Physical Layer Security for Multiple-Antenna Systems: A Unified Approach

Kostas P. Peppas, *Senior Member, IEEE*, Nikos C. Sagias, *Senior Member, IEEE*, and Andreas Maras

***Abstract*—Secrecy capacity is a fundamental information-theoretic performance metric to predict the maximum data rate of reliable communication, while the intended message is not revealed to the eavesdropper. Motivated by this consideration in this paper, a unified communication-theoretic framework for the analysis of the probability of nonzero secrecy capacity, the secrecy outage probability, and the secrecy capacity of multiple-antenna systems over fading channels is proposed. Specifically, a powerful frequency-domain approach is first developed in which the integrals involved in the evaluation of the probability of nonzero secrecy capacity and secrecy outage probability are transformed into the frequency domain, by employing Parseval's theorem. A generic approach for the evaluation of the asymptotic secrecy outage probability at high signal-to-noise ratio (SNR) region is also introduced, thus providing useful insight as to the parameters affecting the secrecy performance. Finally, a unified numerical approach for computing the average secrecy capacity of multiple-antenna systems under arbitrary fading environments is developed. The proposed framework is general enough to accommodate any well-known multiantenna transmission technique and fading model. Finally, the secrecy performance of several multiple-antenna system setups is assessed, in the presence of generalized fading conditions and arbitrary antenna correlation, while various numerical and computer simulation results are shown and compared to substantiate the proposed mathematical analysis.**

***Index Terms*—Characteristic function approach, generalized fading channels, moment generating-function, multiple-antenna systems, physical layer security, secrecy capacity.**

I. Introduction

THE RECENT rapid expansion and proliferation of the wireless communication systems has prompted an increasing demand for transmission security. Future communication systems will be decentralized and ad-hoc, thus rendering the whole system vulnerable and susceptible to eavesdropping. Therefore, there has been a considerable recent attention on studying the fundamental ability of the physical layer to augment secrecy in wireless communications networks. The seminal work on wiretap channel in [1] showed that perfect secrecy can be achieved if the eavesdroppers channel is a degraded version of the main channel. In a recent work [2], it was suggested that it is possible to augment perfect secrecy even when the main channel channel conditions are on average worse compared to those of the eavesdroppers channel.

Manuscript received April 8, 2015; revised July 31, 2015 and September 12, 2015; accepted September 23, 2015. Date of publication October 27, 2015; date of current version January 14, 2016. The associate editor coordinating the review of this paper and approving it for publication was J. Yuan.

The authors are with the Department of Informatics and Telecommunications, University of Peloponnese, Tripoli 22100, Greece (e-mail: peppas@uop.gr; nsagias@ieee.org; amaras@uop.gr).

Digital Object Identifier 10.1109/TCOMM.2015.2495293

Recently, considerable research efforts have been made for investigating various transmission/reception scenarios for secrecy enhancement. In this context, in [3]–[8] it was suggested that multiple-input multiple-output (MIMO) techniques can be employed as an effective means to improve secrecy performance of wireless communication systems. In these works, MIMO wiretap channels have been addressed from an information-theoretic perspective and their secrecy capacity was characterized. The secrecy performance of various multiple-antenna schemes was addressed in a large number of contributions for various system setups, including maximal-ratio combining (MRC) and orthogonal space-time block codes (OSTBC) with transmit antenna selection. Representative examples can be found in [9]–[17] and references therein.

Most of the aforementioned contributions employ the so-called probability density function (PDF)-based approach to compute performance metrics such as the average secrecy capacity, the probability of non-zero secrecy capacity and the secrecy outage probability. This approach requires the knowledge of the PDFs of the received signal-to-noise ratio (SNR) for the main channel and the eavesdropper channel. Such frameworks have provided closed-form solutions for the aforementioned performance metrics assuming simple channel models, namely Rayleigh, or Nakagami-m with integer fading parameters. Such closed form expressions, however, are attainable in the cases where the PDF of the SNR for the main channel and the eavesdropper channel can be expanded in a canonical exponential form, i.e. when the aforementioned fading models are considered. However, the wireless applications in most recent years have become increasingly sophisticated, thereby requiring more complicated channel models and sophisticated diversity techniques [18]. For several system setups and fading scenarios frequently encountered in practice, modeled by generalized fading distributions (e.g, κ-μ, η-μ, generalized correlated Rice-Nakagami), the PDF of the SNR at the receiver end is generally not available in a simple and canonical form. Thus, the evaluation of these PDFs in terms of tabulated functions can be a very cumbersome task. Specifically, in case of a generalized fading scenario, the evaluation of the secrecy performance of multiple-antenna systems involves the numerical evaluation of a multi-fold integral. As the number of diversity branches increases, this approach is rendered computationally intractable and the corresponding results may not converge.

On the other hand, the existing analytical frameworks employ ad-hoc methods very different from each other.

Consequently, the need of a unified framework for assessing the secrecy performance of modern wireless communication systems emerges. Recent advances on performance analysis of digital communication systems over fading channels have demonstrated the potential of employing either a moments-generating function (MGF)- or a characteristic function (CHF)-based approach for simplifying performance analysis in such situations [19]–[21]. Such approaches allow for an efficient computation of important performance indexes in those scenarios where the application of the PDF-based approach seems impractical. It is also noted that so far such frameworks have been extensively used for evaluating metrics such as average bit error probability, outage probability and channel capacity [22].

However, the main motivation behind the introduction of a novel MGF-based approach for secrecy performance analysis is the well-proven flexibility of employing this method, due to the fact that an MGF-based method allows the quick and simple evaluation of the secrecy performance in scenarios where a PDF-based approach would either require very cumbersome analytical derivations or where the method would be too complicated to be used in practice. To prove and appreciate the usefulness of an MGF-based approach for the analysis of secrecy performance, in this work we propose system setups (related to SIMO and MIMO systems) where using an MGF-based approach is beneficial, if not the only practical way to keep the complexity of the analytical development at a low level. For simpler system models and fading scenarios, it is shown that the proposed MGF-based approach can yield closed-form expressions for important performance metrics such as the secrecy outage probability and the probability of non-zero secrecy capacity. Note that, to the best of the authors' knowledge, these approaches have not yet been used in a systematic way for the assessment of the secrecy performance of wireless systems.

The main contributions of this paper are summarized as follows:

- A unified numerical approach for computing the average secrecy capacity of multiple antenna systems in arbitrary fading environments is introduced. The proposed approach only requires the knowledge of the moment generating functions of the receiving SNR for the main channel and the eavesdropper channel, yields accurate results despite its simplicity while being easy to program.
- A generic frequency-domain approach is developed for the evaluation of the probability of non-zero secrecy capacity and secrecy outage probability. The corresponding integrals are transformed into the frequency domain, by employing Parseval's theorem. Such a transformation only requires the knowledge of the CHFs of the receiving SNR for the main channel and the eavesdropper channel, that can be evaluated in a straightforward manner for a variety of multiple-antenna transmission schemes.
- In order to provide useful insights as to the parameters affecting secrecy performance of multiple antenna systems, a comprehensive frequency-domain approach is also developed to assess the secrecy outage probability in the high SNR regime. The proposed approach only requires the knowledge of the moment generating functions of the receiving SNR for the main channel and the eavesdropper channel and can be employed to characterize the secrecy outage probability in terms of the secrecy diversity order.
- The newly derived framework is employed to assess the secrecy performance of several multiple-antenna wiretap channels, namely:
  1) MIMO wiretap channel employing OSTBC and operating under generalized fading. The following two distinct cases of interest are considered: In the first case, a correlated MIMO Rayleigh wiretap channel is considered. The second case addresses the secrecy performance of a non-correlated MIMO wiretap channel where the propagation in the legitimate link is dominated by a strong line-of-sight (LOS) component, whereas for the other link, there is no LOS signal present in its propagation channel. Fading in the legitimate channel is modeled by the $\kappa - \mu$ distribution whereas in the eavesdropper channel by the $\eta - \mu$ distribution [23]. To the best of the authors' knowledge, the secrecy performance of wiretap channels with OSTBC in the presence of mixed generalized fading has not yet been addressed in the open technical literature. This is because of the fact that an exact analytical solution is very difficult, if not impossible, to be obtained, based on the conventional PDF approach.
  2) A Rayleigh single-input multiple-output (SIMO) channel with generalized-selection combining (GSC) at the legitimate receiver and the eavesdropper.
  3) A correlated SIMO channel subject to generalized Ricean fading with MRC at the legitimate receiver and the eavesdropper, assuming arbitrary fading parameters and arbitrary correlation. Again, to the best of the authors' knowledge, the secrecy performance of such wiretap channels in the presence of generalized correlated fading with arbitrary fading parameters has not yet been addressed in the open technical literature, since the conventional PDF-based approach is rendered mathematically intractable. Note that a special case of this very general problem has been addressed in [16], where the secrecy performance of a wiretap channel with OSTBC was addressed, assuming that the legitimate and eavesdropper channels experience correlated Rice and Rayleigh fading, respectively. The authors employed the Moschopoulos' method to provide infinite series representations of the secrecy outage probability [24].

The proposed analysis is presented and verified by numerically evaluated results accompanied with Monte-Carlo simulations results.

The remainder of this paper is structured as follows. Section II outlines the problem under consideration. In Section III the proposed MGF- and CHF-based approaches for the evaluation of the probability of non-zero secrecy capacity and secrecy outage are introduced. In Section IV the proposed framework is employed to derive corresponding analytical expressions for three different system scenarios that are MIMO

wiretap channels with OSTBC under generalized fading, SIMO Rayleigh wiretap channels with GSC and generalized Ricean SIMO wiretap channels with arbitrary correlation and MRC. In Section V the various performance results and their interpretations are presented. Finally, concluding remarks are presented in Section VI.

Mathematical Notations: Throughout this paper, $\imath = \sqrt{-1}$, $\mathbb{C}$ is the set of complex numbers, $\mathrm{vec}\,(\cdot)$ is the vectorizing operator that maps the elements of a given matrix into a column vector, $\|\cdot\|_F^2$ denotes the Frobenius norm of a matrix, $(\cdot)^T$ denotes the matrix transpose operator, $(\cdot)^H$ denotes the matrix hermitian transpose operator, $\mathbf{I}_M$ denotes the $M \times M$ identity matrix, diag[·] denotes the diagonal matrix, $\otimes$ denotes the matrix Kronecker product, $\mathrm{Tr}\,(\cdot)$ denotes the trace of a matrix, $\mathbb{E}\langle\cdot\rangle$ denotes the expectation operator and $\Pr(\cdot)$ denotes probability. The PDF of a random variable X is denoted as $f_X(\cdot)$, its cumulative distribution function (CDF) as $F_X(\cdot)$, its moment generating function (MGF) as $\mathcal{M}_X(\cdot)$, and its characteristic function (CHF) as $\phi_X(\cdot)$. In terms of mathematical functions used in this paper, $\mathrm{sgn}(\cdot)$ denotes the signum function, $\Re\{\cdot\}$ and $\Im\{\cdot\}$ are the real and imaginary parts of a complex number, respectively, $[\cdot]^+ = \max\{x, 0\}$, $\lceil x \rceil$ is the smallest integer not less than x, z^* denotes the conjugate of the complex number z, $\mathcal{F}\{g(t); t; \omega\}$ denotes the Fourier transform of the function $g(t)$, $\mathcal{L}\{g(t); t; s\}$ denotes the Laplace transform of the function $g(t)$, $\mathcal{L}^{-1}\{G(s); s; t\}$ denotes the inverse Laplace transform of the function $G(s)$, $\Gamma(\cdot)$ is the Gamma function [25, eq. (8.310/1)], and $\delta(\cdot)$ is the Dirac's delta function.

II. System Model and Problem Formulation

A generic MIMO wiretap channel is considered which consists of a transmitter $\mathcal{A}$ Alice, the legitimate receiver $\mathcal{B}$ Bob and an eavesdropper Eve $\mathcal{E}$. Throughout this analysis quasi-static fading channels with generally distributed block fading in the main channel from Alice to Bob ($\mathcal{A} \to \mathcal{B}$), as well as in the eavesdroppers channel from Alice to Eve ($\mathcal{A} \to \mathcal{E}$) are considered. In both channels, it is assumed that the transmission block length is less than or equal to the coherence time. Also, the main channel and the eavesdroppers channel are assumed to be independent of each other.

In this work, two eavesdropping scenarios are considered, namely active eavesdropping and passive eavesdropping. Under the active eavesdropping scenario, channel state information (CSI) of the eavesdroppers channel is also known at Alice. In such a scenario, a fundamental secrecy performance metric is the achievable secrecy capacity of the MIMO wiretap channel, defined as [2]

$$C_S = \left[\log_2(1+\gamma_{\mathcal{B}}) - \log_2(1+\gamma_{\mathcal{E}})\right]^+ , \tag{1}$$

where $\gamma_{\mathcal{B}}$ and $\gamma_{\mathcal{E}}$ denote the receiving SNRs for the main and the eavesdropper channels, respectively. The average secrecy capacity is given by [17, eq. (15)]

$$\bar{C}_S = \frac{1}{\ln(2)} \int_0^\infty \frac{F_{\gamma_{\mathcal{E}}}(x)}{1+x} \left[1 - F_{\gamma_{\mathcal{B}}}(x)\right] \mathrm{d}x. \tag{2}$$

Under the passive eavesdropping scenario, CSI of the eavesdroppers channel is not available to either Alice or Bob. In such a scenario, Alice transmits at a constant code rate $\mathcal{R}_S$. The transmission from Alice guarantees perfect secrecy if $C_S \geq \mathcal{R}_S$. On the other hand, if $C_S < \mathcal{R}_S$, the transmission is vulnerable to eavesdropping and perfect secrecy is not guaranteed. A useful and practical metric for assessing the secrecy performance of the wiretap channel is the secrecy outage probability, P_{out}. It is defined as the probability that the secrecy capacity does not exceed a predefined secrecy rate, $\mathcal{R}_S$. Specifically, the secrecy outage probability is the probability that either there exists an outage between Alice and Bob, or Eve can eavesdrop on data such that perfect secrecy cannot be guaranteed. Mathematically speaking, P_{out} can be expressed as [9]–[12]

$$P_{\text{out}} = \Pr\{C_S < \mathcal{R}_S\} = \int_0^\infty F_{\gamma_{\mathcal{B}}}\left[2^{\mathcal{R}_S}(1+x) - 1\right] f_{\gamma_{\mathcal{E}}}(x)\, \mathrm{d}x. \tag{3}$$

Another relevant metric is the probability of non-zero secrecy capacity, [9]–[12] that can be expressed as

$$\begin{aligned} P_{\text{NZ}} &= \Pr\{C_S > 0\} = 1 - \Pr\{C_S < \mathcal{R}_S\}|_{\mathcal{R}_S=0} \\ &= 1 - \int_0^\infty F_{\gamma_{\mathcal{B}}}(x)\, f_{\gamma_{\mathcal{E}}}(x)\, \mathrm{d}x. \end{aligned} \tag{4}$$

Note that (2), (3) and (4) provide a general and unified PDF-based approach for the assessment of the secrecy performance of every communication system, for which the CDF of $\gamma_{\mathcal{B}}$ and the PDF of $\gamma_{\mathcal{E}}$ are readily available. In a general multiple-antenna scenario, the evaluation of (2), (3) and (4) involves multi-fold integrals of PDFs or inverse Laplace transform operations of the product of the corresponding MGFs. Such approaches are certainly computationally inefficient, especially for an increased number of antennas. Concerning this well-recognized and cumbersome problem, it is more insightful to transform the integrals appearing in (2), (3) and (4) in the frequency domain, since simple and yet computationally inefficient expressions for the MGFs or the CHFs of $\gamma_{\mathcal{B}}$ and $\gamma_{\mathcal{E}}$ are readily available, for a variety of multiple-antenna systems with or without correlation, and with the most of them being in closed form.

III. Frequency Domain Approach

In this section, alternative expressions for (2), (3) and (4) in the frequency domain, are derived.

A. Average Secrecy Capacity

Proposition 1: A numerically efficient method to evaluate (2) in the frequency domain is deduced as

$$\begin{aligned} \bar{C}_S \approx \frac{2}{\pi \ln(2)} \sum_{j=1}^{N_J} \sum_{k=1}^{N_K} v_j\, x_j\, w_k \\ \times \Re\left\{ \frac{\mathcal{M}_{\gamma_{\mathcal{E}}}(c_j + \imath\, y_k)}{c_j + \imath\, y_k} \frac{1 - \mathcal{M}_{\gamma_{\mathcal{B}}}(x_j^2 - c_j - \imath\, y_k)}{x_j^2 - c_j - \imath\, y_k} \right\}. \end{aligned} \tag{5}$$

where N_{J}, N_K are the numbers of integration points, x_j, v_j are abscissas and weights, computed using the methodology presented in [26], y_k, w_k are abscissas and weights, defined respectively as [27]

$$y_k = \tan\left[\frac{\pi}{4}\,\cos\left(\frac{2\,k-1}{2\,N_K}\,\pi\right)+\frac{\pi}{4}\right] \tag{6a}$$

$$w_k = \frac{\pi^2\,\sin\left(\frac{2k-1}{2\,N_K}\,\pi\right)}{4\,N_K\,\cos^2\left[\frac{\pi}{4}\,\cos\left(\frac{2k-1}{2\,N_K}\,\pi\right)+\frac{\pi}{4}\right]}. \tag{6b}$$

and c_j are arbitrary constants that guarantee the convergence of (5).

Proof: By employing the well-known identity $(1+s)^{-1}=\int_0^{\infty}\exp[-(s+1)\,t]\,\mathrm{d}t$ and exploiting the definition of the Laplace transform, (2) becomes

$$\bar{C}_S = \frac{1}{\ln(2)}\int_0^{\infty}\exp(-s)\,\mathcal{L}\left\{F_{\gamma_{\mathcal{E}}}(x)(1-F_{\gamma_{\mathcal{B}}}(x));\,x;\,s\right\}\mathrm{d}s. \tag{7}$$

Then by employing [28, eqs. (1.1.1.20), (1.1.5.2), (2.1.1.1)], as well as the change of variables $s=t^2$, (7) becomes

$$\bar{C}_S = \frac{2}{\pi\,\ln(2)}\int_0^{\infty}\exp(-t^2)\times\int_0^{\infty}\Re\left\{\frac{\mathcal{M}_{\gamma_{\mathcal{E}}}(c+\imath\,u)}{c+\imath\,u}\,\frac{1-\mathcal{M}_{\gamma_{\mathcal{B}}}(t^2-c-\imath\,u)}{t^2-c-\imath\,u}\right\}\mathrm{d}u\,\mathrm{d}t \tag{8}$$

where c is arbitrary constant. The integral with respect to u can be evaluated by employing the change of variables $u=\tan(\theta)$ and a N_K point Gauss-Chebyshev quadrature technique with abscissas y_k and weights w_k given by (6a) and (6b), respectively. The integral with respect to t can be evaluated numerically using a N_{J}-point semi-infinite Gauss-Hermite quadrature (SI-GHQ) rule [26]. In particular, integrals of the form $\int_0^{\infty}\exp(-t^2)\,f(t)\,\mathrm{d}t$ can be approximated as

$$\int_0^{\infty}\exp(-t^2)\,f(t)\,\mathrm{d}t \approx \sum_{j=1}^{N_{\mathrm{J}}} v_j\,f(x_j)\,, \tag{9}$$

where the weights v_j and the abscissas x_j are given in [26, Table II] for values of N_{J} up to 15. For $N_{\mathrm{J}}>15$, v_j and x_j can be easily computed using the methodology presented in [26]. Note that for a given value of j, different values of the tuning parameter c may be required to guarantee the convergence of each integral with respect to t. Thus, in general, c is also a function of j, i.e. $c=c_j$. In Section V, for the evaluation of the average secrecy capacity the parameters c_j are selected as $c_j=x_j^2/4$ to ensure convergence of the numerical approximation. By combining both numerical approximations for the corresponding integrals, $\bar{C}_S$ is finally deduced as (5) thus concluding the proof. ■

B. Secrecy Outage Probability and Probability of Non-Zero Secrecy Capacity

In order to provide simpler, alternative expressions for (3) and (4), it is first shown that the following generic result holds.

Proposition 2: Let define the integral

$$\mathcal{I} \triangleq \int_0^{\infty} f_X(x)\;F_Y(Tx+V)\;\mathrm{d}x, \tag{10}$$

with X, Y being two positive random variables and V, T two positive real constants. An equivalent expression for $\mathcal{I}$ can be expressed as

$$\mathcal{I} = \frac{1}{2} - \frac{1}{\pi}\int_0^{\infty}\Im\left\{\frac{1}{\omega}\,\phi_X^*(T\,\omega)\,\phi_Y(\omega)\,\exp(-\imath\,V\,\omega)\right\}\mathrm{d}\omega. \tag{11}$$

Proof: By employing the Parseval's theorem [29], the integral in (10) can be written as

$$\mathcal{I} = \frac{1}{2\pi}\int_{-\infty}^{\infty}\mathcal{F}^*\{f_X(x);\,x;\,\omega\}\,\mathcal{F}\{F_Y(Tx+V);\,x;\,\omega\}\,\mathrm{d}\omega. \tag{12}$$

To this end, the two above Fourier transforms should be first derived. The first Fourier transform, can be readily obtained as

$$\mathcal{F}\{f_X(x);\,x;\,\omega\} = \phi_X(-\omega)\,. \tag{13}$$

By employing the following three identities [29]

$$\mathcal{F}\left\{\int_{-\infty}^{x} g(\tau)\,\mathrm{d}\tau;\,x;\,\omega\right\} = -\frac{\imath}{\omega}\,\mathcal{F}\{g(x);\,x;\,\omega\} + \mathcal{F}\{g(x);\,x;\,0\}\,\pi\,\delta(\omega)\,, \tag{14a}$$

$$\mathcal{F}\{g(Tx);\,x;\,\omega\} = \frac{1}{|T|}\,\mathcal{F}\left\{g(x);\,x;\,\frac{\omega}{T}\right\} \tag{14b}$$

and

$$\mathcal{F}\{g(x-a);\,x;\,\omega\} = \exp(-\imath\,a\,\omega)\,\mathcal{F}\{g(x);\,x;\,\omega\}\,, \tag{14c}$$

yields the next expression for the second Fourier transform

$$\mathcal{F}\{F_Y(Tx+V);\,x;\,\omega\} = \left[-\frac{\imath}{\omega}\,\phi_{X_0}\left(-\frac{\omega}{T}\right)+\pi\,\delta(\omega)\right]\times\exp(i\,V\,\omega)\,. \tag{15}$$

By substituting (13) and (15) into (12), and by employing the fundamental property of the Dirac's delta function, i.e. $\int_{-\infty}^{\infty}\delta(t-t_0)\,g(t)\,\mathrm{d}t=g(t_0)$, yields

$$\mathcal{I} = \frac{1}{2} + \frac{1}{2\,\pi}\int_{-\infty}^{\infty}\frac{\imath}{\omega}\,\phi_X^*(\omega\,T)\,\phi_Y(\omega)\exp(-\imath\,V\,\omega)\,\mathrm{d}\omega\,. \tag{16}$$

In the above equation, by employing the hermitian property of the characteristic functions and after some straightforward manipulations, (11) is finally extracted, and this concludes the proof. ■

Proposition 2 can be readily employed for the evaluation of P_{out} and P_{NZ}, as follows.

Corollary 1: Generic integral representations for the secrecy outage probability and the probability of non-zero secrecy capacity for the multiple-antenna wiretrap channels can be expressed as

$$P_{\mathrm{out}} = \frac{1}{2} - \frac{1}{\pi}\int_0^{\infty}\Im\left\{\frac{1}{\omega}\,\phi_{\gamma_{\mathcal{E}}}^*(2^{\mathcal{R}_S}\,\omega)\,\phi_{\gamma_{\mathcal{B}}}(\omega)\,e^{-\imath\,(2^{\mathcal{R}_S}-1)\omega}\right\}\mathrm{d}\omega \tag{17}$$

and

$$P_{\mathrm{NZ}} = \frac{1}{2} + \frac{1}{\pi}\int_0^{\infty} \Im\left\{\frac{1}{\omega}\,\phi^*_{\gamma_{\mathcal{E}}}(\omega)\,\phi_{\gamma_{\mathcal{B}}}(\omega)\right\} \mathrm{d}\omega\,. \tag{18}$$

It is underlined that both (17) and (18) circumvent the need for the PDF and CDF of the corresponding SNRs. Additionally, the corresponding Fourier transforms can be obtained in a relatively easy manner for a variety of system setups.

C. Asymptotic Secrecy Outage Probability Analysis

In order to provide further insights as to the parameters affecting secrecy outage performance, a comprehensive frequency domain approach for deducing the asymptotic outage probability at high SNR region is hereafter presented.

Proposition 3: Let us assume that the MGF of $\gamma_{\mathcal{B}}$ can be expressed for $s \to \infty$ as $\mathcal{M}_{\gamma_{\mathcal{B}}}(s) = C s^{-d} + o(s^{-d})$ with d being the secrecy diversity gain. Then, an asymptotic expression for P_{out} can be deduced as

$$P_{\mathrm{out}} = \begin{cases} \frac{C}{\Gamma(d+1)} \sum_{k=0}^{d} \binom{d}{k} T^k\, V^{d-k}\, a_k, & \text{if } d \text{ integer} \\ \frac{C V^d}{\Gamma(d+1)\,\Gamma(\lambda)} \sum_{k=0}^{\lceil d \rceil} \binom{\lceil d \rceil}{k} b_k, & \text{if } d \text{ non-integer} \end{cases} \tag{19}$$

where $T = 2^{\mathcal{R}_S}$, $V = 2^{\mathcal{R}_S} - 1$, $\lambda = \lceil d \rceil - d$ and

$$a_k = (-1)^k \left.\frac{\partial^k \mathcal{M}_{\gamma_{\mathcal{E}}}(s)}{\partial s^k}\right|_{s=0} \tag{20a}$$

$$b_k = (-1)^k \int_0^{\infty} \exp(-s)\, s^{\lambda-1}\, \frac{\partial^k \mathcal{M}_{\gamma_{\mathcal{E}}}(s\,T/V)}{\partial s^k}\,\mathrm{d}s\,. \tag{20b}$$

Proof: Assuming that $\mathcal{M}_{\gamma_{\mathcal{B}}}(s) = C s^{-d} + o(s^{-d})$ for $s \to \infty$, $F_{\gamma_{\mathcal{B}}}(\gamma)$ can be deduced as $F_{\gamma_{\mathcal{B}}}(\gamma) = \mathcal{L}^{-1}\left\{\mathcal{M}_{\gamma_{\mathcal{B}}}(s)/s; s; \gamma\right\}$ yielding $F_{\gamma_{\mathcal{B}}}(\gamma) \approx C\gamma^d/\Gamma(d+1)$. Then, for high values of $\overline{\gamma}_{\mathcal{B}}$, (3) can be written as

$$P_{\mathrm{out}} \approx \frac{C}{\Gamma(d+1)} \int_0^{\infty} (Tx+V)^d\, f_{\gamma_{\mathcal{E}}}(x)\,\mathrm{d}x. \tag{21}$$

If d is integer, then by employing the binomial identity as well as the well known relationship between the nth moment of a random variable X and its MGF, i.e. $\mathbb{E}\langle X^n\rangle = (-1)^n \left.\frac{\partial^n \mathcal{M}_X(s)}{\partial s^n}\right|_{s=0}$, the first branch of (19) is readily deduced.

If d is a positive real number, then $d = \lceil d \rceil - \lambda$, and $(Tx+V)^d = (Tx+V)^{\lceil d \rceil - \lambda}$. By employing the well-known identity [25, eq. (17.13/3)]

$$(Tx+V)^{-\lambda} = \frac{V^{-\lambda}}{\Gamma(\lambda)} \int_0^{\infty} e^{-\left(\frac{Tx}{V}+1\right)s}\, s^{\lambda-1}\,\mathrm{d}s,\ \lambda > 0, \tag{22}$$

the binomial identity along with the definition of the MGF of $\gamma_{\mathcal{E}}$ as well as the relationship between the nth moment of a random variable X and its MGF, the second branch of (19) is deduced thus completing the proof. ■

IV. Applications for the Physical Layer Security

In this section we present three important applications for which we derive the secrecy outage probability and the probability of non-zero secrecy capacity. In all three scenarios we consider a MIMO wiretap channel, in which Alice, Bob and Eve are equipped with $N_{\mathcal{A}}$, $N_{\mathcal{B}}$ and $N_{\mathcal{E}}$ antennas, respectively. When generalized fading models are considered, the secrecy outage probability and probability of non-zero secrecy capacity are expressed in terms of a single integral that can be easily evaluated numerically by employing standard numerical integration algorithms or symbolic integration. When simpler system models and fading scenarios are considered, it is also shown that the secrecy outage probability and the probability of non-zero secrecy capacity can be expressed in closed form.

A. MIMO Wiretap Channels With OSTBC

We assume that both $(\mathcal{A}) \to (\mathcal{B})$ and $(\mathcal{A}) \to (\mathcal{E})$ links experience slow fading. Alice selects L transmit symbols, $s_1, s_2, \ldots, s_L$, with $\mathbb{E}\langle s_k^2\rangle = 1$, $\forall k \in \{1, 2, \ldots, L\}$. The symbols are encoded according to an OSTBC matrix $\mathbf{Q} \in \mathbb{C}^{N_{\mathcal{A}} \times T}$ and transmitted during T time slots. The received signal at Bob can be written as

$$\mathbf{Y} = \sqrt{P}\,\mathbf{H}_{\mathcal{AB}}\,\mathbf{Q} + \mathbf{N}_{\mathcal{B}}, \tag{23}$$

where P is the transmitted power, $\mathbf{N}_{\mathcal{B}} \in \mathbb{C}^{N_{\mathcal{B}} \times T}$ is the additive white Gaussian noise (AWGN) matrix, with elements having zero mean and variance σ_b^2, $\mathbf{H}_{\mathcal{AB}} \in \mathbb{C}^{N_{\mathcal{B}} \times N_{\mathcal{A}}}$ is the channel gain matrix.

Since OSTBC is employed, the MIMO channels are reduced to rank$\{\mathbf{H}_{\mathcal{AB}}\}$ parallel single-input single-output (SISO) channels [16]. These channels are combined using MRC and, therefore, the k-th signal at Bob can be expressed as

$$y_k = \sqrt{P}\, s_k\, \|\mathbf{H}_{\mathcal{AB}}\|_F^2 + n_k \tag{24}$$

where $n_{B,k}$ is the filtered zero-mean Gaussian noise with variance $\sigma_b^2\, \|\mathbf{H}_{\mathcal{AB}}\|_F^2$.

The received signal at Eve can be expressed as

$$\mathbf{Z} = \sqrt{P}\,\mathbf{H}_{\mathcal{AE}}\,\mathbf{Q} + \mathbf{N}_{\mathcal{E}}\,, \tag{25}$$

where $\mathbf{N}_{\mathcal{E}} \in \mathbb{C}^{N_{\mathcal{E}} \times T}$ is the AWGN matrix with elements having zero mean and variance σ_e^2 and $\mathbf{H}_{\mathcal{AE}} \in \mathbb{C}^{N_{\mathcal{E}} \times N_{\mathcal{A}}}$ is the channel gain matrix.

Following a similar line of arguments as in the case of the $(\mathcal{A}) \to (\mathcal{B})$ link, the k-th combined signal at Eve can be expressed as

$$z_k = \sqrt{P}\, s_k\, \|\mathbf{H}_{\mathcal{AE}}\|_F^2 + \nu_k \tag{26}$$

where ν_k is zero-mean filtered Gaussian noise with variance $\sigma_e^2\, \|\mathbf{H}_{\mathcal{AB}}\|_F^2$.

In order to assess the secrecy performance of the considered system the MGFs/CHFs of the instantaneous SNR at Bob and Eve should be deduced. The instantaneous SNRs at Bob and Eve can be written as $\gamma_{\mathcal{B}} = \overline{\gamma}_{\mathcal{B}}\, ||\mathbf{H}_{\mathcal{AB}}||^2$ and $\gamma_{\mathcal{E}} = \overline{\gamma}_{\mathcal{E}}\, ||\mathbf{H}_{\mathcal{AE}}||^2$, respectively, with $\overline{\gamma}_{\mathcal{B}} = P/\sigma_b^2$ and $\overline{\gamma}_{\mathcal{E}} = P/\sigma_e^2$.

1) Correlated Rayleigh MIMO Wiretap Channels: In this case, it is assumed that both $\mathbf{H}_{\mathcal{AB}}$ and $\mathbf{H}_{\mathcal{AE}}$ have mutually correlated Rayleigh fading entries. Specifically, the elements of $\mathbf{H}_{\mathcal{AB}}$ are characterized by a $N_{\mathcal{A}}N_{\mathcal{B}} \times N_{\mathcal{A}}N_{\mathcal{B}}$ correlation

matrix $\mathbf{R}_{\mathcal{AB}} = \mathbb{E}\langle \mathbf{h}_{\mathcal{AB}}\, \mathbf{h}_{\mathcal{AB}}^H \rangle$ where $\mathbf{h}_{\mathcal{AB}} = \text{vec}\{\mathbf{H}_{\mathcal{AB}}\}$ [30], [31]. Similarly, the elements of $\mathbf{H}_{\mathcal{AE}}$ are characterized by correlation matrix $\mathbf{R}_{\mathcal{AE}} = \mathbb{E}\langle \mathbf{h}_{\mathcal{AE}}\, \mathbf{h}_{\mathcal{AE}}^H \rangle$ and $\mathbf{h}_{\mathcal{AE}} = \text{vec}\{\mathbf{H}_{\mathcal{AE}}\}$.

Let us further assume that the correlation matrices $\mathbf{R}_{\mathcal{AB}}$ and $\mathbf{R}_{\mathcal{AE}}$ are eigen-decomposed as $\mathbf{R}_{\mathcal{AB}} = \mathbf{U}_{\mathcal{AB}}\, \mathbf{\Lambda}_{\mathcal{AB}}\, \mathbf{U}_{\mathcal{AB}}^H$ and $\mathbf{R}_{\mathcal{AE}} = \mathbf{U}_{\mathcal{AE}}\, \mathbf{\Lambda}_{\mathcal{AE}}\, \mathbf{U}_{\mathcal{AE}}^H$ where $\mathbf{\Lambda}_{\mathcal{AB}} = \text{diag}[\lambda_{1,\mathcal{AB}}, \lambda_{2,\mathcal{AB}}, \ldots, \lambda_{N_{\mathcal{B}} N_{\mathcal{E}},\mathcal{AB}}]$, $\mathbf{\Lambda}_{\mathcal{AE}} = [\lambda_{1,\mathcal{AE}}, \lambda_{2,\mathcal{AE}}, \ldots \lambda_{N_{\mathcal{E}} N_{\mathcal{A}},\mathcal{AE}}]$ and $\lambda_{i,\mathcal{AB}}$, $\lambda_{j,\mathcal{AE}}$ are the non-zero eigenvalues of $\mathbf{R}_{\mathcal{AB}}$ and $\mathbf{R}_{\mathcal{AE}}$, respectively, $\forall i = \{1, 2, \ldots, N_{\mathcal{B}}\, N_{\mathcal{A}}\}$, $j = \{1, 2, \ldots, N_{\mathcal{E}}\, N_{\mathcal{A}}\}$. Then, the CHFs of $\gamma_{\mathcal{B}}$ and $\gamma_{\mathcal{E}}$ are given as [32, eq. (11)]

$$\phi_{\gamma_{\mathcal{B}}}(\omega) = \left[\det\left(\mathbf{I}_{N_{\mathcal{B}} N_{\mathcal{A}}} - \imath\, \omega\, \overline{\gamma}_{\mathcal{B}}\, \mathbf{R}_{\mathcal{AB}}\right)\right]^{-1} = \left[\prod_{i=1}^{N_{\mathcal{B}} N_{\mathcal{A}}} \left(1 - \imath\, \omega\, \overline{\gamma}_{\mathcal{B}}\, \lambda_{i,\mathcal{AB}}\right)\right]^{-1} \tag{27a}$$

and

$$\phi_{\gamma_{\mathcal{E}}}(\omega) = \left[\det\left(\mathbf{I}_{N_{\mathcal{E}} N_{\mathcal{A}}} - \imath\, \omega\, \overline{\gamma}_{\mathcal{E}} \mathbf{R}_{\mathcal{AE}}\right)\right]^{-1} = \left[\prod_{j=1}^{N_{\mathcal{E}} N_{\mathcal{A}}} \left(1 - \imath\, \omega\, \overline{\gamma}_{\mathcal{E}}\, \lambda_{j,\mathcal{AE}}\right)\right]^{-1}, \tag{27b}$$

respectively. The corresponding MGFs can be readily obtained as $\mathcal{M}_{\gamma_{\mathcal{B}}}(s) = \phi_{\gamma_{\mathcal{B}}}(\imath s)$ and $\mathcal{M}_{\gamma_{\mathcal{E}}}(s) = \phi_{\gamma_{\mathcal{E}}}(\imath s)$. Therefore, assuming active eavesdropping, the average secrecy capacity can be readily obtained by employing Proposition 3.

Assuming passive eavesdropping, an integral representation for the secrecy outage probability of the considered MIMO wiretap channel can be deduced as in (28), shown at the bottom of the page, where

$$\theta_{\mathcal{B}}(\omega) = 2 \arctan\left[\frac{\sin\left(\sum_{i=1}^{N_{\mathcal{B}} N_{\mathcal{A}}} \arctan(\overline{\gamma}_{\mathcal{B}}\, \omega\, \lambda_{i,\mathcal{AB}})\right)}{1 + \cos\left(\sum_{i=1}^{N_{\mathcal{B}} N_{\mathcal{A}}} \arctan(\overline{\gamma}_{\mathcal{B}}\, \omega \lambda_{i,\mathcal{AB}})\right)}\right] \tag{29a}$$

and

$$\theta_{\mathcal{E}}(\omega) = 2 \arctan\left[\frac{\sin\left(\sum_{j=1}^{N_{\mathcal{E}} N_{\mathcal{A}}} \arctan(\overline{\gamma}_{\mathcal{B}}\, \omega \lambda_{j,\mathcal{AE}})\right)}{1 + \cos\left(\sum_{j=1}^{N_{\mathcal{E}} N_{\mathcal{A}}} \arctan(\overline{\gamma}_{\mathcal{E}}\, \omega\, \lambda_{i,\mathcal{AE}})\right)}\right]. \tag{29b}$$

The proof of (28) is given in the Appendix A.

Note that by employing the proposed CHF-based approach, a numerically equivalent simple closed-form expression for the secrecy outage probability of the considered MIMO wiretap channel can be deduced. Specifically, in Appendix B it is shown that the secrecy outage probability can be obtained as

$$P_{\text{out}}^{\text{OSTBC}} = 1 + \sum_{i=1}^{N_{\mathcal{B}} N_{\mathcal{A}}} \frac{\imath\, a_i}{\overline{\gamma}_{\mathcal{B}}\, \lambda_{i,\mathcal{AB}}} \exp\left(-\frac{2^{\mathcal{R}_S} - 1}{\overline{\gamma}_{\mathcal{B}}\, \lambda_{i,\mathcal{AB}}}\right), \tag{30}$$

where

$$a_i = \frac{1}{\omega}\left[\prod_{k=1, k\neq i}^{N_{\mathcal{B}} N_{\mathcal{A}}} \left(1 - \imath\, \omega\, \overline{\gamma}_{\mathcal{B}}\, \lambda_{k,\mathcal{AB}}\right)\right]^{-1} \times \left[\prod_{j=1}^{N_{\mathcal{E}} N_{\mathcal{A}}} \left(1 + \imath\, 2^{\mathcal{R}_S}\, \omega\, \overline{\gamma}_{\mathcal{E}}\, \lambda_{j,\mathcal{AE}}\right)\right]^{-1}\Bigg|_{\omega = \frac{1}{\imath\, \overline{\gamma}_{\mathcal{B}}\, \lambda_{i,\mathcal{AB}}}}. \tag{31}$$

The probability of non-zero secrecy capacity can be readily obtained by employing (28). Specifically, an integral representation for the probability of non-zero secrecy capacity of the considered MIMO wiretap channel can be deduced as in (32), shown at the bottom of the page.

Finally, an expression for the asymptotic P_{out} will be deduced. The MGF of $\gamma_{\mathcal{B}}$ can be expressed as $\mathcal{M}_{\gamma_{\mathcal{B}}}(s) = 1/\det(\mathbf{I}_{N_{\mathcal{B}} N_{\mathcal{A}}} + s\, \overline{\gamma}_{\mathcal{B}}\, \mathbf{R}_{\mathcal{AB}})$, which for $s \to \infty$ can be simplified as $\mathcal{M}_{\gamma_{\mathcal{B}}}(s) \approx [\det(s\, \overline{\gamma}_{\mathcal{B}}\, \mathbf{R}_{\mathcal{AB}})]^{-1}$. Thus, $\mathcal{M}_{\gamma_{\mathcal{B}}}(s)$ can be approximated as

$$\mathcal{M}_{\gamma_{\mathcal{B}}}(s) \approx s^{-N_{\mathcal{A}} N_{\mathcal{B}}}\, \overline{\gamma}_{\mathcal{B}}{}^{-N_{\mathcal{A}} N_{\mathcal{B}}}\, [\det(\mathbf{R}_{\mathcal{AB}})]^{-1}, \tag{33}$$

wherefrom it is readily deduced that the secrecy diversity gain of the proposed scheme is $d = N_{\mathcal{A}}\, N_{\mathcal{B}}$ and $C = \overline{\gamma}_{\mathcal{B}}{}^{-N_{\mathcal{A}} N_{\mathcal{B}}}\, [\det(\mathbf{R}_{\mathcal{AB}})]^{-1}$. Since d is always integer, an asymptotic expression for P_{out} assuming high values of $\overline{\gamma}_{\mathcal{B}}$ can be readily deduced using Proposition 3.

2) Generalized MIMO Wiretap Channels: In this case, we consider mixed fading conditions for $\mathcal{A} \to \mathcal{B}$, and $\mathcal{A} \to \mathcal{E}$ links: The $\mathcal{A} \to \mathcal{B}$ link is subject to $\eta - \mu$ fading, and the $\mathcal{A} \to \mathcal{E}$ link is subject to $\kappa - \mu$. Note that these two distributions fit well experimental data and include as special cases well-known fading channel models, such as the Nakagami-m, Rice, and Hoyt models. On one hand, the $\kappa - \mu$ distribution is a generic

$$P_{\text{out}}^{\text{OSTBC}} = \frac{1}{2} + \frac{1}{\pi}\int_0^{\infty} \frac{1}{\omega}\left[\prod_{i=1}^{N_{\mathcal{A}} N_{\mathcal{B}}} \left(1 + \overline{\gamma}_{\mathcal{B}}{}^2\, \lambda_{i,\mathcal{AB}}^2\, \omega^2\right)^{-\frac{1}{2}}\right]\left[\prod_{j=1}^{N_{\mathcal{A}} N_{\mathcal{E}}} \left(1 + 2^{2\mathcal{R}_S}\, \overline{\gamma}_{\mathcal{E}}{}^2\, \lambda_{j,\mathcal{AE}}^2\, \omega^2\right)^{-\frac{1}{2}}\right] \times \sin\left[\theta_{\mathcal{B}}(-\omega) - \theta_{\mathcal{E}}\left(-2^{\mathcal{R}_S}\, \omega\right) + \left(2^{\mathcal{R}_S} - 1\right)\omega\right] \mathrm{d}\omega \tag{28}$$

$$P_{\text{NZ}}^{\text{OSTBC}} = \frac{1}{2} - \frac{1}{\pi}\int_0^{\infty} \frac{1}{\omega}\left[\prod_{i=1}^{N_{\mathcal{A}} N_{\mathcal{B}}} \left(1 + \overline{\gamma}_{\mathcal{B}}{}^2\, \lambda_{i,\mathcal{AB}}^2\, \omega^2\right)^{-\frac{1}{2}}\right]\left[\prod_{j=1}^{N_{\mathcal{A}} N_{\mathcal{E}}} \left(1 + \overline{\gamma}_{\mathcal{E}}{}^2\, \lambda_{j,\mathcal{AE}}^2\, \omega^2\right)^{-\frac{1}{2}}\right] \sin\left[\theta_{\mathcal{B}}(-\omega) - \theta_{\mathcal{E}}(-\omega)\right] \mathrm{d}\omega \tag{32}$$

distribution for modeling a great variety of LOS channels. On the other hand, the $\eta-\mu$ distribution accurately models small-scale fading for various NLOS conditions. Assuming that the entries of $\mathbf{H}_{\mathcal{AB}}$ and $\mathbf{H}_{\mathcal{AE}}$ are independent but non-identically distributed (i.n.i.d) $\kappa-\mu$ and $\eta-\mu$ random variables, respectively, the CHFs of $\gamma_{\mathcal{B}}$ and $\gamma_{\mathcal{E}}$ are given as [33]

$$\phi_{\gamma_{\mathcal{B}}}(\omega)=\prod_{i=1}^{N_{\mathcal{B}}}\left\{\left[\frac{\mu_{\mathcal{B},i}(1+\kappa_{\mathcal{B},i})}{(1+\kappa_{\mathcal{B},i})\,\mu_{\mathcal{B},i}-\imath\,\overline{\gamma}_{\mathcal{B},i}}\right]^{\mu_{\mathcal{B},i}}\times\exp\left[\frac{\imath\,\mu_{\mathcal{B},i}\,\kappa_{\mathcal{B},i}\,\omega\,\overline{\gamma}_{\mathcal{B},i}}{(1+\kappa_{\mathcal{B},i})\,\mu_{\mathcal{B},i}-\imath\,\omega\,\overline{\gamma}_{\mathcal{B},i}}\right]\right\} \tag{34a}$$

and

$$\phi_{\gamma_{\mathcal{E}}}(\omega)=\prod_{j=1}^{N_{\mathcal{E}}}\left\{\frac{1}{\left[1-\frac{\imath\,\omega\,\overline{\gamma}_{\mathcal{E},j}}{2\,\mu_{\mathcal{E},j}\,(h_{\mathcal{E},j}-H_{\mathcal{E},j})}\right]^{\mu_{\mathcal{E},j}}}\times\frac{1}{\left[1-\frac{\imath\,\omega\,\overline{\gamma}_{\mathcal{E},j}}{2\,\mu_{\mathcal{E},j}\,(h_{\mathcal{E},j}+H_{\mathcal{E},j})}\right]^{\mu_{\mathcal{E},j}}}\right\} \tag{34b}$$

respectively, where $\mu_{\mathcal{B},i}$ and $\mu_{\mathcal{E},i}$ are related to the fading severity, $h_{\mathcal{E},j}=(2+\eta_{\mathcal{E},j}^{-1}+\eta_{\mathcal{E},j})/4$, $H=(\eta_{\mathcal{E},j}^{-1}-\eta_{\mathcal{E},j})/4$ with $0<\eta_{\mathcal{E},j}<\infty$, $\kappa_{\mathcal{B},i}>0$ designates the ratio between the total power of the dominant propagation components and that of the scattered waves.

Assuming active eavesdropping, the average secrecy capacity of the considered system can be evaluated numerically by employing Proposition 1, with $\mathcal{M}_{\gamma_{\mathcal{B}}}(s)=\phi_{\gamma_{\mathcal{B}}}(\imath s)$ and $\mathcal{M}_{\gamma_{\mathcal{E}}}(s)=\phi_{\gamma_{\mathcal{E}}}(\imath s)$.

Assuming passive eavesdropping, by following a similar line of arguments as in the proof of (28), i.e. by substituting (34) into (17) and employing (A-1) and (A-2), an integral representation for the secrecy outage probability of the considered SIMO wiretap channel can be deduced, after some straightforward manipulations, as in (35), shown at the bottom of the page, where

$$\begin{aligned}\Theta_{\mathcal{B},\mathcal{E}}(\omega)=&\sum_{j=1}^{N_{\mathcal{E}}}\left\{\mu_{\mathcal{E},j}\,\arctan\left[\frac{\omega\,T\,\overline{\gamma}_{\mathcal{E},j}}{2\,\mu_{\mathcal{E},j}\,(h_{\mathcal{E},j}-H_{\mathcal{E},j})}\right]+\mu_{\mathcal{E},j}\,\arctan\left[\frac{\omega\,T\,\overline{\gamma}_{\mathcal{E},j}}{\mu_{\mathcal{E},j}\,(h_{\mathcal{E},j}+H_{\mathcal{E},j})}\right]\right\}\\&-\sum_{i=1}^{N_{\mathcal{B}}}\left\{\mu_{\mathcal{B},i}\,\arctan\left[\frac{\omega\overline{\gamma}_{\mathcal{B},i}}{\mu_{\mathcal{B},i}\,(1+\kappa_{\mathcal{B},i})}\right]+\frac{\omega\,(1+\kappa_{\mathcal{B},i})\,\mu_{\mathcal{B},i}^2\,\kappa_{\mathcal{B},i}\,\overline{\gamma}_{\mathcal{B},i}}{(1+\kappa_{\mathcal{B},i})^2\,\mu_{\mathcal{B},i}^2+\omega^2\,\overline{\gamma}_{\mathcal{B},i}^2}\right\},\end{aligned} \tag{36}$$

$U=2^{\mathcal{R}_S}-1$ and $T=2^{\mathcal{R}_S}$. To the best of our knowledge, the result in (35) is new.

Next, an asymptotic expression for P_{out} will be deduced. The MGF of $\gamma_{\mathcal{B}}$ can be expressed as

$$\mathcal{M}_{\gamma_{\mathcal{B}}}(s)=\prod_{i=1}^{N_{\mathcal{B}}}\left\{\left[\frac{\mu_{\mathcal{B},i}(1+\kappa_{\mathcal{B},i})}{(1+\kappa_{\mathcal{B},i})\,\mu_{\mathcal{B},i}+s\,\overline{\gamma}_{\mathcal{B},i}}\right]^{\mu_{\mathcal{B},i}}\times\exp\left[\frac{-s\mu_{\mathcal{B},i}\,\kappa_{\mathcal{B},i}\,\overline{\gamma}_{\mathcal{B},i}}{(1+\kappa_{\mathcal{B},i})\,\mu_{\mathcal{B},i}+s\overline{\gamma}_{\mathcal{B},i}}\right]\right\}. \tag{37}$$

For $s\to\infty$, it can be observed that the product of exponentials in (37) can be approximated as $\exp(-\sum_{i=1}^{N_{\mathcal{B}}}\mu_{\mathcal{B},i}\kappa_{\mathcal{B},i})$ whereas the product of the remaining terms as $\prod_{i=1}^{N_{\mathcal{B}}}[\mu_{\mathcal{B},i}(1+\kappa_{\mathcal{B},i})/\overline{\gamma}_{\mathcal{B},i}]^{\mu_{\mathcal{B},i}}$. Thus, $\mathcal{M}_{\gamma_{\mathcal{B}}}(s)$ can be expressed in the form $\mathcal{M}_{\gamma_{\mathcal{B}}}(s)\approx Cs^{-d}$, with $d=\sum_{i=1}^{N_{\mathcal{B}}}\mu_{\mathcal{B},i}$ and

$$C=\exp\left(-\sum_{i=1}^{N_{\mathcal{B}}}\mu_{\mathcal{B},i}\kappa_{\mathcal{B},i}\right)\prod_{i=1}^{N_{\mathcal{B}}}\left[\frac{\mu_{\mathcal{B},i}(1+\kappa_{\mathcal{B},i})}{\overline{\gamma}_{\mathcal{B},i}}\right]^{\mu_{\mathcal{B},i}}. \tag{38}$$

As it is evident, the secrecy diversity gain depends on both the number of antennas $N_{\mathcal{B}}$ as well as the fading parameters $\mu_{\mathcal{B},i}$. Finally, an asymptotic expression for P_{out} assuming high values of $\overline{\gamma}_{\mathcal{B}}$ can be readily deduced using Proposition 3.

B. SIMO Wiretap Channels With GSC

According to this scenario, both the main and the eavesdroppers channels are assumed to undergo quasi-static Rayleigh fading, while $N_{\mathcal{A}}=1$. In the main channel, Bob combines the $L_{\mathcal{B}}$ strongest receive antennas with $1\le L_{\mathcal{B}}\le N_{\mathcal{B}}$. In the eavesdroppers channel, Eve combines the $L_{\mathcal{E}}$ ($1\le L_{\mathcal{E}}\le N_{\mathcal{E}}$) strongest receive channels. Let $|h_{\ell_B,\mathcal{B}}|^2$, $|h_{\ell_E,\mathcal{E}}|^2$ denote the channel power gain from the single transmit to the ℓth receive antenna at Bob and Eve, respectively, with $\mathbb{E}\langle|h_{\ell_B,\mathcal{B}}|^2\rangle=\Omega_{\mathcal{B}}$, $\forall\ell_{\mathcal{B}}=1,2,\ldots,N_{\mathcal{B}}$, and $\mathbb{E}\langle|h_{\ell_{\mathcal{E}},\mathcal{E}}|^2\rangle=\Omega_{\mathcal{E}}$, $\forall\ell_{\mathcal{E}}=1,2,\ldots,N_{\mathcal{E}}$.

Since both Bob end Eve employ GSC, channel coefficients $|h_{\ell_{\mathcal{B}},\mathcal{B}}|^2$ and $|h_{\ell_E,\mathcal{E}}|^2$ are arranged in descending order as $|h_{(1),\mathcal{B}}|^2\ge|h_{(2),\mathcal{B}}|^2\ge\cdots\ge|h_{(N_{\mathcal{B}}),\mathcal{B}}|^2$ and $|h_{(1),\mathcal{E}}|^2\ge|h_{(2),\mathcal{E}}|^2\ge\cdots\ge|h_{(N_{\mathcal{E}}),\mathcal{E}}|^2$, respectively.

The instantaneous received SNR in the main and the eavesdropper channels can be expressed as

$$\gamma_{\mathcal{B}}=\sum_{\ell_{\mathcal{B}}=1}^{L_{\mathcal{B}}}|h_{(\ell_{\mathcal{B}}),\mathcal{B}}|^2\,. \tag{39a}$$

$$P_{\text{out}}^{\text{OSTBC, mixed}}=\frac{1}{2}+\frac{1}{\pi}\int_0^\infty\frac{\sin\left[\Theta_{\mathcal{B},\mathcal{E}}(\omega)+U\omega\right]}{\omega\prod_{i=1}^{N_{\mathcal{E}}}\left[\left(1+\frac{\omega^2\,T^2\overline{\gamma}_{\mathcal{E},i}^2}{4\mu_{\mathcal{E},i}^2(h_{\mathcal{E},i}-H_{\mathcal{E},i})^2}\right)^{\mu_{\mathcal{E},i}/2}\left(1+\frac{\omega^2\,T^2\overline{\gamma}_{\mathcal{E},i}^2}{4\mu_{\mathcal{E},i}^2(h_{\mathcal{E},i}+H_{\mathcal{E},i})^2}\right)^{\mu_{\mathcal{E},i}/2}\right]\prod_{j=1}^{N_{\mathcal{B}}}\left(1+\frac{\omega^2\overline{\gamma}_{\mathcal{B},j}^2}{\mu_{\mathcal{B},j}^2(1+\kappa_{\mathcal{B},j})^2}\right)^{\mu_{\mathcal{B},j}/2}}\times\exp\left[-\sum_{j=1}^{N_{\mathcal{B}}}\frac{\omega^2\mu_{\mathcal{B},j}\kappa_{\mathcal{B},j}\overline{\gamma}_{\mathcal{B},j}^2}{(1+\kappa_{\mathcal{B},j})^2\mu_{\mathcal{B},j}^2+\omega^2\overline{\gamma}_{\mathcal{B},j}^2}\right]\mathrm{d}\omega \tag{35}$$

and

$$\gamma_{\mathcal{E}} = \sum_{\ell_{\mathcal{E}}=1}^{L_{\mathcal{B}}} |h_{(\ell_{\mathcal{E}}),\mathcal{E}}|^2 . \tag{39b}$$

respectively. The characteristic functions of $\gamma_{\mathcal{B}}$ and $\gamma_{\mathcal{E}}$ can be expressed as [34, eq. (B.3)]

$$\phi_{\gamma_{\mathcal{B}}}(\omega) = \frac{1}{(1-\imath\,\omega\,\Omega_{\mathcal{B}})^{L_{\mathcal{B}}-1}} \prod_{r_{\mathcal{B}}=L_{\mathcal{B}}}^{N_{\mathcal{B}}} \frac{1}{(1-\imath\,\omega\,\Omega_{\mathcal{B}} L_{\mathcal{B}}/r_{\mathcal{B}})} \tag{40a}$$

and

$$\phi_{\gamma_{\mathcal{E}}}(\omega) = \frac{1}{(1-\imath\,\omega\,\Omega_{\mathcal{E}})^{L_{\mathcal{E}}-1}} \prod_{r_{\mathcal{E}}=L_{\mathcal{E}}}^{N_{\mathcal{E}}} \frac{1}{(1-\imath\,\omega\,\Omega_{\mathcal{E}} L_{\mathcal{E}}/r_{\mathcal{E}})} , \tag{40b}$$

respectively.

Assuming active eavesdropping, the average secrecy capacity of the considered system can be evaluated numerically by employing Proposition 1, with $\mathcal{M}_{\gamma_{\mathcal{B}}}(s) = \phi_{\gamma_{\mathcal{B}}}(\imath s)$ and $\mathcal{M}_{\gamma_{\mathcal{E}}}(s) = \phi_{\gamma_{\mathcal{E}}}(\imath s)$.

Assuming passive eavesdropping, by following a similar line of arguments as in the proof of (28), i.e. by substituting (40) into (17) and employing (A-1) and (A-2), an integral representation for the secrecy outage probability of the considered SIMO wiretap channel can be deduced, after some straightforward manipulations, as in (41), shown at the bottom of the page, where $U = 2^{\mathcal{R}_S} - 1$, $T = 2^U$,

$$\Theta_{\mathcal{B}}(\omega) = 2\arctan\left[\frac{\sin\left(\sum_{i=L_{\mathcal{B}}}^{N_{\mathcal{B}}} \arctan(\Omega_{\mathcal{B}}\,\omega L_{\mathcal{B}}/i)\right)}{1+\cos\left(\sum_{i=L_{\mathcal{B}}}^{N_{\mathcal{B}}} \arctan(\Omega_{\mathcal{B}}\,\omega L_{\mathcal{B}}/i)\right)}\right] + 2(L_{\mathcal{B}}-1)\arctan\left[\frac{\sin\left(\arctan(\Omega_{\mathcal{B}}\,\omega)\right)}{1+\cos\left(\arctan(\Omega_{\mathcal{B}}\,\omega)\right)}\right] \tag{42a}$$

and

$$\Theta_{\mathcal{E}}(\omega) = 2\arctan\left[\frac{\sin\left(\sum_{i=L_{\mathcal{E}}}^{N_{\mathcal{E}}} \arctan(\Omega_{\mathcal{E}}\,\omega L_{\mathcal{E}}/i)\right)}{1+\cos\left(\sum_{i=L_{\mathcal{E}}}^{N_{\mathcal{E}}} \arctan(\Omega_{\mathcal{E}}\,\omega L_{\mathcal{E}}/i)\right)}\right] + 2(L_{\mathcal{E}}-1)\arctan\left[\frac{\sin\left(\arctan(\Omega_{\mathcal{E}}\,\omega)\right)}{1+\cos\left(\arctan(\Omega_{\mathcal{E}}\,\omega)\right)}\right] . \tag{42b}$$

By employing the proposed CHF-based approach, closed-form expressions for the secrecy outage probability can be deduced in a similar fashion as in the OSTBC MIMO wiretap channel as

$$P_{\text{out}}^{\text{GSC}} = 1 + \sum_{r=1}^{L_{\mathcal{B}}} \frac{U^{r-1} a_r}{\Gamma(r)\,\imath^{r-1}} \exp\left(-\frac{U}{\Omega_{\mathcal{B}}}\right) + \sum_{r=L_{\mathcal{B}}+1}^{N_{\mathcal{B}}} b_{r-L_{\mathcal{B}}} \exp\left(\frac{-U\,r}{\Omega_{\mathcal{B}}\,L_{\mathcal{B}}}\right) , \tag{43}$$

where

$$a_r = \frac{\imath^{N_{\mathcal{B}}-N_{\mathcal{E}}} (T\Omega_{\mathcal{E}})^{1-L_{\mathcal{E}}} \Omega_{\mathcal{B}}^{1-N_{\mathcal{B}}}}{(L_{\mathcal{B}}-r)!} \frac{\mathrm{d}^{L_{\mathcal{B}}-r}}{\mathrm{d}\omega^{L_{\mathcal{B}}-r}} \left[\frac{1}{\omega}(\omega+\imath/\Omega_{\mathcal{B}}) \times (\omega-\imath\,T^{-1}/\Omega_{\mathcal{E}})^{1-L_{\mathcal{E}}} \prod_{r_1=L_{\mathcal{B}}}^{N_{\mathcal{B}}} \frac{r_1/(\Omega_{\mathcal{B}}\,L_{\mathcal{B}})}{\omega + r_1\,\imath/(\Omega_{\mathcal{B}} L_{\mathcal{B}})} \times \prod_{r_2=L_{\mathcal{E}}}^{N_{\mathcal{E}}} \frac{r_2/(T\,\Omega_{\mathcal{E}} L_{\mathcal{E}})}{\omega - r_2\,\imath/(\Omega_{\mathcal{E}}\,L_{\mathcal{E}} T)}\right]\Bigg|_{\omega=-\frac{\imath}{\Omega_{\mathcal{B}}}} \tag{44a}$$

and

$$b_r = \imath^{N_{\mathcal{B}}-N_{\mathcal{E}}} (T\,\Omega_{\mathcal{E}})^{1-L_{\mathcal{E}}} \Omega_{\mathcal{B}}^{1-N_{\mathcal{B}}} \left[\frac{1}{\omega}(\omega+\imath/\Omega_{\mathcal{B}})^{1-L_{\mathcal{B}}} \times (\omega-\imath\,T^{-1}/\Omega_{\mathcal{E}})^{1-L_{\mathcal{E}}} \prod_{r_{\mathcal{B}}=L_{\mathcal{B}}}^{N_{\mathcal{B}}} \frac{r_{\mathcal{B}}/(\Omega_{\mathcal{B}}\,L_{\mathcal{B}})}{\omega + r_{\mathcal{B}}\,\imath/(\Omega_{\mathcal{B}} L_{\mathcal{B}})} \times \left(\omega + \imath\frac{r+L_{\mathcal{B}}}{\Omega_{\mathcal{B}} N_{\mathcal{B}}}\right) \prod_{r_{\mathcal{E}}=L_{\mathcal{E}}}^{N_{\mathcal{E}}} \frac{r_{\mathcal{E}}/(T\Omega_{\mathcal{E}} L_{\mathcal{E}})}{\omega - r_{\mathcal{E}}\,\imath/(\Omega_{\mathcal{E}}\,L_{\mathcal{E}}\,T)}\right]\Bigg|_{\omega=-\frac{\imath\,(r+L_{\mathcal{B}})}{\Omega_{\mathcal{B}}\,L_{\mathcal{B}}}} . \tag{44b}$$

$$P_{\text{out}}^{\text{GSC}} = \frac{1}{2} + \frac{1}{\pi}\int_0^{\infty} \frac{1}{\omega} \left(1+\omega^2\Omega_{\mathcal{B}}^2\right)^{-\frac{L_{\mathcal{B}}-1}{2}} \left(1+\omega^2\,T^2\,\Omega_{\mathcal{E}}^2\right)^{-\frac{L_{\mathcal{E}}-1}{2}} \prod_{r_{\mathcal{B}}=L_{\mathcal{B}}}^{N_{\mathcal{B}}} \left(1+\omega^2\,\Omega_{\mathcal{B}}^2\,\frac{L_{\mathcal{B}}^2}{r_{\mathcal{B}}^2}\right)^{-1/2} \times \prod_{r_{\mathcal{E}}=L_{\mathcal{E}}}^{N_{\mathcal{E}}} \left(1+\omega^2\,T^2\,\Omega_{\mathcal{E}}^2\,\frac{L_{\mathcal{E}}^2}{r_{\mathcal{E}}^2}\right)^{-1/2} \sin\left[\Theta_{\mathcal{B}}(-\omega) - \Theta_{\mathcal{E}}(-T\,\omega) + U\,\omega\right] \mathrm{d}\omega \tag{41}$$

$$P_{\text{NZ}}^{\text{GSC}} = \frac{1}{2} - \frac{1}{\pi}\int_0^{\infty} \frac{1}{\omega} \left(1+\omega^2\Omega_{\mathcal{B}}^2\right)^{-\frac{L_{\mathcal{B}}-1}{2}} \left(1+\omega^2\,\Omega_{\mathcal{E}}^2\right)^{-\frac{L_{\mathcal{E}}-1}{2}} \left[\prod_{r_{\mathcal{B}}=L_{\mathcal{B}}}^{N_{\mathcal{B}}} \left(1+\omega^2\,\Omega_{\mathcal{B}}^2\,\frac{L_{\mathcal{B}}^2}{r_{\mathcal{B}}^2}\right)^{-1/2}\right] \times \left[\prod_{r_{\mathcal{E}}=L_{\mathcal{E}}}^{N_{\mathcal{E}}} \left(1+\omega^2\,\Omega_{\mathcal{E}}^2\,\frac{L_{\mathcal{E}}^2}{r_{\mathcal{E}}^2}\right)^{-1/2}\right] \sin\left[\Theta_{\mathcal{B}}(-\omega) - \Theta_{\mathcal{E}}(-\omega)\right] \mathrm{d}\omega \tag{45}$$

Note that relevant results for wiretap channels with antenna selection are available in [15]–[17].

An integral representation for probability of non-zero secrecy capacity of the considered SIMO wiretap channel can be deduced as in (45), shown at the bottom of the previous page.

Finally, an asymptotic expression for P_{out} will be deduced. The MGF of $\gamma_{\mathcal{B}}$ can be expressed as

$$\mathcal{M}_{\gamma_{\mathcal{B}}}(s) = \frac{1}{(1+s\,\Omega_{\mathcal{B}})^{L_{\mathcal{B}}-1}} \prod_{r_{\mathcal{B}}=L_{\mathcal{B}}}^{N_{\mathcal{B}}} \frac{1}{(1+s\,\Omega_{\mathcal{B}} L_{\mathcal{B}}/r_{\mathcal{B}})}. \quad (46)$$

For $s \to \infty$, it can be observed that $(1+s\,\Omega_{\mathcal{B}})^{L_{\mathcal{B}}-1} \approx (s\,\Omega_{\mathcal{B}})^{L_{\mathcal{B}}-1}$ and $(1+s\,\Omega_{\mathcal{B}} L_{\mathcal{B}}/r_{\mathcal{B}}) \approx s\,\Omega_{\mathcal{B}} L_{\mathcal{B}}/r_{\mathcal{B}}$. Thus, $\mathcal{M}_{\gamma_{\mathcal{B}}}(s)$ can be approximated as $\mathcal{M}_{\gamma_{\mathcal{B}}}(s) \approx C\,s^{-d}$ with $d = N_{\mathcal{B}}\,\mu_{\mathcal{B}}$ and $C = \Omega_{\mathcal{B}}^{-N_{\mathcal{B}}} \prod_{r_{\mathcal{B}}=L_{\mathcal{B}}}^{N_{\mathcal{B}}} \left[r_{\mathcal{B}}/L_{\mathcal{B}}\right]$. As it is evident, the secrecy diversity gain depends only on the number of antennas $N_{\mathcal{B}}$. An asymptotic expression for P_{out} assuming high values of $\overline{\gamma}_{\mathcal{B}}$ can be readily deduced using Proposition 3.

C. Correlated SIMO Wiretap Channels With MRC

According to this scenario, a SIMO wiretap channel model is considered where $N_{\mathcal{A}} = 1$. Let $\mathbf{r}_{\mathcal{B}}$ and $\mathbf{r}_{\mathcal{E}}$ be $N_{\mathcal{B}} \times 1$ and $N_{\mathcal{E}} \times 1$ complex Gaussian random vectors, denoting the complex channel gains from the single transmit antenna to the receive antennas at Bob and Eve, respectively. It is assumed that $\mathbf{r}_{\mathcal{B}}$ and $\mathbf{r}_{\mathcal{E}}$ have mean values $\boldsymbol{\eta}_{\mathcal{B}}$ and $\boldsymbol{\eta}_{\mathcal{E}}$, respectively, and covariance matrices $\mathbf{C}_{\mathcal{A}\mathcal{B}} = \mathbb{E}\langle(\mathbf{r}_{\mathcal{B}} - \boldsymbol{\eta}_{\mathcal{B}})\,(\mathbf{r}_{\mathcal{B}} - \boldsymbol{\eta}_{\mathcal{B}})^H\rangle$ and $\mathbf{C}_{\mathcal{A}\mathcal{E}} = \mathbb{E}\langle(\mathbf{r}_{\mathcal{E}} - \boldsymbol{\eta}_{\mathcal{E}})\,(\mathbf{r}_{\mathcal{E}} - \boldsymbol{\eta}_{\mathcal{E}})^H\rangle$, respectively.

In the main and the eavesdroppers channel, Bob and Eve combine the $N_{\mathcal{B}}$ and $N_{\mathcal{E}}$ receive antennas, respectively, using MRC. The instantaneous SNR in the main channel can be expressed as

$$\gamma_{\mathcal{B}} = \frac{\Omega_{\mathcal{B}}}{m_{\mathcal{B}}\,\left(\boldsymbol{\eta}_{\mathcal{B}}^H\,\boldsymbol{\eta}_{\mathcal{B}} + \text{Tr}\{\mathbf{C}_{\mathcal{A}\mathcal{B}}\}\right)}\,\mathbf{r}_{\mathcal{B}}^H\,\mathbf{r}_{\mathcal{B}} \quad (47a)$$

and in the eavesdropper's channel as

$$\gamma_{\mathcal{E}} = \frac{\Omega_{\mathcal{E}}}{m_{\mathcal{E}}\,\left(\boldsymbol{\eta}_{\mathcal{E}}^H\,\boldsymbol{\eta}_{\mathcal{E}} + \text{Tr}\{\mathbf{C}_{\mathcal{A}\mathcal{E}}\}\right)}\,\mathbf{r}_{\mathcal{E}}^H\,\mathbf{r}_{\mathcal{E}} \quad (47b)$$

The parameters $\Omega_{\mathcal{B}}$ and $\Omega_{\mathcal{E}}$ correspond to the average SNR at the output of the MRC receiver at Bob and Eve, respectively and the parameters $m_{\mathcal{B}}$ and $m_{\mathcal{E}}$ denote the diversity order of the signal recovered by each branch at the legitimate receiver and the eavesdropper, respectively. Based on (47), their CHFs are given as [35, eq. (18)]

$$\phi_{\gamma_{\mathcal{B}}}(\omega) = \frac{\exp\left[\imath\,\omega\,\Omega_{\mathcal{B}}\,\boldsymbol{\lambda}_{\mathcal{B}}^H\left(\mathbf{I}_{N_{\mathcal{B}}^2} - \imath\,\omega\,\frac{\Omega_{\mathcal{B}}}{m_{\mathcal{B}}}\,\mathbf{Q}_{\mathcal{A}\mathcal{B}}\right)^{-1}\boldsymbol{\lambda}_{\mathcal{B}}\right]}{\left[\det\left(\mathbf{I}_{N_{\mathcal{B}}^2} - \imath\,\omega\,\frac{\Omega_{\mathcal{B}}}{m_{\mathcal{B}}}\,\mathbf{Q}_{\mathcal{A}\mathcal{B}}\right)\right]^{m_{\mathcal{B}}}} \quad (48a)$$

and

$$\phi_{\gamma_{\mathcal{E}}}(\omega) = \frac{\exp\left[\imath\,\omega\,\Omega_{\mathcal{E}}\,\boldsymbol{\lambda}_{\mathcal{E}}^H\left(\mathbf{I}_{N_{\mathcal{E}}^2} - \imath\,\omega\,\frac{\Omega_{\mathcal{E}}}{m_{\mathcal{E}}}\,\mathbf{Q}_{\mathcal{A}\mathcal{E}}\right)^{-1}\boldsymbol{\lambda}_{\mathcal{E}}\right]}{\left[\det\left(\mathbf{I}_{N_{\mathcal{E}}^2} - \imath\,\omega\,\frac{\Omega_{\mathcal{E}}}{m_{\mathcal{E}}}\,\mathbf{Q}_{\mathcal{A}\mathcal{E}}\right)\right]^{m_{\mathcal{E}}}} \quad (48b)$$

respectively, where $\mathbf{Q}_{\mathcal{A}\mathcal{B}}$ and $\mathbf{Q}_{\mathcal{A}\mathcal{E}}$ are the normalized covariance matrices defined as $\mathbf{Q}_{\mathcal{A}\mathcal{B}} = \mathbf{C}_{\mathcal{A}\mathcal{B}}/(\boldsymbol{\eta}_{\mathcal{B}}^H\,\boldsymbol{\eta}_{\mathcal{B}} + \text{Tr}(\mathbf{C}_{\mathcal{A}\mathcal{B}}))$, $\mathbf{Q}_{\mathcal{A}\mathcal{E}} = \mathbf{C}_{\mathcal{A}\mathcal{E}}/(\boldsymbol{\eta}_{\mathcal{E}}^H\,\boldsymbol{\eta}_{\mathcal{E}} + \text{Tr}(\mathbf{C}_{\mathcal{A}\mathcal{E}}))$ and $\boldsymbol{\lambda}_{\mathcal{B}}, \boldsymbol{\lambda}_{\mathcal{E}}$ are the normalized mean vectors defined as $\boldsymbol{\lambda}_{\mathcal{B}} = \boldsymbol{\eta}_{\mathcal{B}}/\sqrt{\boldsymbol{\eta}_{\mathcal{B}}^H\,\boldsymbol{\eta}_{\mathcal{B}} + \text{Tr}(\mathbf{C}_{\mathcal{A}\mathcal{B}})}$ and $\boldsymbol{\lambda}_{\mathcal{E}} = \boldsymbol{\eta}_{\mathcal{E}}/\sqrt{\boldsymbol{\eta}_{\mathcal{E}}^H\,\boldsymbol{\eta}_{\mathcal{E}} + \text{Tr}(\mathbf{C}_{\mathcal{A}\mathcal{E}})}$, respectively. Given (48), generic integral representations for P_{out} and P_{NZ} can be readily deduced using (17) and (18). In the special case of $\boldsymbol{\eta}_{\mathcal{E}} = 0$ and $m_{\mathcal{B}} = m_{\mathcal{E}} = 1$, an alternative methodology for the performance evaluation of the wiretap channel has been proposed in [16].

In the special case of correlated Nakagami-m fading, i.e. when $\boldsymbol{\eta}_{\mathcal{E}} = \boldsymbol{\eta}_{\mathcal{B}} = 0$, the CHFs of $\gamma_{\mathcal{B}}$ and $\gamma_{\mathcal{E}}$ can be expressed as

$$\phi_{\gamma_{\mathcal{B}}}(\omega) = \left[\prod_{i=1}^{N_{\mathcal{B}}}\left(1 - \imath\,\omega\,\mu_{i,\mathcal{A}\mathcal{B}}\right)\right]^{-m_{\mathcal{B}}} \quad (49a)$$

and

$$\phi_{\gamma_{\mathcal{E}}}(\omega) = \left[\prod_{i=1}^{N_{\mathcal{E}}}\left(1 - \imath\,\omega\,\mu_{i,\mathcal{A}\mathcal{E}}\right)\right]^{-m_{\mathcal{E}}}, \quad (49b)$$

respectively, where $\mu_{i,\mathcal{A}\mathcal{B}}$ and $\mu_{i,\mathcal{A}\mathcal{E}}$ are the eigenvalues of $\frac{\Omega_{\mathcal{B}}}{m_{\mathcal{B}}}\,\mathbf{Q}_{\mathcal{A}\mathcal{B}}$ and $\frac{\Omega_{\mathcal{E}}}{m_{\mathcal{E}}}\,\mathbf{Q}_{\mathcal{A}\mathcal{E}}$, respectively.

Assuming active eavesdropping, the average secrecy capacity of the considered system can be evaluated numerically by employing Proposition 1, with $\mathcal{M}_{\gamma_{\mathcal{B}}}(s) = \phi_{\gamma_{\mathcal{B}}}(\imath s)$ and $\mathcal{M}_{\gamma_{\mathcal{E}}}(s) = \phi_{\gamma_{\mathcal{E}}}(\imath s)$. Assuming passive eavesdropping, by following a similar line of arguments as that in Section IV-A1, an integral representation for the secrecy outage probability of the considered SIMO wiretap channel can be deduced as in (50), shown at the bottom of the page, where $U = 2^{\mathcal{R}_S} - 1$, $T = 2^U$,

$$\Phi_{\mathcal{B}}(\omega) = m_{\mathcal{B}}\,\arctan\left[\frac{\sin\left(\sum_{i=1}^{N_{\mathcal{B}}}\arctan(\omega\,\mu_{i,\mathcal{A}\mathcal{B}})\right)}{1 + \cos\left(\sum_{i=1}^{N_{\mathcal{B}}}\arctan(\omega\,\mu_{i,\mathcal{A}\mathcal{B}})\right)}\right] \quad (51a)$$

$$P_{\text{out}}^{\text{SIMO}} = \frac{1}{2} + \frac{1}{\pi}\int_0^{\infty}\frac{1}{\omega}\left[\prod_{i=1}^{N_{\mathcal{B}}}(1+\omega^2\,\mu_{i,\mathcal{A}\mathcal{B}}^2)^{-m_{\mathcal{B}}/2}\right]\left[\prod_{i=1}^{N_{\mathcal{E}}}(1+\omega^2\,T^2\,\mu_{i,\mathcal{A}\mathcal{E}}^2)^{-m_{\mathcal{E}}/2}\right]\sin\left[\Phi_{\mathcal{B}}(-\omega) - \Phi_{\mathcal{E}}(-T\,\omega) + U\,\omega\right]\,\text{d}\omega \quad (50)$$

and

$$\Phi_{\mathcal{E}}(\omega) = m_{\mathcal{E}} \arctan\left[\frac{\sin\left(\sum_{i=1}^{N_{\mathcal{E}}} \arctan(\omega\,\mu_{i,\mathcal{AE}})\right)}{1+\cos\left(\sum_{i=1}^{N_{\mathcal{E}}} \arctan(\omega\,\mu_{i,\mathcal{AE}})\right)}\right]. \tag{51b}$$

Finally, using (18) along with (49) the probability of non-zero secrecy capacity of the considered SIMO wiretap channel can be deduced as in (52), shown at the bottom of the page.

Next, an asymptotic expression for P_{out} will be deduced. The MGF of $\gamma_{\mathcal{B}}$ can be expressed as

$$\mathcal{M}_{\gamma_{\mathcal{B}}}(s) = \frac{\exp\left[-s\,\Omega_{\mathcal{B}}\,\boldsymbol{\lambda}_{\mathcal{B}}^{H}\left(\mathbf{I}_{N_{\mathcal{B}}^2} + s\,\frac{\Omega_{\mathcal{B}}}{m_{\mathcal{B}}}\,\mathbf{Q}_{\mathcal{AB}}\right)^{-1}\boldsymbol{\lambda}_{\mathcal{B}}\right]}{\left[\det\left(\mathbf{I}_{N_{\mathcal{B}}^2} + s\,\frac{\Omega_{\mathcal{B}}}{m_{\mathcal{B}}}\,\mathbf{Q}_{\mathcal{AB}}\right)\right]^{m_{\mathcal{B}}}}. \tag{53}$$

For $s \to \infty$, it can be observed that $\mathbf{I}_{N_{\mathcal{B}}^2} + s\,(\Omega_{\mathcal{B}}/m_{\mathcal{B}})\,\mathbf{Q}_{\mathcal{AB}}$ can be approximated as $s\,(\Omega_{\mathcal{B}}/m_{\mathcal{B}})\,\mathbf{Q}_{\mathcal{AB}}$. Therefore, the denominator in (53) can be written as $\left[\det\left(s\,\frac{\Omega_{\mathcal{B}}}{m_{\mathcal{B}}}\,\mathbf{Q}_{\mathcal{AB}}\right)\right]^{m_{\mathcal{B}}} = (s\,\Omega_{\mathcal{B}}/m_{\mathcal{B}})^{N_{\mathcal{B}}\,m_{\mathcal{B}}}\,[\det(\mathbf{Q}_{\mathcal{AB}})]^{m_{\mathcal{B}}}$ and the numerator as $\exp\left(-m_{\mathcal{B}}\,\boldsymbol{\lambda}_{\mathcal{B}}^{H}\mathbf{Q}_{\mathcal{AB}}^{-1}\,\boldsymbol{\lambda}_{\mathcal{B}}\right)$. Thus, $\mathcal{M}_{\gamma_{\mathcal{B}}}(s)$ can be expressed in the compact form $\mathcal{M}_{\gamma_{\mathcal{B}}}(s) \approx C\,s^{-d}$, with $d = N_{\mathcal{B}}\,m_{\mathcal{B}}$ and

$$C = \left(\frac{m_{\mathcal{B}}}{\Omega_{\mathcal{B}}}\right)^{N_{\mathcal{B}}m_{\mathcal{B}}} \frac{\exp\left(-m_{\mathcal{B}}\boldsymbol{\lambda}_{\mathcal{B}}^{H}\mathbf{Q}_{\mathcal{AB}}^{-1}\boldsymbol{\lambda}_{\mathcal{B}}\right)}{[\det(\mathbf{Q}_{\mathcal{AB}})]^{m_{\mathcal{B}}}}. \tag{54}$$

As it is evident, the secrecy diversity gain depends on both the number of antennas $N_{\mathcal{B}}$ as well as the fading parameter $m_{\mathcal{B}}$. Finally, an asymptotic expression for P_{out} assuming high values of $\overline{\gamma}_{\mathcal{B}}$ can be readily deduced using Proposition 3.

V. Framework Validation

Using the analytical results derived in the preceding sections, some representative numerical results are provided herein to demonstrate the secrecy performance of the considered MIMO and SIMO wiretap channels. All results are substantiated by employing semi-analytical Monte-Carlo simulations. Note that in a semi-analytic framework, the knowledge of the system under analysis is exploited to reduce the computational load and complexity that full Monte Carlo simulations would require. In this way, the strengths of both analytical and Monte Carlo methods are effectively combined. Moreover, it is assumed that $N_J \in \{15, 30\}$ and $N_K \geq 100$ for sufficient numerical accuracy. For the evaluation of the secrecy outage probability, it is assumed that $\mathcal{R}_S = 2$ for all considered scenarios. Furthermore, all results are derived assuming $\overline{\gamma}_{\mathcal{E}} \in \{0, 5\}$dB.

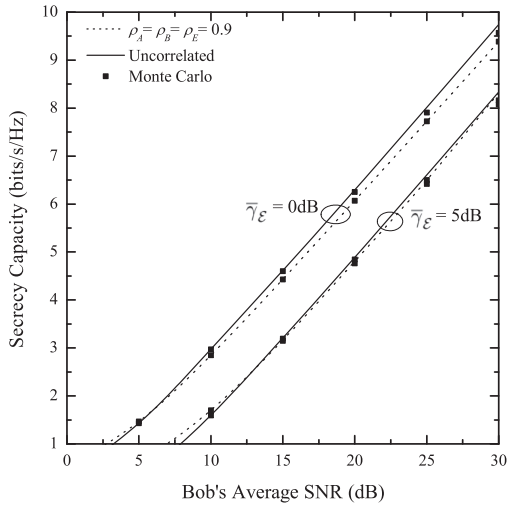

Fig. 1. Average Secrecy Capacity of OSTBC, assuming exponential correlation at both the transmitter and the receiver sides.

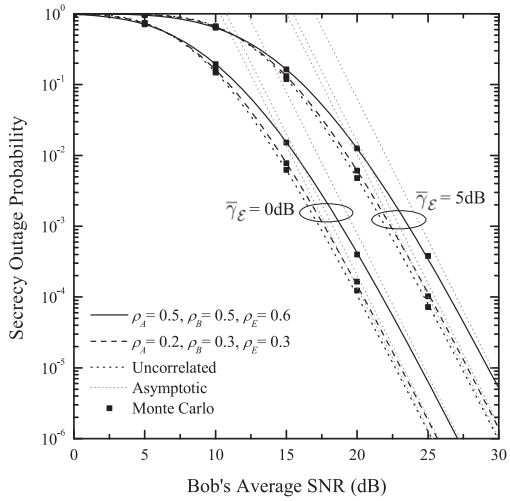

Fig. 2. Secrecy Outage Probability of OSTBC, assuming exponential correlation at both the transmitter and the receiver sides.

A. MIMO OSTBC Wiretap Channel in a Rayleigh Fading Environment

Figs. 1 and 2 depict the average secrecy capacity and the secrecy outage probability of the MIMO OSTBC wiretap channel, respectively, with $N_{\mathcal{A}} = 2$, $N_{\mathcal{B}} = 2$ and $N_{\mathcal{E}} = 2$. Throughout this analysis, the Kronecker correlation model is assumed for both the main and the eavesdropper's channels, where $\mathbf{R}_{\mathcal{AB}} = \mathbf{R}_{\mathcal{A}} \otimes \mathbf{R}_{\mathcal{B}}$, $\mathbf{R}_{\mathcal{AE}} = \mathbf{R}_{\mathcal{A}} \otimes \mathbf{R}_{\mathcal{E}}$ with $\mathbf{R}_{\mathcal{A}}$, $\mathbf{R}_{\mathcal{B}}$ and $\mathbf{R}_{\mathcal{E}}$ denoting the antenna correlation at Alice, Bob and Eve, respectively. An exponential correlation model is assumed, that is $\mathbf{R}_{\mathcal{A}} = \begin{pmatrix} 1 & \rho_A \\ \rho_A & 1 \end{pmatrix}$, $\mathbf{R}_{\mathcal{B}} = \begin{pmatrix} 1 & \rho_B \\ \rho_B & 1 \end{pmatrix}$ and $\mathbf{R}_{\mathcal{E}} =$

$$P_{\text{NZ}}^{\text{SIMO}} = \frac{1}{2} - \frac{1}{\pi}\int_0^{\infty} \frac{1}{\omega}\left[\prod_{i=1}^{N_{\mathcal{B}}}(1+\omega^2\,\mu_{i,\mathcal{AB}}^2)^{-m_{\mathcal{B}}/2}\right]\left[\prod_{i=1}^{N_{\mathcal{E}}}(1+\omega^2\,T^2\,\mu_{i,\mathcal{AE}}^2)^{-m_{\mathcal{E}}/2}\right]\sin\left[\Phi_{\mathcal{B}}(-\omega) - \Phi_{\mathcal{E}}(-\omega)\right]\,\mathrm{d}\omega \tag{52}$$

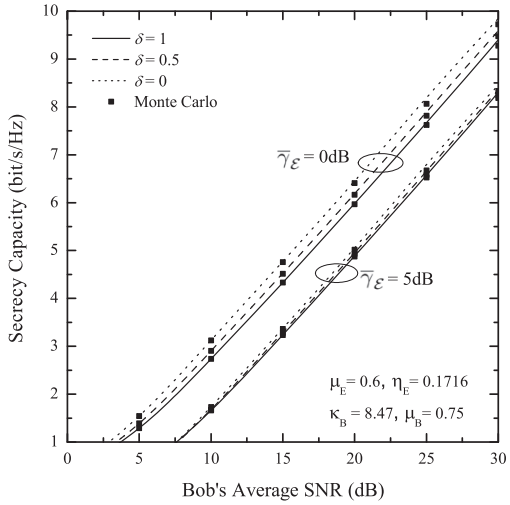

Fig. 3. Average Secrecy Capacity of OSTBC, assuming i.n.i.d κ-μ and η-μ fading conditions at the legitimate receiver and the eavesdropper channels, respectively, for $\mu_{\mathcal{E}} = 0.6$, $\eta_{\mathcal{E}} = 0.1716$, $\mu_{\mathcal{B}} = 0.75$, $\kappa_{\mathcal{B}} = 8.47$, and various values of δ.

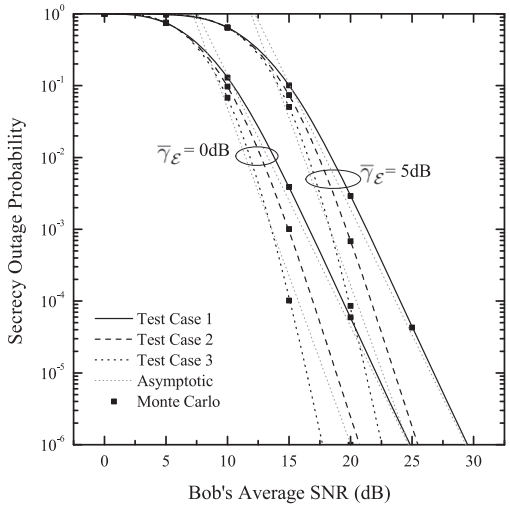

Fig. 4. Secrecy Outage Probability of OSTBC, assuming i.n.i.d κ-μ and η-μ fading conditions at the legitimate receiver and the eavesdropper channels, respectively, with $\delta = 0.1$, $\mu_{\mathcal{E}} = 0.6$, $\eta_{\mathcal{E}} = 0.1716$ for the following test cases: *Test Case 1:* $\mu_{\mathcal{B}} = 0.875$, $\kappa_{\mathcal{B}} = 1.5798$, *Test Case 2:* $\mu_{\mathcal{B}} = 1.1685$, $\kappa_{\mathcal{B}} = 2$, *Test Case 3:* $\mu_{\mathcal{B}} = 0.75$, $\kappa_{\mathcal{B}} = 8.47$,.

$\begin{pmatrix} 1 & \rho_E \\ \rho_E & 1 \end{pmatrix}$ and various values of ρ_A, ρ_B and ρ_E. The correlation matrix of such a model is described by and corresponds to the scenario of multichannel reception from equispaced diversity antennas, since the correlation between the pairs of combined signals decays as the spacing between the antennas increases [22]. In all cases, the comparison among Monte Carlo simulations, (5) (28) and (30) confirms the validity of the proposed analytical framework. Moreover, the asymptotic secrecy outage probability results correctly predict the secrecy diversity gain for high SNR values.

B. MIMO OSTBC Wiretap Channel in a Mixed Generalized Fading Environment

In this case, the eavesdropper channel is subject to $\eta - \mu$ fading with $\mu_{\mathcal{E},i} = \mu_{\mathcal{E}} = 0.6$ and $\eta_{\mathcal{E},i} = \eta_{\mathcal{E}} = 0.1716$, $\forall i = \{1, \ldots, N_{\mathcal{E}}\}$. Fading in the legitimate channel is modeled by the $\kappa - \mu$ distribution with fading parameters obtained from the following test cases: *Test Case 1:* $\mu_{\mathcal{B},j} = \mu_{\mathcal{B}} = 0.875$, $\kappa_{\mathcal{B},j} = \kappa_{\mathcal{B}} = 1.5798$, *Test Case 2:* $\mu_{\mathcal{B},j} = \mu_{\mathcal{B}} = 1.1685$, $\kappa_{\mathcal{B},j} = \kappa_{\mathcal{B}} = 2$, *Test Case 3:* $\mu_{\mathcal{B},j} = \mu_{\mathcal{B}} = 0.75$, $\kappa_{\mathcal{B},j} = \kappa_{\mathcal{B}} = 8.47$, $\forall j = \{1, \ldots, N_{\mathcal{B}}\}$. It is noted that the above mentioned values of fading parameters for both channels have been obtained by field measurements carried out in [23] for different propagation environments. An exponentially decayed power profile is assumed, i.e. $\overline{\gamma}_{\mathcal{B},j} = \overline{\gamma}_{\mathcal{B}} \exp[-\delta\,(j-1)]$ and $\overline{\gamma}_{\mathcal{E},i} = \overline{\gamma}_{\mathcal{E}} \exp[-\delta\,(i-1)]$ with δ being the decaying factor.

Fig. 3 depicts the secrecy outage probability for the considered wiretap channel assuming Test Case 3 and various values of δ. As it can be observed, analytical results and Monte-Carlo simulations are in excellent agreement. Figs. 4 depicts the secrecy outage probability for the considered wiretap channel and, again analytical results and Monte-Carlo simulations are practically indistinguishable to each other. Moreover, the asymptotic expressions for high SNR values correctly predict secrecy performance. However, it should be pointed out that for large values of $\kappa_{\mathcal{B}}$, i.e. when a strong LOS hop exists, a large coding gain can be achieved from this LOS component. This is evident from the presence of the factor $\exp(-\kappa_{\mathcal{B}}\mu_{\mathcal{B}})$ in C of (38). Thus, large SNR values are required so that the asymptotic behavior of the secrecy outage probability will show up. To this end, no asymptotic curves for Test Case 3 are presented.

C. SIMO Wiretap Channel With GSC in a Rayleigh Fading Environment

Figs. 5 and 6 depict the average secrecy capacity and the secrecy outage probability of the SIMO wiretap channel, with GSC at both the legitimate receiver and the eavesdropper, for various configurations of $N_{\mathcal{A}}$, $N_{\mathcal{B}}$ and $N_{\mathcal{E}}$. Once again, the results obtained by employing the proposed analytical framework agree well with the corresponding ones obtained with Monte Carlo simulations.

D. SIMO Wiretap Channel in an Arbitrary Correlated Generalized Fading Environment

Figs. 7 and 8 depict the average secrecy capacity and the secrecy outage probability of SIMO 1×3 wiretap channels in arbitrarily correlated generalized fading environments, respectively, assuming $m_{\mathcal{E}} = 2$, various values of $m_{\mathcal{B}}$, $\boldsymbol{\eta}_{\mathcal{B}} = \boldsymbol{\eta}_{\mathcal{E}} = \left[0.25\, e^{\imath\,\pi/4}\; 0.5\, e^{\imath\,\pi/6}\; e^{\imath\,\pi/8}\right]^T$ and covariance matrices given by [35]

$$\mathbf{C}_{\mathcal{AB}} = \mathbf{C}_{\mathcal{AE}} = \begin{pmatrix} 1 & 0.5\, e^{\frac{\imath\pi}{2}} & 0.25\, e^{\frac{\imath\pi}{4}} \\ 0.5\, e^{-\frac{\imath\pi}{2}} & 2 & 0.125\, e^{\frac{\imath\pi}{8}} \\ 0.25\, e^{-\frac{\imath\pi}{4}} & 0.125\, e^{-\frac{\imath\pi}{8}} & 3 \end{pmatrix}. \tag{55}$$

Again, analytical and simulation results are in very good agreement for all considered test cases. Finally, Fig. 9 portrays the probability of non-zero secrecy capacity of the

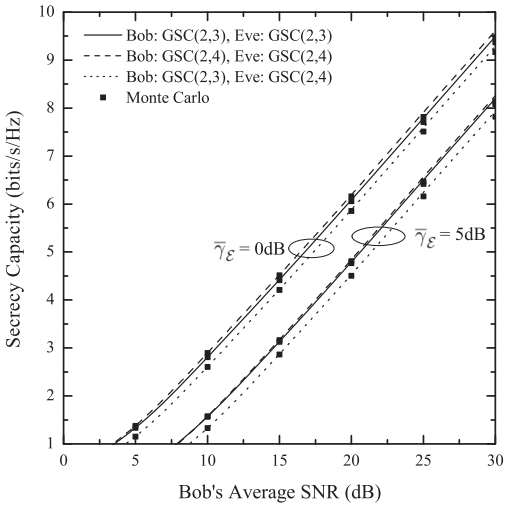

Fig. 5. Average Secrecy Capacity of SIMO Rayleigh wiretap channels with GSC at the legitimate receiver and the eavesdropper.

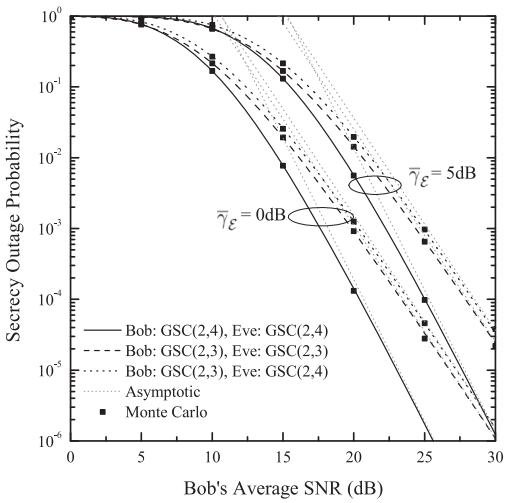

Fig. 6. Secrecy Outage Probability of SIMO Rayleigh wiretap channels with GSC at the legitimate receiver and the eavesdropper.

Nakagami-m SIMO wiretap channel, with MRC diversity reception at both the legitimate receiver and the eavesdropper, for various values of $m_{\mathcal{B}}$, assuming $m_{\mathcal{E}} = 1.5$, $N_{\mathcal{B}} = N_{\mathcal{E}} = 4$. An exponentially decayed power profile is assumed, i.e. $\Omega_{\ell_{\mathcal{B}},\mathcal{B}} = \overline{\gamma}_{\mathcal{B}} \exp[-\delta(\ell_{\mathcal{B}} - 1)]$ and $\Omega_{\ell_{\mathcal{E}},\mathcal{E}} = \overline{\gamma}_{\mathcal{E}} \exp[-\delta(\ell_{\mathcal{E}} - 1)]$ with δ being the decaying factor, assumed to be equal to 0.5. The channel gains are characterized by the envelope correlation matrices $\mathbf{R}_{\mathcal{AB}}$ and $\mathbf{R}_{\mathcal{AE}}$ whose elements can be obtained in terms of the elements of $\mathbf{C}_{\mathcal{AB}}$ and $\mathbf{C}_{\mathcal{AE}}$ by using the methodology presented in [36]. The envelope correlation matrix for both channels is assumed to be [36, eq. (55)]

$$\mathbf{R}_{\mathcal{AB}} = \mathbf{R}_{\mathcal{AE}} = \begin{pmatrix} 1 & 0.795 & 0.604 & 0.372 \\ 0.795 & 1 & 0.795 & 0.604 \\ 0.604 & 0.795 & 1 & 0.795 \\ 0.372 & 0.604 & 0.795 & 1 \end{pmatrix}. \quad (56)$$

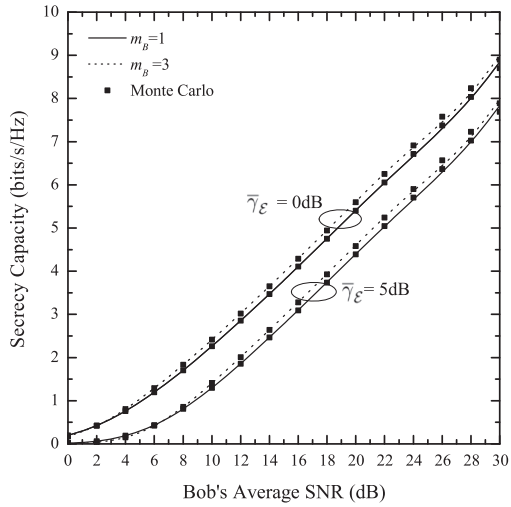

Fig. 7. Average Secrecy Capacity of SIMO 1×3 wiretap channels in arbitrarily correlated generalized fading environments with $m_{\mathcal{E}} = 2$ and various values of $m_{\mathcal{B}}$.

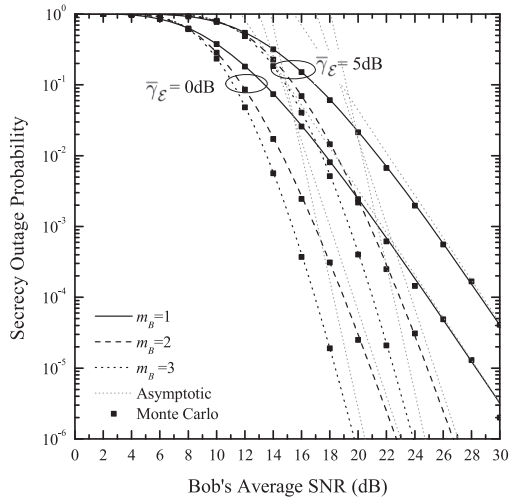

Fig. 8. Secrecy Outage Probability of SIMO 1×3 wiretap channels in arbitrarily correlated generalized fading environments with $m_{\mathcal{E}} = 2$ and various values of $m_{\mathcal{B}}$.

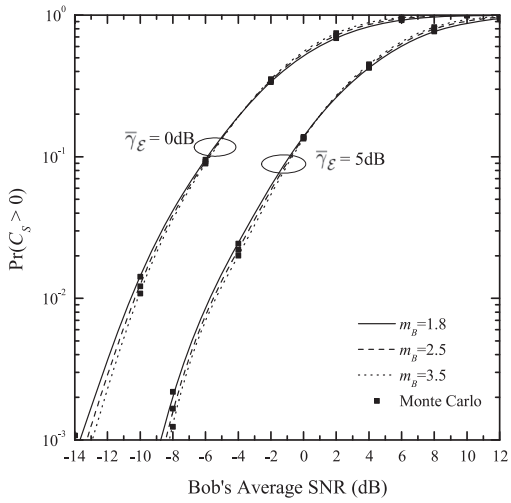

Fig. 9. Probability of Non-Zero Secrecy Capacity of SIMO 1×4 wiretap channels in arbitrarily correlated Nakagami-m fading environment.

As it is evident, the proposed framework provides an efficient means for the secrecy performance evaluation of the wiretap SIMO Nakagami-m channel with arbitrary correlation and arbitrary fading parameters.

VI. Concluding Remarks

In this paper, a new concise, frequency-domain approach for evaluating the secrecy performance of a broad class of SIMO and MIMO wiretap channels has been introduced. The framework enables a simple computation of the average secrecy capacity, the secrecy outage probability and the probability of non-zero secrecy capacity of wiretap channels in a variety of fading environments, provided that the MGF or the CHF of the instantaneous SNR at the legitimate receiver and the eavesdropper is readily available. A unified frequency domain approach for assessing the asymptotic secrecy performance of SIMO and MIMO wiretap channels is also introduced, thus providing useful insights as to the parameters affecting secrecy performance. The generality and computational efficiency of the proposed framework renders it a potentially useful tool to the system engineer for performance evaluation purposes.

Appendix A
Proof of (28)

Proof: By substituting (27) in (17) and by employing the following identities

$$(a+b\,\imath)^{c+d\,\imath} = (a^2+b^2)^{(c+\imath\,d)/2}\, e^{\imath\,(c+\imath\,d)\,\arg(a+\imath\,b)}, \quad \text{(A-1)}$$

with a, b, c, d being real, and

$$\arg(a+\imath\,b) = 2\,\arctan\left(\frac{b}{\sqrt{a^2+b^2}+a}\right), \quad \text{(A-2)}$$

(28) can be obtained after some straightforward algebraic manipulations. ■

Appendix B
Proof of (30)

Proof: By substituting (27) into (16), yields

$$P_{\text{out}}^{\text{OSTBC}} = \frac{1}{2} + \frac{1}{2\pi}\int_{-\infty}^{\infty} \frac{\imath}{\omega} \prod_{i=1}^{N_{\mathcal{B}}\,N_{\mathcal{A}}} \left[\left(1-\imath\,\omega\,\overline{\gamma}_{\mathcal{B}}\,\lambda_{i,\mathcal{A}\mathcal{B}}\right)\right]^{-1} \times \left[\prod_{j=1}^{N_{\mathcal{E}}\,N_{\mathcal{A}}} \left(1+\imath\,2^{\mathcal{R}_S}\,\omega\,\overline{\gamma}_{\mathcal{E}}\,\lambda_{j,\mathcal{A}\mathcal{E}}\right)\right]^{-1} \mathrm{d}\omega. \quad \text{(B-1)}$$

By employing a partial fraction decomposition, (B-1) can be written as

$$P_{\text{out}}^{\text{OSTBC}} = \frac{1}{2} + \frac{\imath}{2\pi}\int_{-\infty}^{\infty} \frac{A\exp(-\imath\,U\,\omega)}{\omega}\,\mathrm{d}\omega + \frac{\imath}{2\pi}\sum_{i=1}^{N_{\mathcal{B}}\,N_{\mathcal{A}}} a_i \int_{-\infty}^{\infty} \frac{\exp(-\imath\,U\,\omega)}{1-\imath\,\omega\,\overline{\gamma}_{\mathcal{B}}\,\lambda_{i,\mathcal{A}\mathcal{B}}}\,\mathrm{d}\omega + \frac{\imath}{2\pi}\sum_{j=1}^{N_{\mathcal{E}}\,N_{\mathcal{A}}} b_j \int_{-\infty}^{\infty} \frac{\exp(-\imath\,U\,\omega)}{1+\imath\,T\,\omega\overline{\gamma}_{\mathcal{E}}\,\lambda_{j,\mathcal{A}\mathcal{E}}}\mathrm{d}\omega, \quad \text{(B-2)}$$

where $U = 2^{\mathcal{R}_S}-1$ and $T = 2^{\mathcal{R}_S}$. Using the Fourier transform pair $\mathcal{F}\{1/x; x; w\} = \pi\,\mathrm{sgn}(w)/\imath$, the integral $\mathcal{J}_1 = \int_{-\infty}^{\infty} A\,\exp(-\imath\,U\,\omega)/\omega\,\mathrm{d}\omega$ can be readily evaluated yielding

$$\mathcal{J}_1 = \frac{\pi U}{\imath}. \quad \text{(B-3)}$$

The remaining integrals can be evaluated by employing [25, eq. (3.382/6)] and [25, eq. (3.382/7)]. The integrals $\mathcal{J}_2 = \int_{-\infty}^{\infty} \frac{\exp(-\imath\,U\,\omega)}{(1+\imath\,T\,\omega\overline{\gamma}_{\mathcal{E}}\,\lambda_{j,\mathcal{A}\mathcal{E}})}\,\mathrm{d}\omega$ are zero $\forall j$; therefore, P_{out} can be deduced as in (30), with a_i given by (31), thus concluding the proof. ■

Appendix C
Proof of (43)

Proof: By substituting (40) into (16), yields

$$P_{\text{out}}^{\text{GSC}} = \frac{1}{2} + \frac{1}{2\pi}\int_{-\infty}^{\infty} \frac{\imath\,\exp(-\imath\,U\,\omega)}{\omega(1-\imath\,\omega\,\Omega_{\mathcal{B}})^{L_{\mathcal{B}}-1}(1+\imath\,T\,\omega\,\Omega_{\mathcal{E}})^{L_{\mathcal{E}}-1}} \times \prod_{r_{\mathcal{B}}=L_{\mathcal{B}}}^{N_{\mathcal{B}}} \frac{1}{(1-\imath\,\omega\,L_{\mathcal{B}}/r_{\mathcal{B}})} \prod_{r_{\mathcal{E}}=L_{\mathcal{E}}}^{N_{\mathcal{E}}} \frac{1}{(1+\imath\,T\,\omega L_{\mathcal{E}}/r_{\mathcal{E}})}\,\mathrm{d}\omega. \quad \text{(C-1)}$$

By performing partial fraction decomposition, (C-1) can be written as

$$\begin{aligned} P_{\text{out}}^{\text{GSC}} = \frac{1}{2} &+ \frac{\imath}{2\pi}\int_{-\infty}^{\infty} \frac{A\,\exp(-\imath\,U\,\omega)}{\omega}\mathrm{d}\omega \\ &+ \frac{\imath}{2\,\pi}\sum_{i=1}^{L_{\mathcal{B}}} a_i \int_{-\infty}^{\infty} \frac{\exp(-\imath\,U\,\omega)}{(\omega+\imath/\Omega_{\mathcal{B}})^i}\mathrm{d}\omega \\ &+ \frac{\imath}{2\,\pi}\sum_{r_{\mathcal{B}}=L_{\mathcal{B}}+1}^{N_{\mathcal{B}}} b_{r-L_{\mathcal{B}}} \int_{-\infty}^{\infty} \frac{\exp(-\imath\,U\,\omega)}{\omega+\imath\,r/(\Omega_{\mathcal{B}}L_{\mathcal{B}})}\mathrm{d}\omega \\ &+ \frac{\imath}{2\pi}\sum_{i=1}^{L_{\mathcal{E}}} c_i \int_{-\infty}^{\infty} \frac{\exp(-\imath\,U\,\omega)}{(\omega-\imath\,T/\Omega_{\mathcal{E}})^i}\mathrm{d}\omega \\ &+ \frac{\imath}{2\,\pi}\sum_{r_{\mathcal{E}}=L_{\mathcal{E}}+1}^{N_{\mathcal{E}}} d_{r-L_{\mathcal{E}}} \int_{-\infty}^{\infty} \frac{\exp(-\imath\,U\,\omega)}{\omega-\imath\,r/(\Omega_{\mathcal{B}}L_{\mathcal{B}}T)}\mathrm{d}\omega, \end{aligned} \quad \text{(C-2)}$$

while using [25, eq. (3.382/6)] and [25, eq. (3.382/7)], P_{out} can be deduced as in (43), with a_i, b_i given by (44a) and (44b), respectively, thus concluding the proof. ■

References

[1] A. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

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

[3] T. Liu and S. S. (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

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

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-part II: The MIMOME wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
[6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2010.
[7] T. F. Wong, M. Bloch, and J. M. Shea, "Secret sharing over fast fading MIMO wiretap channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, pp. 506973/1–506973/17, 2009.
[8] M. Kobayashi, P. Piantanida, S. Yang, and S. S. (Shitz), "On the secrecy degrees of freedom of the multi-antenna block fading wiretap channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 703–711, Sep. 2011.
[9] M. Z. I. Sarkar and T. Ratnarajah, "On the secrecy mutual information of Nakagami-m fading SIMO channel," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Cape Town, South Africa, May 2010.
[10] H. Alves, R. D. Souza, and M. Debbah, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 327–375, Jun. 2012.
[11] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channes," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.
[12] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channel: Secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1754–1758, Sep. 2013.
[13] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 2, pp. 247–258, Feb. 2014.
[14] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Commun. Lett.*, vol. 11, no. 5, pp. 509–511, May 2011.
[15] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 1, pp. 254–259, Jan. 2013.
[16] N. S. Ferdinand, D. B. da Costa, and M. Latvaaho, "Physical layer security in MIMO OSTBC line-of-sight wiretap channels with arbitrary transmit/receive antenna correlation," *IEEE Wireless Commun. Lett.*, vol. 2, no. 5, pp. 467–470, Jun. 2013.
[17] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-m fading channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6054–6067, Nov. 2014.
[18] M. Dohler, R. W. Heath, A. Lozano, C. Papadias, and R. Valenzuela, "Is the PHY layer dead?" *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 159–165, Apr. 2011.
[19] M. K. Simon and M.-S. Alouini, "A unified approach to the performance analysis of digital communications over generalized fading channels," *Proc. IEEE*, vol. 86, no. 9, pp. 1860–1877, Sep. 1998.
[20] A. Annamalai, C. Tellambura, and V. K. Bhargava, "A general method for calculating error probabilities over fading channels," *IEEE Trans. Commun.*, vol. 53, no. 5, pp. 841–852, May 2005.
[21] Y.-C. Ko, M.-S. Alouini, and M. K. Simon, "Outage probability of diversity systems over generalized fading channels," *IEEE Trans. Commun.*, vol. 48, no. 11, pp. 1783–1787, Nov. 2000.
[22] M. K. Simon and M. S. Alouini, *Digital Communication over Fading Channels*, 2nd ed. Hoboken, NJ, USA: Wiley, 2005.
[23] M. D. Yacoub, "The κ-μ and the η-μ distribution," *IEEE Antennas Propag. Mag.*, vol. 49, no. 1, pp. 68–81, Feb. 2007.
[24] P. G. Moschopoulos, "The distribution of the sum of independent gamma random variables," *Ann. Inst. Statist. Math. (Part A)*, vol. 37, pp. 541–544, 1985.
[25] I. Gradshteyn and I. M. Ryzhik, *Tables of Integrals, Series, and Products*, 6th ed. New York, NY, USA: Academic, 2000.
[26] N. M. Steen, G. D. Byrne, and E. M. Gelbard, "Gaussian quadratures for the integrals $\int_0^\infty e^{-x^2} f(x)\mathrm{dx}$ and $\int_0^b e^{-x^2} f(x)\mathrm{dx}$," *Math. Comput.*, vol. 23, no. 107, pp. 661–671, 1969.
[27] F. Yilmaz and M.-S. Alouini, "An MGF-based capacity analysis of equal gain combining over fading channels," in *Proc. IEEE 21st Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Instanbul, Turkey, Sep. 2010, pp. 945–950.
[28] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integrals and Series Volume 4: Direct Laplace Transforms*, 1st ed. Boca Raton, FL, USA: CRC, 1992.
[29] L. Debnath, *Integral Transforms and Their Applications*. Boca Raton, FL, USA: CRC Press, 1995.
[30] L. Hanlen and A. Grant, "Capacity analysis of correlated MIMO channels," *IEEE Trans. Inf. Theory*, vol. 58, no. 11, pp. 6773–6786, Nov. 2012.
[31] D. J. Love and R. W. Heath, "Grassmannian beamforming on correlated MIMO channels," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dallas, TX, USA, Dec. 2004, vol. 1, pp. 106–110.
[32] Q. T. Zhang, "Maximal-ratio combining over Nakagami fading channels with an arbitrary branch covariance matrix," *IEEE Trans. Veh. Technol.*, vol. 48, no. 4, pp. 1141–1150, Jul. 1999.
[33] K. P. Peppas, G. Alexandropoulos, and P. T. Mathiopoulos, "Performance analysis of dual-hop AF relaying systems over mixed η-μ and κ-μ fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 7, pp. 3149–3163, Sep. 2013.
[34] A. Annamalai, G. Deora, and C. Tellambura, "Analysis of generalized selection diversity systems in wireless channels," *IEEE Trans. Veh. Technol.*, vol. 55, no. 6, pp. 1765–1775, Nov. 2006.
[35] F. Yilmaz and M.-S. Alouini, "Computation of the higher-order statistics of the channel capacity over generalized fading channels," *IEEE Wireless Commun. Lett.*, vol. 1, no. 6, pp. 573–576, Dec. 2012.
[36] Q. T. Zhang, "A decomposition technique for efficient generation of correlated Nakagami fading channels," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 11, pp. 2385–2392, Nov. 2000.

Kostas P. Peppas (M'09–SM'14) was born in Athens, Greece, in 1975. He received the Diploma degree in electrical and computer engineering and the Ph.D. degree in wireless communications from the National Technical University of Athens, Kesariani, Greece, in 1997 and 2004, respectively. From 2004 to 2007, he was with the Department of Computer Science, University of Peloponnese, Tripolis, Greece, and from 2008 to 2014, with the National Centre for Scientific Research "Demokritos," Institute of Informatics and Telecommunications, as a Researcher. In 2014, he joined the Department of Telecommunication Science and Technology, University of Peloponnese, where he is currently a Lecturer. He has authored more than 70 journals and conference papers. His research interests include digital communications over fading channels, MIMO systems, wireless and personal communication networks, and system level analysis and design.

Nikos C. Sagias (S'03–M'05–SM'11) was born in Athens, Greece, in 1974. He received the B.Sc. degree in physics from the University of Athens (UoA), Athens, Greece, the M.Sc. and Ph.D. degrees in telecommunication engineering from the UoA, in 1998, 2000, and 2005, respectively. From 2001 to 2010, he was involved in various national and European research and development projects for the Institute of Space Applications and Remote Sensing, National Observatory of Athens, Athens, Greece. From 2006 to 2008, he was a Postdoc Research Scholar with the Institute of Informatics and Telecommunications, National Centre for Scientific Research-Demokritos, Athens, Greece. From 2008 to 2014, he was an Assistant Professor with the Department of Informatics and Telecommunications, University of Peloponnese, Tripolis, Greece, where he currently is an Associate Professor and the Head of the department. His research interests include digital communications, and more specifically MIMO and cooperative systems, fading channels, mobile and satellite communications, optical wireless systems, and communication theory issues. He has authored over 50 papers in prestigious international journals and more than 30 in the proceedings of world recognized conferences. He has been a TPC member for various IEEE conferences (ICC, GLOBECOM, VTC, etc.). From 2009 to 2014, he was an Associate Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. He was the corecipient of the Best Paper Award in PHY in the IEEE Wireless Communications and Networking Conference 2014 (WCNC14) and in the 3rd International Symposium on Communications, Control and Signal Processing 2008 (ISCCSP08).

Andreas Maras was born in Athens, Greece, in 1952. He received the B.Sc. and Ph.D. degrees from the School (formerly, Department) of Electrical and Electronic Engineering, and the M.Sc. degree in applied sciences from the School of Applied Sciences from the University of Newcastle, Newcastle Upon Tyne, U.K., in 1975, 1980, and 1977, respectively. From 1981 to 1982, he served in the Greek Army and from September 1982 to August 1985, he was a Research Assistant and then from September 1985 to August 1987, was a Temporary Lecturer with the Department of Electrical and Electronic Engineering, University of Newcastle. From September 1988 to December 1990, he was a Senior Research Engineer with INTRACOM, Ltd., and in 1990, was a Consultant to the Greek Telecommunications Industry. From March 1991 to August 2002, was appointed in the position of Associate Professor and then promoted to full professorship with the Department of Electronic and Computer Engineering, Technical University of Crete, Chania, Greece. He is currently a Professor of Telecommunications with the Department of Informatics and Telecommunications and the Dean of the School of Economics, Management and Computer Science, University of Peloponnese. His research interests include statistical signal processing for digital communications with emphasis on large MIMO systems, non-Gaussian noise fading channels, and the application of iterative codes to wiretap channels.