IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 22, 2018, accepted June 20, 2018, date of publication July 9, 2018, date of current version August 15, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2854222

Intercept Probability Analysis of Wireless Networks in the Presence of Eavesdropping Attack With Co-Channel Interference

JULES M. MOUALEU[1], (Senior Member, IEEE), WALAA HAMOUDA[2], (Senior Member, IEEE), AND FAMBIRAI TAKAWIRA[1], (Member, IEEE)

[1]School of Electrical and Information Engineering, University of the Witwatersrand, Johannesburg 2000, South Africa
[2]Department of Electrical and Computer Engineering, Concordia University, Montreal, QC H3G 1M8, Canada

Corresponding author: Walaa Hamouda (hamouda@ece.concordia.ca)

This work was supported by the Centre for Telecommunications Access Services (CeTAS) at the University of the Witwatersrand under Project COEF013.

ABSTRACT In this paper, the joint effect of fading and co-channel interference on the secrecy performance of a wireless communications system is studied. Considering a practical setting where a transmitter (Alice) communicates with a multi-antenna legitimate receiver (Bob) in the presence of a multi-antenna eavesdropper (Eve), we study the secrecy performance of the proposed system when maximal ratio combining is employed. The probability density function and cumulative distribution function of the output signal-plus-interference-to-noise ratio are derived. Given these formulations, we derive a novel analytical expression for the exact intercept probability, which takes into account the number of interfering signals and the fading characteristics of the wireless environment. In addition, we provide a comprehensive diversity analysis, where we derive simple asymptotic intercept probability expressions and explicitly show the impact of system parameters on the diversity order and secrecy coding gain. Throughout the asymptotic analysis, we consider various scenarios based on the interfernece-to-noise ratios at the legitimate receiver and the eavesdropper, as well as the average signal-to-noise ratio of the eavesdropper and examine their impact on the physical layer security of the wireless system. Finally, Monte-Carlo simulations are conducted to assess our proposed analysis.

INDEX TERMS Co-channel interference (CCI), intercept probability, maximal ratio combining (MRC), Nakagami-*m* fading, optimum combining, PHY security, secrecy capacity.

I. INTRODUCTION

Due to the distributed nature of the broadcasting wireless channel, it is difficult to protect a transmission between a transmitter and a legitimate receiver against security attacks and threats of unexpected eavesdropping. To prevent such attacks, high-layer encryption protocols have been widely used. However, such techniques are computationally complex and have become expensive and vulnerable to attacks [1]. In light of these circumstances, there has been renewed interest in information-theoretic secrecy to ensure confidentiality without the need for cryptographic techniques. The study of physical-layer (PHY) security was pioneered by Wyner [2] and Leung-Yan-Cheong and Hellman [3]. In [2], a discrete memoryless wiretap channel in the presence of an eavesdropper was investigated for secure transmission. The work of [2] was extended from the discrete memoryless wiretap channel to the Gaussian wiretap channel by [3]. Leung *et al.* developed the secrecy capacity which was shown to be the difference between the channel capacity of the main channel (transmitter to legitimate receiver) and that of the wiretap channel (transmitter to eavesdropper). In [4], the secrecy capacity was studied from an information theoretic perspective for both single-antenna and multi-antenna wiretap channels. The perfect security in a wiretap channel can be attained provided the capacity of the main channel is higher than that of the wiretap link. Therefore, in order to reduce the probability that an intercept event occurs due to eavesdropping attacks, it is important to find ways to increase the secrecy capacity.

Some recent studies have considered various diversity combining schemes at the receiver in an effort to improve the PHY security [5]–[10]. In [5], He *et al.* discussed the PHY security improvement through the use of maximal ratio combining (MRC) at the receiver. The works of [6] and [7] investigated a transmit antenna selection (TAS) at the transmitter in order to improve PHY security in the presence

of a multi-antenna eavesdropper. Yang *et al.* [7] considered TAS scheme at the transmitter with selection combining (SC) and MRC schemes adopted at the receiver and eavesdropper. Extended from [7], the effect of antenna correlation was studied in [8]. To bridge the gap between SC and MRC, generalized selection combining (GSC) at the receiver and/or eavesdropper was studied in [9] and [10]. The above-mentioned works [5]–[10] assumed perfect channel estimation for receive combining. However, in practice channel estimation errors are inevitable and must therefore be taken into account. In [11] and [12], the effect of Gaussian distributed weighting errors on maximal ratio diversity combining for PHY security was investigated. Results showed that achievable secrecy diversity order cannot be attained with imperfect channel estimates.

In wireless networks, frequency reuse is necessary to increase spectrum efficiency. Although frequency reuse yields spectrum efficiency improvement, it also causes co-channel interference (CCI) [13]–[15]. A key assumption of all the prior works [5]–[12] is that a scenario with no CCI is considered. However, in practical PHY security networks with dense frequency reuse, both the receiver and eavesdropper can be vulnerable to interference from other transmitters using the same frequency band in neighboring cells. Recently, the effect of interference on the secure performance has received much interest [16]–[23]. Duy *et al.* [16] and Fan *et al.* [17] studied the PHY security of cooperative networks in the presence of Rayleigh faded CCI with single-antenna nodes, by deriving the analytical expressions of the secrecy outage probability (SOP). Nevertheless, El-Malek *et al.* [19] studied the secrecy performance of a cooperative wireless network in terms of intercept probability wherein all the nodes are equipped with a single antenna. In [20], a single-input multiple-output multiple-antenna eavesdropper (SIMOME) wiretap channel was considered and the SOP performance of the proposed scheme was derived. However, the authors assumed that the effect of noise at the receiver was negligible due to the high interference power. In addition, they assumed that the same interference sources affecting the legitimate receiver also affect the eavesdropper which in practice might not be viable. Unlike in [16]–[21], the works of [22] and [23] studied the interference issues of PHY security in random wireless networks under a stochastic geometry framework. In [22], Zheng *et al.* comprehensively investigated the benefits of full-duplex (FD) receiver jamming aimed at enhancing the PHY security of two-tier wireless network. In [23], a SIMOME wiretap channel in the presence of randomly placed multiple friendly single-antenna jammers was studied. Zheng *et al.* [22] and Wang *et al.* [23] studied the impact of CCI on the secrecy performance in SIMOME transmissions with MRC adopted at the intended receiver and eavesdropper under a stochastic geometry approach. However, the interferers used in these studies act as jammers and are used to intentionally confound the eavesdroppers while protecting the legitimate receiver from any passive or active attack.

Different from [16]–[19] wherein CCI is present, we consider a direct-transmission system similar to [5]–[10] from the receiver diversity viewpoint. To the best of the authors' knowledge, the joint effect of CCI and the fading characteristics of the interference signals is seldom investigated in the open literature. In [21], Karas *et al.* addressed the above-mentioned problem by considering a more simplistic single-input single-output single-antenna eavesdropper (SISOSE) system. Moreover, it was assumed that all the links are subject to Rayleigh fading channels. As aforementioned, multi-antenna techniques in PHY-security networks have become an important research topic in both academia and industry. Motivated by this, we study the joint impact of CCI and the fading characteristics of the interference signals in a secure communication based on multi-antenna techniques. Such an investigation is crucial to system designers in order to provide secure wireless communications for future wireless networks. Although, the works of [22] and [23] also considered a SIMOME scenario as in our work, they considered friendly interferers in the forms of jammers which inject artificial noise to confound the eavesdroppers in an effort to improve the secure system performance. Different from [22] and [23], our work considers not necessarily friendly interferers in the form of co-channel interferers (for spectral efficiency improvement) which affect both the intended receiver and the eavesdropper. Also, the interfering signals affecting both the legitimate receiver and the eavesdropper are subject to Nakagami-*m* fading [24] whereas the desired signals experience Rayleigh fading distribution. A common assumption in [16]–[21] is that all the desired and interference signals have the same statistical characteristics, i.e., Rayleigh distribution in this case. This assumption can be valid in some instances such as medium to large cell systems. However, in microcellular systems, it is more realistic to expect that both the interference and desired signals undergo different fading statistics (see [25] and [26]). Here, we note the choice of the Nakagami-*m* model as it represents the best fit of the statistical characteristics of land mobile systems, complex indoor environments and also represents a generalized distribution for a large set of fading environments (no fading, light or severe). Given the wide applicability of the Nakagami-*m* distribution, it makes more sense to assume that the interference signals experience such fading statistics since the focus of this work is to investigate the joint effect of CCI and the fading characteristics (interference channels).

In this paper, we study a SIMOME wiretap channel in the presence of multiple Nakagami-distributed equal-power interferers. In the proposed system, both the legitimate receiver and eavesdropper employ maximal ratio diversity combining and are affected by CCI. This combining scheme is not the optimal receiving strategy for the receiver in the presence of co-channel interference. A better solution is to adopt some signal processing techniques such as the optimum diversity combining also known as minimum mean square error (MMSE) combining (see [20] and [27]–[32]) to fully or partially cancel the interference. In this scheme,

the signals received by multiple branches are weighted and combined so as to maximize the signal-plus-interference-to-noise ratio (SINR). However, in fading scenarios, providing an exact analytical performance for optimum combining (OC) is quite intricate and the practical implementation of such combining scheme for more than two branches is excessively complex. Although, the MMSE combining or OC yields an optimal performance, the performance difference when MRC is adopted is not substantial. Hence, under the presence of interference, MRC is often preferred to OC because of its near-optimal performance and low complexity. Furthermore, as aforementioned, our goal is to study the joint effects of CCI and the fading characteristics of the secure performance in terms of intercept probability and identify the performance benefits by exploiting CCI.

In spite of the fact that the MRC scheme does not represent the optimal receiving strategy for secure communications in the presence of CCI, our key goal is twofold: a) to investigate the joint effect of CCI and fading characteristics of the interference signals (fading type) on the intercept probability performance in a SIMOME scenario, and b) to identify the secure performance (in terms of intercept probability) benefits that can be provided by exploiting CCI. Moreover, we aim to gain insights into the secrecy performance of the system as we investigate the impact of Nakagami-m faded interferences on the system. To this end, the main contributions of our work are listed as follows:

- We first derive expressions for the probability density function (PDF) and cumulative distribution function (CDF) for the MRC combiner output SINR. Subsequently, the resulting expressions are used to derive a novel analytical expression for the exact intercept probability.
- In addition, a comprehensive asymptotic analysis of the intercept probability at high signal-to-noise ratio (SNR) is provided. Expressions for the asymptotic intercept probability are derived for different scenarios. The secrecy diversity gain and secrecy coding gain which are two key indicators of the intercept probability at high SNR are analyzed for fixed/varying (varying with respect to the average SNR of the main channel) interference-to-noise ratio (INR) at Bob/Eve, as well the fixed/ varying average SNR of the wiretap channel. Our results reveal important design insights into the joint impact of CCI and the fading type of the interference channels on both the legitimate receiver and eavesdropper.
- We have carried out various Monte-Carlo simulations to verify the accuracy of our mathematical analysis.

The remainder of this paper is organized as follows. The system model is illustrated in Section II. A closed-form expression for the intercept probability is derived in Section III. In Section IV, we derive the simple and explicit asymptotic expressions for the intercept probability at high SNR. Numerical results are discussed in Section V and some conclusions are drawn in Section VI.

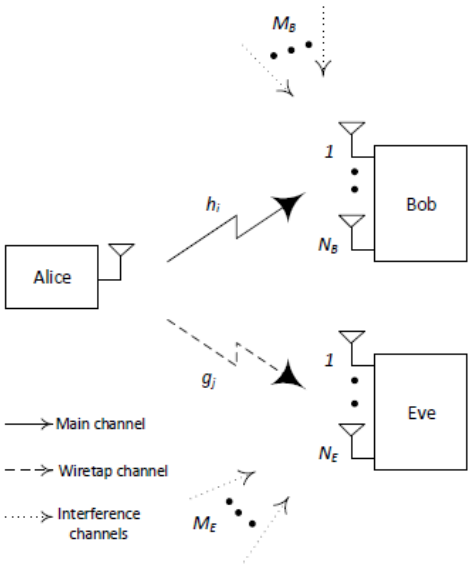

FIGURE 1. A single-antenna multiple-output multiple-antenna eavesdropper in the presence of co-channel interference.

II. SYSTEM MODEL AND CHANNEL STATISTICS

A. SYSTEM MODEL

Consider a SIMOME wiretap channel, where the single-antenna transmitter Alice ($\mathcal{A}$)[1] communicates with the receiver Bob ($\mathcal{B}$) under the malicious attack of the eavesdropper Eve ($\mathcal{E}$) as shown in Fig. 1 in the presence of Nakagami-m faded CCIs. Both Bob and Eve are equipped with $N_{\mathcal{B}}$ and $N_{\mathcal{E}}$ antennas respectively. In the sequel, we refer to branch as a link between Alice and one of Bob's antennas. Moreover, in this network, $M_{\mathcal{B}}$ interference sources close to Bob–these sources are single-antenna transmitters–are using the same frequency bands as Alice, and therefore causing some interference to each branch at the receiver. Similarly, Eve is assumed to operate in an environment prone to interference, in which a general model with $M_{\mathcal{E}}$ interference signals is adopted. The latter scenario is plausible when multiple single-antenna transmitters present in the vicinity of Eve also transmit simultaneously with Alice and therefore interfere with the received signals at the former. We assume without loss of generality that the same number of interfering signals are present on each diversity branch for both Bob and Eve.[2] In addition, it is assumed that the effect of thermal noise at the receivers of Bob and Eve cannot be ignored due to the level of interference. The communication between Alice and Bob, as well as the one between Alice and Eve experience flat

[1] In practice, Alice could represent a mobile or sensor unit which may not be able to accommodate multiple transmit antennas due to hardware complexity, size or cost restrictions.

[2] In our system model, in spite of the fact that the interference sources are geographically randomly distributed, it is assumed that the interference signals are identical since the distances between the affected node and the interference sources are approximately the same. This scenario can be found in cellular networks where the interference sources are in the second tier and the distance to the base station or mobile unit is assumed to be identical.

Rayleigh fading. On the other hand, all the interfering signals are subject to Nakagami-*m* fading. All the channels are considered to be independent and identically distributed (i.i.d). Also, we consider a passive eavesdropping scenario wherein the receiver and eavesdropper have knowledge of the channel state information (CSI) of their own channels. At Bob, MRC is employed to combine the signals received on the $N_{\mathcal{B}}$ diversity branches for a maximum output SNR. Meanwhile, Eve also employs the same combining scheme.

For this network, Alice transmits a message x with a fixed power P_s for each antenna of Bob while Eve overhears it. The received signals at Bob and Eve are respectively given by

$$\boldsymbol{y}_{\mathcal{B}} = \sqrt{P_s}\boldsymbol{h}x + \sum_{l_{\mathcal{B}}=1}^{M_{\mathcal{B}}} \sqrt{P_{I_{l_{\mathcal{B}}}}}\alpha_{l_{\mathcal{B}}} s_{l_{\mathcal{B}}} + \boldsymbol{n}, \tag{1}$$

$$\boldsymbol{y}_{\mathcal{E}} = \sqrt{P_s}\boldsymbol{g}x + \sum_{l_{\mathcal{E}}=1}^{M_{\mathcal{E}}} \sqrt{P_{I_{l_{\mathcal{E}}}}}\beta_{l_{\mathcal{E}}} s_{l_{\mathcal{E}}}^{,} + \boldsymbol{z}, \tag{2}$$

where $\boldsymbol{h}$ and $\boldsymbol{g}$ are the complex gain vectors for the signal of interest and eavesdropping signals respectively, $\alpha_{l_{\mathcal{B}}}$ and $\beta_{l_{\mathcal{E}}}$ are the complex gains for the interfering signals at Bob and Eve respectively,[3] $\boldsymbol{n}$ and $\boldsymbol{z}$ are the the additive white Gaussian noise (AWGN) vectors at the receivers of Bob and Eve respectively, with zero mean and variance $\sigma_{\mathcal{B}}^2$ ($\sigma_{\mathcal{E}}^2$) per each antenna, $M_{\mathcal{B}}$ is the number of interferers affecting Bob, $M_{\mathcal{E}}$ is the number of interferers affecting Eve respectively, $P_{I_{l_{\mathcal{B}}}}$ and $P_{I_{l_{\mathcal{E}}}}$ are the power of the interfering signals affecting Bob and Eve respectively, $s_{l_{\mathcal{B}}}$ is the transmitted signal from the $l_{\mathcal{B}}^{\text{th}}$ interferer affecting Bob, and $s_{l_{\mathcal{E}}}^{,}$ is the transmitted signal from the $l_{\mathcal{E}}^{\text{th}}$ interferer affecting Eve.

B. CHANNEL STATISTICS

In this subsection, we present the statistics of the SINR γ_{χ} with $\chi = \{\mathcal{B}, \mathcal{E}\}$. Using (1) and the weight vector $\boldsymbol{w} = \boldsymbol{h}^H$, the output of the maximum ratio combiner yields

$$\boldsymbol{h}^{\text{H}}\boldsymbol{y}_{\mathcal{B}} = \sqrt{P_s}\boldsymbol{h}^{\text{H}}\boldsymbol{h}x + \sum_{l_{\mathcal{B}}=1}^{M_{\mathcal{B}}} \sqrt{P_{I_{l_{\mathcal{B}}}}}\boldsymbol{h}^{\text{H}}\alpha_{l_{\mathcal{B}}} s_{l_{\mathcal{B}}} + \boldsymbol{h}^{\text{H}}\boldsymbol{n}, \tag{3}$$

where $\boldsymbol{A}^{\text{H}}$ denotes the conjugate transpose of $\mathbf{A}$. From (3), the output SINR is expressed as [34], [35]

$$\gamma_{\mathcal{B}} = \frac{P_s|\boldsymbol{h}^{\text{H}}\boldsymbol{h}|^2}{\boldsymbol{h}^{\text{H}}\left(\sum_{l_{\mathcal{B}}=1}^{M_{\mathcal{B}}} P_{I_{l_{\mathcal{B}}}}\alpha_{l_{\mathcal{B}}}\alpha_{l_{\mathcal{B}}}^{\text{H}} + \sigma_{\mathcal{B}}^2\boldsymbol{I}\right)\boldsymbol{h}}, \tag{4}$$

[3]In some practical scenarios, the distances between various interferers and the receive antennas may differ. In such instances, the channel gain can be modeled as in [21] and [33] where $\alpha_{l_{\mathcal{B}}} = \frac{\phi_{l_{\mathcal{B}}}}{\sqrt{1-d_{l_{\mathcal{B}}}^{\mu}}}$ with $d_{l_{\mathcal{B}}}$, μ and $\phi_{l_{\mathcal{B}}}$ denoting the distance between the $l_{\mathcal{B}}^{\text{th}}$ interferer and Bob, the pathloss coefficients and the Nakagami-*m* fading channel respectively. The analysis of the proposed system with identical distances of the interferers to Bob/Eve, can easily be extended to the one with different positions of the interferers relative to the Bob or Eve.

where $\mathbf{I}$ is the identity matrix. After some manipulations, the expression in (4) can further be given by

$$\gamma_{\mathcal{B}} = \frac{\sum_{i=1}^{N_{\mathcal{B}}} \frac{P_s}{\sigma_{\mathcal{B}}^2}|h_i|^2}{\sum_{l_{\mathcal{B}}=1}^{M_{\mathcal{B}}} \frac{P_{I_{l_{\mathcal{B}}}}|\alpha_{l_{\mathcal{B}}}|^2}{\sigma_{\mathcal{B}}^2} + 1}. \tag{5}$$

We define $\gamma_{\mathcal{B}_i} = \frac{P_s}{\sigma_{\mathcal{B}}^2}|h_i|^2$, $\gamma_{I_{l_{\mathcal{B}}}} = \frac{P_{I_{l_{\mathcal{B}}}}}{\sigma_{\mathcal{B}}^2}|\alpha_{l_{\mathcal{B}}}|^2$ and after substituting these into (5), we have

$$\gamma_{\mathcal{B}} = \frac{\sum_{i=1}^{N_{\mathcal{B}}} \gamma_{\mathcal{B}_i}}{1 + \sum_{l_{\mathcal{B}}=1}^{M_{\mathcal{B}}} \gamma_{I_{l_{\mathcal{B}}}}}. \tag{6}$$

Using (2) and following the above-mentioned steps, we can obtain the output SINR at Eve as

$$\gamma_{\mathcal{E}} = \frac{\sum_{j=1}^{N_{\mathcal{E}}} \gamma_{\mathcal{E}_j}}{1 + \sum_{l_{\mathcal{E}}=1}^{M_{\mathcal{E}}} \gamma_{I_{l_{\mathcal{E}}}}}, \tag{7}$$

where $\gamma_{\mathcal{E}_j} = |g_j|^2\frac{P_s}{\sigma_{\mathcal{E}}^2}$ and $\gamma_{I_{l_{\mathcal{E}}}} = |\beta_{l_{\mathcal{E}}}|^2\frac{P_{I_{l_{\mathcal{E}}}}}{\sigma_{\mathcal{E}}^2}$. For the sake of easy notation, let $X = \sum_{i=1}^{N_{\chi}} \gamma_{\chi i}$, $Y = \sum_{l_{\chi}=1}^{M_{\chi}} \gamma_{I_{l_{\chi}}}$. In what follows, we derive the PDF and CDF for the MRC combiner output SINR of the random variable (RV) γ_{χ} defined in (6) and (7).

The PDF of γ_{χ} is given by [36],

$$f_{\gamma_{\chi}}(\gamma) = \int_0^{\infty} (1+y) f_X\big((1+y)\gamma\big) f_Y(y)\text{d}y, \tag{8}$$

$f_X(\bullet)$ and $f_Y(\bullet)$ are respectively given by

$$f_X(\gamma) = \frac{1}{\bar{\gamma}_{\chi}^{N_{\chi}}(N_{\chi}-1)!}\gamma^{N_{\chi}-1}\exp\left(-\frac{\gamma}{\bar{\gamma}_{\chi}}\right), \tag{9}$$

$$f_Y(y) = \frac{1}{\Gamma(m_{I_{\chi}}M_{\chi})}\left(\frac{m_{I_{\chi}}}{\bar{\gamma}_{I_{\chi}}}\right)^{m_{I_{\chi}}M_{\chi}} y^{m_{I_{\chi}}M_{\chi}-1}e^{-\frac{m_{I_{\chi}}y}{\bar{\gamma}_{I_{\chi}}}}, \tag{10}$$

where $m_{I_{\chi}}$ is the Nakagami fading parameter, $\bar{\gamma}_{\chi} = \frac{P_s}{\sigma_{\chi}^2}$, $\bar{\gamma}_{I_{l_{\chi}}} = \frac{P_{I_{l_{\chi}}}}{\sigma_{\chi}^2}$ and $\Gamma(\bullet)$ is the gamma function defined in [37, eq. (8.310.1)]. Substituting (9) and (10) in (8), and after some manipulations and with the aid of [37, eq. (9.211.4)], (8) can further be written as

$$f_{\gamma_{\chi}}(\gamma) = \left(\frac{m_{I_{\chi}}}{\bar{\gamma}_{I_{\chi}}}\right)^{m_{I_{\chi}}M_{\chi}} \frac{\gamma^{N_{\chi}-1}e^{-\frac{\gamma}{\bar{\gamma}_{\chi}}}}{\bar{\gamma}_{\chi}^{N_{\chi}}(N_{\chi}-1)!} \times \Psi\left(m_{I_{\chi}}M_{\chi}, m_{I_{\chi}}M_{\chi}+N_{\chi}+1; \frac{\gamma}{\bar{\gamma}_{\chi}}+\frac{m_{I_{\chi}}}{\bar{\gamma}_{I_{\chi}}}\right), \tag{11}$$

where $\Psi(a, b; z)$ is the confluent hypergeometric function of the second kind defined in [37, eq. (9.210.2)].

Proof: The detailed steps to obtain (11) are shown in the appendix. ■

Using (11) to obtain the CDF of γ_{χ} is very complicated. To overcome this, we use $F_{\gamma_{\chi}}(\gamma) = \int_0^{\infty} f_{\gamma_{\chi}}(y)\text{d}y$ and with the help of the substitution method, $F_{\gamma_{\chi}}(\gamma)$ can be expressed as

$$F_{\gamma_{\chi}}(\gamma) = \int_0^{\infty} F_X\big((1+y)\gamma\big) f_Y(y)\text{d}y, \tag{12}$$

where the CDF of the RV X is given by

$$F_X(\gamma) = 1 - \exp\left(-\frac{\gamma}{\bar{\gamma}_\chi}\right)\sum_{n=0}^{N_\chi}\frac{1}{n!}\left(\frac{\gamma}{\bar{\gamma}_\chi}\right)^n. \quad (13)$$

Substituting (10) and (13) in (12), and after some manipulations and with the aid of [37, Eq. 9.211.4], (12) can be further expressed as

$$F_{\gamma_\chi}(\gamma) = 1 - \left(\frac{m_{I_\chi}}{\bar{\gamma}_{I_\chi}}\right)^{m_{I_\chi}M_\chi}\exp\left(-\frac{\gamma}{\bar{\gamma}_\chi}\right)\sum_{n=0}^{N_\chi-1}\frac{1}{n!}\left(\frac{\gamma}{\bar{\gamma}_\chi}\right)^n \times\Psi\left(m_{I_\chi}M_\chi, m_{I_\chi}M_\chi + n + 1; \frac{\gamma}{\bar{\gamma}_\chi} + \frac{m_{I_\chi}}{\bar{\gamma}_{I_\chi}}\right) \quad (14)$$

III. INTERCEPT PROBABILITY ANALYSIS

In this section, we derive an analytical expression of the intercept probability of the underlying scheme. The intercept probability is a key performance metric used to describe the performance of the secrecy of wireless communication systems. It is defined as the probability that the eavesdropper succeeds in intercepting the signal intended for the legitimate receiver or that the secrecy capacity C_s falls below zero. It is proven in [3] that the secrecy capacity is the difference between the capacity of the main channel and that of the eavesdropper link. Mathematically, this can be expressed as

$$C_s = C_\mathcal{B} - C_\mathcal{E}, \quad (15)$$

where $C_\chi = \log_2(1+\gamma_\chi)$. From (15), it is easy to see that an intercept event occurs when the capacity of the main channel is worse than that of the eavesdropper channel. Unlike in [38] and [39], the main focus of this work is not to seek to improve the intercept probability performance, but rather to investigate the joint impact of the interference and fading on the above-mentioned key performance metric. In what follows, we express the intercept probability mathematically as

$$P_{int} = \mathbb{P}\{C_s < 0\} = 1 - \int_0^\infty\int_0^{\gamma_\mathcal{B}} f_{\gamma_\mathcal{E}}(\gamma_\mathcal{E})f_{\gamma_\mathcal{B}}(\gamma_\mathcal{B})\mathrm{d}\gamma_\mathcal{E}\mathrm{d}\gamma_\mathcal{B} = 1 - \int_0^\infty F_{\gamma_\mathcal{E}}(\gamma_\mathcal{B})f_{\gamma_\mathcal{B}}(\gamma_\mathcal{B})\mathrm{d}\gamma_\mathcal{B}. \quad (16)$$

We first rewrite the confluent hypergeometric function in (11) and (14) using the identity [40, eq. (13.2.8)]

$$\Psi(a, a+n+1; z) = \sum_{s=0}^{n}\binom{n}{s}(a)_s z^{-a-s}, \quad (17)$$

where $(a)_s = \frac{\Gamma(a+s)}{\Gamma(a)}$ is the Pochhammer symbol. The resulting expressions of the PDF and CDF are substituted in (16) and after some manipulations, we obtain

$$P_{int} = \left(\frac{m_{I_\mathcal{B}}}{\bar{\gamma}_{I_\mathcal{B}}}\right)^{m_{I_\mathcal{B}}M_\mathcal{B}}\frac{(m_{I_\mathcal{E}}/\bar{\gamma}_{I_\mathcal{E}})^{m_{I_\mathcal{E}}M_\mathcal{E}}}{\bar{\gamma}_\mathcal{B}^{N_\mathcal{B}}(N_\mathcal{B}-1)!}\sum_{n=0}^{N_\mathcal{E}-1}\frac{1}{n!\bar{\gamma}_\mathcal{E}^n} \times\sum_{i=0}^{N_\mathcal{B}}\sum_{j=0}^{n}\binom{N_\mathcal{B}}{i}\binom{n}{j}(m_{I_\mathcal{B}}M_\mathcal{B})_i(m_{I_\mathcal{E}}M_\mathcal{E})_j \times\int_0^\infty\gamma_\mathcal{B}^{N_\mathcal{B}+n-1}\left(\frac{m_{I_\mathcal{B}}}{\bar{\gamma}_{I_\mathcal{B}}}+\frac{\gamma_\mathcal{B}}{\bar{\gamma}_\mathcal{B}}\right)^{-m_{I_\mathcal{B}}M_\mathcal{B}-i} \times\left(\frac{m_{I_\mathcal{E}}}{\bar{\gamma}_{I_\mathcal{E}}}+\frac{\gamma_\mathcal{B}}{\bar{\gamma}_\mathcal{E}}\right)^{-m_{I_\mathcal{E}}M_\mathcal{E}-j}e^{-\left(\frac{1}{\bar{\gamma}_\mathcal{B}}+\frac{1}{\bar{\gamma}_\mathcal{E}}\right)\gamma_\mathcal{B}}\mathrm{d}\gamma_\mathcal{B}. \quad (18)$$

The integral part of (18) is mathematically intractable and cannot be obtained in closed-form as currently shown. To circumvent this, we replace the exponential function by its series representation $e^{-y} = \sum_{k=0}^{\infty}(-1)^k\frac{y^k}{k!}$ in (18) and with the aid of [37, eq. (3.197.1)] and after many algebraic manipulations, the intercept probability expression is given by

$$P_{int} = \frac{1}{\bar{\gamma}_\mathcal{B}^{N_\mathcal{B}}(N_\mathcal{B}-1)!}\sum_{n=0}^{N_\mathcal{E}-1}\sum_{i=0}^{N_\mathcal{B}}\sum_{j=0}^{n}\binom{N_\mathcal{B}}{i}\binom{n}{j}\frac{(m_{I_\mathcal{B}}M_\mathcal{B})_i}{n!\bar{\gamma}_\mathcal{E}} \times(m_{I_\mathcal{E}}M_\mathcal{E})_j\sum_{k=0}^{\infty}\frac{(-1)^k}{k!}\left(\frac{1}{\bar{\gamma}_\mathcal{B}}+\frac{1}{\bar{\gamma}_\mathcal{E}}\right)^k\left(\frac{\bar{\gamma}_\mathcal{E}m_{I_\mathcal{E}}}{\bar{\gamma}_{I_\mathcal{E}}}\right)^{N_\mathcal{B}+n+k} \times\mathrm{B}\left(N_\mathcal{B}+n+k, m_{I_\mathcal{B}}M_\mathcal{B}+m_{I_\mathcal{E}}M_\mathcal{E}-N_\mathcal{B}-n-k\right) \times{}_2F_1\left(m_{I_\mathcal{B}}M_\mathcal{B}, N_\mathcal{B}+n+k; m_{I_\mathcal{B}}M_\mathcal{B}+m_{I_\mathcal{E}}M_\mathcal{E}; \zeta\right), \quad (19)$$

where $\zeta = 1 - \frac{m_{I_\mathcal{E}}\bar{\gamma}_\mathcal{E}\bar{\gamma}_{I_\mathcal{B}}}{m_{I_\mathcal{B}}\bar{\gamma}_{I_\mathcal{E}}\bar{\gamma}_\mathcal{B}}$, $\mathrm{B}(w, y)$ is the Beta function or Euler's integral of the first kind defined in [37, eq. (8.380.1)] and ${}_2F_1(a, b; c; z)$ is the Gauss hypergeometric function defined in [37, eq. (9.100)] and [37, eq. (9.14)]. It is worth mentioning that such functions are readily available in some mathematical software packages such as MATHEMATICA. Moreover, it can be noticed that (19) has an infinite series. However, (19) converges rapidly and steadily after a finite number of terms to yield an accurate expression of the intercept probability (seen in simulations). A study of the convergence for the above-mentioned expression is beyond the scope of this work. This expression is general as it encompasses the case where both the desired and interference signals are subject to Rayleigh fading ($m_{I_\mathcal{B}} = 1$) in medium to large cell systems. Furthermore, for microcellular systems where the desired and interference signals experience different statistical fading characteristics, the expression in (19) gives the intercept probability in such an instance (less fading $m_{I_\chi} > 1$ or severe fading $m_{I_\chi} < 1$).

IV. ASYMPTOTIC SECRECY ANALYSIS

In this section, we provide a comprehensive asymptotic analysis on the intercept probability at high SNR of the underlying scheme. Although the closed-form expression in (19) enables the evaluation of the proposed scheme, it is too complex to provide valuable insights into how various system parameters affect the secrecy diversity order and secrecy coding gain.[4] To this end, we assume that $\bar{\gamma}_\mathcal{B} = \bar{\gamma} \to \infty$ and we consider a set of scenarios where $\bar{\gamma}_{I_\mathcal{B}}$, $\bar{\gamma}_\mathcal{E}$ and $\bar{\gamma}_{I_\mathcal{E}}$ are either fixed or varying (i.e., equal to $\bar{\gamma}$). Table 1 summarizes all

[4]The concept of secrecy coding gain characterized the SNR advantages of the asymptotic probability of intercept. Various works in the literature have considered this in the case of secrecy outage probability (see for example [41])

TABLE 1. Possible scenarios corresponding to the combinations of $\bar{\gamma}_{I_{\mathcal{B}}}$, $\bar{\gamma}_{\mathcal{E}}$ and $\bar{\gamma}_{I_{\mathcal{E}}}$.

Scenario	$\bar{\gamma}_{I_{\mathcal{B}}}$	$\bar{\gamma}_{\mathcal{E}}$	$\bar{\gamma}_{I_{\mathcal{E}}}$
A	fixed	fixed	fixed
B	varying	fixed	fixed
C	fixed	fixed	varying
D	varying	fixed	varying
E	fixed	varying	fixed
F	varying	varying	fixed
G	fixed	varying	varying
H	varying	varying	varying

the possible scenarios for a given average SNR of the main channel $\bar{\gamma}_{\mathcal{B}}$, i.e., $\bar{\gamma}_{\mathcal{B}} = \bar{\gamma}$.[5] In the sequel, we are going to derive the diversity gains and coding gains corresponding to each scenario (*Scenario A* $\rightarrow$ *Scenario G*).

A. SCENARIO A: $\bar{\gamma}_{I_{\mathcal{B}}}$, $\bar{\gamma}_{\mathcal{E}}$ AND $\bar{\gamma}_{I_{\mathcal{E}}}$ ARE FIXED

In this scenario, it is assumed that $\bar{\gamma}_{I_{\mathcal{B}}}$, $\bar{\gamma}_{\mathcal{E}}$ and $\bar{\gamma}_{I_{\mathcal{E}}}$ are all fixed (constant values which are not necessarily identical). Substituting (17) in (11) and using the following approximation $e^{\frac{\eta}{\bar{\gamma}}} \approx 1 - \frac{\eta}{\bar{\gamma}}$ for $\bar{\gamma} \rightarrow \infty$, it is easy to obtain

$$f_{\gamma_{\mathcal{B}}}(\gamma) \approx \frac{\gamma^{N_{\mathcal{B}}-1}}{\bar{\gamma}_{\mathcal{B}}^{N_{\mathcal{B}}}(N_{\mathcal{B}}-1)!} \sum_{k=0}^{N_{\mathcal{B}}} \binom{N_{\mathcal{B}}}{k} (m_{I_{\mathcal{B}}} M_{\mathcal{B}})_k \left(\frac{\bar{\gamma}_{I_{\mathcal{B}}}}{m_{I_{\mathcal{B}}}}\right)^k. \tag{20}$$

Substituting (14) and (20) in (16), and after some manipulations and with the aid [37, eq. (3.383.5)], the asymptotic intercept probability is given by $P_{int}^{\infty} \approx G_c \bar{\gamma}^{-N_{\mathcal{B}}}$, where the secrecy diversity order is equal to the number of receive antennas at Bob, i.e., $N_{\mathcal{B}}$ and the secrecy coding gain is given by

$$\begin{aligned} G_c = & \left(\frac{1}{(N_{\mathcal{B}}-1)!} \sum_{k=0}^{N_{\mathcal{B}}} \binom{N_{\mathcal{B}}}{k} (m_{I_{\mathcal{B}}} M_{\mathcal{B}})_k \left(\frac{\bar{\gamma}_{I_{\mathcal{B}}}}{m_{I_{\mathcal{B}}}}\right)^k\right) \\ & \times \sum_{n=0}^{N_{\mathcal{E}}-1} \sum_{s=0}^{n} \frac{(m_{I_{\mathcal{E}}} M_{\mathcal{E}})_s}{n!} \binom{n}{s} \bar{\gamma}_{\mathcal{E}}^{N_{\mathcal{B}}} \left\{ \left(\frac{m_{I_{\mathcal{E}}}}{\bar{\gamma}_{I_{\mathcal{E}}}}\right)^{N_{\mathcal{B}}+n-s} \right. \\ & \times \Gamma(N_{\mathcal{B}}+n)(m_{I_{\mathcal{E}}} M_{I_{\mathcal{E}}})_{-N_{\mathcal{B}}-n_1} {}_1F_1(a_1, 1+b_1; z) \\ & \left. + \left(\frac{m_{I_{\mathcal{E}}}}{\bar{\gamma}_{I_{\mathcal{E}}}}\right)^{m_{I_{\mathcal{E}}} M_{I_{\mathcal{E}}}} \Gamma(b_1) {}_1F_1(a_2, 1+b_2; z) \right\}, \end{aligned} \tag{21}$$

where $a_1 = N_{\mathcal{B}} + n$, $b_1 = N_{\mathcal{B}} + n - m_{I_{\mathcal{E}}} M_{\mathcal{E}} - s$, $a_2 = m_{I_{\mathcal{E}}} M_{\mathcal{E}} + s$, $b_2 = m_{I_{\mathcal{E}}} M_{\mathcal{E}} + s - N_{\mathcal{B}} - n$, $z = \frac{m_{I_{\mathcal{E}}}}{\bar{\gamma}_{I_{\mathcal{E}}}}$ and ${}_1F_1(a, b; z)$ is the confluent hypergeometric function of the first kind defined in [37, eq. (9.210.1)]. From a diversity perspective, all other system parameters have no effect on the probability of intercept but rather on the coding gain as shown in (21). This scenario yields a low probability of intercept as the number of receive antennas $N_{\mathcal{B}}$ at Bob increases.. This can be explained by the fact the average SNR of the legitimate receiver $\bar{\gamma}_{\mathcal{B}}$ is infinitesimally large whereas $\bar{\gamma}_{I_{\mathcal{B}}}$, $\bar{\gamma}_{\mathcal{E}}$ and $\bar{\gamma}_{I_{\mathcal{E}}}$ are fixed, i.e., small with respect to the former. Intuitively, it can be inferred that the eavesdropper has little effect in intercepting the transmission between Alice and Bob and also the interferences affecting its antennas further act in favor of Bob or Alice (from a security point of view). Such a scenario can equally be compared to a system where Alice transmits to Bob with no outside interfering sources (no eavesdropper or any other form of interferences).

[5] We only consider these 8 possible scenarios for $\bar{\gamma}_{\mathcal{B}} = \bar{\gamma} \rightarrow \infty$ since we are interested in the diversity analysis at high SNR in this Section. Hence, the possible scenarios corresponding to fixed $\bar{\gamma}_{\mathcal{B}}$ are irrelevant here.

B. SCENARIO B: $\bar{\gamma}_{I_{\mathcal{B}}} = \bar{\gamma} \rightarrow \infty$, AND $\bar{\gamma}_{\mathcal{E}}$ AND $\bar{\gamma}_{I_{\mathcal{E}}}$ ARE FIXED

For a varying INR at Bob, it is assumed that $\bar{\gamma}_{I_{\mathcal{B}}} = \bar{\gamma}_{\mathcal{B}} = \bar{\gamma} \rightarrow \infty$. Hence, (11) can be rewritten as

$$\begin{aligned} f_{\gamma_{\mathcal{B}}}(\gamma) = & \frac{m_{I_{\mathcal{B}}}^{m_{I_{\mathcal{B}}} M_{\mathcal{B}}} \gamma^{N_{\mathcal{B}}-1} e^{-\frac{\gamma}{\bar{\gamma}_{\mathcal{B}}}}}{\bar{\gamma}_{\mathcal{B}}^{N_{\mathcal{B}}+m_{I_{\mathcal{B}}} M_{\mathcal{B}}} (N_{\mathcal{B}}-1)!} \\ & \times \Psi\left(m_{I_{\mathcal{B}}} M_{\mathcal{B}}, m_{I_{\mathcal{B}}} M_{\mathcal{B}} + N_{\mathcal{B}} + 1; \frac{\gamma + m_{I_{\mathcal{B}}}}{\bar{\gamma}}\right). \end{aligned} \tag{22}$$

For $z \rightarrow 0$, the confluent hypergeometric function of the second kind can be approximated as [40, eq. (13.2.16)]

$$\Psi(a, b; z) = \frac{\Gamma(b-1)}{\Gamma(a)} z^{1-b}. \tag{23}$$

Using (23) in (22) and the approximation $e^{-\frac{\gamma}{\bar{\gamma}}} \approx 1 - \frac{\gamma}{\bar{\gamma}}$ for $\bar{\gamma} \rightarrow \infty$ and after performing some manipulations, (22) can be given by

$$f_{\gamma_{\mathcal{B}}}(\gamma) = \frac{m_{I_{\mathcal{B}}}^{m_{I_{\mathcal{B}}} M_{\mathcal{B}}}}{(N_{\mathcal{B}}-1)!} (m_{I_{\mathcal{B}}} M_{\mathcal{B}})_{N_{\mathcal{B}}} \gamma^{N_{\mathcal{B}}-1} (\gamma + m_{I_{\mathcal{B}}})^{-\psi}. \tag{24}$$

where $\psi = m_{I_{\mathcal{B}}} M_{\mathcal{B}} + N_{\mathcal{B}}$. Taking (14) and (24) in (16) and with the aid of [37, eq. (3.197.1)], the intercept probability can be approximated as

$$\begin{aligned} P_{int}^{\infty} \approx & \frac{(m_{I_{\mathcal{B}}} M_{\mathcal{B}})_{N_{\mathcal{B}}}}{m_{I_{\mathcal{B}}}^{N_{\mathcal{B}}} (N_{\mathcal{B}}-1)!} \sum_{n=0}^{N_{\mathcal{E}}-1} \sum_{k=0}^{n} \binom{n}{k} \frac{(m_{I_{\mathcal{E}}} M_{\mathcal{E}})_k \bar{\gamma}_{\mathcal{E}}^{N_{\mathcal{B}}}}{n!} \\ & \times \sum_{j=0}^{\infty} \frac{(-1)^j}{j!} \left(\frac{m_{I_{\mathcal{E}}}}{\bar{\gamma}_{I_{\mathcal{E}}}}\right)^{N_{\mathcal{B}}+n+j-k} \\ & \times \mathrm{B}\left(N_{\mathcal{B}} + n + j, m_{I_{\mathcal{B}}} M_{\mathcal{B}} + m_{I_{\mathcal{E}}} M_{\mathcal{E}} + k - n - j\right) \\ & \times {}_2F_1\left(N_{\mathcal{B}} + m_{I_{\mathcal{B}}} M_{\mathcal{B}}, N_{\mathcal{B}} + n + j; \rho; \frac{\bar{\gamma}_{\mathcal{E}} m_{I_{\mathcal{E}}}}{\bar{\gamma}_{I_{\mathcal{E}}} m_{I_{\mathcal{B}}}}\right), \end{aligned} \tag{25}$$

where $\rho = N_{\mathcal{B}} + m_{I_{\mathcal{B}}} M_{\mathcal{B}} + m_{I_{\mathcal{E}}} M_{\mathcal{E}} + k$ and it can be observed that (25) is independent of $\bar{\gamma}$. This shows that regardless of the number of receive antennas at Bob or Eve, or any value of the fading parameter m_{I_χ} affecting the various branches at Bob or Eve, the secrecy diversity order is zero (error floor). Hence, in the high-SNR regime, the probability of the confidential message being intercepted remains high and does not decrease which shows a poor secure performance.

This scenario can be assimilated to one without the presence of the eavesdropper, i.e., a system where Alice transmits to Bob affected by some external interferences, since the average SNR at the eavesdropper is fixed as well as the interference power affecting it. For such a system, the diversity order is not affected neither by the eavesdropper nor by the interference signals affecting it but is rather dependent on Bob and the interference power affecting it and it is equal to zero as $\bar{\gamma}_{I_{\mathcal{B}}} = \bar{\gamma}_{\mathcal{B}} = \bar{\gamma} \to \infty$.

C. SCENARIO C: $\bar{\gamma}_{I_{\mathcal{B}}}$ AND $\bar{\gamma}_{\mathcal{E}}$ ARE FIXED, $\bar{\gamma}_{I_{\mathcal{E}}} = \bar{\gamma} \to \infty$

In this scenario, it is assumed that both $\bar{\gamma}_{I_{\mathcal{B}}}$ and $\bar{\gamma}_{\mathcal{E}}$ are constant while $\bar{\gamma}_{I_{\mathcal{E}}} = \bar{\gamma} \to \infty$. With the aid of (17) in (14), the CDF of the RV $\gamma_{\mathcal{E}}$ can be given by

$$F_{\gamma_{\mathcal{E}}}(\gamma) = 1 - \left(\frac{m_{I_{\mathcal{E}}}}{\bar{\gamma}}\right)^{m_{I_{\mathcal{E}}}M_{\mathcal{E}}} \exp\left(-\frac{\gamma}{\bar{\gamma}_{\mathcal{E}}}\right) \sum_{n=0}^{N_{\mathcal{E}}-1} \frac{1}{n!} \sum_{s=0}^{s} \binom{n}{s} \times (m_{I_{\mathcal{E}}}M_{\mathcal{E}})_s \left(\frac{\gamma}{\bar{\gamma}_{\mathcal{E}}}\right)^{n-m_{I_{\mathcal{E}}}M_{\mathcal{E}}-s}. \quad (26)$$

Substituting (20) and (26) in (16), and after performing some manipulations and using [37, eq. (3.351.3)], the asymptotic intercept probability at high SNR is given by $P_{int}^{\infty} = G_c \bar{\gamma}^{-(N_{\mathcal{B}}+m_{I_{\mathcal{E}}}M_{\mathcal{E}})}$, which shows a diversity gain equal to $N_{\mathcal{B}}+m_{I_{\mathcal{E}}}M_{\mathcal{E}}$, and G_c is given by

$$G_c = \frac{m_{I_{\mathcal{E}}}^{m_{I_{\mathcal{E}}}M_{\mathcal{E}}} \bar{\gamma}_{\mathcal{E}}^{N_{\mathcal{B}}}}{(N_{\mathcal{B}}-1)} \sum_{k=0}^{N_{\mathcal{B}}} \binom{N_{\mathcal{B}}}{k} (m_{I_{\mathcal{B}}}M_{\mathcal{B}})_k \left(\frac{\bar{\gamma}_{I_{\mathcal{B}}}}{m_{I_{\mathcal{B}}}}\right)^k \times \sum_{n=0}^{N_{\mathcal{E}}-1} \frac{1}{n!} \sum_{s=0}^{n} \binom{n}{s} (m_{I_{\mathcal{E}}}M_{\mathcal{E}})_s \Gamma\left(N_{\mathcal{B}}+n-m_{I_{\mathcal{E}}}M_{\mathcal{E}}-s\right). \quad (27)$$

For a fixed $\bar{\gamma}_{\mathcal{E}}$ and varying $\bar{\gamma}_{I_{\mathcal{E}}} = \bar{\gamma} \to \infty$, one can intuitively deduce that the latter plays to the advantage of Bob by increasing the transmission security. In this scenario, from the derived asymptotic intercept probability, it can be observed that the secrecy diversity order is given by $N_{\mathcal{B}} + m_{I_{\mathcal{E}}}M_{\mathcal{E}}$. A high value of $m_{I_{\mathcal{E}}}$, i.e., light interference fading on the diversity branches of the eavesdropper or a high number of interferers affecting the eavesdropper $M_{\mathcal{E}}$ yields a high secrecy diversity order. Also, one can note that an increase in the number of receive antennas at Bob decreases the probability of intercept leading to an improvement of the security performance of the underlying scheme.

D. SCENARIO D: $\bar{\gamma}_{I_{\mathcal{B}}} = \bar{\gamma}_{I_{\mathcal{E}}} = \bar{\gamma} \to \infty$, AND $\bar{\gamma}_{\mathcal{E}}$ IS FIXED

In *Scenario D*, we assume that $\bar{\gamma}_{I_{\mathcal{B}}} = \bar{\gamma}_{I_{\mathcal{E}}} = \bar{\gamma} \to \infty$. Using (24) and (26) in (16), and after many algebraic manipulations and with the aid of [37, eq. (3.194.3)], the intercept probability at high SNR can be approximated as $P_{int}^{\infty} \approx G_c \bar{\gamma}^{-m_{\mathcal{E}}M_{\mathcal{E}}}$, where the diversity is deduced to be $m_{I_{\mathcal{E}}}M_{\mathcal{E}}$ and the constant G_c is given by

$$G_c = \frac{m_{I_{\mathcal{B}}}^{m_{I_{\mathcal{B}}}M_{\mathcal{B}}} m_{I_{\mathcal{E}}}^{m_{I_{\mathcal{E}}}M_{\mathcal{E}}}}{(N_{\mathcal{B}}-1)!} (m_{I_{\mathcal{B}}}M_{\mathcal{B}})_{N_{\mathcal{B}}} \sum_{n=0}^{N_{\mathcal{E}}-1} \frac{1}{n!} \sum_{s=0}^{n} \binom{n}{s} \times (m_{I_{\mathcal{E}}}M_{\mathcal{E}})_s \bar{\gamma}_{\mathcal{E}}^{m_{I_{\mathcal{E}}}M_{\mathcal{E}}+s-n} \left\{ m_{I_{\mathcal{B}}}^{n-m_{I_{\mathcal{E}}}M_{\mathcal{E}}-m_{I_{\mathcal{B}}}M_{\mathcal{B}}-s} \times (m_{I_{\mathcal{B}}}M_{\mathcal{B}})_{m_{I_{\mathcal{B}}}M_{\mathcal{B}}+s-N_{\mathcal{B}-n1}} F_1\left(a_4, b_4; \frac{m_{I_{\mathcal{B}}}}{\bar{\gamma}_{\mathcal{E}}}\right) \times \left(\frac{1}{\bar{\gamma}_{\mathcal{E}}}\right)^{m_{I_{\mathcal{B}}}M_{\mathcal{B}}+m_{I_{\mathcal{E}}}M_{\mathcal{E}}+s-n} {}_1F_1\left(a_5, b_5; \frac{m_{I_{\mathcal{B}}}}{\bar{\gamma}_{\mathcal{E}}}\right) \right\}, \quad (28)$$

where $a_3 = n-m_{I_{\mathcal{E}}}M_{\mathcal{E}}-s$, $a_4 = N_{\mathcal{B}}+a_3$, $b_4 = 1+m_{I_{\mathcal{B}}}M_{\mathcal{B}}-a_3$, $a_5 = N_{\mathcal{B}} + m_{I_{\mathcal{B}}}M_{\mathcal{B}}$ and $1 + m_{I_{\mathcal{B}}}M_{\mathcal{B}} + s - m_{I_{\mathcal{E}}}M_{\mathcal{E}} - n$. This scenario is equivalent to a system where Alice transmits to Bob with the help of $M_{\mathcal{E}}$ interfering sources at the eavesdropper. In this scenario, a varying INR affecting Bob yields an intercept probability that does not depend on the number of receive antennas at high SNR but rather improve with an increase in the number of interference sources $M_{\mathcal{E}}$ or the fading parameter $m_{I_{\mathcal{E}}}$ affecting the eavesdropper.

E. SCENARIO E: $\bar{\gamma}_{I_{\mathcal{B}}}$ AND $\bar{\gamma}_{I_{\mathcal{E}}}$ ARE FIXED, AND $\bar{\gamma}_{\mathcal{E}} = \bar{\gamma} \to \infty$

Unlike *Scenarios A–D* where $\bar{\gamma}_{\mathcal{E}}$ is fixed, *Scenario E* assumes that $\bar{\gamma}_{\mathcal{E}} = \bar{\gamma} \to \infty$. By replacing $N_{\mathcal{B}}$, $m_{I_{\mathcal{B}}}$, $M_{\mathcal{B}}$, $\gamma_{I_{\mathcal{B}}}$ by $N_{\mathcal{E}}$, $m_{I_{\mathcal{E}}}$, $M_{\mathcal{E}}$, $\gamma_{I_{\mathcal{E}}}$ respectively in (20), it is easy to obtain the CDF $F_{\gamma_{\mathcal{E}}}(\gamma)$. However, substituting the resulting expression and (20) in (16) does not yield a simple and explicit asymptotic intercept probability. To circumvent this, (18) is used and with the help of [37, eq. (3.351.3)] and the approximation $e^{-\frac{1}{x}} \approx e^{-\frac{\kappa}{x}}$ for $x \to \infty$ where κ is a constant, we obtain

$$P_{int}^{\infty} \approx \frac{1}{(N_{\mathcal{B}}-1)!} \sum_{n}^{N_{\mathcal{E}}-1} \frac{\kappa^{-N_{\mathcal{B}}-n}}{n!} \sum_{i=0}^{N_{\mathcal{B}}} \sum_{j=0}^{N_{\mathcal{E}}} \binom{N_{\mathcal{B}}}{i} \binom{N_{\mathcal{E}}}{j} \times (m_{I_{\mathcal{B}}}M_{\mathcal{B}})_i (m_{I_{\mathcal{E}}}M_{\mathcal{E}})_j \left(\frac{\bar{\gamma}_{I_{\mathcal{B}}}}{m_{I_{\mathcal{B}}}}\right)^i \left(\frac{\bar{\gamma}_{I_{\mathcal{E}}}}{m_{I_{\mathcal{E}}}}\right)^j. \quad (29)$$

It can be seen that (29) is independent of $\bar{\gamma}$, hence the secrecy diversity gain is zero resulting in an error floor (no improvement in the system security performance) in the high-SNR regime regardless of the number of receive antennas at either Bob/Eve and the fading parameters of the interference channels affecting either of the aforementioned node. For fixed INR at both the legitimate receiver and eavesdropper and with varying $\bar{\gamma}_{\mathcal{E}}$, this system is analogous to one where the transmission between Alice and Bob is affected by a varying source of interference which in this case is played by the eavesdropper. As $\bar{\gamma}_{\mathcal{E}}$ and $\bar{\gamma}_{\mathcal{B}}$ both tend to ∞, no diversity can be achieved as corroborated by the aforementioned analysis.

F. SCENARIO F: $\bar{\gamma}_{I_{\mathcal{B}}} = \bar{\gamma}_{\mathcal{E}} = \bar{\gamma} \to \infty$, AND $\bar{\gamma}_{I_{\mathcal{E}}}$ IS FIXED

Using (20), the CDF $F_{\gamma_{\mathcal{E}}}(\gamma)$ is obtained and expressed as

$$F_{\gamma_{\mathcal{E}}}(\gamma) = \frac{\gamma^{N_{\mathcal{E}}}}{\bar{\gamma}^{N_{\mathcal{E}}} N_{\mathcal{E}}!} \sum_{k=0}^{N_{\mathcal{E}}} \binom{N_{\mathcal{E}}}{k} (m_{I_{\mathcal{E}}} M_{\mathcal{E}})_k \left(\frac{\bar{\gamma}_{I_{\mathcal{E}}}}{m_{I_{\mathcal{E}}}}\right)^k. \quad (30)$$

Substituting (24) and (30) in (16), the asymptotic intercept probability can be obtained using [37, eq. (3.194.3)] and is given by

$$P_{int}^{\infty} \approx 1 - \frac{1}{\bar{\gamma}^{N_{\mathcal{E}}}} \left\{ \frac{(m_{I_{\mathcal{B}}} M_{\mathcal{B}})_{N_{\mathcal{B}}} m_{I_{\mathcal{B}}}^{N_{\mathcal{E}}}}{N_{\mathcal{E}}!(N_{\mathcal{B}}-1)!} \sum_{k=0}^{N_{\mathcal{E}}} \binom{N_{\mathcal{E}}}{k} \left(\frac{\bar{\gamma}_{I_{\mathcal{E}}}}{m_{I_{\mathcal{E}}}}\right)^k \times (m_{I_{\mathcal{E}}} M_{\mathcal{E}})_k \mathrm{B}\big(N_{\mathcal{B}} + N_{\mathcal{E}}, m_{I_{\mathcal{B}}} M_{\mathcal{B}} - N_{\mathcal{E}}\big) \right\}, \quad (31)$$

where the second term of the summation in (31) rapidly diminishes as $\bar{\gamma} \to \infty$. Hence, the asymptotic intercept probability approaches unity at high SNR which represents the secrecy coding gain and therefore shows a zero secrecy diversity order regardless of the fading characteristics of the interference channels and the number of antennas at Bob/Eve. This can be explained as follows: as the effects of the impairments affecting Bob become significant, i.e., $\bar{\gamma}_{I_{\mathcal{B}}} = \bar{\gamma}_{\mathcal{E}} = \bar{\gamma} \to \infty$, when the interference sources affecting the eavesdropper have minimal effect due to its fixed INR, one can deduce by intuition that the wireless transmission between Alice and Bob is likely to be intercepted almost all the time. Therefore, the resulting probability of intercept approaches one as the main average SNR increases as shown in (31).

G. SCENARIO G: $\bar{\gamma}_{I_{\mathcal{B}}}$ IS FIXED, AND $\bar{\gamma}_{\mathcal{E}} = \bar{\gamma}_{I_{\mathcal{E}}} = \bar{\gamma} \to \infty$

As $\bar{\gamma}_{\mathcal{E}} = \bar{\gamma}_{I_{\mathcal{E}}} = \bar{\gamma} \to \infty$, the asymptotic intercept probability for this scenario can be obtained using (18) and with the help of [37, eq. (3.194.3)] and is expressed as

$$P_{int}^{\infty} \approx \frac{1}{\bar{\gamma}^{N_{\mathcal{B}}}} \left\{ \frac{1}{(N_{\mathcal{B}}-1)!} \sum_{i=0}^{N_{\mathcal{B}}} \binom{N_{\mathcal{B}}}{i} (m_{I_{\mathcal{B}}} M_{\mathcal{B}})_i \left(\frac{\bar{\gamma}_{I_{\mathcal{B}}}}{m_{I_{\mathcal{B}}}}\right)^i \times \sum_{n=0}^{N_{\mathcal{E}}-1} \frac{1}{n!} \sum_{j=0}^{n} \binom{n}{j} (m_{I_{\mathcal{E}}} M_{\mathcal{E}})_j m_{I_{\mathcal{E}}}^{N_{\mathcal{B}}+n-j} \times \mathrm{B}\big(N_{\mathcal{B}} + n, m_{I_{\mathcal{E}}} M_{\mathcal{E}} + j - N_{\mathcal{B}} - n\big) \right\}, \quad (32)$$

which shows a secrecy diversity gain equal to the number of receive antennas mounted at Bob, i.e., $N_{\mathcal{B}}$. This scenario shows that the intercept probability behavior in the high-SNR regime is dictated solely by $N_{\mathcal{B}}$. In addition, the intercept probability can also be improved but not from a secrecy diversity order viewpoint, by varying the fading parameters of the interference signals and the structure of the eavesdropper (increase in the number of antennas at Eve). As $\bar{\gamma}_{\mathcal{E}}$ and $\bar{\gamma}_{I_{\mathcal{E}}}$ grow infinitesimally large, the effect of the eavesdropper on the wireless transmission is greatly reduced. Additionally, a fixed INR affecting Bob has little effect on the security of the transmission in the high-SNR regime. Hence, from an intercept probability point of view, the diversity order is only dependent on the number of antennas at Bob which corroborates (32).

H. SCENARIO H: $\bar{\gamma}_{I_{\mathcal{B}}} = \bar{\gamma}_{\mathcal{E}} = \bar{\gamma}_{I_{\mathcal{E}}} = \bar{\gamma} \to \infty$

For this scenario, we first derive the CDF of the RV $\gamma_{\mathcal{E}}$. Using (24) and [37, eq. (3.194.1)] it is easy to obtain CDF of $\gamma_{\mathcal{E}}$ which is given by

$$F_{\gamma_{\mathcal{E}}}(\gamma) = \frac{(m_{I_{\mathcal{E}}} M_{\mathcal{E}})_{N_{\mathcal{E}}}}{N_{\mathcal{E}}! m_{I_{\mathcal{E}}}^{N_{\mathcal{E}}}} \gamma^{N_{\mathcal{E}}-1} \times {}_2F_1\left(N_{\mathcal{E}}, m_{I_{\mathcal{E}}} M_{\mathcal{E}} + N_{\mathcal{E}}, 1 + N_{\mathcal{E}}; -\frac{\gamma}{m_{I_{\mathcal{E}}}}\right). \quad (33)$$

Substituting (24) and (33) in (16) yields the asymptotic expression of the intercept probability given by

$$P_{int}^{\infty} \approx 1 - \frac{m_{I_{\mathcal{B}}}^{m_{I_{\mathcal{B}}} M_{\mathcal{B}}}}{N_{\mathcal{E}}!(N_{\mathcal{B}}-1)! m_{I_{\mathcal{E}}}^{N_{\mathcal{E}}}} \big(m_{I_{\mathcal{B}}} M_{\mathcal{B}}\big)_{N_{\mathcal{B}}} \big(m_{I_{\mathcal{E}}} M_{\mathcal{E}}\big)_{N_{\mathcal{E}}} \times \int_0^{\infty} \gamma_{\mathcal{B}}^{N_{\mathcal{B}}+N_{\mathcal{E}}-1} \big(\gamma_{\mathcal{B}} + m_{I_{\mathcal{B}}}\big)^{-m_{I_{\mathcal{B}}} M_{\mathcal{B}} - N_{\mathcal{B}}} \times {}_2F_1\left(N_{\mathcal{E}}, m_{I_{\mathcal{E}}} M_{\mathcal{E}} + N_{\mathcal{E}}, 1 + N_{\mathcal{E}}; -\frac{\gamma_{\mathcal{B}}}{m_{I_{\mathcal{E}}}}\right) \mathrm{d}\gamma_{\mathcal{B}}. \quad (34)$$

The integral in (34) is complicated to obtain in closed form. However, it can be evaluated numerically to yield a constant value. Therefore, (34) is independent of the average SNR which shows that the secrecy diversity order is equal to zero. Therefore an error floor exists in the high-SNR regime of intercept probability performance regardless of the fading characteristics of the interference signals and the number interference sources at both the legitimate receiver and the eavesdropper. This can be explained by noticing that as $\bar{\gamma}_{\mathcal{E}} = \bar{\gamma}_{I_{\mathcal{E}}} \to \infty$, the effect of the eavesdropper on the transmission is very minimal. On the other hand, as $\bar{\gamma}_{I_{\mathcal{B}}} \to \infty$, the interference sources affecting Bob significantly degrade the main channel. Given that the average main channel SNR also grows infinitesimally large, this will result in a zero-diversity order as shown by the asymptotic intercept probability in (34).

From the comprehensive asymptotic analysis of the intercept probability provided for scenarios *A*-*H*, it can be seen that the maximum diversity order is given by $G_d^{\max} = N_{\mathcal{B}} + m_{I_{\mathcal{E}}} M_{\mathcal{E}}$ whereas the minimum secrecy diversity order is $G_d^{\min} = 0$. One can also observe that secrecy diversity order depends on the physical structure of the intended receiver (i.e., on the number of receive antennas mounted on Bob) and/or the number of interference sources and the fading parameter of the interference signals affecting the eavesdropper.

V. NUMERICAL RESULTS AND DISCUSSION

In this section, we provide some simulations and numerical results to highlight the impact of interference on the secrecy performance of SIMOME using MRC and to assess the accuracy of the proposed analytical framework. It is worth

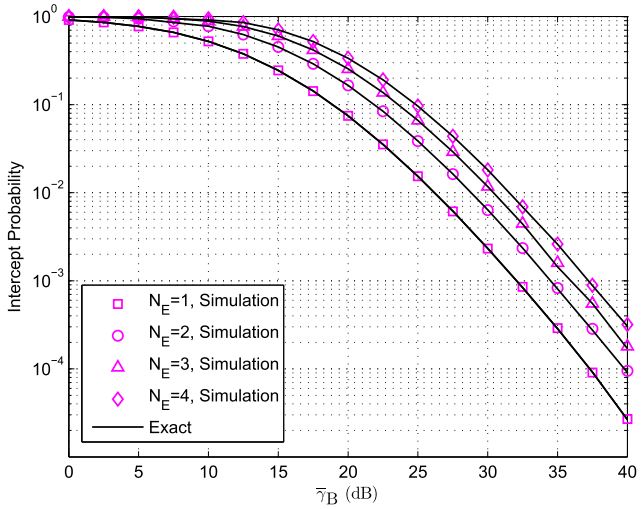

FIGURE 2. Simulated, exact intercept probability versus main channel average SNR for various number of antennas at the eavesdropper N_E with $\bar{\gamma}_{\mathcal{E}} = \bar{\gamma}_{I_{\mathcal{B}}} = \bar{\gamma}_{I_{\mathcal{E}}} = 15$dB, $M_{\mathcal{B}} = 3$, $M_{\mathcal{E}} = 4$, $m_{I_{\mathcal{B}}} = 3$ and $m_{I_{\mathcal{E}}} = 0.65$.

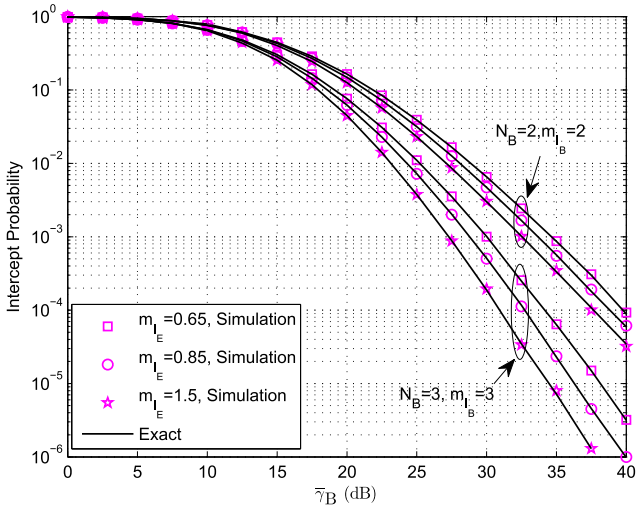

FIGURE 3. Simulated, exact intercept probability versus main channel average SNR for various Nakagami fading parameters $m_{I_{\mathcal{E}}}$ affecting the antennas of the eavesdropper with $\bar{\gamma}_{\mathcal{E}} = \bar{\gamma}_{I_{\mathcal{B}}} = \bar{\gamma}_{I_{\mathcal{E}}} = 15$dB, $N_{\mathcal{E}} = 2$, $M_{\mathcal{B}} = 3$ and $M_{\mathcal{E}} = 4$.

mentioning that for the numerical evaluation, the values are chosen without loss of generality.

Fig. 2 illustrates the intercept probability of the underlying scheme with various number of antennas at Eve. It is clear that the exact curves are in precise agreement with the Monte-Carlo simulations in all cases. Furthermore, the intercept probability becomes smaller as $N_{\mathcal{E}}$ decreases for the same number of interference at the eavesdropper. This is because such interfering signals will have more detrimental effects on a single-antenna eavesdropper than on a 4-antenna eavesdropper. Such effects will impede the eavesdropper in its quest to intercept the message intended for the receiver, and therefore reduce the probability that this event occurs. This means that interfering signals affecting the eavesdropper can enhance the PHY security against eavesdropping attacks especially when the number of receive antennas of the unauthorized user decreases.

In Fig. 3, we show both the simulated and exact intercept probability with various Nakagami fading parameters of the interfering channels affecting the eavesdropper, i.e $m_{I_{\mathcal{E}}}$. Firstly, we observe that the simulated results closely match the exact intercept probability. Secondly, it can be seen that as the Nakagami fading parameter $m_{I_{\mathcal{E}}}$ increases for fixed values of $N_{\mathcal{B}}$ and $m_{I_{\mathcal{B}}}$, the wiretap links deteriorate. Intuitively, the deterioration of the wiretap channels leads to the improvement of the wireless PHY security. For low values of $m_{I_{\mathcal{E}}}$ (more severe fading), i.e. as $m_{I_{\mathcal{E}}}$ decreases, the interferers have less severe impact on the performance of the wiretap channels from a capacity point of view, and hence the event that an intercept may occur is highly probable. On the other hand, for less severe faded interferers (i.e., as $m_{I_{\mathcal{E}}}$ increases), the wiretap channel is more impacted leading to a smaller probability of intercept. Similarly, for fixed $m_{I_{\mathcal{E}}}$, as the Nakagami fading parameter $m_{I_{\mathcal{B}}}$ affecting the legitimate receiver changes, the intercept probability is also affected. We also note from Fig. 3 that the impact of the interferers affecting Bob and Eve on the intercept probability differs as the Nakagami fading parameters varies, namely the performance gap with varying $m_{I_{\mathcal{E}}}$ is greater than the one with varying $m_{I_{\mathcal{B}}}$. This implies that the Nakagami faded interferers on the eavesdropper as opposed to the legitimate receiver, greatly impact the intercept probability.

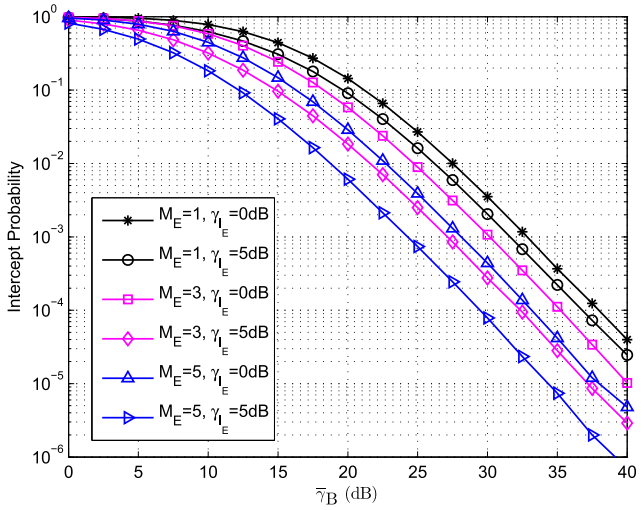

FIGURE 4. Simulated, exact intercept probability versus main channel average SNR for various number of interferers $M_{\mathcal{E}}$ and INR $\bar{\gamma}_{I_{\mathcal{E}}}$ with $\bar{\gamma}_{\mathcal{E}} = \bar{\gamma}_{I_{\mathcal{B}}} = 5$dB, $N_{\mathcal{B}} = 2$, $M_{\mathcal{B}} = 3$, $N_{\mathcal{E}} = 3$.

Fig. 4 plots the intercept probability for different values of $M_{\mathcal{E}}$ and different values of $\bar{\gamma}_{I_{\mathcal{E}}}$ where $\bar{\gamma}_{\mathcal{E}}$ and $\bar{\gamma}_{I_{\mathcal{B}}}$ are fixed at 15dB. For fixed $M_{\mathcal{E}}$, the underlying scheme is more secure from a PHY security point of view when $\bar{\gamma}_{I_{\mathcal{E}}} = 5$dB as opposed to $\bar{\gamma}_{I_{\mathcal{E}}} = 0$dB, since the intercept probability is lower for the former than for the latter. This observation is similar for $M_{\mathcal{E}} = 3$ and $M_{\mathcal{E}} = 5$. This is because, a high

interfering power at the eavesdropper will negatively impact its performance and therefore the event of intercepting Bob's message is likely to reduce.

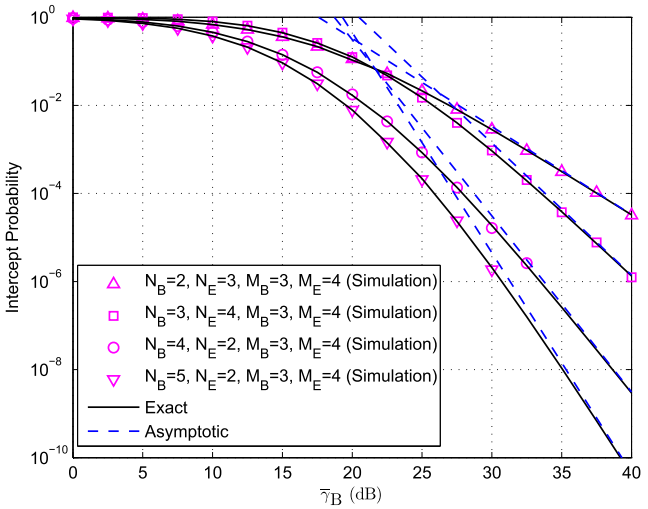

FIGURE 5. Simulated, exact and asymptotic intercept probability versus main channel average SNR for $\bar{\gamma}_{\mathcal{E}} = \bar{\gamma}_{I_{\mathcal{B}}} = \bar{\gamma}_{I_{\mathcal{E}}} = 15$dB, $m_{I_{\mathcal{B}}} = 0.65$ and $m_{I_{\mathcal{E}}} = 3$.

Fig. 5 depicts *scenario A* and compares the simulated, exact and asymptotic intercept probability for fixed $\bar{\gamma}_{I_{\mathcal{B}}}$, $\bar{\gamma}_{I_{\mathcal{E}}}$ and $\bar{\gamma}_{\mathcal{E}}$, and Nakagami fading parameters $m_{I_{\mathcal{B}}} = 0.65$ and $m_{I_{\mathcal{E}}} = 3$. It is observed from Fig. 5 that both the simulated and exact intercept probability closely match the asymptotic one in the high-SNR regime. Without loss of generality, the following parameters are used for the simulations (Fig. 5 only): $M_{\mathcal{B}} = 3$ and $M_{\mathcal{E}} = 4$. Further, one can see that as the number of antennas at Bob $N_{\mathcal{B}}$ increases, the intercept probability significantly decreases which corroborates our proposed diversity analysis. This observation shows that the wireless security improves with an increase in the number of antennas at the legitimate receiver. On the contrary, comparison of the simulated and asymptotic intercept probability is shown in Fig. 6 for $\bar{\gamma}_{I_{\mathcal{B}}} \to \infty$ and fixed $\bar{\gamma}_{I_{\mathcal{E}}}$ and $\bar{\gamma}_{\mathcal{E}}$ representing *scenario B*. Both the simulated and asymptotic curves agree in the high-SNR region for various cases. In addition, it can be seen that the intercept probability remain constant in that region (error floor) regardless of the number of antennas $N_{\mathcal{B}}$ showing a degradation in the PHY security of the underlying system.

In Fig. 7, we show the asymptotic and simulated probability of intercept corresponding to *Scenario C*. It can be observed that both the simulated and asymptotic curves are in good agreement in the high-SNR region. Moreover, the achievable diversity for this scenario is equal to $N_{\mathcal{B}} + m_{I_{\mathcal{E}}} M_{\mathcal{E}}$ which corroborates our diversity analysis. These results show that the interferences affecting the eavesdropper with a varying INR provides more secure degree of freedom to the wireless system, especially when the effect of the such interferences is stronger. This is in agreement with the results presented in Fig. 4 where it is shown that an increase in the INR yields a decrease in the intercept

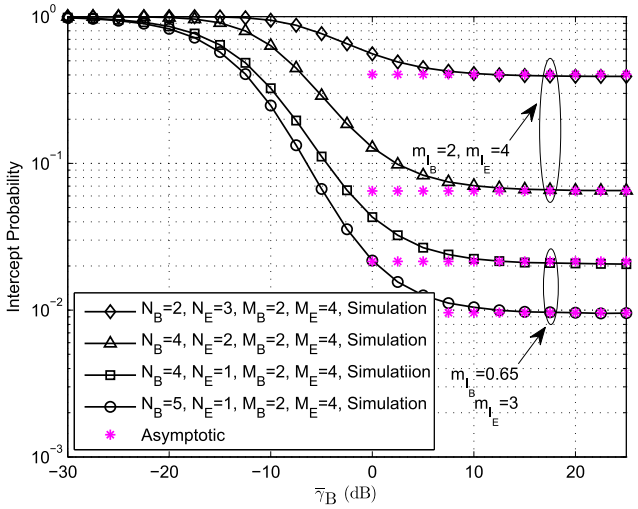

FIGURE 6. Simulated and asymptotic intercept probability versus main channel average SNR for varying $\bar{\gamma}_{I_{\mathcal{B}}}$, $\bar{\gamma}_{\mathcal{E}} = \bar{\gamma}_{I_{\mathcal{E}}} = 15$dB, and various Nakagami fading parameters $m_{I_{\mathcal{B}}}$ and $m_{I_{\mathcal{E}}}$.

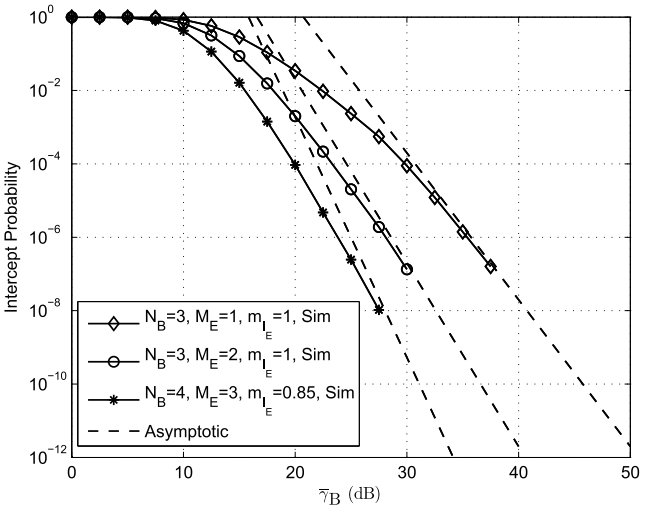

FIGURE 7. Simulated and asymptotic intercept probability versus main channel average SNR for $\bar{\gamma}_{\mathcal{E}} = \bar{\gamma}_{I_{\mathcal{B}}} = 10$dB, $m_{I_{\mathcal{B}}} = 3$.

probability and therefore provides more security to the wireless transmission.

Fig. 8 depicts *scenario D* with a varying $\bar{\gamma}_{I_{\mathcal{E}}}$ as opposed to *Scenario B* where $\bar{\gamma}_{I_{\mathcal{E}}}$ is fixed. It is noted from Fig. 8 that diversity of the system is a function of the interfering Nakagami fading $m_{I_{\mathcal{E}}}$ and the number of interfering sources $M_{\mathcal{E}}$. For fixed values of $m_{I_{\mathcal{E}}} = 0.65$ and $M_{\mathcal{E}}$, the diversity of the intercept probability remains unchanged as $N_{\mathcal{B}}$ increases. However, it should be pointed that such an increase in the number of antennas at Bob yields a decrease in the probability of intercept from a coding gain point of view. A drastic decrease in the intercept probability is achieved when either $m_{I_{\mathcal{E}}}$ or $M_{\mathcal{E}}$ increases and therefore provides a better security of the wireless transmission. For this scenario, an extra secure degree of freedom is achieved as opposed to *Scenario D*

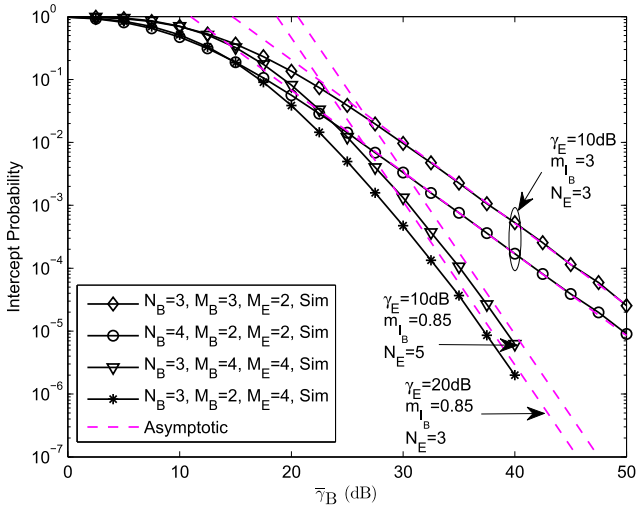

FIGURE 8. Simulated and asymptotic intercept probability versus main channel average SNR for varying $\bar{\gamma}_{I_B}$ and $\bar{\gamma}_{I_E}$, $m_{I_E} = 0.65$.

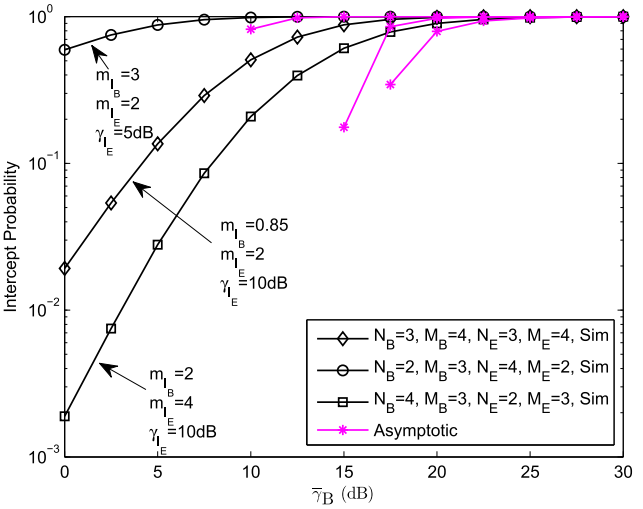

FIGURE 10. Simulated and asymptotic intercept probability versus main channel average SNR for varying $\bar{\gamma}_{I_B}$ and $\bar{\gamma}_E$, and various Nakagami fading parameters m_{I_B} and m_{I_E}.

with fixed $\bar{\gamma}_{I_E}$ (See Fig. 6) where no security improvement is guaranteed from medium to high SNR. The results in Fig. 8 show that strong inteference on the eavesdropper provides security improvement of the wireless transmission when the average SNR of the eavesdropper $\bar{\gamma}_E$ is fixed.

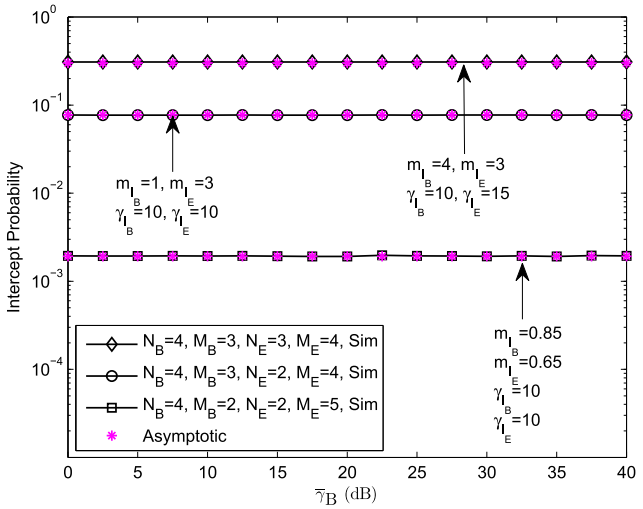

FIGURE 9. Simulated and asymptotic intercept probability versus main channel average SNR for varying $\bar{\gamma}_E$, and various interfering Nakagami fading parameters m_{I_B} and m_{I_E}.

Fig. 5–Fig. 8 depict the scenarios in which the average SNR of the eavesdropper is fixed. In what follows, we present the results for the scenarios where $\bar{\gamma}_E$ is varying. In Fig. 9, the security performance of the underlying system in terms of intercept probability is presented for *Scenario E*. Although the intercept probability can be low in some instances as it is the case for $N_B = 4, M_B = 2, N_E = 2, M_E = 5$ (see Fig. 9), it remains constant from low to high SNR. Our results show that for this scenario a varying $\bar{\gamma}_E$ does not provide an improvement of the PHY security of the transmission as the main average SNR increases. This can be seen by the achieved diversity gain of the system which is zero and confirmed by the diversity analysis provided.

Fig. 10 presents the intercept probability for *Scenario F*. It can be seen that the intercept probability increases and converges to one as the average SNR increases which is tantamount to the deterioration of the PHY security. This scenario yields the worst security performance in terms of probability of intercept. This is due to the fact as the INR affecting Bob increases ($\bar{\gamma}_{I_B} \to \infty$), it affects Bob's ability to successfully receive the message sent by Alice. Simultaneously, the average SNR of the eavesdropper increases ($\bar{\gamma}_E \to \infty$) and has a detrimental effect on the security of performance of the system. Combining the aforementioned cases ($\bar{\gamma}_{I_B} = \bar{\gamma}_E = \bar{\gamma} \to \infty$) with fixed $\bar{\gamma}_{I_E}$ which has little effect in interfering with the eavesdropper's ability to intercept the transmission between Alice and Bob, the event of an intercept is certain to occur. As can be seen in the figure, the probability that Eve intercepts the message intended for Bob approaches one in the high-SNR regime ($\bar{\gamma} \to \infty$). Moreover, both the simulated and asymptotic intercept probability are in good agreement in the high SNR.

Fig. 11 shows the intercept probability performance corresponding to *Scenario G* for some interfering Nakagami fading parameters and $N_B = 2, N_B = \{2, 4\}, N_E = 3$ and $M_B = 5$. It can be seen that the achievable diversity gain for both curves is two which is equivalent to the number of antennas placed at Bob, i.e., N_B. This is in precise agreement with the diversity analysis proposed for this scenario. In Fig. 12, we depict *Scenario H* for various interfering Nakagami fading parameters and $M_E = 5$. It can be seen that the diversity gain is equal to zero which is tantamount to no PHY security improvement of the system especially from medium to high SNR. In addition, the simulated intercept probability corroborates with the proposed diversity analysis.

In Fig. 2–Fig. 12, we have illustrated the intercept probability performance of the underlying scheme. In the sequel,

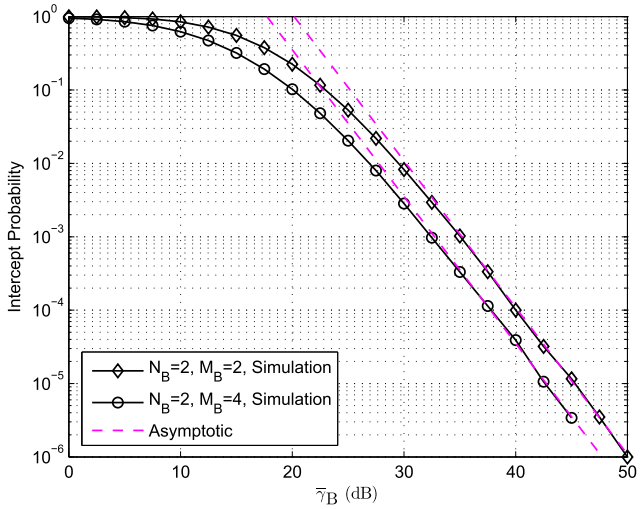

FIGURE 11. Simulated and asymptotic intercept probability versus main channel average SNR for $\bar{\gamma}_{I_{\mathcal{B}}} = 15$dB, $m_{I_{\mathcal{B}}} = 0.65$ and $m_{I_{\mathcal{E}}} = 1$, $N_{\mathcal{E}} = 3$ and $M_{\mathcal{E}} = 5$.

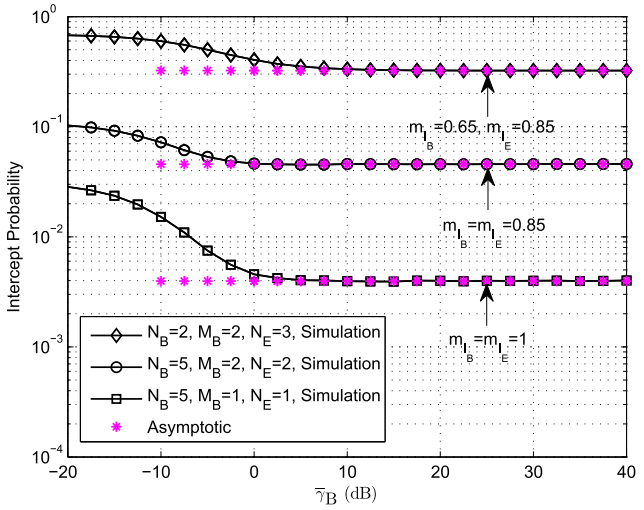

FIGURE 12. Simulated and asymptotic intercept probability versus main channel average SNR corresponding to *Scenario H*, for $M_{\mathcal{E}} = 5$.

we provide a summary of the important design insights for improving the security of the SIMOME wiretap channels with MRC in the presence of CCI. As shown in Section IV, the intercept probability can be improved for *Scenarios A*, *C*, *D* and *G* as the average main channel SNR $\bar{\gamma}_{\mathcal{B}}$ increases. In the aforementioned scenarios, it can be noted that both $\bar{\gamma}_{I_{\mathcal{E}}}$ and $\bar{\gamma}_{\mathcal{E}}$ play a major role in improving the PHY security of the scheme under consideration. However, the average SNR of the eavesdropper $\bar{\gamma}_{\mathcal{E}}$ cannot easily be controlled by the system designer. On the other hand, the interference signals affecting the eavesdropper can be used and adjusted by the designer to have the same functions as cooperative jamming signals (i.e., confound the undesired signals) since such signals originate from other sources operating in the same frequency band as Alice and close enough to the eavesdropper. It can be implied that, the latter is viable from an implementation perspective for improving the security of the wireless transmission of the scheme under consideration.

VI. CONCLUSIONS

We have investigated the joint impact of CCI and Nakagami fading on the secrecy performance of a SIMOME. We have derived a closed-form expression for the exact intercept probability. In addition, simple and explicit asymptotic expressions are obtained. Our results reveal that the impact of the Nakagami faded CCI on Eve or Bob affect the system performance from a wireless security viewpoint. Depending on the severity of the fading affecting either Eve or Bob, as well as the INR at Bob or Eve, the security performance can improve or deteriorate. It is shown that, as the interferers power increases or the Nakagami fading parameter increases, the intercept probability decreases showing an improvement of the wireless security. Also, as the number of antennas at the eavesdropper increases, the intercept probability decreases with the effect of CCI. Although, CCI negatively impacts Bob, its effect on Eve can be used to the advantage of Alice by providing an increasing security of the wireless transmission. Such interference sources inadvertently play the role of jammers for Alice. Further, we have studied asymptotically the impact of the INRs at the legitimate receiver and the eavesdropper (varying or fixed), and the average SNR of the eavesdropper (varying/fixed) on the PHY security of the wireless transmission. Finally, Monte-Carlo simulations have been conducted to verify the accuracy of our analytical work.

APPENDIX

Using the expressions (9) and (10) in (8), the resulting expression is given by

$$f_{\gamma_\chi}(\gamma) = \frac{\gamma^{N_\chi - 1} e^{-\frac{\gamma}{\bar{\gamma}_\chi}}}{\bar{\gamma}_\chi^{N_\chi - 1}(N_\chi - 1)!\Gamma(m_{I_\chi} M_\chi)} \left(\frac{m_{I_\chi}}{\bar{\gamma}_{I_\chi}}\right)^{m_{I_\chi} M_\chi} \times \int_0^\infty y^{m_{I_\chi} M_\chi - 1}(1+y)^{N_\chi} \exp\left(-\left(\frac{\gamma}{\bar{\gamma}_\chi} + \frac{m_{I_\chi}}{\bar{\gamma}_{I_\chi}}\right) y\right) \mathrm{d}y. \tag{35}$$

In (35), after noting the exponent of y as $\alpha - 1$ where $\alpha = m_{I_\chi} M_\chi$, we can rewrite the exponent of the term $(1 + y)$ as $\beta - \alpha - 1$ with $\beta = N_\chi + \alpha + 1$. Subsequently, we can identify [37, eq. (9.211.4)]

$$\int_0^\infty y^{\alpha-1}(1+y)^{\beta-\alpha-1} \exp(-zy)\, \mathrm{d}y = \Gamma(\alpha)\Psi(\alpha, \beta; z), \tag{36}$$

where $z = \frac{\gamma}{\bar{\gamma}_\chi} + \frac{m_{I_\chi}}{\bar{\gamma}_{I_\chi}}$ and $\Psi(a, b; z)$ is the confluent hypergeometric function of the second kind defined in [37, eq. (9.210.2)] and is readily available in mathematical software packages such as MATHEMATICA. Substituting (36) in (35) completes the proof.

REFERENCES

[1] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.
[4] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[5] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 509–511, May 2011.
[6] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.
[7] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.
[8] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 254–259, Jan. 2013.
[9] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1754–1757, Sep. 2013.
[10] L. Chen, Y. Yang, and G. Wei, "Physical layer security enhancement with generalized selection diversity combining," in *Proc. IEEE 24th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, London, U.K., Sep. 2013, pp. 518–521.
[11] A. S. Shrestha and K. S. Kwak, "On maximal ratio diversity with weighting errors for physical layer security," *IEEE Commun. Lett.*, vol. 18, no. 4, pp. 580–583, Apr. 2014.
[12] K. S. Ahn, S.-W. Choi, and J.-M. Ahn, "Secrecy performance of maximum ratio diversity with channel estimation error," *IEEE Signal Process. Lett.*, vol. 22, no. 11, pp. 2167–2171, Nov. 2015.
[13] S. S. Ikki, P. Ubaidulla, and S. Aïssa, "Performance study and optimization of cooperative diversity networks with co-channel interference," *IEEE Trans. Wireless Commun.*, vol. 13, no. 1, pp. 14–23, Jan. 2014.
[14] N. Suraweera and N. C. Beaulieu, "Outage probability of decode-and-forward relaying with optimum combining in the presence of co-channel interference and Nakagami fading," *IEEE Wireless Commun. Lett.*, vol. 2, no. 5, pp. 495–498, Oct. 2013.
[15] J. M. Moualeu, W. Hamouda, and F. Takawira, "Outage analysis of relay selection in AF with outdated channel information in the presence of co-channel interference," in *Proc. IEEE Wireless Commun. Netw. Conf.*, New Orleans, LA, USA, Mar. 2015, pp. 498–503.
[16] T. T. Duy, T. Q. Duong, T. L. Thanh, and V. N. Q. Bao, "Secrecy performance analysis with relay selection methods under impact of co-channel interference," *IET Commun.*, vol. 9, no. 11, pp. 1427–1435, Jul. 2015.
[17] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying with cochannel interference," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1494–1505, Dec. 2016.
[18] N. S. Ferdinand, D. B. da Costa, and M. Latva-Aho, "Physical layer security of MISO TAS wiretap channels with interference-limited eavesdropper," in *Proc. IEEE 24th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, London, U.K., Sep. 2013, pp. 441–445.
[19] A. H. A. El-Malek, A. M. Salhab, and S. A. Zummo, "Optimal power allocation for enhancing physical layer security in opportunistic relay networks in the presence of co-channel interference," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, San Diego, CA, USA, Dec. 2015, pp. 1–5.
[20] Y. Gao, P. Wang, J. Ge, and H. Gao, "Secrecy outage probability of maximal ratio combining and optimum combining in interference-limited wiretap channels," in *Proc. Int. Conf. Commun. Netw. China (ChinaCom)*, Shanghai, China, Aug. 2015, pp. 771–775.
[21] D. S. Karas, A.-A. Boulogeorgos, G. K. Karagiannidis, and A. Nallanathan, "Physical layer security in the presence of interference," *IEEE Commun. Lett.*, vol. 6, no. 6, pp. 802–805, Dec. 2017.
[22] T.-X. Zheng, H.-M. Wang, Q. Yang, and M. H. Lee, "Safeguarding decentralized wireless networks using full-duplex jamming receivers," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 278–292, Jan. 2017.
[23] C. Wang, H. M. Wang, X. G. Xia, and C. Liu, "Uncoordinated jammer selection for securing SIMOME wiretap channels: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2596–2612, May 2015.
[24] N. C. Beaulieu and C. Cheng, "Efficient Nakagami-*m* fading channel simulation," *IEEE Trans. Veh. Technol.*, vol. 54, no. 2, pp. 413–424, Mar. 2005.
[25] Y.-D. Yao and A. U. H. Sheikh, "Investigations into cochannel interference in microcellular mobile radio systems," *IEEE Trans. Veh. Technol.*, vol. 41, no. 2, pp. 114–123, May 1992.
[26] Y.-D. Yao and A. U. H. Sheikh, "Outage probability analysis for microcell mobile radio systems with cochannel interferers in Rician/Rayleigh fading environment," *Electron. Lett.*, vol. 26, no. 13, pp. 864–866, Jun. 1990.
[27] J. H. Winter, "Optimum combining in digital mobile radio with cochannel interference," *IEEE J. Sel. Areas Commun.*, vol. SAC-2, pp. 539–583, Jul. 1984.
[28] A. Afana, S. Ikki, T. M. N. Ngatched, and O. A. Dobre, "Performance analysis of cooperative networks with optimum combining and co-channel interference," in *Proc. IEEE Int. Conf. Commun. Workshop (ICCW)*, London, U.K., Jun. 2015, pp. 949–954.
[29] N. Suraweera and N. C. Beaulieu, "Optimum combining for cooperative relaying in a Poisson field of interferers," *IEEE Trans. Commun.*, vol. 63, no. 9, pp. 3132–3142, Sep. 2015.
[30] C. Liu, N. Yang, J. Yuan, and R. Malaney, "Location-based secure transmission for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 7, pp. 1458–1470, Jul. 2015.
[31] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2170–2181, Apr. 2016.
[32] C. Liu and R. Malaney, "Location-based beamforming and physical layer security in Rician wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7847–7857, Nov. 2016.
[33] Z. Ding, Z. Yang, P. Fan, and H. V. Poor, "On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users," *IEEE Signal Process. Lett.*, vol. 21, no. 12, pp. 1501–1505, Dec. 2014.
[34] J. Cui and A. U. H. Sheikh, "Outage probability of cellular radio systems using maximal ratio combining in the presence of multiple interferers," *IEEE Trans. Commun.*, vol. 47, no. 8, pp. 1121–1124, Aug. 1999.
[35] Y. Tokgoz and B. D. Rao, "The effect of imperfect channel estimation on the performance of maximum ratio combining in the presence of cochannel interference," *IEEE Trans. Veh. Technol.*, vol. 55, no. 5, pp. 1527–1534, Sep. 2006.
[36] A. Papoulis and S. U. Pillai, *Probability, Random Variables and Stochastic Processes With Errata Sheet*, 4th ed. New York, NY, USA: McGraw-Hill, 2002.
[37] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 3rd ed. New York, NY, USA: Academic, 2007.
[38] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.
[39] X. Ding, T. Song, Y. Zou, and X. Chen, "Intercept probability analysis of relay selection for wireless communications in the presence of multiple eavesdroppers," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Doha, Qatar, Apr. 2016, pp. 1–6.
[40] F. W. J. Olver *et al.* (Dec. 21, 2016). *NIST Digital Library of Mathematical Functions*. [Online]. Available: http://dlmf.nist.gov/
[41] F. S. Al-Qahtani, C. Zhong, and H. M. Alnuweiri, "Opportunistic relay selection for secrecy enhancement in cooperative networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1756–1770, May 2015.

JULES M. MOUALEU (S'06–M'14–SM'18) received the M.Sc.Eng. and Ph.D. degrees in electronic engineering from the University of KwaZulu-Natal, Durban, South Africa, in 2008 and 2013, respectively. He was a Visiting Scholar with Concordia University, Montreal, Canada.

He joined the Department of Electrical and Information Engineering, University of the Witwatersrand, Johannesburg, South Africa, in 2015. He is currently an NRF Y-Rated Researcher. His current research interests include cooperative and relay communications, cognitive radio networks, energy harvesting, multiple-input multiple-output systems, non-orthogonal multiple access schemes, and physical-layer security.

WALAA HAMOUDA (S'97–M'02–SM'06) received the M.A.Sc. and Ph.D. degrees in electrical and computer engineering from Queen's University, Kingston, ON, Canada, in 1998 and 2002, respectively. Since 2002, he has been with the Department of Electrical and Computer Engineering, Concordia University, Montreal, QC, Canada, where he is currently a Professor. Since 2006, he has been the Concordia University Research Chair in communications and networking. His current research interests include single/multiuser multiple-input-multiple-output communications, space–time processing, cooperative communications, wireless networks, multiuser communications, cross-layer design, and source and channel coding.

Dr. Hamouda has received numerous awards, including the Best Paper Award at ICC 2009 and the IEEE Canada Certificate of Appreciation in 2007 and 2008. He served as the Technical Co-Chair for the Fifth International Conference on Selected Topics in Mobile and Wireless Networking (2016), a Track Co-Chair for the Multiple Antenna and Cooperative Communications, the IEEE Vehicular Technology Conference (VTC-Fall 2016), and a Co-Chair for the ACM Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, the Wireless Networks Symposium, 2012 Global Communications Conference, the Ad-hoc, Sensor, and Mesh Networking Symposium of the 2010 ICC, and the 25th Queen's Biennial Symposium on Communications. He also served as a Track Co-Chair for the Radio Access Techniques of the Fall 2006 VTC and the Transmission Techniques of the Fall 2012 IEEE VTC. From 2005 to 2008, he was the Chair of the IEEE Montreal Chapter in Communications and Information Theory. He served as an Associate Editor for the IEEE COMMUNICATIONS LETTERS and the IEEE TRANSACTIONS ON SIGNAL PROCESSING. He currently serves as an Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and an Editor for the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS and the IEEE WIRELESS COMMUNICATIONS LETTERS.

FAMBIRAI TAKAWIRA (M'96) received the B.Sc. degree (Hons.) in electrical and electronic engineering from The University of Manchester, Manchester, U.K., in 1981, and the Ph.D. degree from the University of Cambridge, Cambridge, U.K, in 1984. At the University of KwaZulu-Natal (UKZN), he held various academic positions including that of the Head of the School of Electrical, Electronic and Computer Engineering, and just before his departure, he was the Dean of the Faculty of Engineering. He has also held appointments at the University of Zimbabwe, the University of California at San Diego, British Telecom Research Laboratories, and the National University of Singapore. He joined the University of the Witwatersrand, Johannesburg, South Africa, in 2012, after 19 years at UKZN. His research interests are in wireless communication systems and networks.

Dr. Takawira has served on several conference organizing committees. He served as the Communications Society Director of the Europe, Middle East, and Africa region for the 2012–2013 term. He is a Past Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.