNR regime, the secrecy sum-capacity for the independent messages case is bounded by

$$\widetilde{\mathcal{C}}^{-}_{\text{H-SNR}} \le \widetilde{\mathcal{C}}_{\rm s} \le \widetilde{\mathcal{C}}^{+}_{\text{H-SNR}}, \quad (27)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2500563, IEEE Transactions on Wireless Communications

such as $\widetilde{\mathcal{C}}^{-}_{\text{H-SNR}}=\underset{\substack{\gamma_e,\gamma^{\text{est}}_{\max},\\ \hat{\gamma}_{\max}\geq\tau}}{\mathbb{E}}\left[\log\left(\frac{\gamma^{\text{est}}_{\max}}{\gamma_e}\right)\right]$, where the threshold τ satisfies $\underset{\gamma^{\text{est}}_{\max}|\hat{\gamma}_{\max}}{\mathbb{E}}\left[\log(\gamma^{\text{est}}_{\max})\,|\hat{\gamma}_{\max}=\tau\right]-\underset{\gamma_e}{\mathbb{E}}\left[\log(\gamma_e)\right]=0$, and

$$\widetilde{\mathcal{C}}^{+}_{\text{H-SNR}}=\min\left\{\underset{\gamma_{\max},\tilde{\gamma}}{\mathbb{E}}\left[\left\{\log\left(\frac{\gamma_{\max}}{\tilde{\gamma}}\right)\right\}^{+}\right],K\underset{\gamma,\tilde{\gamma}}{\mathbb{E}}\left[\left\{\log\left(\frac{\gamma}{\tilde{\gamma}}\right)\right\}^{+}\right]\right\}.$$

3) Perfect Main CSI case:

Corollary 4: When the transmitter has perfect knowledge of the legitimate receivers' CSI, the secrecy sum-capacity is bounded as

$$\widetilde{\mathcal{C}}^{-}_{\text{P-CSI}}\leq\widetilde{\mathcal{C}}_{\text{s}}\leq\widetilde{\mathcal{C}}^{+}_{\text{P-CSI}}, \tag{28}$$

such as $\widetilde{\mathcal{C}}^{-}_{\text{P-CSI}}=\max\limits_{P(\tau)}\underset{\gamma_e,\gamma_{\max}\geq\tau}{\mathbb{E}}\left[\log\left(\frac{1+\gamma_{\max}P(\tau)}{1+\gamma_eP(\tau)}\right)\right]$, with $P(\tau)=P_{\text{avg}}/\left(1-F_{\gamma_{\max}}(\tau)\right)$, and

$$\widetilde{\mathcal{C}}^{+}_{\text{P-CSI}}=\max_{P(\gamma_{\max})}\underset{\gamma_{\max},\gamma_e}{\mathbb{E}}\left[\left\{\log\left(\frac{1+\gamma_{\max}P(\gamma_{\max})}{1+\gamma_eP(\gamma_{\max})}\right)\right\}^{+}\right],$$

with $\mathbb{E}[P(\gamma_{\max})]\leq P_{\text{avg}}$.

B. Ergodic Capacity Analysis

In this subsection, we establish the obtained results for the ergodic secrecy sum-capacity presented in the previous subsection.

1) Proof of Achievability in Theorem 2:

The lower bound on the secrecy capacity is achieved using a time division multiplexing scheme that selects instantaneously one receiver to transmit to. That is, at each time, the source only transmits to the user with the best estimated channel gain $\hat{h}_{\max}$. Since we are transmitting to only one legitimate receiver at a time, the achieving coding scheme consists on using independent standard single user wiretap codebooks with power $P(\hat{\gamma}_{\max})$ satisfying the constraint $\mathbb{E}[P(\hat{\gamma}_{\max})]\leq P_{\text{avg}}$. We consider an on-off power scheme that instantaneously adapts the power according to the value of $\hat{\gamma}_{\max}$ with regards to a prefixed threshold τ, i.e.,

$$P(\hat{\gamma}_{\max})=\begin{cases}P(\tau)=\dfrac{P_{\text{avg}}}{1-F_{\hat{\gamma}_{\max}}(\tau)} & \hat{\gamma}_{\max}\geq\tau\\ 0 & \text{otherwise.}\end{cases} \tag{29}$$

The achievable sum-rate is then given by

$$\widetilde{\mathcal{R}}^{-}=\underset{\substack{\gamma_e,\gamma^{\text{est}}_{\max},\\ \hat{\gamma}_{\max}\geq\tau}}{\mathbb{E}}\left[\log\left(\frac{1+\gamma^{\text{est}}_{\max}P(\tau)}{1+\gamma_eP(\tau)}\right)\right]. \tag{30}$$

To finish the proof, we maximize $\widetilde{\mathcal{R}}^{-}$ over $P(\tau)$ yielding the lower bound presented in (25).

Remark 3: Using Gelfand-Pinsker coding(GPC) [23] in a broadcast context, by treating other users' signals as side information, is an effective scheme that can outperform the time division multiplexing technique [24]. In the context of secure broadcasting, and to the best of our knowledge, the works dealing with the use of GPC to establish the secrecy rate region of the broadcast channel with confidential messages, consider fixed channel gains known perfectly at the transmitter [25], [26]. Using GPC for secure broadcasting over fading channel may be a good direction that is worth investigating whether in the perfect or the imperfect CSIT cases.

2) Proof of the Upper Bound in Theorem 2:

We represent the upper bound on the secrecy sum-capacity as the minimum between two upper bounds, i.e., $\widetilde{\mathcal{C}}^{+}_{\text{s}}=\min\left\{\widetilde{\mathcal{C}}^{+}_{1},\widetilde{\mathcal{C}}^{+}_{2}\right\}$ with

$$\begin{aligned}\widetilde{\mathcal{C}}^{+}_{1}&=\max_{P(\hat{\Gamma})}\underset{\gamma_{\max},\hat{\Gamma},\tilde{\gamma}}{\mathbb{E}}\left[\left\{\log\left(\frac{1+\gamma_{\max}P(\hat{\Gamma})}{1+\tilde{\gamma}P(\hat{\Gamma})}\right)\right\}^{+}\right]\\ \widetilde{\mathcal{C}}^{+}_{2}&=K\max_{P(\hat{\gamma})}\underset{\gamma,\hat{\gamma},\tilde{\gamma}}{\mathbb{E}}\left[\left\{\log\left(\frac{1+\gamma P(\hat{\gamma})}{1+\tilde{\gamma}P(\hat{\gamma})}\right)\right\}^{+}\right].\end{aligned} \tag{31}$$

The reason behind choosing this particular representation was to ensure having the tightest possible upper bound for all the values of the error variance α. We would note that $\widetilde{\mathcal{C}}^{+}_{2}$ is a loose upper bound for the secrecy sum-rate for most values of α, especially when the number of users K is large. However, when the CSI available at the transmitter gets very noisy, i.e., $\alpha\to1$, $\widetilde{\mathcal{C}}^{+}_{2}$ becomes tighter then $\widetilde{\mathcal{C}}^{+}_{1}$. Moreover, for $\alpha=1$, $\widetilde{\mathcal{C}}^{+}_{2}$ vanishes, reflecting the fact that the secrecy capacity is zero for the no CSI case, while $\widetilde{\mathcal{C}}^{+}_{1}$ does not. To prove that $\widetilde{\mathcal{C}}^{+}_{\text{s}}$ is an upper bound, we need then to prove that both $\widetilde{\mathcal{C}}^{+}_{1}$ and $\widetilde{\mathcal{C}}^{+}_{2}$ upper bound the secrecy sum-capacity of the system.

Using the result in (12), the secrecy capacity of each legitimate receiver is upper bounded by

$$\mathcal{UB}_k=\max_{P(\hat{\gamma_k})}\underset{\gamma_k,\hat{\gamma_k},\tilde{\gamma_k}}{\mathbb{E}}\left[\left\{\log\left(\frac{1+\gamma_kP(\hat{\gamma_k})}{1+\tilde{\gamma_k}P(\hat{\gamma_k})}\right)\right\}^{+}\right], \tag{32}$$

with $k\in\{1,\cdots,K\}$. Thus, $\sum_{k=1}^{K}\mathcal{UB}_k$ is a straightforward upper bound on the secrecy sum-capacity for the independent messages case. Since all the channel gains are identically distributed, we can directly deduce that $\widetilde{\mathcal{C}}^{+}_{2}$ upper bounds the secrecy sum-capacity of the system.

Now, we need to prove that $\widetilde{\mathcal{C}}^{+}_{1}$ is also an upper bound on the secrecy sum-capacity. For that, we consider a new channel whose capacity upper bounds the capacity of the K-receivers channel with imperfect CSI at the transmitter. In order to design this new genie aided channel, we need to take two facts into consideration:

- On one hand, the receiver in the new channel needs to instantaneously get the signal transmitted over the strongest channel.

- On the other hand, the transmitter has to know the estimated gains of all K channels of the original K-receivers channel.

In point of fact, if we only consider that the transmission is intended for the strongest receiver at each time, the capacity of this channel cannot be proven to upper bound the capacity of our K-receivers channel as the transmitter will have the estimated gain of only the strong channel. That is, the new channel needs to observe all the K channels and to account for the strongest one at each time. This is what explain the idea behind considering a genie aided channel with a selection combining receiver equipped with a number of antennas equivalent to the number of legitimate receivers in the K-receivers channel. The selection combiner chooses the signal with the highest instantaneous gain and uses it for decoding. Picking the signal is equivalent to choosing the corresponding

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2500563, IEEE Transactions on Wireless Communications

antenna among all receive antennas. The output signal of the genie aided receiver after selecting the strongest signal is $Y(i) = h_{\max}(i)X(i) + v(i)$, at time instant i, with $h_{\max}$ being the channel gain of the best legitimate channel, i.e., $|h_{\max}|^2{=}\gamma_{\max}$ and $\gamma_{\max}{=}\max_{1\le k\le K}\gamma_k$. The new channel can then be modelled as

$$\begin{cases} Y(i) = h_{\max}(i)X(i) + v(i) \\ Z(i) = \ g(i)X(i) \ + \ w(i). \end{cases} \tag{33}$$

We assume that the genie-aided receiver is aware of all the channel gains $h_1, h_2, \cdots, h_K$ as well as of the transmitter's estimated gains $\hat{h}_1, \hat{h}_2, \cdots, \hat{h}_k$. The proof is conducted in two steps. First, we prove that the secrecy capacity of this new channel upper bounds the secrecy sum-capacity of the K-receivers channel with imperfect CSI (***Step 1***). Then, we prove that $\widetilde{\mathcal{C}}_1^+$ in (31) upper bounds the secrecy capacity of the genie-aided channel (***Step 2***).

Step 1: To prove this first step, it is sufficient to show that if a secrecy rate point $(\mathcal{R}_1, \mathcal{R}_2, \cdots, \mathcal{R}_K)$ is achievable on the K-receivers channel with imperfect CSI then a secrecy sum-rate $\sum_{k=1}^{K}\mathcal{R}_k$ is achievable on the new channel.
Let $(W_1,W_2,\cdots,W_K)$ be the independent transmitted messages corresponding to the rates $(\mathcal{R}_1,\mathcal{R}_2,\cdots,\mathcal{R}_K)$, and $(\hat{W}_1, \hat{W}_2, \cdots, \hat{W}_K)$ the decoded messages. Thus, for any $\epsilon{>}0$ and n large enough, there exists a code of length n such that $\Pr[\hat{W}_k \neq W_k] \le \epsilon$ at each of the K receivers, and

$$H(W_k|W_1,\cdots,W_{k-1},W_{k+1},\cdots,W_K,Z^n,g^n,H^n,\hat{H}^n)/n \ge \mathcal{R}_k - \epsilon, \tag{34}$$

with $H^n = \{h_1(1), \cdots, h_1(n), h_2(1), \cdots, h_2(n), \cdots, h_K(1), \cdots, h_K(n)\}$ and $\hat{H}^n$ defined similarly by taking $\hat{h}$ instead of h. Now, we consider the transmission of message $W{=}(W_1, W_2, \cdots, W_K)$ to the genie-aided receiver using the same encoding scheme as for the K-receivers case. Adopting a decoding scheme similar to the one used at each of the K legitimate receivers, the genie-aided receiver can decode message W with a negligible probability of error, i.e., $\Pr(\hat{W} \neq W) \le \epsilon$. For the secrecy condition, we have

$$\begin{aligned} &H(W|Z^n, g^n, H^n, \hat{H}^n)/n \\ &= H(W_1, W_2, \cdots, W_K|Z^n, , g^n, H^n, \hat{H}^n)/n && (35)\\ &\ge \sum_{k=1}^{K} H(W_k|W_1,\cdots,W_{k-1},W_{k+1},\cdots,W_K,Z^n,g^n,H^n,\hat{H}^n)/n && (36)\\ &\ge \sum_{k=1}^{K} \mathcal{R}_k - K\epsilon, && (37) \end{aligned}$$

which completes the first step of the proof.

Step 2: We have to prove that $\widetilde{\mathcal{C}}_1^+$ upper bounds the secrecy capacity of the genie-aided channel. Let $\widetilde{\mathcal{R}}_{\mathrm{e}}$ be the equivocation rate in the new channel. An upper bound on this rate is derived as

$$\begin{aligned} n\widetilde{\mathcal{R}}_{\mathrm{e}} &= H(W|Z^n, g^n, H^n, \hat{H}^n) && (38)\\ &= I(W; Y^n|Z^n,g^n,H^n,{}^{\prime}!\hat{H}^n) + H(W|Y^n,Z^n,g^n,H^n,\hat{H}^n) && (39)\\ &\le I(W; Y^n|Z^n, g^n, H^n, \hat{H}^n) + n\epsilon && (40)\\ &= \sum_{i=1}^{n} I(W; Y(i)|Z^n, g^n, H^n, \hat{H}^n, Y^{i-1}) + n\epsilon && (41)\\ &= \sum_{i=1}^{n} H(Y(i)|Z^n, g^n, H^n, \hat{H}^n, Y^{i-1}) \\ &\qquad - H(Y(i)|W, Z^n, g^n, H^n, \hat{H}^n, Y^{i-1}) + n\epsilon && (42)\\ &\le \sum_{i=1}^{n} H(Y(i)|Z(i), g(i), h_{\max}(i), \hat{H}^i) \\ &\qquad - H(Y(i)|W, X(i), Z^n, g^n, H^n, \hat{H}^n, Y^{i-1}) + n\epsilon && (43)\\ &= \sum_{i=1}^{n} H(Y(i)|Z(i), g(i), h_{\max}(i), \hat{H}^i) \\ &\qquad - H(Y(i)|X(i), Z(i), g(i), h_{\max}(i), \hat{H}^i) + n\epsilon && (44)\\ &= \sum_{i=1}^{n} I(X(i); Y(i)|Z(i), g(i), h_{\max}(i), \hat{H}^i) + n\epsilon && (45)\\ &= \sum_{i=1}^{n} \Big\{ I(X(i); Y(i)|h_{\max}(i), \hat{H}^i) - I(X(i), Z(i)|g(i), \hat{H}^i) \Big\}^+ + n\epsilon && (46) \end{aligned}$$

where inequality (40) follows from the fact that $H(W|Y^n, Z^n, g^n, H^n, \hat{H}^n) \le H(W|Y^n, H^n, \hat{H}^n)$ and Fano's inequality: $H(W|Y^n, H^n, \hat{H}^n) \le n\epsilon$, and (46) is obtained by selecting the appropriate value for the noise correlation to form the Markov chain $X(i){\to}Y(i){\to}Z(i)$ if $|h_{\max}(i)|{>}|g(i)|$ or $X(i){\to}Z(i){\to}Y(i)$ if $|h_{\max}(i)|{\le}|g(i)|$, as explained in [27].

We know that the right-hand side of (46) is maximized by a Gaussian input, then taking $X(i) \sim \mathcal{CN}\Big(0, \sqrt{\rho_i(\hat{\Gamma}^i)}\Big)$ with $\frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\Big[\rho_i(\hat{\Gamma}^i)\Big] \le P_{\text{avg}}$, we can write

$$n\widetilde{\mathcal{R}}_{\mathrm{e}} \le \sum_{i=1}^{n} \mathop{\mathbb{E}}_{\substack{\gamma_e(i),\hat{\Gamma}^i,\\ \gamma_{\max}(i)}} \left[\left\{ \log\left(\frac{1+\gamma_{\max}(i)\,\rho_i(\hat{\Gamma}^i)}{1+\gamma_e(i)\,\rho_i(\hat{\Gamma}^i)} \right) \right\}^+ \right] + n\epsilon \tag{47}$$

$$= \sum_{i=1}^{n} \mathop{\mathbb{E}}_{\substack{\gamma_e(i),\hat{\Gamma}(i),\\ \gamma_{\max}(i)}} \left[\mathop{\mathbb{E}}_{\hat{\Gamma}^{i-1}} \left[\left\{ \log\left(\frac{1+\gamma_{\max}(i)\,\rho_i(\hat{\Gamma}^i)}{1+\gamma_e(i)\,\rho_i(\hat{\Gamma}^i)} \right) \right\}^+ \Big| \hat{\Gamma}(i) \right] \right] + n\epsilon \tag{48}$$

$$\le \sum_{i=1}^{n} \mathop{\mathbb{E}}_{\substack{\gamma_e(i),\hat{\Gamma}(i),\\ \gamma_{\max}(i)}} \left[\left\{ \log\left(\frac{1+\gamma_{\max}(i) \mathop{\mathbb{E}}_{\hat{\Gamma}^{i-1}}\left[\rho_i(\hat{\Gamma}^i)|\hat{\Gamma}(i)\right]}{1+\gamma_e(i) \mathop{\mathbb{E}}_{\hat{\Gamma}^{i-1}}\left[\rho_i(\hat{\Gamma}^i)|\hat{\Gamma}(i)\right]} \right) \right\}^+ \right] + n\epsilon, \tag{49}$$

$$\le n \mathop{\mathbb{E}}_{\substack{\gamma_e,\hat{\Gamma},\\ \gamma_{\max}}} \left[\left\{ \log\left(\frac{1+\gamma_{\max}\,P(\hat{\Gamma})}{1+\gamma_e\,P(\hat{\Gamma})} \right) \right\}^+ \right] + n\epsilon, \tag{50}$$

where (49) and (50) are obtained using Jensen's inequality. The i.i.d. assumption is also used to get (50) with $P(\hat{\Gamma}){=}\frac{1}{n}\sum_{i=1}^{n}\mathop{\mathbb{E}}_{\hat{\Gamma}^{i-1}}\Big[\rho_i(\hat{\Gamma}^i)\Big|\hat{\Gamma}(i)\Big]$.

Finally, since $\gamma_{\max}{=}\max_k |\sqrt{1{-}\alpha}\hat{h}_k{+}\sqrt{\alpha}\tilde{h}_k|^2$ with $\tilde{h}_k$ independent and identically distributed as g, and since the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2500563, IEEE Transactions on Wireless Communications

transmitter only knows $\hat{h}_k$, the channel estimation error $\tilde{h}_k$ is independent of X and we can substitute g by $\tilde{h}_k$, i.e., $g{=}\tilde{h}_k$. The justification for this substitution follows along similar lines as in [12]. Therefore, $\widetilde{\mathcal{C}}_1^+$ in (31) is an upper bound on the secrecy sum-capacity. This completes the proof.

We note that, since upper bound $\widetilde{\mathcal{C}}_1^+$ is obtained by considering a new genie aided channel where the receiver gets the signal of the strongest channel and the transmitter adapts its power with all the estimated channel gains $\hat{\Gamma}{=}(\hat{\gamma}_1, \hat{\gamma}_2, \cdots, \hat{\gamma}_K)$, the argument of function $P(.)$ is a vector in this case.

3) Proof of the High-SNR Results in Corollary 3:

The proof can be conducted similarly to the common message case.

4) Proof of the Perfect CSI Results in Corollary 4:

Note that for the case of perfect main CSI at the transmitter, i.e., $\alpha{=}0$, we have $\widetilde{\mathcal{C}}_s^+{=}\widetilde{\mathcal{C}}_1^+$, with $\widetilde{\mathcal{C}}_1^+$ and $\widetilde{\mathcal{C}}_2^+$ as defined in (31). Taking this fact into consideration, the proof follows along similar lines as for the common message case.

5) Proof of the High-SNR Results in Corollary 3:

The proof can be conducted similarly to the common message case.

6) Proof of the Perfect CSI Results in Corollary 4:

Note that for the case of perfect main CSI at the transmitter, i.e., $\alpha{=}0$, we have $\widetilde{\mathcal{C}}_s^+{=}\widetilde{\mathcal{C}}_1^+$, with $\widetilde{\mathcal{C}}_1^+$ and $\widetilde{\mathcal{C}}_2^+$ as defined in (31). Taking this fact into consideration, the proof follows along similar lines as for the common message case.

V. Rayleigh Fading Channels

In this section, we examine the obtained expressions for the lower and the upper bounds on the secrecy capacity in the case of independent and identically distributed (i.i.d.) Rayleigh fading channels.

A. Broadcasting a Common Message

1) Achievable Rate: The achievable common message secrecy rate with imperfect main CSI at the transmitter, presented in (3a), can be expressed for the i.i.d. Rayleigh case as

$$\mathcal{C}_{\rm s}^- = \max_{\tau} \Bigg\{ \exp\left(\frac{\mathrm{e}^{-\tau}}{P_{\rm avg}}\right) \mathrm{Ei}\left(-\frac{\mathrm{e}^{-\tau}}{P_{\rm avg}}\right) \mathrm{e}^{-\tau} + \int_0^\infty \log(1{+}\gamma P_{\rm avg}\mathrm{e}^{\tau}) \exp(-\gamma)\, \mathrm{Q}\left(\sqrt{2\frac{1-\alpha}{\alpha}\gamma}, \sqrt{\frac{2\gamma}{\alpha}}\right) \mathrm{d}\gamma \Bigg\}, \tag{51}$$

where $\mathrm{Ei}(.)$ is the exponential integral function [28, Eq.(8.211.1)], both $\exp(.)$ and $\mathrm{e}^{(.)}$ represent the exponential function, and $\mathrm{Q}(.,.)$ stands for the Q-function [29, Eq.(16)]. Note that the integral term in (51) can be further represented in the form

$$\int_0^\infty \log(1{+}\gamma P_{\rm avg}\mathrm{e}^{\tau}) \exp(-\gamma)\, \mathrm{Q}\left(\sqrt{2\frac{1-\alpha}{\alpha}\gamma}, \sqrt{\frac{2\gamma}{\alpha}}\right) \mathrm{d}\gamma = \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} \frac{(1-\alpha)^{n+m}\tau^m \exp(-\tau/\alpha))}{\alpha^{m-1}\Gamma(1+m)\Gamma(1{+}n{+}m)}\, \mathrm{G}_{3,2}^{1,3}\left(\alpha P_{\rm avg}\mathrm{e}^{\tau}\middle|\begin{matrix}1,1,-n-m\\1,0\end{matrix}\right), \tag{52}$$

where $\Gamma(.)$ represents the gamma function [28, Eq.(8.310.1)], and $\mathrm{G}_{\cdots}^{\cdots}\left(.\middle|\begin{matrix}\cdot\\\cdot\end{matrix}\right)$ is the Meijer G-function [28, Eq.(9.301)]. Details of derivation are provided in Appendix B.

- High-SNR Regime:

At high SNR, the lower bound on the common message secrecy capacity in (4) reduces for i.i.d. Rayleigh fading channels to

$$\mathcal{C}_{\text{H-SNR}}^- = \max_{\tau} \Bigg\{ -\mathrm{Ei}(-\tau) + \mathrm{Ei}\left(-\frac{\tau}{\alpha}\right) - \mathrm{e}^{-\tau}\left(\mathrm{Ei}\left(-\frac{1-\alpha}{\alpha}\tau\right) - \log((1{-}\alpha)\tau) - \mathbf{C}\right) \Bigg\}, \tag{53}$$

where $\mathbf{C}$ is Euler's constant [28, Eq.(8.367)].

- Perfect CSI Case:

When the transmitter has perfect CSI, the lower bound on the common message secrecy capacity in (5) is given for i.i.d. Rayleigh fading channels as

$$\mathcal{C}_{\text{P-CSI}}^- = \max_{\tau} \Bigg\{ -\exp\left(\frac{\mathrm{e}^{-\tau}}{P_{\rm avg}}\right) \mathrm{Ei}\left(\frac{-\mathrm{e}^{-\tau}}{P_{\rm avg}} - \tau\right) + \mathrm{e}^{-\tau}\left(\log(1{+}P_{\rm avg}\tau\mathrm{e}^{\tau}) + \exp\left(\frac{\mathrm{e}^{-\tau}}{P_{\rm avg}}\right)\mathrm{Ei}\left(\frac{-\mathrm{e}^{-\tau}}{P_{\rm avg}}\right)\right) \Bigg\}. \tag{54}$$

2) Upper Bound: The upper bound on the common message secrecy capacity, presented in (3b), can be expressed for the i.i.d. Rayleigh fading channels' case as

$$\mathcal{C}_{\rm s}^+ = \max_{P(\hat{\rho})} \int_{-\pi}^{\pi}\int_0^\infty \int_0^{\frac{\hat{\rho}}{\rho_0(u)}} \log\left(\frac{1{+}\xi(\hat{\rho},\tilde{\rho},u)\,P(\hat{\rho})}{1{+}\tilde{\rho}^2 P(\hat{\rho})}\right) \times f_{\hat{\rho}}(\hat{\rho}) f_{\tilde{\rho}}(\tilde{\rho}) f_u(u)\mathrm{d}\hat{\rho}\mathrm{d}\tilde{\rho}\mathrm{d}u, \tag{55}$$

where $f_{\hat{\rho}}(\hat{\rho}){=}f_{\tilde{\rho}}(\hat{\rho}){=}2\hat{\rho}\,\mathrm{e}^{-\hat{\rho}^2}$,

$$\xi(\hat{\rho}_k,\tilde{\rho}_k,u_k) = (1{-}\alpha)\hat{\rho}_k^2 + \alpha\tilde{\rho}_k^2 + 2\sqrt{\alpha(1-\alpha)}\hat{\rho}_k\tilde{\rho}_k\cos(u_k),$$

$$\rho_0(u_k) = \frac{\sqrt{(1{-}\alpha)(\alpha\cos(u_k)^2{-}\alpha{+}1)} - \sqrt{\alpha(1{-}\alpha)}\cos(u_k)}{1-\alpha},$$

and

$$f_u(u) = \begin{cases} (2\pi+u)/(2\pi)^2 & -2\pi \le u < 0 \\ (2\pi-u)/(2\pi)^2 & 0 \le u < 2\pi \\ 0 & \text{elsewhere.} \end{cases}$$

- High-SNR Regime:

At high SNR, the upper bound on the common message secrecy capacity in (4) can be written for i.i.d. Rayleigh fading channels as

$$\mathcal{C}_{\text{H-SNR}}^+ = \frac{1}{\pi}\int_{-\pi}^{\pi}\int_{\rho_0(u)}^\infty \log\left((1{-}\alpha)\rho^2 + \sqrt{\alpha(1{-}\alpha)}\cos(u)\rho{+}\alpha\right) \times \frac{\rho}{(1{+}\rho^2)^2}\,\mathrm{d}\rho\mathrm{d}u. \tag{56}$$

- Perfect CSI Case:

When the transmitter has perfect CSI, the upper bound on the common message secrecy capacity in (5) is given for i.i.d. Rayleigh fading channels as

$$\mathcal{C}_{\text{P-CSI}}^+ = \max_{P(\gamma)} \int_0^\infty \mathrm{e}^{-\gamma}\left(\log(1{+}\gamma P(\gamma)) + \exp\left(\frac{1}{P(\gamma)}\right) \times \left(\mathrm{Ei}\left(-\frac{1}{P(\gamma)}\right) - \mathrm{Ei}\left(-\frac{1}{P(\gamma)} - \gamma\right)\right)\right) \mathrm{d}\gamma. \tag{57}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2500563, IEEE Transactions on Wireless Communications

B. Broadcasting Independent Messages

1) Achievable Rate: When broadcasting independent messages to K legitimate receivers over i.i.d. Rayleigh fading channels with imperfect main CSI at the transmitter, the lower bound on the secrecy capacity, presented in (25), is given by

$$\widetilde{\mathcal{C}}_{\mathrm{s}}^{-}=\max_{\tau}\left\{\exp\left(\frac{1}{P(\tau)}\right)\mathrm{Ei}\left(-\frac{1}{P(\tau)}\right)\left(1-\left(1-\mathrm{e}^{-\tau}\right)^{K}\right)\right.$$
$$+K\sum_{k=0}^{K-1}\binom{K-1}{k}\frac{(-1)^k}{1+\alpha k}\int_0^{\infty}\log(1+\gamma P(\tau))\exp\left(-\frac{(1+k)\gamma}{1+\alpha k}\right)$$
$$\left.\times\,\mathrm{Q}\left(\sqrt{2\frac{1-\alpha}{\alpha(1+\alpha k)}}\gamma,\sqrt{\frac{2\tau}{\alpha}(1+\alpha k)}\right)\mathrm{d}\gamma\right\}, \quad (58)$$

where $P(\tau)=P_{\text{avg}}/\left(1-\left(1-\mathrm{e}^{-\tau}\right)^{K}\right)$ and $\binom{\cdot}{\cdot}$ is the binomial coefficient. Note that the integral term in (58) can be further represented in the form

$$\int_0^{\infty}\log(1+\gamma P(\tau))\exp\left(-\frac{(1+k)\gamma}{1+\alpha k}\right)\mathrm{Q}\left(\sqrt{2\frac{1-\alpha}{\alpha(1+\alpha k)}}\gamma,\sqrt{\frac{2\tau}{\alpha}(1+\alpha k)}\right)\mathrm{d}\gamma$$
$$=\sum_{n=0}^{\infty}\sum_{m=0}^{\infty}\frac{(1-\alpha)^{n+m}(1+\alpha k)^{-n}\tau^m}{\alpha^{m-1}\Gamma(1+m)\Gamma(1+n+m)}\exp\left(-\frac{\tau(1+\alpha k)}{\alpha}\right)$$
$$\times\,\mathrm{G}_{3,2}^{1,3}\left(\alpha P(\tau)\middle|\begin{matrix}1,1,-n-m\\1,0\end{matrix}\right). \quad (59)$$

Details of derivation are provided in Appendix C.

- High-SNR Regime:

At high SNR, the lower bound on the independent messages secrecy capacity in (27) reduces for i.i.d. Rayleigh fading channels to

$$\widetilde{\mathcal{C}}_{\text{H-SNR}}^{-}=\max_{\tau}\left\{K\sum_{k=0}^{K-1}\binom{K-1}{k}\frac{(-1)^k}{1+\alpha k}\left(-\mathrm{Ei}(-(1+k)\tau)\right.\right.$$
$$+\mathrm{Ei}\left(-\frac{\tau(1+\alpha k)}{\alpha}\right)-\mathrm{e}^{-(1+k)\tau}\left(\mathrm{Ei}\left(\frac{\alpha-1}{\alpha}\tau\right)-\log\left(\frac{1-\alpha}{1+\alpha k}(1+k)\tau\right)\right.$$
$$\left.\left.\left.+\log\left(\frac{1+k}{1+\alpha k}\right)\right)+\mathbf{C}\left(1-\left(1-\mathrm{e}^{-\tau}\right)^{K}\right)\right)\right\}. \quad (60)$$

- Perfect CSI Case:

When the transmitter has perfect CSI, the lower bound on the independent messages secrecy capacity in (28) is given for i.i.d. Rayleigh fading channels as

$$\widetilde{\mathcal{C}}_{\text{P-CSI}}^{-}=\max_{\tau}\left\{\exp\left(\frac{1}{P(\tau)}\right)\mathrm{Ei}\left(-\frac{1}{P(\tau)}\right)\left(1-\left(1-\mathrm{e}^{-\tau}\right)^{K}\right)\right.$$
$$+K\sum_{k=0}^{K-1}\binom{K-1}{k}\frac{(-1)^k}{1+k}\left(\mathrm{e}^{-(1+k)\tau}\log(1+\tau P(\tau))\right.$$
$$\left.\left.-\exp\left(\frac{1+k}{P(\tau)}\right)\mathrm{Ei}\left(-(1+k)\left(\frac{1}{P(\tau)}+\tau\right)\right)\right)\right\}. \quad (61)$$

2) Upper Bound: The upper bound on the independent messages secrecy capacity with imperfect main CSI at the transmitter, presented in (25), can be expressed as $\widetilde{\mathcal{C}}_s^{+}=\min\left\{\widetilde{\mathcal{C}}_1^{+},\widetilde{\mathcal{C}}_2^{+}\right\}$, with $\widetilde{\mathcal{C}}_1^{+}$ and $\widetilde{\mathcal{C}}_2^{+}$ defined in (31). When transmitting to K legitimate receivers over i.i.d. Rayleigh fading channels, we have $\widetilde{\mathcal{C}}_2^{+}=K\mathcal{C}_s^{+}$, where $\mathcal{C}_s^{+}$ is given in (55), and

$$\widetilde{\mathcal{C}}_1^{+}=\max_{P(\hat{\Gamma})}\int_0^{\infty}\int_0^{\infty}\int_0^{\gamma}\log\left(\frac{1+\gamma P(\hat{\Gamma})}{1+\tilde{\gamma}P(\hat{\Gamma})}\right)f_{\hat{\Gamma}|\gamma_{\max},\tilde{\gamma}}(\hat{\Gamma}|\gamma,\tilde{\gamma})$$
$$\times\,f_{\gamma_{\max}|\tilde{\gamma}}(\gamma|\tilde{\gamma})f_{\tilde{\gamma}}(\tilde{\gamma})\,\mathrm{d}\tilde{\gamma}\mathrm{d}\gamma\mathrm{d}\hat{\Gamma}, \quad (62)$$

where $f_{\tilde{\gamma}}(\tilde{\gamma})=\mathrm{e}^{-\tilde{\gamma}}$,

$$f_{\gamma_{\max}|\tilde{\gamma}}(\gamma|\tilde{\gamma})=\frac{(1-\mathrm{e}^{-\gamma})^{K-1}}{1-\alpha}\exp\left(-\frac{\gamma+\alpha\tilde{\gamma}}{1-\alpha}\right)\mathrm{I}_0\left(2\sqrt{\frac{\alpha}{(1-\alpha)^2}\gamma\tilde{\gamma}}\right)$$
$$+(K-1)\mathrm{e}^{-\gamma}\left(1-\mathrm{e}^{-\gamma}\right)^{K-2}\left(1-\mathrm{Q}\left(\sqrt{\frac{2\alpha}{1-\alpha}}\tilde{\gamma},\sqrt{\frac{2}{1-\alpha}}\gamma\right)\right), \quad (63)$$

and

$$f_{\hat{\Gamma}|\gamma_{\max},\tilde{\gamma}}(\hat{\Gamma}|\gamma,\tilde{\gamma})=\frac{1}{\alpha}\exp\left(-\frac{\gamma+(1-\alpha)\hat{\gamma}}{\alpha}\right)\mathrm{I}_0\left(2\sqrt{\frac{1-\alpha}{\alpha^2}\gamma\hat{\gamma}}\right)$$
$$\times\frac{\mathrm{e}^{-\hat{\gamma}}\mathrm{e}^{-\hat{\gamma}_2}\cdots\mathrm{e}^{-\hat{\gamma}_K}}{\mathrm{e}^{-\gamma}(1-\mathrm{e}^{-\gamma})^{K-1}}\left(1-\mathrm{Q}\left(\sqrt{\frac{2(1-\alpha)}{\alpha}}\hat{\gamma},\sqrt{\frac{2}{\alpha}}\gamma\right)\right)^{K-1}. \quad (64)$$

- High-SNR Regime:

At high SNR, we have $\widetilde{\mathcal{C}}_2^{+}=K\mathcal{C}_{\text{H-SNR}}^{+}$, where $\mathcal{C}_{\text{H-SNR}}^{+}$ is given in (56), and

$$\widetilde{\mathcal{C}}_1^{+}=\int_0^{\infty}\int_0^{\gamma}\log\left(\frac{\gamma}{\tilde{\gamma}}\right)\mathrm{e}^{-\tilde{\gamma}}f_{\gamma_{\max}|\tilde{\gamma}}(\gamma|\tilde{\gamma})\,\mathrm{d}\tilde{\gamma}\mathrm{d}\gamma \quad (65)$$

- Perfect CSI Case:

When the transmitter has perfect CSI, the upper bound on the independent messages secrecy capacity in (28) is given for i.i.d. Rayleigh fading channels as

$$\widetilde{\mathcal{C}}_{\text{P-CSI}}^{+}=\max_{P(\gamma)}K\sum_{k=0}^{K-1}\binom{K-1}{k}(-1)^k\int_0^{\infty}\mathrm{e}^{-(k+1)\gamma}\left(\log(1+\gamma P(\gamma))\right.$$
$$\left.+\exp\left(\frac{1}{P(\gamma)}\right)\left(\mathrm{Ei}\left(-\frac{1}{P(\gamma)}\right)-\mathrm{Ei}\left(-\frac{1}{P(\gamma)}-\gamma\right)\right)\right)\mathrm{d}\gamma. \quad (66)$$

3) Scaling Law: In this subsection, we present an asymptotic analysis of the secrecy sum-capacity when transmitting to a large number of legitimate receivers, in the high-SNR regime, and over Rayleigh fading channels.

Corollary 5: The secrecy sum-capacity when broadcasting independent messages to a large number of legitimate receivers, i.e., $K\to\infty$, with an infinite average power constraint, i.e., $P_{\text{avg}}\to\infty$, is bounded by

$$\log((1-\alpha)\log(K))\le\widetilde{\mathcal{C}}_s\le\log\log K,\quad\text{for all }\alpha\neq1. \quad (67)$$

Proof of Corollary 5: In the high-SNR regime, the secrecy sum-capacity is bounded by

$$\widetilde{\mathcal{C}}_{\text{H-SNR}}^{-}\le\widetilde{\mathcal{C}}_s\le\widetilde{\mathcal{C}}_{\text{H-SNR}}^{+}, \quad (68)$$

where $\widetilde{\mathcal{C}}_{\text{H-SNR}}^{-}$ and $\widetilde{\mathcal{C}}_{\text{H-SNR}}^{+}$ are given in (27). On one hand, we have,

$$\widetilde{\mathcal{C}}_{\text{H-SNR}}^{-}=\max_{\tau}\mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma_{\max}^{\text{est}},\\ \hat{\gamma}_{\max}\ge\tau}}\left[\log\left(\frac{\gamma_{\max}^{\text{est}}}{\gamma_e}\right)\right]\ge\mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma_{\max}^{\text{est}},\\ \hat{\gamma}_{\max}}}\left[\log\left(\frac{\gamma_{\max}^{\text{est}}}{\gamma_e}\right)\right]. \quad (69)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2500563, IEEE Transactions on Wireless Communications

Since the distribution of the maximum $f_{\hat{\gamma}_{\max}}(\hat{\gamma}_{\max})$ converges toward $\delta(\hat{\gamma}_{\max}-\log K)$ as $K\to\infty$, with $\delta(.)$ is the Dirac-Delta function, it is almost sure that $\hat{\gamma}_{\max}=\log K$ as $K\to\infty$. We have then

$$\lim_{K\to\infty}\widetilde{\mathcal{C}}^{-}_{\text{H-SNR}} \geq \lim_{K\to\infty}\left(\Pr\left(\hat{\gamma}_{\max}=\log K\right) \times \mathop{\mathbb{E}}_{\gamma^{\text{est}}_{\max}}\left[\log\left(\gamma^{\text{est}}_{\max}\right)\left|\hat{\gamma}_{\max}=\log K\right.\right] - \mathop{\mathbb{E}}_{\gamma_e}\left[\log\left(\gamma_e\right)\right]\right). \quad (70)$$

Now, since $\Pr\left(\hat{\gamma}_{\max}=\log K\right)=1$ as $K\to\infty$, and the variable γ_e does not depend on K; the term $\mathop{\mathbb{E}}_{\gamma_e}\left[\log\left(\gamma_e\right)\right]$ is asymptotically dominated by $\log\log K$, i.e., $\mathop{\mathbb{E}}_{\gamma_e}\left[\log\left(\gamma_e\right)\right]=o(\log\log K)$, then

$$\lim_{K\to\infty}\widetilde{\mathcal{C}}^{-}_{\text{H-SNR}} \geq \lim_{K\to\infty}\mathop{\mathbb{E}}_{\gamma^{\text{est}}_{\max}}\left[\log\left(\gamma^{\text{est}}_{\max}\right)\left|\hat{\gamma}_{\max}=\log K\right.\right]. \quad (71)$$

Furthermore, since $\gamma^{\text{est}}_{\max}=|\sqrt{1-\alpha}\hat{h}_{\max}+\sqrt{\alpha}\tilde{h}|^2$ and

$$\sqrt{1-\alpha}|\hat{h}_{\max}|-\sqrt{\alpha}|\tilde{h}| \leq |\sqrt{1-\alpha}\hat{h}_{\max}+\sqrt{\alpha}\tilde{h}| \leq \sqrt{1-\alpha}|\hat{h}_{\max}|+\sqrt{\alpha}|\tilde{h}|, \quad (72)$$

with $|\hat{h}_{\max}|=\sqrt{\hat{\gamma}_{\max}}\to\sqrt{\log K}$, and $|\tilde{h}|=o(\log\log K)$ as $K\to\infty$, then, $\gamma^{\text{est}}_{\max}\to(1-\alpha)\log K$ as $K\to\infty$. Thus, we have

$$\lim_{K\to\infty}\mathop{\mathbb{E}}_{\gamma^{\text{est}}_{\max}}\left[\log\left(\gamma^{\text{est}}_{\max}\right)\left|\hat{\gamma}_{\max}=\log K\right.\right]-\log\left((1-\alpha)\log K\right)=0,$$

yielding

$$\lim_{K\to\infty}\widetilde{\mathcal{C}}^{-}_{\text{H-SNR}}-\log\left((1-\alpha)\log K\right)\geq 0. \quad (73)$$

An alternative, more analytical, proof of the lower bound is provided in Appendix D.

On the other hand, we have

$$\widetilde{\mathcal{C}}^{+}_{\text{H-SNR}}=\min\left\{\mathop{\mathbb{E}}_{\gamma_{\max},\tilde{\gamma}}\left[\left\{\log\left(\frac{\gamma_{\max}}{\tilde{\gamma}}\right)\right\}^{+}\right], K\mathop{\mathbb{E}}_{\gamma,\tilde{\gamma}}\left[\left\{\log\left(\frac{\gamma}{\tilde{\gamma}}\right)\right\}^{+}\right]\right\} \leq \mathop{\mathbb{E}}_{\gamma_{\max},\tilde{\gamma}}\left[\left\{\log\left(\frac{\gamma_{\max}}{\tilde{\gamma}}\right)\right\}^{+}\right]. \quad (74)$$

Considering the fact that $f_{\gamma_{\max}}(\gamma_{\max})\to\delta(\gamma_{\max}-\log K)$ and $\tilde{\gamma}=o(\log\log K)$ as $K\to\infty$, we get

$$\lim_{K\to\infty}\widetilde{\mathcal{C}}^{+}_{\text{H-SNR}}-\log\log K\leq 0. \quad (75)$$

Substituting (73) and (75) in (68) concludes the proof. It can be seen that, in the limit of large number of legitimate receivers K, the gap between the lower and the upper bounds on the secrecy sum-capacity is $\log(1-\alpha)$ for all $\alpha\neq 1$. Besides, we can see that this difference vanishes as the estimation error variance of the CSI decreases, i.e., $\alpha\to 0$.

VI. Numerical Results

In this section, we provide selected numerical results for the case of independent and identically distributed Rayleigh fading channels. We consider that the system's variables, the main channel gains h_k, $k\in\{1,\cdots,K\}$, the estimated channel gains $\hat{h}_k$, the channel estimation errors $\tilde{h}_k$ and the eavesdropper's channel gain g, are all drawn from the zero-mean, unit-variance complex Gaussian distribution.

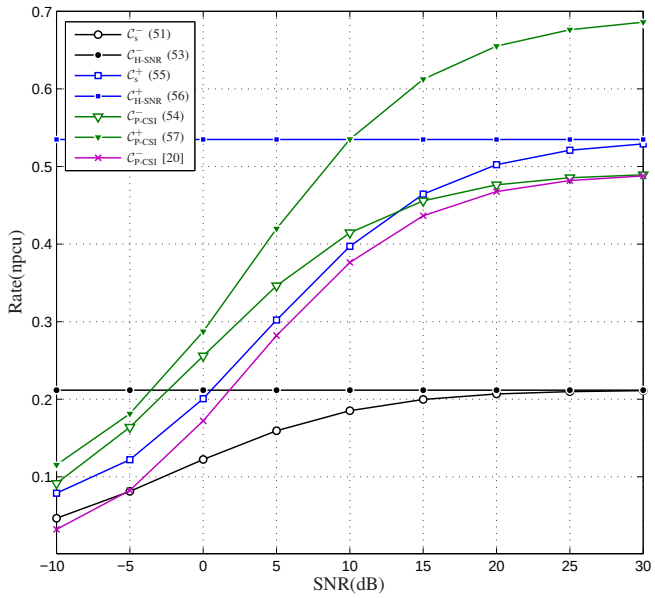

Fig. 2. Comparison of the asymptotic results for high SNR and perfect CSI with the lower and upper bounds on the common message secrecy capacity with $\alpha=0.5$.

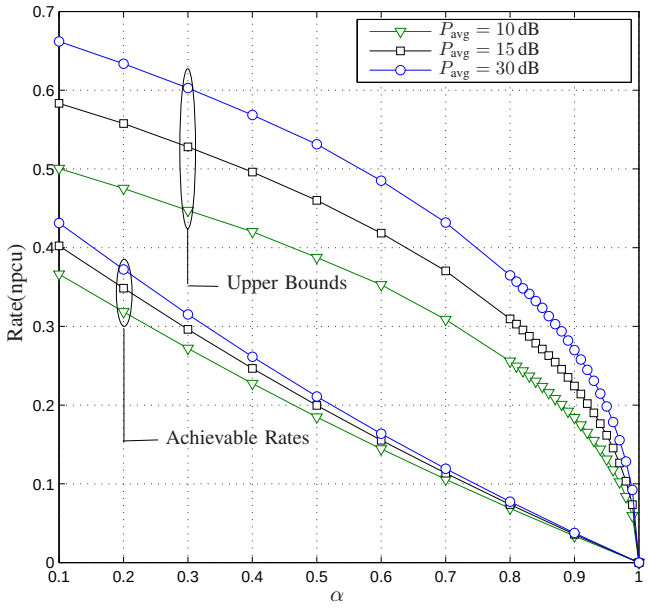

Fig. 3. Lower and upper bounds on the common message secrecy capacity in function of α.

Figure 2 presents the lower and the upper bounds on the secrecy capacity, in nats per channel use (npcu), when transmitting a common message to two legitimate receivers with $\alpha=0.5$. The special cases of high-SNR and perfect main CSI are also depicted. We can see that, at high SNR, the lower bound with perfect main CSI at the transmitter presented in this paper coincides with the one provided in [20]. However, at low SNR, the curves of the two bounds differ. This difference, at the low SNR regime, is explained by the use of different power transmission schemes.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2500563, IEEE Transactions on Wireless Communications

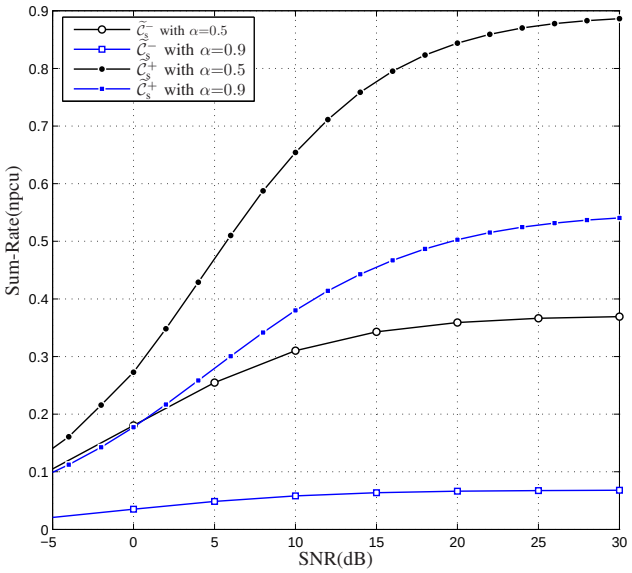

Fig. 4. Lower and upper bounds on the independent messages secrecy sum-capacity in the case of Rayleigh fading channels with K=2 and two values of the estimation error variance α, i.e., α=0.5 and α=0.9.

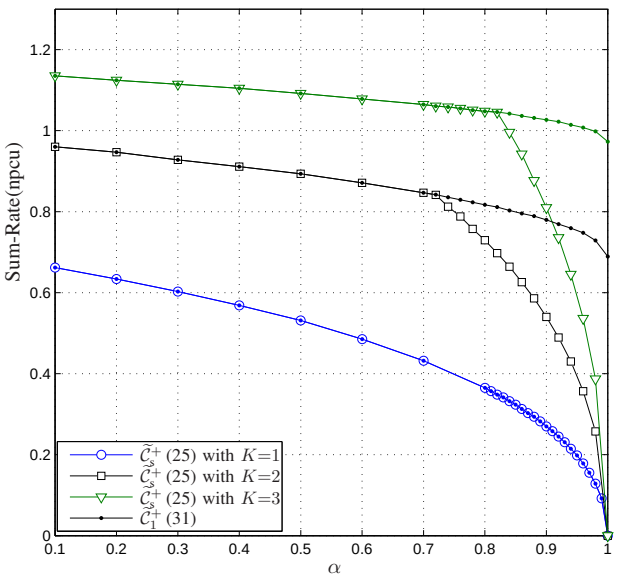

Fig. 6. Comparison between the upper bounds $\widetilde{\mathcal{C}}_s^+$ in (25) and $\widetilde{\mathcal{C}}_1^+$ in (31) for the independent messages case, in terms of α.

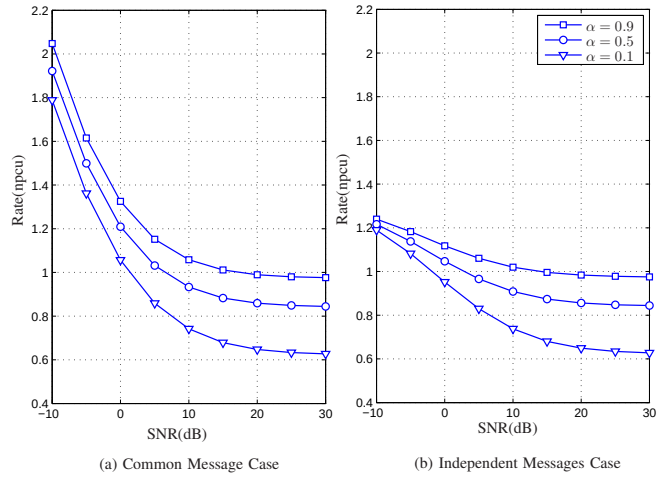

Fig. 5. Optimal on-off power parameter τ versus SNR, for Rayleigh fading channels, with K=2 and various values of α. Subfigure (a) illustrates the common message case while subfigure (b) represents the independent messages case.

The effect of changing the estimation error variance on the lower and the upper bounds on the secrecy capacity when broadcasting a common message to two legitimate receivers is illustrated in Fig. 3. We consider three different values of the average power constraint P_{avg}=10 dB, P_{avg}=15 dB and P_{avg}=30 dB. It is clear from this figure that the secrecy capacity vanishes when no main CSI is available at the transmitter (α=1). Moreover, we can see that the gap between the achievable secrecy rate and the upper bound on the secrecy capacity gets narrower as the value of P_{avg} decreases.

Figure 4 illustrates the lower and the upper bounds on the secrecy capacity when transmitting independent messages to two legitimate receivers, i.e., K=2, with two different values of the error variance, α=0.5 and α=0.9.

The variation of the threshold τ, of the On-Off power scheme, is presented in Fig. 5 for both the common message and the independent messages cases. We can see that, at high SNR, and for a given channel estimation error α, τ converges towards a fixed value. Note also that for a given SNR value, τ decreases with the channel estimation quality.

The motivation behind choosing the upper bound on the secrecy capacity as the minimum between $\widetilde{\mathcal{C}}_1^+$ and $\widetilde{\mathcal{C}}_2^+$, for the independent messages case, is highlighted in Fig. 6. Indeed, a comparison between the upper bounds $\widetilde{\mathcal{C}}_s^+$ in (25) and $\widetilde{\mathcal{C}}_1^+$ in (31) is presented, in terms of α, for K=1, 2, and 3 with P_{avg}=30 dB. In accordance with what was stated in the proof of Theorem 2, we can see that $\widetilde{\mathcal{C}}_2^+$ is a loose upper bound for the secrecy sum-rate for most values of α, especially when the number of users K is large. That is, $\tilde{\mathcal{C}}_s^+$=$\tilde{\mathcal{C}}_1^+$ for most values of α. However, when the CSI available at the transmitter gets very noisy, i.e., $\alpha\to$1, $\widetilde{\mathcal{C}}_2^+$ becomes tighter then $\widetilde{\mathcal{C}}_1^+$. Moreover, for α=1, $\widetilde{\mathcal{C}}_2^+$ vanishes, reflecting the fact that the secrecy capacity is zero for the no CSI case, while $\widetilde{\mathcal{C}}_1^+$ does not.

The upper bound on the secrecy capacity, for the independent messages case, is presented in Fig. 7 in function of the number of legitimate receiver K with P_{avg}=30 dB. We can observe that, when $K\to\infty$, the curves representing $\widetilde{\mathcal{C}}_s^+$ converge toward the perfect CSI curve (α=0) for all $\alpha > 1$. For the no CSI case (α=1), the secrecy capacity is zero.

Figure 8 considers the case when broadcasting independent messages to K legitimate receivers with an estimation error variance α=0.5 and two values for the average power constraint P_{avg}=10 dB and P_{avg}=30dB. From this figure, we can see that both the achievable secrecy sum-rate and the upper bound on the secrecy sum-rate, scale with the number of users K. That is, and in accordance with the multiuser diversity aim, the proposed achievable scheme is asymptotically optimal as the number of legitimate receivers grows. The figure shows also that the difference between the lower and the upper

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2500563, IEEE Transactions on Wireless Communications

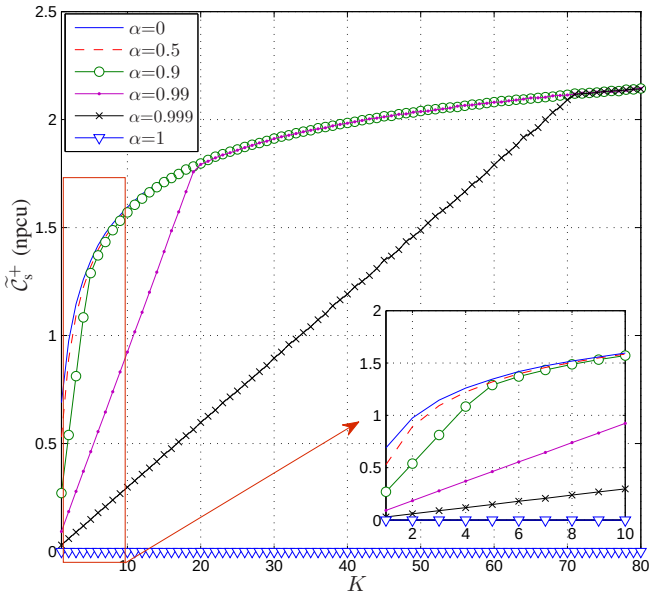

Fig. 7. Upper bound on the secrecy capacity versus the number of legitimate receivers K for the independent messages case with different values of α.

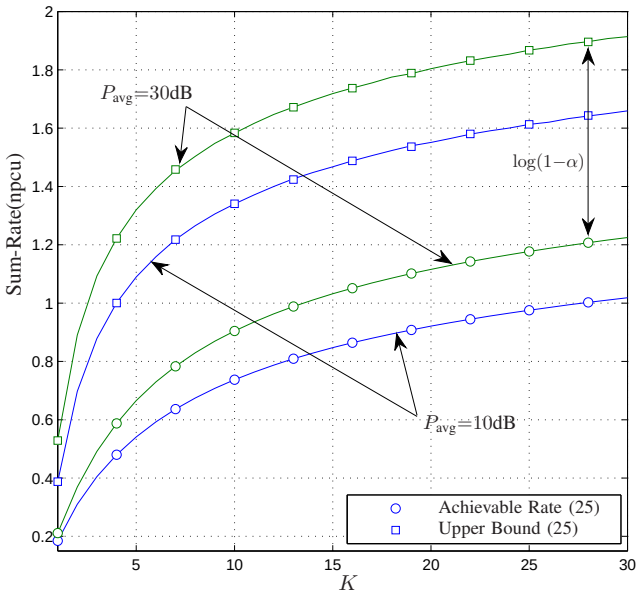

Fig. 8. Upper and Lower bounds on the secrecy sum-rate versus the number of users K with α=0.5 and two values of P_{avg}.

bounds on the secrecy sum-rate approaches $\log(1-\alpha)$ as the number of users increases. This supports our claim in Corollary 5. Note that all the results presented in this section have been verified through Monte Carlo simulations.

VII. Conclusion

In this work, we investigated the ergodic secrecy capacity of a broadcast wiretap channel over fast fading channels with imperfect main CSI at the transmitter. In particular, we analyzed the effect of the noisy estimation of the CSI on the throughput of a broadcast channel where the transmission is intended for multiple legitimate receivers in the presence of an eavesdropper and we proved that a non-zero secrecy rate can still be achieved even when the CSI at the transmitter is noisy. The obtained results show that the secrecy rate when broadcasting a common message is limited by the legitimate receiver having, on average, the worst main channel link, i.e., the legitimate receiver with the lowest average SNR. For the independent messages case, we proved that the achievable secrecy sum-rate scales with the number of users K according to the scaling law $\log((1-\alpha)\log(K))$, where α is the estimation error variance of the CSI at the transmitter. Asymptotic analysis at high-SNR, perfect and no-main CSI were addressed and the results were illustrated for the case of Rayleigh fading channels.

Appendix A
Proof of Achievability in Theorem 1

To prove the achievability of the lower bound on the secrecy capacity in (2), we adopt a coding scheme similar to the one presented in [20]. We denote the message to be transmitted by W, and we let U be a sequence of independent random variables over some alphabet $\mathcal{U}$. Also, we adopt the following notation $H=\{h_1,\cdots,h_K\}$, $H^i=\{h_1(1),\cdots,h_1(i),h_2(1),\cdots,h_2(i),\cdots,h_K(1),\cdots,h_K(i)\}$, $\hat{H}=\{\hat{h}_1,\cdots,\hat{h}_K\}$, and $\hat{H}^i=\{\hat{h}_1(1),\cdots,\hat{h}_1(i),\hat{h}_2(1),\cdots,\hat{h}_2(i),\cdots,\hat{h}_K(1),\cdots,\hat{h}_K(i)\}$. Let η_1 and η_2 be two positive constants, we define $\mathcal{R}_e = I(U;Z|g,H,\hat{H}) - \eta_2$, and $\mathcal{R}=\min_{1\le k\le K}\left\{I(U;Y_k|H,\hat{H}) - I(U;Z|g,H,\hat{H})\right\} - \eta_1$.

We construct K independent random codebooks $C_1,\cdots,C_{K+1}$, for the K legitimate subchannels. For each message W, codebook C_k is randomly partitioned into $2^{n\mathcal{R}}$ bins, such that each bin contains $2^{n\mathcal{R}_e}$ codewords. To decode the received signal, each receiver will try to find a message W that is jointly typical with the channel output Y_k. The error probability analysis are similar to the case of perfect CSI [20].

For the secrecy analysis, we need to prove that, for n sufficiently large $\frac{1}{n}I(W;Z^n|g^n,H^n,\hat{H}^n)\le\epsilon$. We have $I(W;Z^n|g^n,H^n,\hat{H}^n)=H(W|g^n,H^n,\hat{H}^n)-H(W|Z^n,g^n,H^n,\hat{H}^n)$, and

$$
\begin{aligned}
&H(W|Z^n,g^n,H^n,\hat{H}^n)\\
&=H(W,U^n|Z^n,g^n,H^n,\hat{H}^n)-H(U^n|W,Z^n,g^n,H^n,\hat{H}^n) &(76)\\
&=H(U^n|Z^n,g^n,H^n,\hat{H}^n)-H(U^n|W,Z^n,g^n,H^n,\hat{H}^n) &(77)\\
&\ge H(U^n|Z^n,g^n,H^n,\hat{H}^n)-n\epsilon_1 &(78)\\
&=H(U^n|g^n,H^n,\hat{H}^n)-I(U^n;Z^n|g^n,H^n,\hat{H}^n)-n\epsilon_1 &(79)\\
&=H(U^n,W|g^n,H^n,\hat{H}^n)-I(U^n;Z^n|g^n,H^n,\hat{H}^n)-n\epsilon_1 &(80)\\
&=H(W|g^n,H^n,\hat{H}^n)+H(U^n|W,g^n,H^n,\hat{H}^n)\\
&\qquad -I(U^n;Z^n|g^n,H^n,\hat{H}^n)-n\epsilon_1 &(81)\\
&=H(W|g^n,H^n,\hat{H}^n)+nI(U;Z|g,H,\hat{H})\\
&\qquad -I(U^n;Z^n|g^n,H^n,\hat{H}^n)-n\epsilon_1 &(82)\\
&\ge H(W|g^n,H^n,\hat{H}^n)-n\epsilon_1-n\eta_2-n\epsilon_2, &(83)
\end{aligned}
$$

where (77) and (80) follows from the fact that each codeword U^n corresponds to one message W, i.e., W is deterministic

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2500563, IEEE Transactions on Wireless Communications

given U^n, where (78) is obtained using Fano's inequality, i.e.,

$$\frac{1}{n}H(U^n|W,Z^n,g^n,H^n,\hat{H}^n) \leq \frac{1}{n}+\eta_2 R_e \triangleq \epsilon_1,$$

where (82) follows from the fact that each bin contains nR_e codewords, i.e., $H(U^n|W,g^n,H^n,\hat{H}^n)=nI(U;Z|g,H,\hat{H})-n\eta_2$, and where (83) results from the fact that the codewords are equally likely to be transmitted [1], i.e.,

$$\frac{1}{n}I(U^n;Z^n|g^n,H^n,\hat{H}^n) \leq I(U;Z|g,H,\hat{H})+\epsilon_2.$$

Taking $\epsilon=\epsilon_1+\epsilon_2+\eta_2$, we deduce the secrecy constraint. To finish the proof, we consider the proposed on-off power scheme in (7), set $X=U\sim\mathcal{CN}(0,P(\tau))$ and adopt a probabilistic transmission model as explained in Section III-B1.

Appendix B
Derivation Details of (51)

When transmitting over i.i.d. Rayleigh fading, the lower bound on the common message secrecy capacity with imperfect main CSI at the transmitter, presented in (3a), can be written as

$$\mathcal{C}_{\rm s}^{-} = \max_{P(\tau)} \int_{\gamma=0}^{\infty}\int_{\hat{\gamma}=\tau}^{\infty}\int_{\gamma_e=0}^{\infty} \log\left(\frac{1+\gamma P(\tau)}{1+\gamma_e P(\tau)}\right) \times f_{\gamma_e}(\gamma_e) f_{\gamma|\hat{\gamma}}(\gamma|\hat{\gamma}) f_{\hat{\gamma}}(\hat{\gamma}) {\rm d}\gamma_e {\rm d}\gamma {\rm d}\hat{\gamma}, \quad (84)$$

with $P(\tau)=P_{\rm avg}{\rm e}^{\tau}$, $f_{\gamma_e}(\gamma_e)={\rm e}^{-\gamma_e}$, $f_{\hat{\gamma}}(\hat{\gamma})={\rm e}^{-\hat{\gamma}}$, and

$$f_{\gamma|\hat{\gamma}}(\gamma|\hat{\gamma}) = \frac{1}{\alpha}\exp\left(-\frac{\gamma+(1-\alpha)\hat{\gamma}}{\alpha}\right){\rm I}_0\left(2\sqrt{\frac{1-\alpha}{\alpha^2}\gamma\hat{\gamma}}\right), \quad (85)$$

where ${\rm I}_0(.)$ is the modified Bessel function of the first kind [28, Eq.(8.406.3)]. We can then express (84) such as $\mathcal{C}_{\rm s}^{-}=\max_{\tau}\left\{\mathcal{I}_1-\mathcal{I}_2\right\}$, with integrals $\mathcal{I}_2$ and $\mathcal{I}_1$, respectively, given by

$$\mathcal{I}_2 = {\rm e}^{-\tau}\int_0^{\infty}\log(1+\gamma_e P_{\rm avg}{\rm e}^{\tau})\,{\rm e}^{-\gamma_e}{\rm d}\gamma_e \quad (86)$$

$$= -\exp\left(\frac{{\rm e}^{-\tau}}{P_{\rm avg}}\right){\rm Ei}\left(-\frac{{\rm e}^{-\tau}}{P_{\rm avg}}\right){\rm e}^{-\tau}, \quad (87)$$

where (87) is obtained using [28, Eq.(4.337.2)], and

$$\mathcal{I}_1 = \frac{1}{\alpha}\int_0^{\infty}\log(1+\gamma P_{\rm avg}{\rm e}^{\tau})\exp\left(-\frac{\gamma}{\alpha}\right) \times \int_{\tau}^{\infty}\exp\left(-\frac{\hat{\gamma}}{\alpha}\right){\rm I}_0\left(2\sqrt{\frac{1-\alpha}{\alpha^2}\gamma\hat{\gamma}}\right){\rm d}\hat{\gamma}{\rm d}\gamma. \quad (88)$$

Using the definition of the Q-function [29, Eq.(16)] and the appropriate change of variables, we have

$$\int_{\tau}^{\infty}\exp\left(-\frac{\hat{\gamma}}{\alpha}\right){\rm I}_0\left(2\sqrt{\frac{1-\alpha}{\alpha^2}\gamma\hat{\gamma}}\right){\rm d}\hat{\gamma} = \alpha\exp\left(\frac{1-\alpha}{\alpha}\gamma\right){\rm Q}\left(\sqrt{2\frac{1-\alpha}{\alpha}\gamma},\sqrt{\frac{2\tau}{\alpha}}\right), \quad (89)$$

which allows us to write

$$\mathcal{I}_1 = \int_0^{\infty}\log(1+\gamma P_{\rm avg}{\rm e}^{\tau})\,{\rm e}^{-\gamma}{\rm Q}\left(\sqrt{2\frac{1-\alpha}{\alpha}\gamma},\sqrt{\frac{2\tau}{\alpha}}\right){\rm d}\gamma. \quad (90)$$

Substituting $\mathcal{I}_2$ and $\mathcal{I}_1$ by their respective expressions in (87) and (90), we get (51). Now, using [30, Eq.(9)], we have

$${\rm Q}(a,b)={\rm e}^{-\frac{a^2+b^2}{2}}\sum_{n=0}^{\infty}\sum_{m=0}^{\infty}\frac{a^{2(n+m)}b^{2m}}{2^{n+2m}\Gamma(1+m)\Gamma(1+m+n)}, \quad (91)$$

we can then rewrite $\mathcal{I}_1$ in the form

$$\mathcal{I}_1 = \sum_{n=0}^{\infty}\sum_{m=0}^{\infty}\frac{(1-\alpha)^{n+m}\tau^m\exp(-\tau/\alpha))}{\alpha^{n+2m}\Gamma(1+m)\Gamma(1+n+m)} \times \int_0^{\infty}\gamma^{n+m}\log(1+\gamma P_{\rm avg}{\rm e}^{\tau})\exp\left(-\frac{\gamma}{\alpha}\right){\rm d}\gamma. \quad (92)$$

Finally, we make use of [31, Eq.(01.03.26.0004.01)], [31, Eq.(01.04.26.0003.01)], and [31, Eq.(07.34.21.0011.01)], to get

$$\mathcal{I}_1 = \sum_{n=0}^{\infty}\sum_{m=0}^{\infty}\frac{(1-\alpha)^{n+m}\tau^m\exp(-\tau/\alpha))}{\alpha^{m-1}\Gamma(1+m)\Gamma(1+n+m)} \times {\rm G}_{3,2}^{1,3}\left(\alpha P_{\rm avg}{\rm e}^{\tau}\,\middle|\,\begin{matrix}1,1,-n-m\\1,0\end{matrix}\right). \quad (93)$$

Appendix C
Derivation Details of (58)

The lower bound on the secrecy sum capacity with imperfect main CSI at the transmitter, presented in (26a), can be written for the i.i.d. Rayleigh fading channels as

$$\widetilde{\mathcal{C}}_{\rm s}^{-} = \max_{P(\tau)} \int_{\gamma=0}^{\infty}\int_{\hat{\gamma}=\tau}^{\infty}\int_{\gamma_e=0}^{\infty} \log\left(\frac{1+\gamma P(\tau)}{1+\gamma_e P(\tau)}\right) \times f_{\gamma_e}(\gamma_e) f_{\gamma_{\rm max}^{\rm est}|\hat{\gamma}_{\rm max}}(\gamma|\hat{\gamma}) f_{\hat{\gamma}_{\rm max}}(\hat{\gamma}) {\rm d}\gamma_e {\rm d}\gamma {\rm d}\hat{\gamma}, \quad (94)$$

with $P(\tau) = P_{\rm avg}/\left(1-\left(1-{\rm e}^{-\tau}\right)^K\right)$, $f_{\gamma_e}(\gamma_e)={\rm e}^{-\gamma_e}$, $f_{\hat{\gamma}_{\rm max}}(\hat{\gamma})=K{\rm e}^{-\hat{\gamma}}(1-{\rm e}^{-\hat{\gamma}})^{K-1}$, and

$$f_{\gamma_{\rm max}^{\rm est}|\hat{\gamma}_{\rm max}}(\gamma|\hat{\gamma}) = \frac{1}{\alpha}\exp\left(-\frac{\gamma+(1-\alpha)\hat{\gamma}}{\alpha}\right){\rm I}_0\left(2\sqrt{\frac{1-\alpha}{\alpha^2}\gamma\hat{\gamma}}\right).$$

We can then express (94) such as

$$\mathcal{C}_{\rm s}^{-} = \max_{\tau}\left\{\widetilde{\mathcal{I}}_1-\widetilde{\mathcal{I}}_2\right\}, \quad (95)$$

with integrals $\widetilde{\mathcal{I}}_2$ and $\widetilde{\mathcal{I}}_1$, respectively, given by

$$\widetilde{\mathcal{I}}_2 = K\int_{\tau}^{\infty}\int_0^{\infty}\log\left(1+\gamma_e P(\tau)\right){\rm e}^{-\gamma_e}{\rm e}^{-\hat{\gamma}}(1-{\rm e}^{-\hat{\gamma}})^{K-1}{\rm d}\gamma_e{\rm d}\hat{\gamma} \quad (96)$$

$$= \left(1-\left(1-{\rm e}^{-\tau}\right)^K\right)\int_0^{\infty}\log\left(1+\gamma_e P(\tau)\right){\rm e}^{-\gamma_e}{\rm d}\gamma_e \quad (97)$$

$$= -\left(1-\left(1-{\rm e}^{-\tau}\right)^K\right)\exp\left(\frac{1}{P(\tau)}\right){\rm Ei}\left(-\frac{1}{P(\tau)}\right), \quad (98)$$

where (98) is obtained using [28, Eq.(4.337.2)], and

$$\widetilde{\mathcal{I}}_1 = \frac{K}{\alpha}\int_0^{\infty}\int_{\tau}^{\infty}\log\left(1+\gamma P(\tau)\right)\exp\left(-\frac{\gamma+(1-\alpha)\hat{\gamma}}{\alpha}\right) \times {\rm I}_0\left(2\sqrt{\frac{1-\alpha}{\alpha^2}\gamma\hat{\gamma}}\right){\rm e}^{-\hat{\gamma}}(1-{\rm e}^{-\hat{\gamma}})^{K-1}{\rm d}\hat{\gamma}{\rm d}\gamma. \quad (99)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2500563, IEEE Transactions on Wireless Communications

Using the binomial theorem [28, Eq.(1.111)] along with equation (89), integral $\widetilde{\mathcal{I}}_1$ can be given by

$$\widetilde{\mathcal{I}}_1=K\sum_{k=0}^{K-1}\binom{K-1}{k}\frac{(-1)^k}{1+\alpha k}\int_0^{\infty}\log(1+\gamma P(\tau))\exp\left(-\frac{(1+k)\gamma}{1+\alpha k}\right)\times \mathrm{Q}\left(\sqrt{2\frac{1-\alpha}{\alpha(1+\alpha k)}\gamma},\sqrt{\frac{2\tau}{\alpha}(1+\alpha k)}\right)\mathrm{d}\gamma. \quad (100)$$

Substituting $\widetilde{\mathcal{I}}_2$ and $\widetilde{\mathcal{I}}_1$ in (95) by their respective expressions in (98) and (100), we get (58).

Appendix D
Alternative Proof of the Lower Bound in Corollary 5

At high-SNR, the achievable secrecy sum-rate is given by (27), i.e.,

$$\widetilde{\mathcal{C}}^{-}_{\text{H-SNR}}=\mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma^{\text{est}}_{\max},\\ \hat{\gamma}_{\max}\geq\tau}}\left[\log\left(\frac{\gamma^{\text{est}}_{\max}}{\gamma_e}\right)\right] \quad (101)$$

$$=\int_0^{\infty}\int_{\tau}^{\infty}\int_0^{\infty}\log\left(\frac{\gamma}{\gamma_e}\right)f_{\gamma_e}(\gamma_e)f_{\gamma^{\text{est}}_{\max}|\hat{\gamma}_{\max}}(\gamma|\hat{\gamma})f_{\hat{\gamma}_{\max}}(\hat{\gamma})\mathrm{d}\gamma_e\mathrm{d}\hat{\gamma}\mathrm{d}\gamma.$$

Since $f_{\hat{\gamma}_{\max}}(\hat{\gamma}_{\max})\xrightarrow[K\to\infty]{}\delta(\hat{\gamma}_{\max}-\log K)$ as $K\to\infty$, then, we can write

$$\lim_{K\to\infty}\widetilde{\mathcal{C}}^{-}_{\text{H-SNR}}=\lim_{K\to\infty}\left(\frac{1}{\alpha}\int_0^{\infty}\log(\gamma)\exp\left(-\frac{\gamma+(1-\alpha)\log K}{\alpha}\right)\times\mathrm{I}_0\left(2\sqrt{\frac{1-\alpha}{\alpha^2}\log K\gamma}\right)\mathrm{d}\gamma-\mathop{\mathbb{E}}_{\gamma_e}\left[\log\gamma_e\right]\right), \quad (102)$$

and since the variable γ_e does not depend on K, the term $\mathop{\mathbb{E}}_{\gamma_e}\left[\log\left(\gamma_e\right)\right]$ is asymptotically dominated by $\log\log K$, i.e., $\mathop{\mathbb{E}}_{\gamma_e}\left[\log\left(\gamma_e\right)\right]=o(\log\log K)$. Thus, we have

$$\lim_{K\to\infty}\widetilde{\mathcal{C}}^{-}_{\text{H-SNR}}=\lim_{K\to\infty}\left(\frac{1}{\alpha}\exp\left(\frac{\alpha-1}{\alpha}\log K\right)\times\int_0^{\infty}\log(\gamma)\exp\left(-\frac{\gamma}{\alpha}\right)\mathrm{I}_0\left(2\sqrt{\frac{1-\alpha}{\alpha^2}\log K\gamma}\right)\mathrm{d}\gamma\right) \quad (103)$$

$$\overset{(a)}{=}\lim_{K\to\infty}\left(\frac{1}{\alpha}\exp\left(\frac{\alpha-1}{\alpha}\log K\right)\sum_{m=0}^{\infty}\frac{1}{\Gamma(m+1)m!}\times\left(\frac{1-\alpha}{\alpha^2}\log K\right)^m\int_0^{\infty}\gamma^m\log(\gamma)\exp\left(-\frac{\gamma}{\alpha}\right)\mathrm{d}\gamma\right)$$

$$\overset{(b)}{=}\lim_{K\to\infty}\left(\frac{1}{\alpha}\exp\left(\frac{\alpha-1}{\alpha}\log K\right)\left(\left(\log\alpha-\mathbf{C}\right)\times\sum_{m=0}^{\infty}\frac{(1-\alpha)^m(\log K)^m}{\alpha^{m-1}m!}+\sum_{m=0}^{\infty}\frac{\mathrm{H}_m(1-\alpha)^m(\log K)^m}{\alpha^{m-1}m!}\right)\right)$$

$$\overset{(c)}{=}\lim_{K\to\infty}\left(\log((1-\alpha)\log K)-\mathrm{Ei}\left(-\frac{1-\alpha}{\alpha}\log K\right)\right),$$

where (a) is obtained using $\mathrm{I}_v(z)=\sum_{m=0}^{\infty}\frac{\left(\frac{z}{2}\right)^{2m+v}}{\Gamma(m+v+1)m!}$, (b) follows from

$$\int_0^{\infty}\gamma^m\log(\gamma)\exp\left(-\frac{\gamma}{\alpha}\right)\mathrm{d}\gamma=\alpha^{m+1}\Gamma(m+1)\left(\log\alpha+\mathrm{H}_m-\mathbf{C}\right),$$

with H_m is the harmonic number, and (c) comes from

$$\sum_{m=0}^{\infty}\frac{(1-\alpha)^m(\log K)^m}{\alpha^{m-1}m!}=\alpha K^{\frac{1-\alpha}{\alpha}},$$

and

$$\sum_{m=0}^{\infty}\frac{\mathrm{H}_m(1-\alpha)^m(\log K)^m}{\alpha^{m-1}m!}=\alpha K^{\frac{1-\alpha}{\alpha}}\times\left(\mathbf{C}-\mathrm{Ei}\left(-\frac{1-\alpha}{\alpha}\log K\right)+\log\left(\frac{1-\alpha}{\alpha}\log K\right)\right). \quad (104)$$

Now, since $\lim_{K\to\infty}\mathrm{Ei}\left(-\frac{1-\alpha}{\alpha}\log K\right)=0$, then we have $\lim_{K\to\infty}\left[\widetilde{\mathcal{C}}^{-}_{\text{H-SNR}}-\log((1-\alpha)\log K)\right]=0$.

References

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

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

[3] E. A. Jorswieck, A. Wolf, and S. Gerbracht, *Trends in Telecommunications Technologies: Secrecy on the Physical Layer in Wireless Networks*. InTech, 2010.

[4] 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.

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

[6] Z. Li, R. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *Proc. International Symposiumon on Information Theory (ISIT'2007)*, Nice, France, jul. 2007, pp. 1296–1300.

[7] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "An opportunistic physical-layer approach to secure wireless communications," in *Proc. 44th Allerton conference on Communication Control and Computing*, Monticello, IL,USA, Sep. 2006.

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

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

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

[11] Z. Rezki, A. Khisti, and M.-S. Alouini, "On the ergodic secrecy capacity of the wiretap channel under imperfect main channel estimation," in *Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR'2011)*, Pacific Grove, CA, Nov. 2011, pp. 952–957.

[12] ——, "On the secrecy capacity of the wiretap channel under imperfect main channel estimation," *IEEE Transactions on Communications*, vol. 62, no. 10, pp. 3652–3664, Sep. 2014.

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

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

[15] 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)*, Baltimore, MD, Mar. 2007, pp. 905 –910.

[16] S. Shafiee and S. Ulukus, "Achievable rates in gaussian MISO channels with secrecy constraints," in *Proc. International Symposiumon on Information Theory (ISIT'2007)*, Nice, France, Jun. 2007, pp. 2466–2470.

[17] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. International Symposiumon on Information Theory (ISIT'2007)*, Nice, France, Jun. 2007, pp. 2471–2475.

[18] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference (VTC-2005-Fall)*, Dallas, USA, Sept. 2005, pp. 1906–1910.

[19] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

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

[21] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel with collective secrecy constraints," in *Proc. International Symposiumon on Information Theory (ISIT'2006)*, Seattle, USA, Jul. 2006, pp. 1164–1168.

[22] A. Khisti, A. Tchamkerten, and G. Wornell, "Secure broadcasting with multiuser diversity," in *Proc. 44th Allerton Conference on Communication, Control, and Computing*, Monticello, IL,USA, Sep. 2006.

[23] S. Gelfand and M. Pinsker, "Coding for channels with random parameters," *Problems of Control and Information Theory*, vol. 9, no. 1, p. 1931, 1980.

[24] G. Caire and S. Shamai, "On the achievable throughput of a multiantenna Gaussian broadcast channel," *IEEE Transactions on Information Theory*, vol. 49, no. 7, pp. 1691–1706, Jul. 2003.

[25] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[26] R. Liu and H. V. Poor, "Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages," *IEEE Transactions on Information Theory*, vol. 55, no. 3, p. 12351249, Mar. 2009.

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

[28] I. S. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Amsterdam: Elsevier/Academic Press, 2007.

[29] J. I. Marcum, "Statistical theory of target detection by pilsed radar: Mathematical appendix," in *RAND Corporation*, Santa Monica, California, Research Memorandum No. RM-753, Jul. 1948.

[30] D. Morales-Jimenez, F. Lopez-Martinez, E. Martos-Naya, J. Paris, and A. Lozano, "Connections between the generalized Marcum Q-function and a class of hypergeometric functions," *IEEE Transactions on Information Theory*, vol. 60, no. 2, pp. 1077–1082, Feb. 2014.

[31] I. Wolfram Research, *Mathematica Edition: Version 8.0.* Champaign Illinois: Wolfram Research, Inc., 2010.

Amal Hyadi (S'12) was born in Rabat, Morocco. She received the Diplôme d'Ingénieur from the Institut Nationale des Postes et Télécommunications (INPT), Rabat, Morocco, in 2011, and the M.S. degree from King Abdullah University of Science and Technology (KAUST), Thuwal, Mekkah Province, Saudi Arabia, in 2013, where she is currently working toward the Ph.D. degree in Electrical Engineering. Her research interests include: physical-layer security, performance analysis of cooperative cognitive systems and relay selection techniques.

Zouheir Rezki (S'01-M'08-SM'13) was born in Casablanca, Morocco. He received the Diplôme d'Ingénieur degree from the École Nationale de l'Industrie Minérale (ENIM), Rabat, Morocco, in 1994, the M.Eng. degree from École de Technologie Supérieure, Montreal, Québec, Canada, in 2003, and the Ph.D. degree from École Polytechnique, Montreal, Québec, in 2008, all in electrical engineering. From October 2008 to September 2009, he was a postdoctoral research fellow with Data Communications Group, Department of Electrical and Computer Engineering, University of British Columbia. He is now a Senior Research Scientist at King Abdullah University of Science and Technology (KAUST), Thuwal, Mekkah Province, Saudi Arabia. His research interests include: performance limits of communication systems, physical-layer security, cognitive and sensor networks and low-complexity detection algorithms.

Ashish Khisti is an Associate Professor at the University of Toronto and holds a Canada Research Chair in Wireless Networks. He obtained his BASc degree from the Engineering Sciences program (Electrical Engineering Option) at the same university in 2002, and his SM and PhD degrees from the Massachusetts Institute of Technology (MIT) in Electrical Engineering and Computer Science in 2004 and 2009 respectively. His research interests include Information Theory, Physical Layer Security and Error Control Coding for Multimedia Applications. He also actively consults telecommunication companies. He is a recipient of the HP-IRP award from Hewlett-Packard and an Ontario Early Researcher Award. He presently serves as a Associate Editor in Shannon Theory for the IEEE Transactions on Information Theory.

Mohamed-Slim Alouini (S'94-M'98-SM'03-F'09) was born in Tunis, Tunisia. He received the Ph.D. degree in Electrical Engineering from the California Institute of Technology (Caltech), Pasadena, CA, USA, in 1998. He served as a faculty member in the University of Minnesota, Minneapolis, MN, USA, then in the Texas A&M University at Qatar, Education City, Doha, Qatar before joining King Abdullah University of Science and Technology (KAUST), Thuwal, Makkah Province, Saudi Arabia as a Professor of Electrical Engineering in 2009. His current research interests include the modeling, design, and performance analysis of wireless communication systems.