Secrecy Capacity of Wireless Channels

João Barros
Department of Computer Science & LIACC/UP
Universidade do Porto, Portugal
http://www.dcc.fc.up.pt/~barros

Miguel R. D. Rodrigues
Computer Laboratory
University of Cambridge, United Kingdom
http://www.cl.cam.ac.uk/Research/DTG/~mrdr3/

***Abstract*— We consider the transmission of confidential data over wireless channels with multiple communicating parties. Based on an information-theoretic problem formulation in which two legitimate partners communicate over a quasi-static fading channel and an eavesdropper observes their transmissions through another independent quasi-static fading channel, we define the *secrecy capacity* in terms of outage probability and provide a complete characterization of the maximum transmission rate at which the eavesdropper is unable to decode any information.**
In sharp contrast with known results for Gaussian wiretap channels (without feedback), our contribution shows that in the presence of fading information-theoretic security is achievable even when the eavesdropper has a better average signal-to-noise ratio (SNR) than the legitimate receiver — fading thus turns out to be a friend and not a foe.

I. Introduction

The issues of privacy and security in wireless communication networks have taken on an increasingly important role as these networks continue to flourish worldwide. Traditionally, security is viewed as an independent feature with little or no relation to the remaining data communication tasks and, therefore, state-of-the-art encryption algorithms are insensitive to the physical nature of the wireless medium.

In contrast with this paradigm, there exist both theoretical and practical contributions (most notably [1], [2], [3] and [4]) that support the potential of physical layer security ideas to significantly strengthen the security of digital communication systems. The basic principle of *information-theoretic security* — widely accepted as the strictest notion of security — calls for the combination of cryptographic schemes with channel coding techniques that exploit the randomness of the communication channels to guarantee that the sent messages cannot be decoded by a third party maliciously eavesdropping on the wireless medium (see Fig. 1).

The theoretical basis for this information-theoretic approach, which builds on Shannon's notion of *perfect secrecy* [5], was laid by Wyner [6] and later by Csiszár and Körner [7], who proved in seminal papers that there exist channel codes guaranteeing both robustness to transmission errors and a prescribed degree of data confidentiality. In the wiretap channel proposed by Wyner, two legitimate users communicate over a main channel and an eavesdropper has access to degraded versions of the channel outputs that reach the legitimate receiver. In [8] it was shown that if both the main channel and the wiretap channel are additive white Gaussian noise (AWGN) channels, and the latter has less capacity than the former, the *secrecy capacity* (i.e. the maximum transmission rate at which the eavesdropper is unable to decode any information) is equal to the difference between the two channel capacities. Consequently, confidential communication is not possible unless the Gaussian main channel has a better signal-to-noise ratio (SNR) than the Gaussian wiretap channel.

Motivated by the general problem of securing transmissions over wireless channels, we consider the impact of fading on the secrecy capacity. Our contributions are as follows: (a) an information-theoretic formulation of the problem of secure communication over wireless channels; (b) a characterization of the secrecy capacity of single-antenna quasi-static Rayleigh fading channels in terms of outage probability; (c) a simple analysis of the impact of user location on the achievable level of secrecy; (d) a rigorous comparison with the Gaussian wiretap channel evidencing the benefits of fading towards achieving a higher level of security. Among the different conclusions to be drawn from our results perhaps the most striking one is that, in the presence of fading, information-theoretic security is achievable even when the eavesdropper's channel has a better average SNR than the main channel.

The rest of the paper is organized as follows. First, Section II provides an information-theoretic formulation of the problem of secure communication over fading channels. Then, Section III analyzes the secrecy capacity of a quasi-static Rayleigh fading channel in terms of outage probability. The main results and their implications are finally discussed in detail in Section IV, which concludes the paper.

II. Problem Statement

Consider the problem setup illustrated in Fig. 2. A legitimate user named Alice wants to send messages w to another user, say

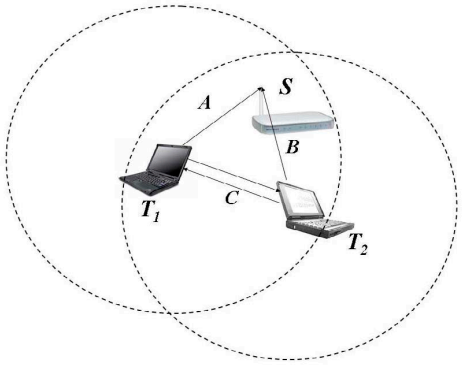

Fig. 1. Example of a wireless network with potential eavesdropping. Terminals T_1 and T_2 communicate with a base station S over a wireless medium (channels A and B). By listening to the transmissions of terminal T_1 (through channel C), terminal T_2 may acquire confidential information. If T_1 wants to exchange a secret key or guarantee the confidentiality of its transmitted data, it can exploit the *physical* properties of the wireless channel to secure the information by *coding* against Terminal T_2.

Part of this work is based on results of the IST FP6 Integrated Project DAIDALOS, which receives research funding from the European Community's Sixth Framework Programme. Apart from this, the European Commission has no responsibility for the content of this paper. The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

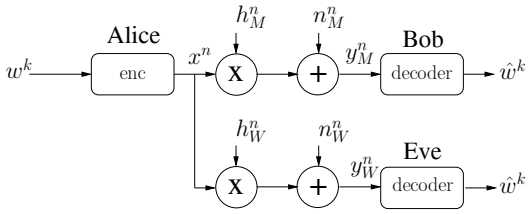

Fig. 2. Problem setup.

Bob. The message block w^k is encoded into the codeword $x^n = [x(1), \ldots, x(i), \ldots, x(n)]$ to be transmitted over a discrete-time Rayleigh fading channel (the *main* channel) with output

$$y_M(i) = h_M(i)x(i) + n_M(i),$$

where $h_M(i)$ is the time-varying complex fading coefficient and $n_M(i)$ denotes the zero-mean circularly symmetric complex Gaussian noise. The coefficient $h_M(i)$, also referred to as *channel side information* (CSI), is independent from the channel output and assumed to be drawn i.i.d. according to the probability distribution $p(h_M)$, which is zero-mean complex Gaussian for Rayleigh fading. We assume quasi-static fading, i.e. the fading coefficients are constant for all channel uses (or, equivalently, for all time), i.e., $h_M(i) = h_M, \forall i$.

A third party, whose name is Eve, is capable of eavesdropping the signals sent by Alice by observing the channel output

$$y_W(i) = h_W(i)x(i) + n_W(i),$$

of an independent Rayleigh fading channel, with quasi-static fading coefficient $h_W(i) = h_W, \forall i$, and zero-mean circularly symmetric complex Gaussian noise $n_W(i)$.

The channel is power limited in the sense that

$$\frac{1}{n}\sum_{i=1}^{n} \mathrm{E}\left[|X(i)|^2\right] \leq P,$$

where P corresponds to the average transmit signal power. Furthermore, we denote the power of the noise in the main channel and the eavesdropper's channel as N_M and N_W, respectively. The instantaneous SNR at Bob's receiver is thus given by

$$\gamma_M(i) = P|h_M(i)|^2/N_M = P|h_M|^2/N_M = \gamma_M$$

and the average SNR value is

$$\overline{\gamma}_M(i) = P\,\mathrm{E}\left[|h_M(i)|^2\right]/N_M = P\,\mathrm{E}\left[|h_M|^2\right]/N_M = \overline{\gamma}_M.$$

Likewise, the instantaneous SNR at Alice's receiver is given by

$$\gamma_W(i) = P|h_W(i)|^2/N_W = P|h_W|^2/N_W = \gamma_W$$

and the average SNR value is

$$\overline{\gamma}_W(i) = P\,\mathrm{E}\left[|h_W(i)|^2\right]/N_W = P\,\mathrm{E}\left[|h_W|^2\right]/N_W = \overline{\gamma}_W.$$

It will also be useful to consider the probability density function (pdf) of γ_M and γ_W. Since the channel fading coefficients h are zero-mean complex Gaussian random variables [9, p. 188] and the instantaneous SNR $\gamma \propto |h|^2$, it follows that γ is exponentially distributed, specifically

$$p(\gamma_M) = \frac{1}{\overline{\gamma}_M}\exp\left(-\frac{\gamma_M}{\overline{\gamma}_M}\right), \qquad \gamma_M > 0 \tag{1}$$

and

$$p(\gamma_W) = \frac{1}{\overline{\gamma}_W}\exp\left(-\frac{\gamma_W}{\overline{\gamma}_W}\right), \qquad \gamma_W > 0. \tag{2}$$

The transmission rate between Alice and Bob is $R = H(W^k)/n$ and the error probability is defined as $\mathcal{P}_\epsilon^k = \mathcal{P}(W^k \neq \hat{W}^k)$, where $\hat{W}^k$ denotes Bob's estimate of the sent messages. We are interested in maximizing not only the transmission rate between Alice and Bob but also Eve's uncertainty about w, i.e. the equivocation rate $\Delta = H(W^k|Y_W^n)/H(W^k)$[1].

We say that (R', d') is achievable if for all $\epsilon > 0$ there exists an encoder-decoder pair such that $R \geq R' - \epsilon$, $\Delta \geq d' - \epsilon$, and $\mathcal{P}_\epsilon^k \leq \epsilon$. Our goal is to characterize the *secrecy capacity* C_s defined as the maximum transmission rate R at $\Delta = 1$.

In the rest of the paper, we will assume that Alice and Bob have perfect CSI about the main channel, but no CSI about the wiretap channel. Eve in turn has CSI on the wiretap channel [2]. The operational significance of this set of definitions and the implications of the underlying assumptions will become clear in the next section.

III. Secrecy Capacity of Quasi-Static Rayleigh Fading Channels

This section characterizes the secrecy capacity of a quasi-static Rayleigh fading channel in terms of outage probability. First, we consider a single realization of the fading coefficients and compute its secrecy capacity. Then, we discuss the existence of (strictly positive) secrecy capacity in the general case, and build upon the resulting insights to characterize the outage probability and the outage secrecy capacity.

A. Preliminaries

We start by deriving the secrecy capacity for one realization of a pair of quasi-static fading channels with complex noise and complex fading coefficients.

For this purpose, we start by recalling the results of [8] for the real-valued Gaussian wiretap channel, where it is assumed that Alice and Bob communicate over a standard real additive white Gaussian noise (AWGN) channel with noise power N_M and Eve's observation is also corrupted by Gaussian noise with power $N_W > N_M$, i.e. Eve's receiver has lower SNR than Bob's. The power is constrained according to $\frac{1}{n}\sum_{i=1}^{n}\mathrm{E}\left[X(i)^2\right] \leq P$. For this instance, the secrecy capacity is given by

$$C_s = C_M - C_W, \tag{3}$$

where

$$C_M = \frac{1}{2}\log\left(1 + \frac{P}{N_M}\right)$$

is the capacity of the main channel and

$$C_W = \frac{1}{2}\log\left(1 + \frac{P}{N_W}\right)$$

denotes the capacity[3] of the eavesdropper's channel.

Suppose now that both the main and the wiretap channel are complex AWGN channels, i.e. transmit and receive symbols are

[1] A stricter security condition can be introduced using the tools in [10]

[2] Note that CSI on the main channel is of no use to Eve, because the equivocation rate depends only on the output of the wiretap channel.

[3] Unless otherwise specified, all logarithms are taken to base two.

complex and both additive noise processes are zero mean circularly symmetric complex Gaussian. The power of the complex input X is constrained according to $\frac{1}{n}\sum_{i=1}^{n}\mathrm{E}\left[|X(i)|^2\right] \leq P$. Since each use of the complex AWGN channel can be viewed as two uses of a real-valued AWGN channel [9, Appendix B], the secrecy capacity of the complex wiretap channel follows from (3) as

$$C_s = \log\left(1+\frac{P}{N_M}\right) - \log\left(1+\frac{P}{N_W}\right),$$

per complex dimension[4].

In a final step, we consider complex fading coefficients for both the main channel and the eavesdropper's channel, as detailed in Section II. Since in the quasi-static case h_M and h_W are random but remain constant for all time, it is perfectly reasonable to view the main channel (with fading) as a complex AWGN channel [9, Chapter 5] with SNR $\gamma_M = P|h_M|^2/N_M$ and capacity

$$C_M = \log\left(1+|h_M|^2\frac{P}{N_M}\right).$$

Similarly, the capacity of the eavesdropper's channel is given by

$$C_W = \log\left(1+|h_W|^2\frac{P}{N_W}\right),$$

with SNR $\gamma_W = P|h_W|^2/N_W$. Thus, once again based on (3) and the nonnegativity of channel capacity, we may write the secrecy capacity for one realization of the quasi-static fading scenario as

$$C_s = \begin{cases} \log(1+\gamma_M) - \log(1+\gamma_W) & \text{if } \gamma_M > \gamma_W \\ 0 & \text{if } \gamma_M \leq \gamma_W. \end{cases} \quad (4)$$

B. Existence of Secrecy Capacity

We will now consider the existence of a secrecy capacity between Alice and Bob. As explained in Section III-A, for specific fading realizations, the main channel (from Alice to Bob) and the eavesdropper's channel (from Alice to Eve) can be viewed as complex AWGN channels with SNR γ_M and γ_W, respectively. Moreover, from (4) it follows that the secrecy capacity is positive when $\gamma_M > \gamma_W$ and is zero when $\gamma_M \leq \gamma_W$. Invoking independence between the main channel and the eavesdropper's channel and knowing that the random variables γ_M and γ_W are exponentially distributed with probability density functions given by (1) and (2), respectively, we may write the probability of existence of a non-zero secrecy capacity as

$$\begin{aligned} \mathcal{P}(C_s>0) &= \mathcal{P}(\gamma_M>\gamma_W) \\ &= \int_0^\infty\int_0^{\gamma_M} p(\gamma_M,\gamma_W)d\gamma_W d\gamma_M \\ &= \int_0^\infty\int_0^{\gamma_M} p(\gamma_M)p(\gamma_W)d\gamma_W d\gamma_M \\ &= \frac{\overline{\gamma}_M}{\overline{\gamma}_M+\overline{\gamma}_W}. \end{aligned} \quad (5)$$

From the point of view of user location, noting that $\overline{\gamma}_M \propto 1/d_M^\alpha$ and $\overline{\gamma}_W \propto 1/d_W^\alpha$ where d_M is the distance between Alice and Bob, d_W is the distance between Alice and Eve, and α is the pathloss exponent [11], the probability in (5) is given by

$$\mathcal{P}(C_s>0) = \frac{1}{1+(d_M/d_W)^\alpha} \quad (6)$$

[4]Alternatively, this result can be proven by repeating step by step the proofs of [8] using complex-valued random variables instead of real-valued ones.

Note that when $\gamma_M \gg \gamma_W$ (or $d_M \ll d_W$) then $\mathcal{P}(C_s>0)\approx 1$ (or $\mathcal{P}(C_s=0)\approx 0$). Conversely, when $\gamma_W \gg \gamma_M$ (or $d_W \ll d_M$) then $\mathcal{P}(C_s>0)\approx 0$ (or $\mathcal{P}(C_s=0)\approx 1$).

It is interesting to note that to guarantee the existence of a non-zero secrecy capacity with probability greater than p_0 then it follows from (5) and (6) that

$$\frac{\overline{\gamma}_M}{\overline{\gamma}_W} > \frac{p_0}{1-p_0}$$

or

$$\frac{d_M}{d_W} < \sqrt[\alpha]{\frac{1-p_0}{p_0}}.$$

In particular, a non-zero secrecy capacity exists even when $\overline{\gamma}_M < \overline{\gamma}_W$ or $d_M > d_W$, albeit with probability less than 0.5.

C. Outage Probability and Outage Secrecy Capacity

We are now ready to characterize the outage probability

$$\mathcal{P}_{\text{out}}(R_s) = \mathcal{P}(C_s < R_s),$$

i.e. the probability that the instantaneous secrecy capacity is less than a target secrecy rate $R_s > 0$. The operational significance of this definition of outage probability is that when setting the secrecy rate R_s Alice is assuming that the capacity of the wiretap channel is given by $C'_W = C_M - R_s$. As long as $R_s < C_s$, Eve's channel will be worse than Alice's estimate, i.e. $C_W < C'_W$, and so the wiretap codes used by Alice will ensure perfect secrecy. Otherwise, if $R_s > C_s$ then $C_W > C'_W$ and information-theoretic security is compromised.

Invoking the total probability theorem,

$$\begin{aligned} \mathcal{P}_{\text{out}}(R_s) &= \mathcal{P}(C_s<R_s \mid \gamma_M>\gamma_W)\mathcal{P}(\gamma_M>\gamma_W) \\ &\quad +\mathcal{P}(C_s<R_s \mid \gamma_M\leq\gamma_W)\mathcal{P}(\gamma_M\leq\gamma_W) \end{aligned}$$

Now, from (5) we know that

$$\mathcal{P}(\gamma_M>\gamma_W) = \frac{\overline{\gamma}_M}{\overline{\gamma}_M+\overline{\gamma}_W}.$$

Consequently, we have

$$\mathcal{P}(\gamma_M\leq\gamma_W) = 1-\mathcal{P}(\gamma_M>\gamma_W) = \frac{\overline{\gamma}_W}{\overline{\gamma}_M+\overline{\gamma}_W}.$$

On the other hand, we also have that

$$\begin{aligned} &\mathcal{P}(C_s<R_s \mid \gamma_M>\gamma_W) \\ &= \mathcal{P}(\log(1+\gamma_M)-\log(1+\gamma_W)<R_s \mid \gamma_M>\gamma_W) \\ &= \mathcal{P}(\gamma_M<2^{R_s}(1+\gamma_W)-1 \mid \gamma_M>\gamma_W) \\ &= \int_0^\infty\int_{\gamma_W}^{2^{R_s}(1+\gamma_W)-1} p(\gamma_M,\gamma_W \mid \gamma_M>\gamma_W)d\gamma_W d\gamma_M \\ &= \int_0^\infty\int_{\gamma_W}^{2^{R_s}(1+\gamma_W)-1} \frac{p(\gamma_M)p(\gamma_W)}{\mathcal{P}(\gamma_M>\gamma_W)}d\gamma_W d\gamma_M \\ &= 1-\frac{\overline{\gamma}_M+\overline{\gamma}_W}{\overline{\gamma}_M+2^{R_s}\overline{\gamma}_W}\exp\left(-\frac{2^{R_s}-1}{\overline{\gamma}_M}\right) \end{aligned}$$

and, since $R_s>0$,

$$\mathcal{P}(C_s<R_s \mid \gamma_M\leq\gamma_W) = 1.$$

Combining the previous five equations, we get

$$\mathcal{P}_{\text{out}}(R_s) = 1-\frac{\overline{\gamma}_M}{\overline{\gamma}_M+2^{R_s}\overline{\gamma}_W}\exp\left(-\frac{2^{R_s}-1}{\overline{\gamma}_M}\right). \quad (7)$$

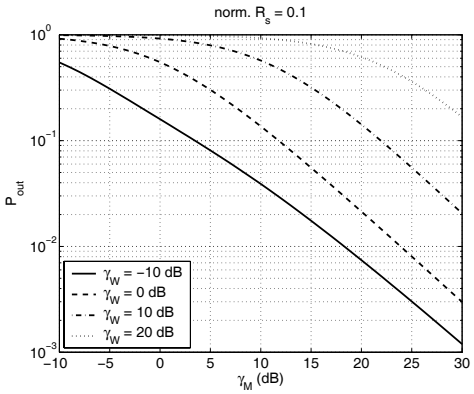

Fig. 3. Outage probability versus $\overline{\gamma}_M$, for selected values of $\overline{\gamma}_W$ and for a normalized target secrecy rate equal to 0.1. Normalization is effected with respect to the capacity of an AWGN channel with SNR equal to $\overline{\gamma}_M$.

Another performance measure of interest is the ϵ-outage secrecy capacity, defined as the largest secrecy rate such that the outage probability is less than ϵ, i.e.

$$\mathcal{P}_{\text{out}}(C_{\text{out}}(\epsilon)) = \epsilon \ .$$

Although it is hard to obtain the outage secrecy capacity analytically — the outage probability is a complicated function of the secrecy rate — it is possible to compute its value numerically based on (7), the result of which is discussed in the next section.

IV. Discussion

A. Asymptotic Behavior

It is illustrative to examine the asymptotic behavior of the outage probability for extreme values of the target secrecy rate R_s. From (7) it follows that when $R_s \to 0$,

$$\mathcal{P}_{\text{out}} \to \frac{\overline{\gamma}_W}{\overline{\gamma}_M + \overline{\gamma}_W}$$

and when $R_s \to \infty$, we have that $\mathcal{P}_{\text{out}} \to 1$, such that it becomes impossible for Alice and Bob to transmit secret information (at very high rates).

Also of interest is the asymptotic behavior of the outage probability for extreme values of the average SNRs of the main channel and the eavesdropper's channel. When $\overline{\gamma}_M \gg \overline{\gamma}_W$, equation (7) yields

$$\mathcal{P}_{\text{out}}(R_s) \approx 1 - \exp\left(-\frac{2^{R_s}-1}{\overline{\gamma}_M}\right),$$

and in a high SNR regime $\mathcal{P}_{\text{out}} \approx (2^{R_s}-1)/\overline{\gamma}_M$, i.e. the outage probability decays as $1/\overline{\gamma}_M$. Conversely, when $\overline{\gamma}_W \gg \overline{\gamma}_M$,

$$\mathcal{P}_{\text{out}}(R_s) \approx 1,$$

and confidential communication becomes impossible.

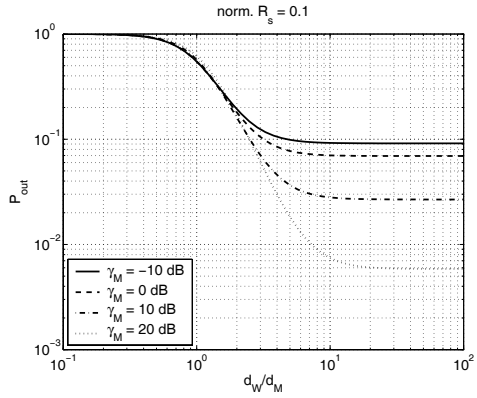

Fig. 4. Outage probability versus d_W/d_M, for selected values of $\overline{\gamma}_M$ and for a normalized target secrecy rate equal to 0.1. Normalization is effected with respect to the capacity of an AWGN channel with SNR equal to $\overline{\gamma}_M$.

Fig. 3 depicts the outage probability versus $\overline{\gamma}_M$, for selected values of $\overline{\gamma}_W$ and for a normalized target secrecy rate equal to 0.1. Observe that the higher $\overline{\gamma}_M$ the lower the outage probability, and the higher $\overline{\gamma}_W$ the higher the probability of an outage. Moreover, if $\overline{\gamma}_M \gg \overline{\gamma}_W$, the outage probability decays as $1/\overline{\gamma}_M$. Conversely, if $\overline{\gamma}_W \gg \overline{\gamma}_M$ the outage probability approaches one.

With respect to the asymptotic behavior of the outage secrecy capacity, it is not difficult to see that $C_{\text{out}} \to 0$ yields $\mathcal{P}_{\text{out}} \to \overline{\gamma}_W/(\overline{\gamma}_M + \overline{\gamma}_W)$, and when $C_{\text{out}} \to \infty$, we have $\mathcal{P}_{\text{out}} \to 1$.

The impact of the distance ratio on the performance is illustrated in Fig. 4, which depicts the outage probability versus d_W/d_M, for selected values of $\overline{\gamma}_M$ and for a normalized target secrecy rate equal to 0.1. The pathloss exponent is set to be equal to a typical value of 3 [11]. When $d_W/d_M \to \infty$ (or $\overline{\gamma}_M/\overline{\gamma}_W \to \infty$), we have that $\mathcal{P}_{\text{out}} \to 1 - \exp(-(2^{R_s}-1)/\overline{\gamma}_M)$. If $d_W/d_M \to 0$ (or $\overline{\gamma}_M/\overline{\gamma}_W \to 0$), then $\mathcal{P}_{\text{out}} \to 1$.

B. Fading Channels versus Gaussian Channels

It is important to emphasize that under a fading scenario — in contrast with the Gaussian wiretap channel [8]— the goal of a strictly positive (outage) secrecy capacity does *not* require the average SNR of the main channel to be greater than the average SNR of the eavesdropper's channel. This is due to the fact that in the presence of fading there is always a finite probability, however small, that the instantaneous SNR of the main channel γ_M is higher than the instantaneous SNR of the eavesdropper's channel γ_W.

Specifically, the results in Section III demonstrate that a non-zero outage secrecy capacity requires $\overline{\gamma}_M > \overline{\gamma}_W$ for $\mathcal{P}_{\text{out}} < 0.5$, but we may have $\overline{\gamma}_M < \overline{\gamma}_W$ for $\mathcal{P}_{\text{out}} > 0.5$. In other words, if we are willing to tolerate some outage, then there is no obstacle to information-theoretic security over wireless fading channels. In fact, it is possible to trade off outage probability for outage secrecy capacity: a higher outage secrecy capacity corresponds to a higher outage probability, and vice versa.

It also turns out that the outage secrecy capacity of a fading channel can actually be higher than the secrecy capacity of a Gaussian wiretap channel. Consider the examples shown in Fig. 5 and Fig. 6, which depict the normalized outage secrecy capacity versus $\overline{\gamma}_M$, for selected values of $\overline{\gamma}_W$, and for an outage probability of 0.1 and 0.75, respectively. The normalized secrecy capacity of the Gaussian wiretap channel with main channel SNR equal to $\overline{\gamma}_M$ and wiretap channel SNR equal to $\overline{\gamma}_W$ is also included for comparison. Observe that in the Gaussian case the secrecy capacity is zero when $\overline{\gamma}_M \leq \overline{\gamma}_W$. In contrast, in the case of Rayleigh fading channels the outage secrecy capacity is non-zero even when $\overline{\gamma}_M \leq \overline{\gamma}_W$ (as long as $\mathcal{P}_{\text{out}} > 0.5$). More importantly, the outage secrecy capacity in the Rayleigh fading case exceeds the secrecy capacity of the equivalent Gaussian wiretap channel, for higher outage probabilities. These key

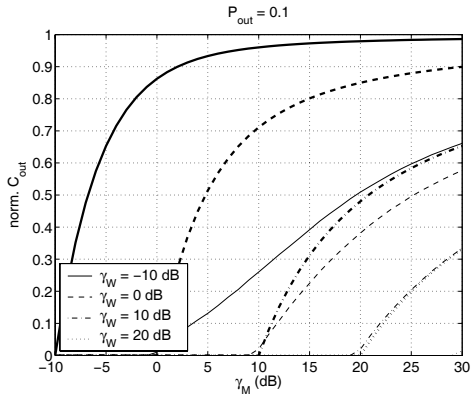

Fig. 5. Normalized outage secrecy capacity versus $\overline{\gamma}_M$, for selected values of $\overline{\gamma}_W$, and for an outage probability of 0.1. Thinner lines correspond to the normalized outage secrecy capacity in the case of Rayleigh fading channels, while thicker lines correspond to the secrecy capacity of the Gaussian wiretap channel. Normalization is effected with respect to the capacity of an AWGN channel with SNR equal to $\overline{\gamma}_M$.

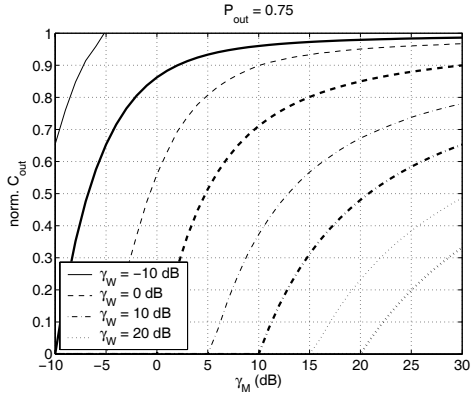

Fig. 6. Normalized outage secrecy capacity versus $\overline{\gamma}_M$, for selected values of $\overline{\gamma}_W$, and for an outage probability of 0.75. Thinner lines correspond to the normalized outage secrecy capacity in the case of the Rayleigh fading channels, while thicker lines correspond to the secrecy capacity of the Gaussian wiretap channel. Normalization is effected with respect to the capacity of an AWGN channel with SNR equal to $\overline{\gamma}_M$.

observations are also corroborated by Fig. 7, which compares the normalized (outage) secrecy capacity for fading channels to the secrecy capacity of Gaussian channels, for various outage probabilities.

V. Conclusions

We provided a preliminary characterization of the outage secrecy capacity of wireless channels with quasi-static fading. Specifically, we assumed that Alice — having access to the CSI of the main channel only — chooses a target secrecy rate R_s (without knowing the wiretap channel) and we investigated the outage probability defined as $\mathcal{P}(R_s > C_s)$. Our results reveal that (a) perfectly secure communication over wireless channels is possible even when the eavesdropper has a better average SNR than the legitimate partners, and (b) the outage secrecy capacity of wireless channels can actually be higher than the secrecy capacity of a Gaussian wiretap channel with the same averaged SNRs γ_M and γ_W.

Suppose now that Alice has access to CSI on both the main channel and the eavesdropper's channel. This is the case, for example in a Time Division Multiple Access (TDMA) environment, when Eve is not a covert eavesdropper, but simply another user interacting with the wireless network, thus sending communication signals that allow Alice to estimate the CSI of the channel between them. A natural way for Alice to exploit the available CSI on both channels to achieve secrecy is by transmitting useful symbols to Bob only when the instantaneous SNR values are such that the instantaneous secrecy capacity is strictly positive ($\gamma_M > \gamma_W$). This observation thus suggests an *opportunistic* secret key agreement scheme for wireless networks — even when the outage probability is very high, the available secrecy capacity is still likely to enable Alice and Bob to generate an (information-theoretically secured) encryption key that could then be used to secure the data exchange while the system is in outage of secrecy capacity.

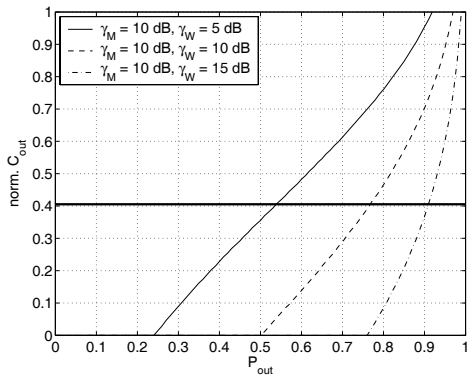

Fig. 7. Normalized outage secrecy capacity versus outage probability, for selected values of $\overline{\gamma}_M$ and $\overline{\gamma}_W$ Thinner lines correspond to the normalized outage secrecy capacity of the eavesdropper's Rayleigh fading channel, while thicker lines correspond to the secrecy capacity of the Gaussian wiretap channel (in the last two cases this capacity is zero). Normalization is effected with respect to the capacity of an AWGN channel with SNR equal to $\overline{\gamma}_M$.

Acknowledgements

The authors gratefully acknowledge inspiring discussions with Steven W. McLaughlin, Matthieu Bloch, Prakash Narayan and Andrew Thangaraj.

References

[1] Ueli M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[2] III Alfred O. Hero, "Secure space-time communication," *IEEE Trans. on Inform. Theory*, vol. 49, no. 12, pp. 3235–3249, December 2003.

[3] Andrew Thangaraj, Souvik Dihidar, A. Robert Calderbank, Steven W. McLaughlin, and Jean-Marc Merolla, "Capacity achieving codes for the wire tap channel with applications to quantum key distribution," *CoRR*, vol. cs.IT/0411003, 2004.

[4] Matthieu Bloch, Andrew Thangaraj, Steven W. McLaughlin, and Jean-Marc Merolla, "LDPC-based Gaussian key reconciliation," in *Proc. of the IEEE International Workshop on Information Theory*, Punta del Este, Uruguay, March 2006.

[5] C.E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. Journ.*, vol. 29, pp. 656–715, 1949.

[6] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. Journ.*, vol. 54, pp. 1355–1387, 1975.

[7] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. on Inform. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[8] S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wiretap channel," *IEEE Trans. on Inform. Theory*, vol. 24, no. 4, pp. 451456, July 1978.

[9] David Tse and Pramod Viswanath, *Fundamentals of Wireless Communication*, Cambridge University Press, 2005.

[10] Ueli Maurer and Stefan Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," *Eurocrypt 2000, Lecture Notes in Computer Science*, vol. 1807, pp. 351+, 2000.

[11] Theodore Rappaport, *Wireless Communications: Principles and Practice, 2nd Edition*, Prentice Hall, 2001.