Wireless Information-Theoretic Security — Part I: Theoretical Aspects

Matthieu Bloch, João Barros, Miguel R. D. Rodrigues, and Steven W. McLaughlin

Abstract

In this two-part paper, we consider the transmission of confidential data over wireless wiretap channels. The first part presents 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. The issue of imperfect channel state information is also addressed. Practical schemes for wireless information-theoretic security are presented in Part II, which in some cases comes close to the secrecy capacity limits given in this paper.

Index Terms: Information Theoretic Security, Gaussian Channels, Wireless Channels, Secrecy Capacity, LDPC Codes, Secret Key Agreement

Matthieu Bloch and Steven W. McLaughlin are with GT-CNRS UMI 2958, Metz, France, and also with the School of ECE, Georgia Institute of Technology, Altlanta, GA.

João Barros is with the Departament of Computer Science & LIACC/UP, Universidade do Porto, Portugal.

Miguel R. D. Rodrigues is with the Computer Laboratory, University of Cambridge, United Kingdom.

Parts of this work have been presented at the IEEE International Symposium on Information Theory 2006 [1], at the 44th Allerton conference on Communication Control and Computing [2], and at the IEEE Information Theory Wokshop 2006 in Chengdu [3].

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 addressed above the physical layer and all widely used cryptographic protocols (e.g. RSA, AES etc) are designed and implemented assuming the physical layer has already been established and is error free.

In contrast with this paradigm, there exist both theoretical and practical contributions 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* [4], was laid by Wyner [5] and later by Csiszár and Körner [6], who proved in seminal papers that there exist channel codes guaranteeing both robustness to transmission errors and a prescribed degree of data confidentiality.

A general setup for the so called wiretap channel is shown in *Fig. 2*. In the original version, proposed by Wyner in [5], two legitimate users communicate over a main channel and an eavesdropper has access

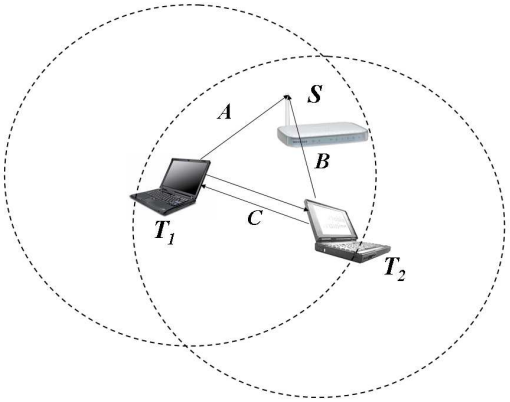

Fig. 1. Example of a wireless network with potential eavesdropping. Terminals T_1 and T_2 communicate with a base station S over a wireless medium (channels A and B). By listening to the transmissions of terminal T_1 (through channel C), terminal T_2 may acquire confidential information. If T_1 wants 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.

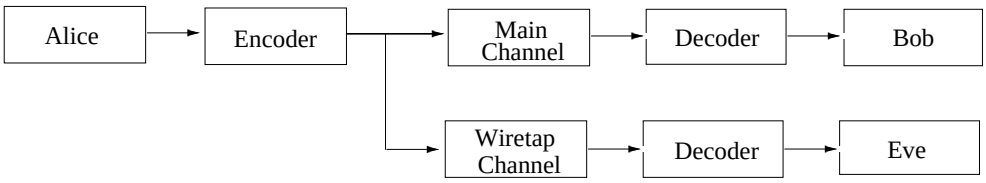

Fig. 2. In the wiretap channel problem, the goal of the legitimate users, Alice and Bob, is to communicate reliably over the noisy main channel, while ensuring that an eavesdropper, say Eve, is unable to obtain any information from the outputs of the wiretap channel.

to degraded versions of the channel outputs that reach the legitimate receiver. In [7] 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.

In the seventies and eighties, the impact of these works was limited, partly because practical wiretap codes were not available, but mostly because due the fact that a strictly positive secrecy capacity in the classical wiretap channel setup requires the legitimate sender and receiver to have some advantage (a better SNR) over the attacker. Moreover, almost at the same time, Diffie and Hellman [8] published the basic principles of public-key cryptography, which was to be adopted by nearly all contemporary security schemes.

More recently, information-theoretic security witnessed a renaissance arguably due to the work of Maurer [9], who proved that even when the legitimate users (say Alice and Bob) have a worse channel than the eavesdropper (say Eve), it is possible for them to generate a secret key through public communication over an insecure yet authenticated channel. In [10] Maurer and Wolf showed that a stronger (and technically more convincing) secrecy condition for discrete memoryless channels yields the same secrecy rates as the weaker condition in [5] and [6]. A key ingredient for secret key generation over noisy channels is privacy amplification (see Bennett et al [11]), which provides Alice and Bob with the means to distill perfectly secret symbols (e.g. a secret key) from a large set of only partially secret data. This general approach is used and modified in Part II of this paper to develop efficient protocols for the Gaussian and quasi-static fading wiretap channel.

In [12], Hero introduced space-time signal processing techniques for secure communication over

wireless links. More recently, Parada and Blahut [13] considered the secrecy capacity of various degraded fading channels. In a shorter prelude to some of the results in this paper [1], Barros and Rodrigues provided the first characterization of the outage secrecy capacity of slow fading channels and showed 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— without the need for public communication over a feedback channel. The ergodic secrecy capacity of fading channels was soon derived by Liang and Poor [14], and, independently, by Li et al. [15]. Power and rate allocation schemes for secret communication over fading channels were presented by Gopala et al. in [16]. Secure broadcasting over wireless channels is considered in [17].

Practical secrecy capacity-achieving codes for erasure channels were presented by Thangaraj et al. in [18]. LDPC codes were also shown by Bloch et al. [19] to be useful tools for reconciliation of correlated continuous random variables, with implications in quantum key distribution. A related scheme was presented by Ye and Reznik in [20]. Experimental results supporting the possibility of information-theoretic secret key agreement over wireless channels were reported by Imai et al in [21].

Secrecy systems with multiple users have also recently become an object of intense research. Csiszár and Narayan [22] presented the fundamental limits of secret key generation in multi-terminal setups. Secret key constructions for this problem are reported by Ye and Narayan in [23]. A detailed study of the multiple access channel with secrecy constraints between users was provided by Liang and Poor in [24]. Liu et al presented results for the same problem in [25] and, investigated in [26] also broadcast and interference channels with confidential messages. The Gaussian multiple access channel with an eavesdropper was studied in [27].

A. Our Contributions

Motivated by the general problem of securing transmissions over wireless channels, we consider the impact of fading on the secrecy capacity. Our contributions in Part I 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;

(e) a mathematical characterization of the impact of imperfect CSI about the eavesdropper's channel on the secrecy capacity;

(f) a comparison between information-theoretic security techniques at the physical layer and classical cryptographic methods at higher layers of the protocol stack.

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.

B. Organization of the Paper

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 implications of channel state information are analyzed in Section IV. Finally, Section V compares classical cryptographic methods with information-theoretic security for wireless channels, and Section VI concludes the paper.

II. Secure Communication over Quasi-Static Rayleigh Fading Channels

A. Wireless System Setup

Consider the wireless system setup depicted in *Fig. 3*. A legitimate user, say Alice, wants to send messages to another user, say Bob. Alice encodes the message block w^k into the codeword x^n for transmission over the channel (the *main* channel). Bob observes the output of a discrete-time Rayleigh fading channel given by

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

where $h_M(i)$ is a circularly symmetric complex Gaussian random variable with zero-mean and unit-variance representing the main channel fading coefficient and $n_M(i)$ is a zero-mean circularly symmetric complex Gaussian noise random variable.

A third party (Eve) is also capable of eavesdropping Alice's transmissions. In particular, Eve observes the output of an independent discrete-time Rayleigh fading channel (the *wiretap* channel) given by

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

where $h_W(i)$ denotes a circularly symmetric complex Gaussian random variable with zero-mean and unit-variance representing the wiretap channel fading coefficient and $n_W(i)$ denotes a zero-mean circularly symmetric complex Gaussian noise random variable.

It is assumed that the channels' input, the channels' fading coefficients and the channels' noises are all independent. It is also assumed that both the main and the wiretap channels are quasi-static fading channels, that is, the fading coefficients, albeit random, are constant during the transmission of an entire codeword ($h_M(i) = h_M, \forall i = 1, \ldots, n$ and $h_W(i) = h_W, \forall i = 1, \ldots, n$) and, moreover, independent from codeword to codeword.

We take the average transmit power to be P, that is

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

and the average noise power in the main and the wiretap channels to be N_M and N_W, respectively. Consequently, the instantaneous SNR at Bob's receiver is

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

and its average 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 Eve's receiver is

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

and its average value is

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

Since the channel fading coefficients h are zero-mean complex Gaussian random variables 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

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

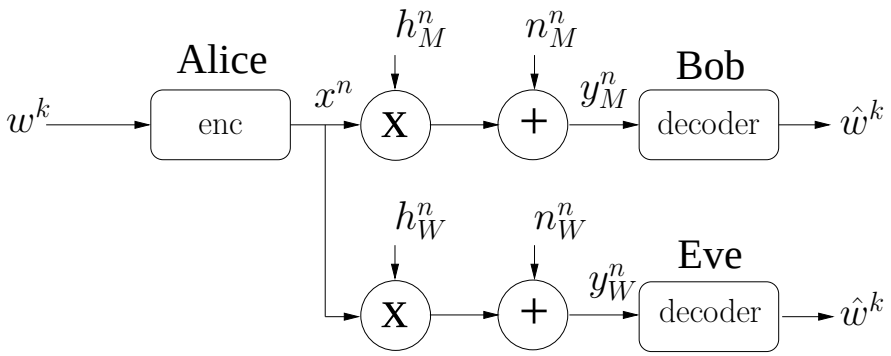

Fig. 3. Wireless system setup.

B. Problem Statement

Let the transmission rate between Alice and Bob be $R = H(W^k)/n$, the equivocation rate[1] or Eve's uncertainty be $\Delta = H(W^k|Y_W^n)/H(W^k)$, and the error probability $\mathcal{P}_\epsilon = \mathcal{P}(W^k \neq \hat{W}^k)$, where W^k denotes the sent messages and $\hat{W}^k$ denotes Bob's estimate of the sent messages.

In general, one is interested in characterizing the rate-equivocation region, that is, the set of achievable pairs (R', d'). A pair (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 $\mathcal{P}_\epsilon \leq \epsilon$. Here, however, we are interested in characterizing the *secrecy capacity* C_s, that is, the maximum transmission rate R at $\Delta = 1$.

In the rest of the paper, we will study the secrecy capacity of this wireless system for different channel state information (CSI) regimes. We will always assume that Bob has perfect knowledge of the main channel fading coefficient and that Eve also has perfect knowledge of the wiretap channel fading coefficient [2]. We will also always assume that Alice has perfect knowledge of the main channel fading coefficient. Note that these assumptions are realistic for this slow fading wireless environment: both receivers can always obtain close to perfect channel estimates and, additionally, the legitimate receiver can also feedback the channel estimates to the legitimate transmitter. However, we will assume various

[1]Notice that the secrecy condition used here (and in [5], [7]) is weaker than the one proposed by Maurer and Wolf in [10], where the information obtained by the eavesdropper is negligibly small not just in terms of rate but in absolute terms. Unfortunately, it is unclear whether the techniques used for discrete memoryless channels in [10] can be extended for Gaussian channels, in particular information reconciliation and privacy amplification. Resolving this issue is part of our ongoing efforts.

[2]By virtue of the independence of the main channel and the wiretap channel, there are no additional benefits/penalities if Bob knows the wiretap fading coefficient and/or Eve knows the main channel fading coefficient

regimes for Alice knowledge of the eavesdropper channel:

(a) No knowledge of the wiretap channel fading coefficient;

(b) Partial knowledge of the wiretap channel fading coefficient;

(c) Perfect knowledge of the wiretap channel fading coefficient.

Case 1 corresponds to the situation where Eve is a passive and malicious eavesdropper in the wireless network. Cases 2 and 3 correspond to the situation where Eve is another active user in the wireless network, so that, e.g. in a TDMA environment, Alice can estimate the wiretap channel during Eve transmissions.

In the following sections, we will characterize the secrecy capacity in terms of outage events for the wireless system setup in *Fig. 3*.

III. Secrecy Capacity and Outage without CSI on the Eavesdropper's Channel

In this section, we will consider the situation where the legitimate transmitter (Alice) knows nothing about the state of the eavesdropper's channel. However, we assume that the legitimate transmitter and receiver know the state of the main channel perfectly and that the eavesdropper also knows the state of the eavesdropper channel perfectly (see Section II).

Consequently, 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 instantaneous 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. Instantaneous Secrecy Capacity

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 recall the results of [7] 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. From this result, we can derive the following lemma which describes the instantaneous secrecy capacity for the wireless fading scenario defined in Section II.

Lemma 1: The secrecy capacity for one realization of the quasi-static complex fading wiretap-channel is given by

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

Proof: Suppose that both the main and the wiretap channel are complex AWGN channels, i.e. transmit and receive symbols are 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 [28, 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].

To complete the proof, we introduce 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 [28, 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 (4). ■

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

[4]Alternatively, this result can be proven by repeating step by step the proofs of [7] using complex-valued random variables instead of real-valued ones.

B. Probability of Strictly Positive Secrecy Capacity

We will now determine the probability $\mathcal{P}(C_s > 0)$ of a strictly positive secrecy capacity between Alice and Bob.

Lemma 2: For average signal-to-noise ratios $\overline{\gamma}_M$ and $\overline{\gamma}_W$ on the main channel and the wiretap channel, respectively, we have that

$$\mathcal{P}(C_s > 0) \;\; = \;\; \frac{\overline{\gamma}_M}{\overline{\gamma}_M + \overline{\gamma}_W}. \tag{5}$$

Proof: 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

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

■

It is also useful to express this probability in terms of parameters related to user location.

Corollary 1: For distance d_M between Alice and Bob, distance d_W between Alice and Eve, and pathloss exponent α, we have that

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

Proof: The corollary follows directly from the fact that $\overline{\gamma}_M \propto 1/d_M^\alpha$ and $\overline{\gamma}_W \propto 1/d_W^\alpha$ [29]. ■

Remark 1: 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 also interesting to observe 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 $1/2$.

C. Outage Probability of 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.

Theorem 1: The outage probability for a target secrecy rate R_s is given by

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

Proof: 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

$$\mathcal{P}(C_s < R_s \mid \gamma_M > \gamma_W)$$

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

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

$$\mathcal{P}_{\text{out}}(R_s) = 1 - \frac{\overline{\gamma}_M}{\overline{\gamma}_M + 2^{R_s}\overline{\gamma}_W} \exp\left(-\frac{2^{R_s}-1}{\overline{\gamma}_M}\right). \tag{8}$$

■

D. Outage Secrecy Capacity

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).

E. 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

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

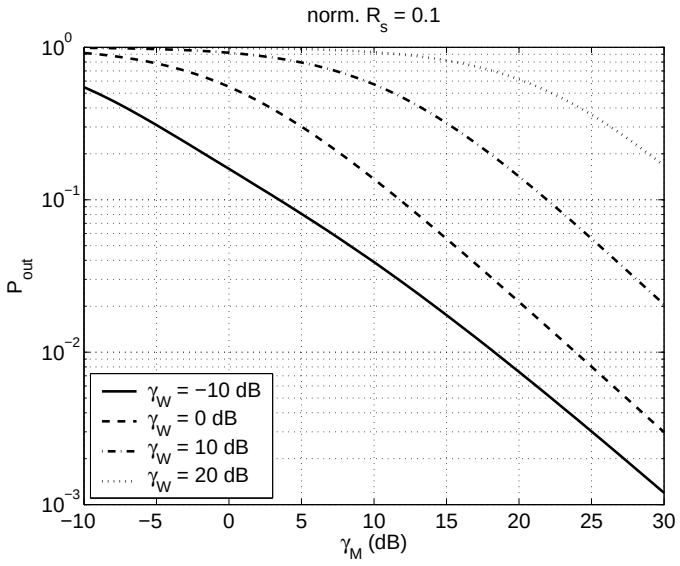

Fig. 4. Outage probability versus $\overline{\gamma}_M$, for selected values of $\overline{\gamma}_W$ and for a normalized target secrecy rate equal to 0.1. Normalization is effected with respect to the capacity of an AWGN channel with SNR equal to $\overline{\gamma}_M$.

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 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. 5*, 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 [29]. 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 $\mathcal{P}_{\text{out}} \to 1$.

F. Fading Channels versus Gaussian Channels

It is important to emphasize that under a fading scenario — in contrast with the Gaussian wiretap channel [7]— 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. 6* and *Fig. 7*, 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

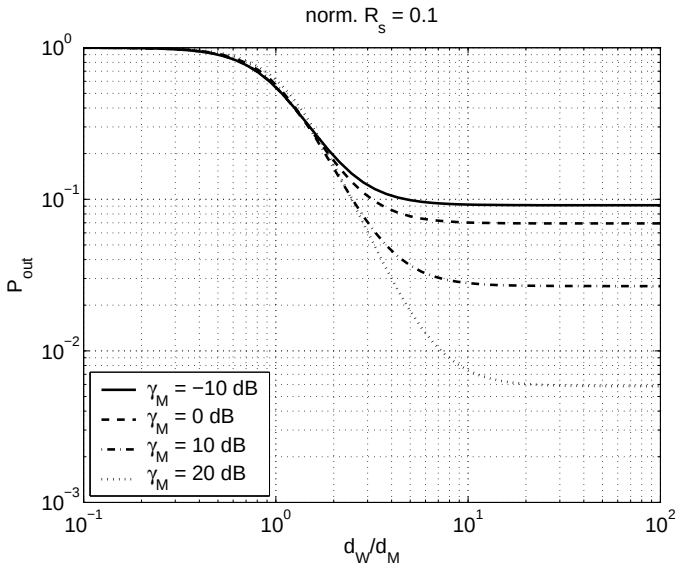

Fig. 5. Outage probability versus d_W/d_M, for selected values of $\overline{\gamma}_M$ and for a normalized target secrecy rate equal to 0.1. Normalization is effected with respect to the capacity of an AWGN channel with SNR equal to $\overline{\gamma}_M$.

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 observations are also corroborated by *Fig. 8*, which compares the normalized (outage) secrecy capacity for fading channels to the secrecy capacity of Gaussian channels, for various outage probabilities.

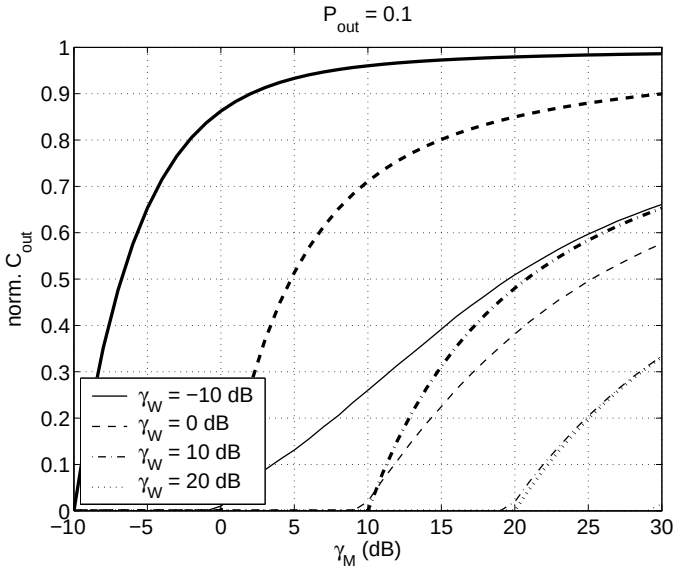

Fig. 6. Normalized outage secrecy capacity versus $\overline{\gamma}_M$, for selected values of $\overline{\gamma}_W$, and for an outage probability of 0.1. Thinner lines correspond to the normalized outage secrecy capacity in the case of Rayleigh fading channels, while thicker lines correspond to the secrecy capacity of the Gaussian wiretap channel. Normalization is effected with respect to the capacity of an AWGN channel with SNR equal to $\overline{\gamma}_M$.

Finally, it is also interesting to examine the average secrecy rate given by

$$\bar{R}_s = (1 - \mathcal{P}_{\text{out}}(R_s)) \cdot R_s$$

The average secrecy rate $\bar{R}_s$ is a function of Alice's target instantaneous secrecy rate R_s, so that Alice is in principle able to optimize the target instantaneous secrecy rate to maximize the average secrecy rate (see *Fig. 9*). *Fig. 10* compares the optimum average secrecy rate in the case of Rayleigh fading channels to the secrecy capacity of AWGN channels. It is interesting to observe once again that there is a positive secrecy rate in a Rayleight fading channel even when the average SNR in the main channel is lower than that in the eavesdropper channel.

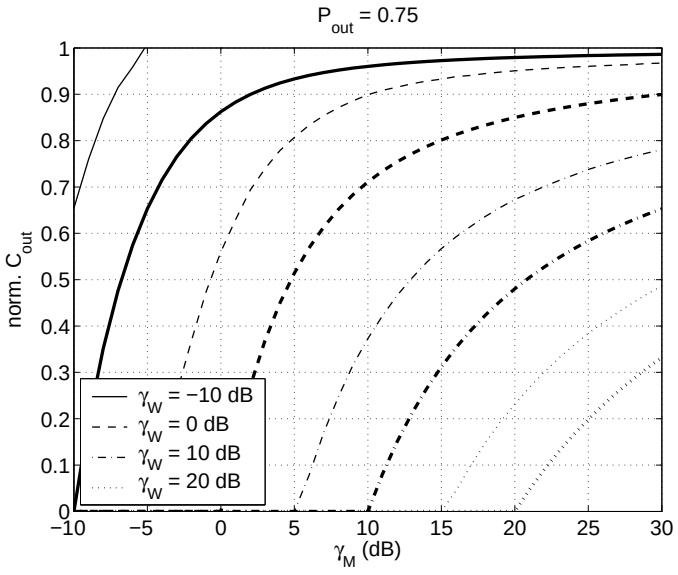

Fig. 7. Normalized outage secrecy capacity versus $\overline{\gamma}_M$, for selected values of $\overline{\gamma}_W$, and for an outage probability of 0.75. Thinner lines correspond to the normalized outage secrecy capacity in the case of the Rayleigh fading channels, while thicker lines correspond 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 $\overline{\gamma}_M$.

IV. Performance Analysis with Perfect and Imperfect CSI on the Eavesdropper's Channel

In this section, we move from the paradigm where the legitimate transmitter (Alice) knows nothing about the state of the eavesdropper's channel to one where Alice knows the state of the eavesdropper's channel partially or even perfectly. However, we still assume that the legitimate transmitter and receiver know the state of the main channel perfectly and that the eavesdropper also knows the state of the eavesdropper channel perfectly (see Section II).

We model Alice's estimate of Bob's channel as

$$\hat{h}_M = h_M,$$

where $\hat{h}_M$ is the estimate fading coefficient of the main channel and h_M is the true fading coefficient of the main channel. Thus, the estimate main channel instantaneous SNR is equal to the true main channel instantaneous SNR, that is

$$\hat{\gamma}_M = \gamma_M.$$

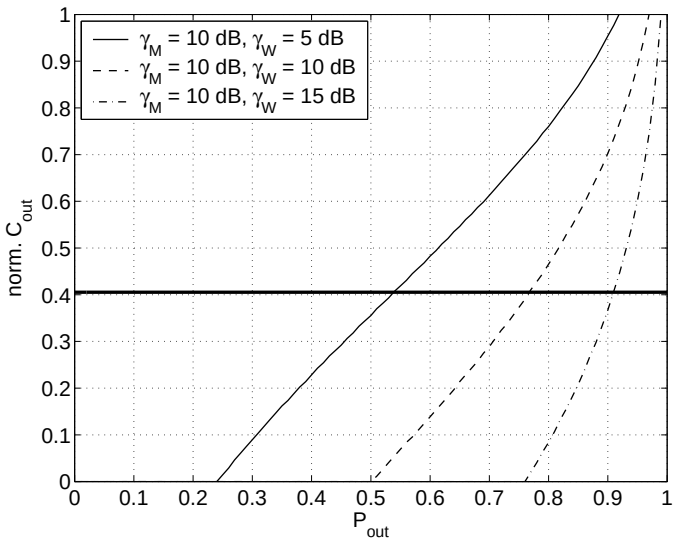

Fig. 8. Normalized outage secrecy capacity versus outage probability, for selected values of $\overline{\gamma}_M$ and $\overline{\gamma}_W$ Thinner lines correspond to the normalized outage secrecy capacity of the eavesdropper's Rayleigh fading channel, while thicker lines correspond to the secrecy 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 $\overline{\gamma}_M$.

We also model Alice's estimate of Eve's channel as

$$\hat{h}_W = h_W + \delta_W,$$

where $\hat{h}_W$ is the estimate fading coefficient of the wiretap channel, h_W is the true fading coefficient of the wiretap channel and δ_W is a circularly symmetric complex Gaussian random variable with mean zero and variance σ^2 per dimension. Thus, the true value and the estimate of wiretap channel instantaneous SNR may be different, that is

$$\hat{\gamma}_W \neq \gamma_W.$$

In this new scenario, we will assume that Alice always sets the instantaneous information transmission rate R_s to be equal to the instantaneous secrecy capacity estimate $\hat{C}_s$ of the channel where

$$\hat{C}_s = \begin{cases} \hat{C}_M - \hat{C}_W & \text{if } \hat{C}_M \geq \hat{C}_W \\ 0 & \text{if } \hat{C}_M < \hat{C}_W \end{cases}$$

and $\hat{C}_M = \log(1+\hat{\gamma}_M)$ is the instantaneous main channel capacity estimate and $\hat{C}_W = \log(1+\hat{\gamma}_W)$ is the instantaneous wiretap channel capacity estimate. We will now characterize the fundamental secrecy limits when Alice knows the state of the eavesdropper's channel both imperfectly and perfectly, including

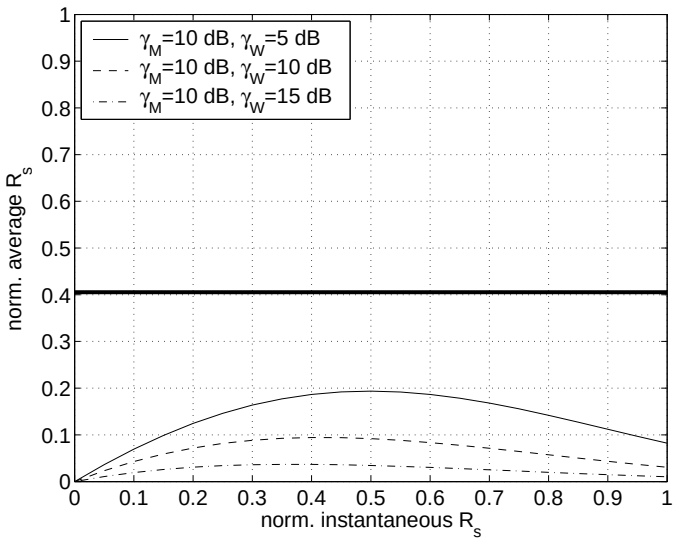

Fig. 9. Normalized average secrecy rate versus normalized instantaneous secrecy rate, for selected values of $\overline{\gamma}_M$ and $\overline{\gamma}_W$. Thinner lines correspond to the normalized average secrecy rate of Rayleigh fading channels, while thicker lines correspond to the secrecy capacity 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 $\overline{\gamma}_M$.

the probability of a secrecy outage, the average secure throughput (from Alice to Bob) and the average leaked throughput (from Alice to Eve).

A. Imperfect Knowledge of CSI of Eavesdropper's Channel

In this situation, Alice conveys information to Bob at a rate $R_s = \hat{C}_s$ using a wiretap code designed for the operating point $(\hat{C}_M, \hat{C}_W) = (C_M, \hat{C}_W)$, when $\hat{C}_M > \hat{C}_W$. If $\hat{C}_W > C_W$ (i.e., $\hat{C}_s < C_s$) transmission in perfect secrecy is guaranteed, that is, a secrecy outage does not occur. Otherwise, if $\hat{C}_W < C_W$ (i.e., $\hat{C}_s > C_s$) transmission in perfect secrecy cannot be guaranteed, that is, a secrecy outage occurs. It is now relevant to characterize the probability of a secrecy outage.

Theorem 2: The probability of a secrecy outage is upper bounded by

$$\mathcal{P}_{\text{out}} \leq \frac{1}{2} - \frac{1}{2}\frac{1}{\sqrt{1+2/\sigma^2}}. \tag{9}$$

Proof: The probability of a secrecy outage is given by

$$\mathcal{P}_{\text{out}} = \mathcal{P}(\hat{C}_W < C_M, \hat{C}_W < C_W) = \mathcal{P}(\hat{\gamma}_W < \gamma_M, \hat{\gamma}_W < \gamma_W) = \mathcal{P}(\hat{\gamma}_W < min(\gamma_M, \gamma_W))$$

Consequently, the probability of a secrecy outage is upper bounded by

$$\mathcal{P}_{\text{out}} = \mathcal{P}(\hat{\gamma}_W < min(\gamma_M, \gamma_W)) \leq \mathcal{P}(\hat{\gamma}_W < \gamma_W)$$

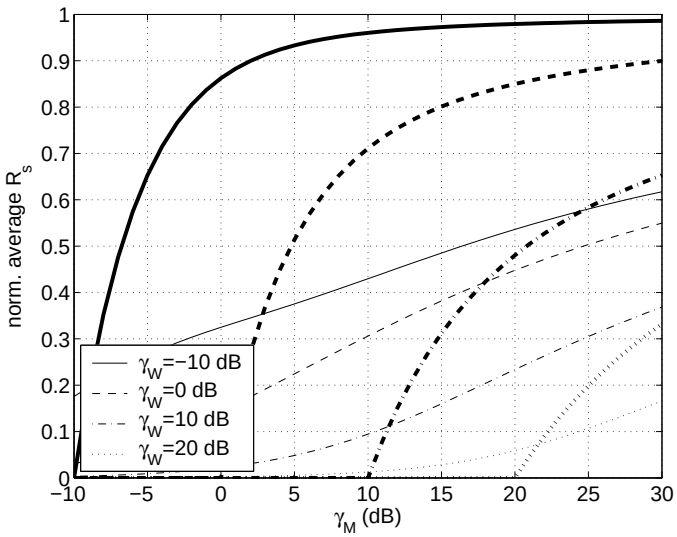

Fig. 10. Normalized average secrecy rate versus $\overline{\gamma}_M$, for selected values of $\overline{\gamma}_W$. Thinner lines correspond to the normalized average secrecy rate in the case of Rayleigh fading channels, while thicker lines correspond to the secrecy capacity of the Gaussian wiretap channel. Normalization is effected with respect to the capacity of an AWGN channel with SNR equal to $\overline{\gamma}_M$.

Now, $\mathcal{P}(\hat{\gamma}_W < \gamma_W)$ can be written as follows

$$\mathcal{P}(\hat{\gamma}_W < \gamma_W) = \int_0^\infty \mathcal{P}(\hat{\gamma}_W < \gamma_W|\gamma_W)p(\gamma_W)d\gamma_W$$

where $p(\gamma_W)$ is the probability density function of γ_W (see (2)). Moreover, $\mathcal{P}(\hat{\gamma}_W < \gamma_W|\gamma_W)$ can also be written as follows

$$\mathcal{P}(\hat{\gamma}_W < \gamma_W|\gamma_W) = \int_0^{\gamma_W} p(\hat{\gamma}_W|\gamma_W)d\gamma_W$$

where $p(\hat{\gamma}_W|\gamma_W)$ is the probability density function of $\hat{\gamma}_W$ conditioned on γ_W. This probability density function is non-central χ^2 with two degrees of freedom, i.e.

$$p(\hat{\gamma}_W|\gamma_W) = \frac{1}{2\bar{\gamma}_W\sigma^2}e^{-\frac{(\gamma_W+\hat{\gamma}_W)}{2\bar{\gamma}_W\sigma^2}}I_0\left(\frac{\sqrt{\gamma_W\hat{\gamma}_W}}{\bar{\gamma}_W\sigma^2}\right), \hat{\gamma}_W > 0$$

where $I_0(\cdot)$ is the zeroth-order modified Bessel function of the first kind [30]. Thus, the probability $\mathcal{P}(\hat{\gamma}_W < \gamma_W|\gamma_W)$ reduces to

$$\mathcal{P}(\hat{\gamma}_W < \gamma_W|\gamma_W) = 1 - Q_1\big(\sqrt{\gamma_W/(\bar{\gamma}_W\sigma^2)}, \sqrt{\gamma_W/(\bar{\gamma}_W\sigma^2)}\big)$$

where $Q_1(\cdot,\cdot)$ is the generalized Marcum Q function [30]. Moreover, using standard results for integrals involving the generalized Marcum Q function [31], the upper bound to the outage probability reduces to

$$\mathcal{P}_{\text{out}} \leq \frac{1}{2} - \frac{1}{2}\frac{1}{\sqrt{1+2/\sigma^2}}. \tag{10}$$

■

It is also relevant to characterize two other quantities with operational significance: the average secure throughput (or average secrecy rate) and the average leaked throughput. These quantities correspond to the average of the instantaneous secure throughput and the instantaneous leaked throughput over every possible realization of the main channel and the eavesdropper's channel. Now, the average secure throughput is lower bounded by the average of the transmission rate over instances where the secrecy capacity estimate is lower than the true secrecy capacity, i.e.

$$\bar{R}_s \geq \int_0^\infty \hat{C}_s \, p(\hat{C}_s | \hat{C}_s < C_s) \, d\hat{C}_s$$

In turn, the average leaked throughput is upper bounded by the average of the transmission rate over instances where the secrecy capacity estimate is higher than the true secrecy capacity, i.e.

$$\bar{R}_l \leq \int_0^\infty \hat{C}_s \, p(\hat{C}_s | \hat{C}_s > C_s) \, d\hat{C}_s$$

These quantities will be characterized numerically due to the difficulty in determining closed-form expressions.

A number of comments on the behavior of the various performance measures are now in order. *Fig. 11* shows that the upper bound to the outage probability is considerably tight in a regime where the average SNR of the main channel is greater than the average SNR of the eavesdropper channel. More importantly, the outage probability is a monotone decreasing function of the variance of the channel estimation error, so that for $\sigma^2 > 0$ the higher the variance of the channel estimation errors the lower the outage probability.

This counterintuitive result is based on the fact that for moderate values of the variance of the channel estimation error Alice tends to consistently underestimate the secrecy capacity of the system. Consequently, the attempted instantaneous transmission rate is consistently lower than the instantaneous secrecy capacity so that the outage probability is also lower. This in turn results in a lower average secure throughput and a lower average leaked throughput as shown in *Fig. 12* and *Fig. 13*.

Yet, of extreme relevance is the fact that even in the presence of channel estimation errors it is possible to convey information in a secure manner over a wireless environment (that is, with an average secure throughput substantially greater than the average leaked throughput) provided now that the average SNR of the main channel is greater than the average SNR of the eavesdropper channel (cf. *Fig. 12* and *Fig. 13*).

B. Perfect Knowledge of CSI of Eavesdropper's Channel

In this situation, Alice conveys information to Bob at a rate $R_s = \hat{C}_s = C_s$ using a wiretap code designed for the operating point $(\hat{C}_M, \hat{C}_W) = (C_M, C_W)$, so that a secrecy outage never occurs. It

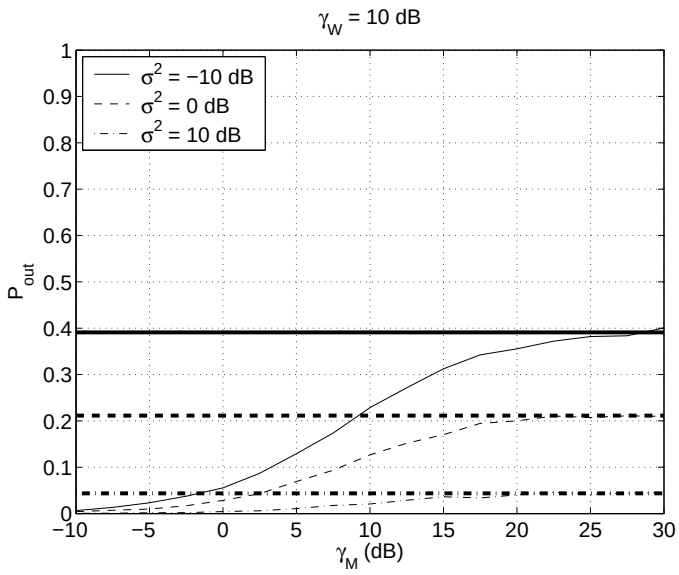

Fig. 11. Outage probability versus $\overline{\gamma}_M$ for $\overline{\gamma}_W = 10$ dB, and for selected values of σ^2. Thicker lines correspond to the upper bound to the outage probability while thinner lines correspond to the true outage probability.

follows that the average secure throughput (average secrecy rate) is

$$\bar{R}_s = \int_0^\infty R_s dF_{C_s}(R_s),$$

where [5]

$$F_{C_s}(R_s) = \mathcal{P}(C_s < R_s) = 1 - \frac{\bar{\gamma}_M}{\bar{\gamma}_M + 2^{R_s}\bar{\gamma}_W} e^{\frac{2^{R_s}-1}{\bar{\gamma}_M}},$$

and the average leaked throughput is zero.

Fig. 14 compares the average secrecy rate in a "wiretap" Rayleigh fading channel to the secrecy capacity in the classic wiretap Gaussian channel. Strikingly, one observes that the average secrecy rate in the fading channel is indeed higher than or close to the secrecy capacity in the Gaussian channel. One also observes that, in contrast to the situation in the Gaussian channel, the average secrecy rate in the fading channel is non-zero even when the average SNR of the main channel is lower than the average SNR of the eavesdropper channel. These observations underline once again the potential of fading channels to secure the transmission of information between two legitimate parties against a possible eavesdropper.

[5]Note that the expression for the cumulative distribution function of the instantaneous secrecy capacity is exactly the same as the expression for the outage probability in (7).

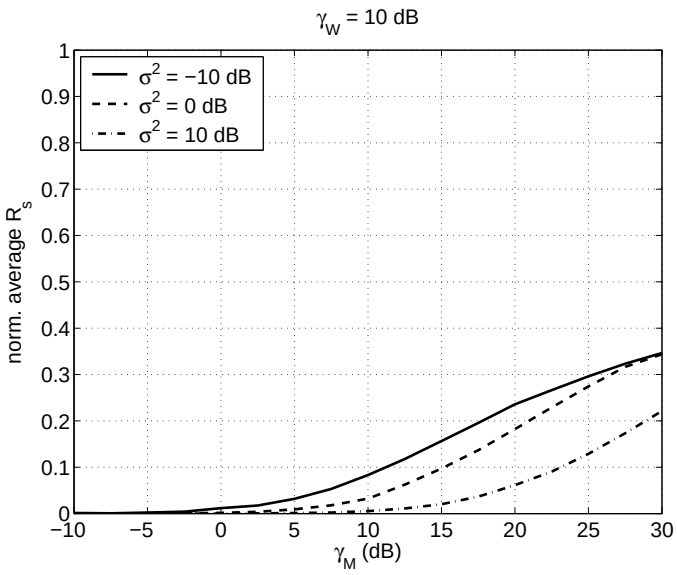

Fig. 12. Normalized average secure throughput versus $\overline{\gamma}_M$ for $\overline{\gamma}_W = 10$ dB, and for selected values of σ^2. Normalization is effected with respect to the capacity of an AWGN channel with SNR equal to $\overline{\gamma}_M$.

V. Information-Theoretic vs. Computational Security in Wireless Networks

Due to the many fundamental differences between classical cryptography and information-theoretic security, it is useful to recognize what those differences are and how they affect the choice of technology in a wireless scenario. It is fair to state that classical cryptographic security under the computational model offers the following advantages:

- there are so far no publicly-known, efficient attacks on public-key systems such as RSA, and hence they are deemed secure for a large number of applications;
- very few assumptions are made about the plaintext to be encoded, and security is provided on a block-to-block basis, meaning as long as the cryptographic primitive is secure, then every encoded block is secure;
- Systems are widely deployed, technology is readily available and inexpensive.

On the other hand, we must consider also the following disadvantages of the computational model:

- Security is based on unproven assumptions regarding the hardness of certain one-way functions. Plaintext is insecure if assumptions are wrong or if efficient attacks are developed;
- In general there are no precise metrics or absolute comparisons between various cryptographic primitives that show the trade off between reliability and security as a function of the block length of plaintext and ciphertext messages - in general, the security of the cryptographic protocol is

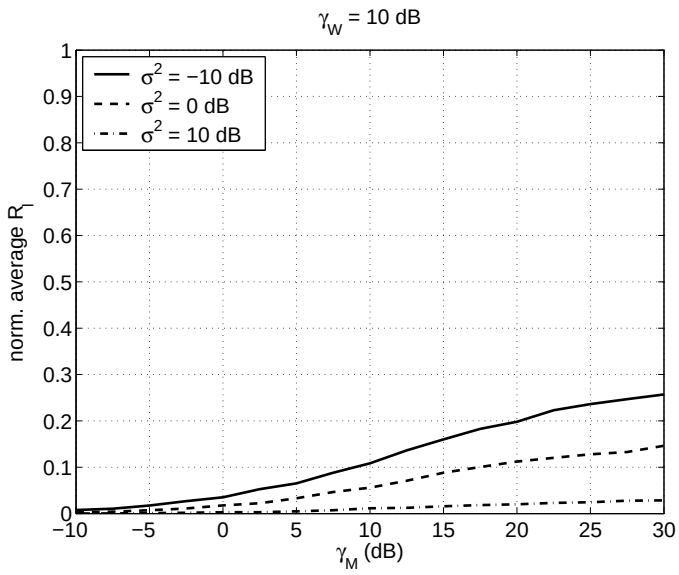

Fig. 13. Normalized average leaked throughput versus $\overline{\gamma}_M$ for $\overline{\gamma}_W = 10$ dB, and for selected values of σ^2. Normalization is effected with respect to the capacity of an AWGN channel with SNR equal to $\overline{\gamma}_M$.

measured by whether it survives a set of attacks or not;

- In general, these will not be information theoretically secure if the communication channel between friendly parties and the eavesdropper are noiseless, because the secrecy capacity of these application-layer systems is zero;
- State-of-the art key distribution schemes for wireless networks based on the computational model require a trusted third party as well as complex protocols and system architectures [32].

The advantages of physical layer security under the information-theoretic (perfect) security models can be summarized as follows:

- No computational restrictions are placed on the eavesdropper;
- Very precise statements can be made about the information that is leaked to the eavesdropper as a function of channel quality and blocklength of the messages [11];
- Has been realized in practice through quantum key distribution [33];
- In theory, suitably long codes used for privacy amplification can get exponentially close to perfect secrecy [11];
- Instead of distributing keys it is possible to generate on-the-fly as many secret keys as desired.

In contrast, we have to take into consideration the following disadvantages of information-theoretic security:

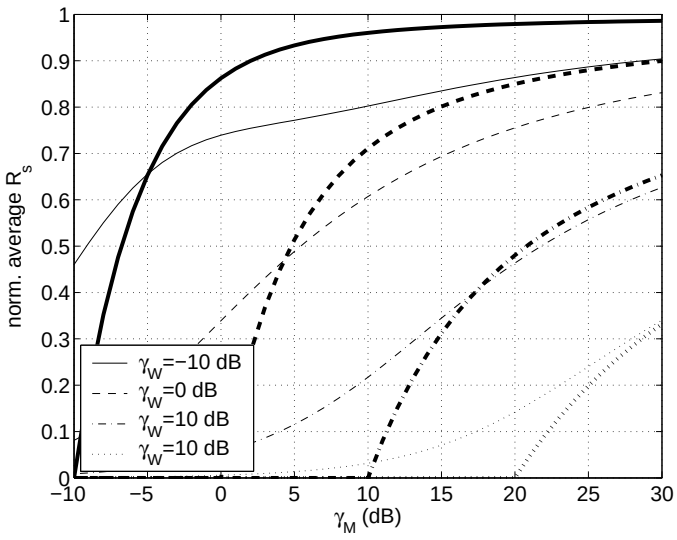

Fig. 14. Normalized average secrecy rate versus $\overline{\gamma}_M$, for selected values of $\overline{\gamma}_W$. Thinner lines correspond to the normalized average secrecy rate in the case of Rayleigh fading channels, while thicker lines correspond to the secrecy capacity of the Gaussian wiretap channel. Normalization is effected with respect to the capacity of an AWGN channel with SNR equal to $\overline{\gamma}_M$.

- Information-theoretic security is an average-information measure. The system can be designed and tuned for a specific level of security - e.g. with very high probability a block will be secure, but it may not be able to guarantee security with probability 1;
- Requires assumptions about the communication channels that may not be accurate in practice. In many cases one would make very conservative assumptions about the channels. This will likely result in low secrecy capacities and low secret-key or -message exchange rates. This gives extremely high security and reliability, but at low communication rates;
- A few systems (e.g Quantum Key Distribution) are deployed but the technology is not as widely available and is expensive;
- A short secret key is still required for authentication [9].

In light of the brief comparisons above, it is likely that any deployment of a physical-layer security protocol in a classical system would be part of a ”layered security” solution where security is provided at a number of different layers, each with a specific goal in mind. This modular approach is how virtually all systems are designed today, so in this context, physical-layer security provides an additional layer of security that does not exist today in classical systems.

VI. 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. Furthermore, we analyzed the impact of imperfect channel state information on the outage probability and the outage secrecy capacity. In particular, we have demonstrated that even in the presence of imperfect CSI it is possible to convey information in an almost secure manner, that is, with an average secure throughput substantially greater than the average leaked throughput.

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. Implementing such a scheme is the goal of Part II of this paper.

References

[1] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. of the IEEE International Symposium on Information Theory (ISIT'06)*, Seattle, WA, July 2006.

[2] 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*, Allerton, USA, September 2006.

[3] ——, "LDPC-based secure wireless communication with imperfect knowledge of the eavesdropper's channel," in *Proc. IEEE Information Theory Workshop*, Chengdu, China, October 2006.

[4] C. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 29, pp. 656–715, 1949.

[5] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

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

[7] S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wiretap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, p. 451–456, July 1978.

[8] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–652, Nov. 1976.

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

[10] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," *Eurocrypt 2000*, *Lecture Notes in Computer Science*, vol. 1807, pp. 351+, 2000. [Online]. Available: citeseer.ist.psu.edu/maurer00informationtheoretic.html

[11] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized privacy amplification," *IEEE Transaction on Information Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

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

[13] P. Parada and R. Blahut, "Secrecy capacity of simo and slow fading channels," in *Proc. of the IEEE International Symposium on Information Theory*, Adelaide, Australia, September 2005.

[14] Y. Liang and V. H. Poor, "Secure communication over fading channels," in *Proc. of the Forty-Fourth Annual Allerton Conference*, Monticello, IL, September 2006.

[15] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Proc. of the Forty-Fourth Annual Allerton Conference*, Monticello, IL, September 2006.

[16] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," 2006, preprint available at http://arxiv.org/abs/cs.IT/0610103.

[17] A. Khisti, A. Tchamkerten, and G. Wornell, "Secure broadcasting with multiuser diversity," in *Proc. of the Forty-Fourth Annual Allerton Conference*, 2006.

[18] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Capacity achieving codes for the wire tap channel with applications to quantum key distribution," *CoRR*, vol. cs.IT/0411003, 2004. [Online]. Available: http://arxiv.org/abs/cs.IT/0411003

[19] M. Bloch, A. Thangaraj, and S. W. McLaughlin, "Efficient reconciliation of correlated continuous random variables using ldpc codes," arxiv preprint cs.IT/0509041, 2005.

[20] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly gaussian random variables," in *Proc. of the IEEE International Symposium on Information Theory*, Seattle, WA, July 2006.

[21] H. Imai, K. Kobara, and K. Morozov, "On the possibility of key agreement using variable directional antenna," in *Joint Workshop on Information Security*, Seoul, Korea, September 2006.

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

[23] C. Ye and P. Narayan, "Secret key and private key constructions for simple multiterminal source models," in *Proc. of the IEEE International Symposium on Information Theory*, Adelaide, Australia, September 2005.

[24] Y. Liang and H. V. Poor, "Generalized multiple access channels with confidential messages," in *Proc. of IEEE International Symposium on Information Theory (ISIT'06)*, Seattle, WA,, July 2006.

[25] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *Proc. of the IEEE International Symposium on Information Theory (ISIT'06)*, Seattle, WA, July 2006.

[26] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages," in *Proc. of the Forty-Fourth Allerton Conference on Communications, Control and Computing*, Monticello, IL, September 2006.

[27] E. Tekin and A. Yener, "The gaussian multiple access wire-tap channel with collective secrecy constraints," in *Proc. of the IEEE International Symposium on Information Theory*, Seattle, WA, July 2006.

[28] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

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

[30] J. G. Proakis, *Digital Communications*, 4th ed. New York: McGraw-Hill, 2001.

[31] M. Simon and M.-S. Alouini, "Some new results for integrals involving the generalized marcum q-function and their application to performance evaluation over fading channels," *IEEE Transactions on Wireless Communications*, vol. 2, no. 4, pp. 611–615, July 2003.

[32] A. Aziz and W. Diffie, "Privacy and authentication for wireless local area networks," *IEEE Personal Communications*, vol. 1, no. 1, pp. 25–31, 1993. [Online]. Available: citeseer.ist.psu.edu/aziz93privacy.html

[33] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, Bangalore,India, December 1984, pp. 175–179.