Average Secrecy Outage Rate and Average Secrecy Outage Duration of Wireless Communication Systems With Diversity Over Nakagami-m Fading Channels

Aymen Omri, *Member, IEEE*, and Mazen O. Hasna, *Senior Member, IEEE*

***Abstract*— This paper presents an analytical methodology for the evaluation of two important physical layer security metrics in wiretap channels. Specifically, we first introduce the concept and the expression of average secrecy outage rate (ASOR) to quantify the average secrecy level crossing rate at a predefined secrecy threshold level. Then, we derive the expression of a new metric, namely, average secrecy outage duration (ASOD), which is a measure (in seconds) that describes how long on average the system remains in the secrecy outage status. The results are quite general and account for diversity-based systems operating over independent and identically distributed (i.i.d.) Nakagami-m fading channels. Monte Carlo simulations are conducted to confirm and discuss the analytical results. These results show that the ASOR and the ASOD are essentially affected by the diversity order, and the maximum Doppler frequency shift. In particular, and unlike the ASOD, the ASOR has a maximum value that should be considered in designing systems that are sensitive to secrecy level drops, even for short periods of time. In addition, the proposed new metric of ASOD might have large values even if the currently used metric of average fade duration shows low values on the communication link under consideration.**

***Index Terms*— Average secrecy outage duration, average secrecy outage rate, maximum ratio combining, nakagami-m fading channels, wiretap channels.**

I. Introduction

WIRELESS communications have become indispensable for providing mobile and broadband data transfer. However, the broadcast nature of radio waves allows eavesdroppers to overhear the transmitted signals that may include highly sensitive and personal informations [1]–[4]. For this reason, the issues of security and privacy in wireless communication networks have taken special attentions [3]–[8]. Traditionally, wireless communication security has used cryptographic methods that are performed in the upper layers of the communication systems [5]–[7]. These methods are based mainly on generating, exchanging, and employing cryptographic keys. However, sharing of secret keys between the authorized users is a great challenge in terms of key distribution and management [4], [8]. In addition, rapid advances in computing power and resources make it feasible for eavesdroppers to decode the encrypted wireless signals [2]. As a result, new efficient wireless security mechanisms that do not rely on the overhead-heavy and coordination-intense cryptographic protocols are needed.

Recently, physical-layer security has been proposed as a promising alternative (or at least a complement) for protection against malicious eavesdroppers without possibly the need of cryptographic methods [3], [4], [8]. In principle, it is able to secure communications even in the presence of eavesdroppers with unlimited computation ability [9], [10]. The interesting concept is to make use of physical layer characteristics to improve the security and reliability of the communication channel. One approach to meet such requirements was first proposed by Wyner [9], who laid the foundations of information theoretic security, where he introduced the concept of a wiretap discrete memoryless channel and analyzed its inherent achievable secrecy rate capacity. In light of this, considerable amount of research has been conducted on the topic of improving physical layer security in wireless communications. In [11], the Wyner's results for discrete memoryless wiretap channels have been extended to the Gaussian wiretap channel, where the authors have shown that the secrecy capacity is the difference between the capacities of the main and wiretap channels. To further enhance communication security, joint cooperative beamforming and jamming techniques have been proposed in [1], [12], and [13]. In [14]–[16], physical layer security with artificial noise has been presented and evaluated. Physical layer security for different cooperative schemes has been studied and investigated in [17]–[22], where the authors have confirmed that cooperation can greatly improve the security. In [23], the authors have proposed power minimization and secrecy rate maximization for a MIMO secrecy channel in the presence of a multiple-antenna eavesdropper.

The performance analysis of those proposed schemes and techniques that have appeared thus far in the literature have focused mainly on first order statistics, in particular the secrecy

Manuscript received May 15, 2017; revised October 3, 2017, December 24, 2017, and February 19, 2018; accepted March 6, 2018. Date of publication April 16, 2018; date of current version June 8, 2018. This publication was made possible by the sponsorship agreement in support of research and collaboration by Ooredoo, Doha, Qatar. The statements made herein are solely the responsibility of the authors. The associate editor coordinating the review of this paper and approving it for publication was J. Park. *(Corresponding author: Aymen Omri.)*

The authors are with the Department of Electrical Engineering, Qatar University, Doha, Qatar (e-mail: eaymenomri@gmail.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2018.2816648

capacity and/or the secrecy outage probability, which have been traditionally the most commonly used security measures for wiretap channels [1], [9], [23], [24]. To fully understand the performance of such systems, we need second order measures to have insights on the dynamics of such performance. For example, secrecy outage probability provides an idea about the fraction of fading realizations for which the channel can support a certain rate. However, it fails to provide an idea on the average length (in terms of realizations) for which the channel cannot support secure communication. Mobility is another dimension where second order statistics come to play. In a scenario where transmitters, receivers, and eavesdroppers are on the move, we may need to check what speed results in what average secrecy outage duration, and hence the system may plan for specific measures in relocating or changing the speed of its components whenever applicable. Moreover, and recently in [25], there is an interest in coupling physical layer security and secret key generations where intervals of good secrecy performance are used to exchange such keys so that they can be used in the rest of the transmission. Average secrecy outage duration will play an important role in such scenarios. In general, whenever we have adaptive transmission schemes and dynamic deployment of systems, average secrecy outage rate (ASOR) [or average secrecy level crossing rate (ASLCR)], and average secrecy outage duration (ASOD) measures can substantially help in both design and deployment of the system when security is a concern.

To the best of our knowledge, few published analytical work have paid attention to the impact of the fading statistics of the desired and interfering users on the average outage rate, and the system outage duration [26]–[30]. In addition, previous work on second order statistics focused mainly on the effect of fading and interference, without tackling the physical layer security side of the problem. For example, such work helped in better understanding error bursts [31], [32] and in the design of interleaver size and coded modulation [33]. However, when the secrecy capacity measure is of concern and not only the main channel fading measures, our proposed metrics come into play. In fact, published analytical work on the ASOR, and the ASOD of general maximum ratio combining (MRC) based wireless communication systems over Nakagami-m fading channels is still not available in the literature.

In light of the aforementioned related work, our main contributions can be summarized as follows:

- We introduce the concept of ASOR to quantify the average secrecy level crossing rate at a predefined secrecy threshold level, and we derive its analytical expressions for both noise limited and interference limited systems.
- To measure the average time period, during which the system remains in the secrecy outage status, we introduce the concept of ASOD. Then, based on the derived expressions of secrecy outage probability (SOP), and ASOR, we presents the expressions of ASOD for the two general systems under consideration.

The rest of this paper is organized as follows: In Section II, the system and channel models are described. The expressions of SOP, ASOR, and ASOD are detailed and derived in Section III. In Section IV, Monte Carlo simulation results are presented to evaluate the accuracy of the derived expressions, and to investigate the variations of the proposed security metrics. Finally, conclusions are drawn in Section V.

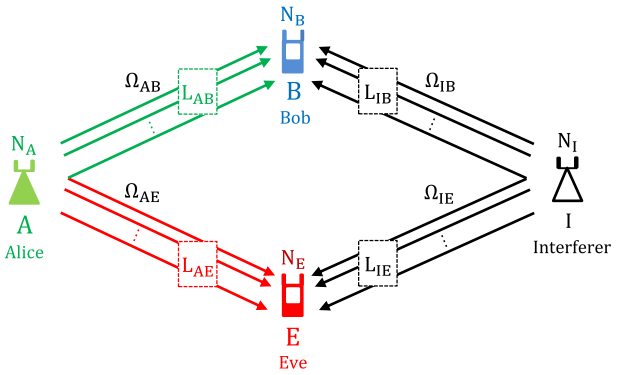

Fig. 1. The system model.

II. System and Channel Models

We consider a wireless communication system, in which a source (Alice) intends to send information to a legitimate destination (Bob), in the presence of a passive eavesdropper (Eve) and a source of interference as presented in Fig. 1. All the nodes are assumed to be equipped with multiple antennas, where $N_{\rm A}$, $N_{\rm B}$, $N_{\rm E}$, and $N_{\rm I}$ denote the number of antennas at Alice, Bob, Eve, and the interferer, respectively. We assume that the channels between the different antennas are not correlated. Consequently, the desired signal is received at Bob (Eve) over $L_{\rm AB}(L_{\rm AE})$ independent and identically distributed (i.i.d.) diversity paths,[1] with the same average fading power $\Omega_{\rm AB}$ ($\Omega_{\rm AE}$), where $L_{\rm AB} = N_{\rm A} \times N_{\rm B}$, and $L_{\rm AE} = N_{\rm A} \times N_{\rm E}$. Moreover, the interfering signal is received at Bob (Eve) over $L_{\rm IB}(L_{\rm IE})$ independent and identically distributed (i.i.d.) diversity paths, with the same average fading power $\Omega_{\rm IB}$ ($\Omega_{\rm IE}$), where $L_{\rm IB} = N_{\rm I} \times N_{\rm B}$, and $L_{\rm IE} = N_{\rm I} \times N_{\rm E}$. For the different nodes, we assume also that all the diversity paths are subject to flat Nakagami fading with parameter m. To exploit the diversity paths and to provide wireless link improvement, a MRC receiver is used at Bob and at Eve to combine the received signals.

In this paper, we consider two kinds of systems, namely: noise limited systems and interference limited systems. In noise limited systems, the performance is mainly affected by the level of noise emerging from different parts of the system as well as from the background, and the main parameter to consider is the signal to noise ratio (SNR), where the effect of interference signals is ignored either because the system is not affected by interference, e.g., by using orthogonal frequencies, or perfect interference cancellation schemes are used. For interference limited systems, the performance suffers mainly from interference sources,[2] and the level of noise is

[1]The analysis presented in the paper on space diversity is also applicable to other diversity methods, such as time or frequency diversities.

[2]In this paper we are considering non cooperative interferers emerging from internal or external sources, affecting both the intended receiver as well as the eavesdropper.

considered negligible compared to that of the interference. The main parameter to consider here is signal to interference ratio (SIR).

For a noise limited system, the SNRs at Bob ($\gamma_{\rm B}$) and at Eve ($\gamma_{\rm E}$) with MRC reception can be written as

$$\gamma_{\rm B} = \frac{\alpha_{\rm AB}^2}{N_0} = \frac{\sum_{\rm l=1}^{L_{\rm AB}} \alpha_{\rm AB,l}^2}{N_0}, \tag{1}$$

and,

$$\gamma_{\rm E} = \frac{\alpha_{\rm AE}^2}{N_0} = \frac{\sum_{\rm l'=1}^{L_{\rm AE}} \alpha_{\rm AE,l'}^2}{N_0}, \tag{2}$$

respectively, where, $\alpha_{\rm AB}^2$ ($\alpha_{\rm AE}^2$) is the total received desired signal power at Bob (Eve), $\alpha_{\rm AB,l}^2$ ($\alpha_{\rm AE,l'}^2$) is the received desired signal power at Bob (Eve) over the $\rm l^{\mathit{th}}$ ($\rm l'^{\mathit{th}}$) diversity path, and N_0 is the additive white Gaussian noise (AWGN) power.

For an interference limited system, the SIR at Bob ($\lambda_{\rm B}$) and at Eve ($\lambda_{\rm E}$) can be written as

$$\lambda_{\rm B} = \frac{\alpha_{\rm AB}^2}{\alpha_{\rm IB}^2} = \frac{\sum_{\rm l=1}^{L_{\rm AB}} \alpha_{\rm AB,l}^2}{\sum_{\rm n=1}^{L_{\rm IB}} \alpha_{\rm IB,n}^2}, \tag{3}$$

and,

$$\lambda_{\rm E} = \frac{\alpha_{\rm AE}^2}{\alpha_{\rm IE}^2} = \frac{\sum_{\rm l'=1}^{L_{\rm AE}} \alpha_{\rm AE,l'}^2}{\sum_{\rm n'=1}^{L_{\rm IE}} \alpha_{\rm IE,n'}^2}, \tag{4}$$

respectively, where $\alpha_{\rm IB}^2$ ($\alpha_{\rm IE}^2$) is the total received interference signal power at Bob (Eve), and $\alpha_{\rm IB,n}^2$ ($\alpha_{\rm IE,n'}^2$) is the received interference signal power at Bob (Eve) from the $\rm n^{\mathit{th}}$ ($\rm n'^{\mathit{th}}$) antenna of the interferer.

It is known that the square of a Nakagami random variable is a Gamma random variable, and the sum of independent Gamma random variables, with the same scaling parameter, is a Gamma random variable [26], hence α_χ^2, $\forall\ \chi \in \{AB, AE, IB, IE\}$, is a Gamma random variable with the general probability density function (PDF) expression is given by [26]

$$p_{\alpha_\chi^2}(\nu) = \left(\frac{m}{\Omega_\chi}\right)^{mL_\chi} \frac{\nu^{mL_\chi - 1}}{\Gamma(mL_\chi)} \exp\left(-\frac{m}{\Omega_\chi}\nu\right). \tag{5}$$

Based on the PDF expression of $p_{\alpha_\chi^2}$, the general PDF expression of the instantaneous fading amplitude α_χ is expressed as [26]

$$p_{\alpha_\chi}(\alpha_\chi) = \left(\frac{m}{\Omega_\chi}\right)^{mL_\chi} \frac{2\ \alpha_\chi^{2mL_\chi - 1}}{\Gamma(mL_\chi)} \exp\left(-\frac{m}{\Omega_\chi}\alpha_\chi^2\right). \tag{6}$$

For the Nakagami-m fading channel model, the time derivative of the signal amplitude process, denoted by $\dot{\alpha}_\chi$, is always independent of the signal amplitude, and the PDF expression of $\dot{\alpha}_\chi$ is given by [26]

$$p_{\dot{\alpha}_\chi}(\dot{\alpha}_\chi) = \frac{1}{\sqrt{2\ \pi}\ \sigma_\chi} \exp\left(-\frac{\dot{\alpha}_\chi^2}{2\ \sigma_\chi^2}\right), \tag{7}$$

where, $\sigma_\chi^2 = \pi^2 f_{\rm max}^2 (\Omega_\chi / m)$, and $f_{\rm max}$ is the maximum Doppler frequency shifts.

III. Performances Analysis

In this section, we derive the expressions of SOP, ASOR, and ASOD for both noise limited and interference limited systems.

A. Secrecy Capacity (SC)

For general wireless communication systems, the secrecy capacity is defined as the maximum between zero and the value of the difference between the capacities of the main and wiretap channels [34]–[36], which can be expressed as follows

$$SC = \begin{cases} C_{\rm B} - C_{\rm E}, & \text{if } (C_{\rm B} > C_{\rm E}) \\ 0, & \text{else,} \end{cases} \tag{8}$$

where, $C_{\rm B}$ and $C_{\rm E}$ are the instantaneous capacities at Bob and at Eve, respectively.

B. Secrecy Outage Probability (SOP)

A secrecy outage can be defined as the event in which the instantaneous secrecy capacity (SC) is equal to or falls below a predefined threshold ($\xi_{\rm th}$), i.e., ($SC \le \xi_{\rm th}$) [34], where $\xi_{\rm th}$ is defined as the threshold capacity at or under which secure communication cannot be achieved. Accordingly, the secrecy outage probability for the two systems under consideration are derived as follows:

1) Noise Limited Systems: For a noise limited system, the secrecy outage probability is defined as [34]

$$P_{\rm out}^{\rm (N)}(\xi_{\rm th}) = {\rm P}\{SC \le \xi_{\rm th}\}. \tag{9}$$

Based on (8), and (9), the expression of $P_{\rm out}^{\rm (N)}(\xi_{\rm th})$ can be rewritten as

$$\begin{aligned} P_{\rm out}^{\rm (N)}(\xi_{\rm th}) &= {\rm P}\Big\{C_{\rm B} \le (C_{\rm E} + \xi_{\rm th})\Big\} \\ &= {\rm P}\Big\{\Big[\log_2(1+\gamma_{\rm B}) - \log_2(1+\gamma_{\rm E})\Big] \le \xi_{\rm th}\Big\} \\ &= {\rm P}\Big\{\gamma_{\rm B} \le \Big[2^{\xi_{\rm th}}(1+\gamma_{\rm E}) - 1\Big]\Big\} \\ &= \int_0^\infty \int_0^{2^{\xi_{\rm th}}(1+y)-1} p_{\gamma_{\rm B}}(x)\ p_{\gamma_{\rm E}}(y)\ {\rm d}x\ {\rm d}y, \end{aligned} \tag{10}$$

where, $p_{\gamma_{\rm B}}$ and $p_{\gamma_{\rm E}}$ are the PDFs of $\gamma_{\rm B}$ and $\gamma_{\rm E}$, respectively. Based on (1), (2), and (5), the corresponding PDF expressions are given by

$$p_{\gamma_{\rm B}}(\gamma_{\rm B}) = \left(\frac{m}{\omega_{\rm B}}\right)^{mL_{\rm AB}} \frac{\gamma_{\rm B}^{mL_{\rm AB}-1}}{\Gamma(mL_{\rm AB})} \exp\left(-\frac{m}{\omega_{\rm B}}\gamma_{\rm B}\right), \tag{11}$$

and,

$$p_{\gamma_{\mathrm{E}}}(\gamma_{\mathrm{E}}) = \left(\frac{m}{\omega_{\mathrm{E}}}\right)^{mL_{\mathrm{AE}}} \frac{\gamma_{\mathrm{E}}^{mL_{\mathrm{AE}}-1}}{\Gamma(mL_{\mathrm{AE}})} \exp\left(-\frac{m}{\omega_{\mathrm{E}}}\gamma_{\mathrm{E}}\right), \quad (12)$$

where, $\omega_{\mathrm{B}} = \Omega_{\mathrm{AB}}/N_0$, and $\omega_{\mathrm{E}} = \Omega_{\mathrm{AE}}/N_0$. Based on (10-12), the final exact closed form expression of $P_{\mathrm{out}}^{(\mathrm{N})}(\xi_{\mathrm{th}})$ is derived in Appendix A and is given by (13), shown on the top of the next page.

For the special case of ($\xi_{\mathrm{th}} = 0$), which is the case of having outage in the strictly positive secrecy capacity sense, the expression of $P_{\mathrm{out}}^{(\mathrm{N})}(0)$ can be further simplified to

$$P_{\mathrm{out}}^{(\mathrm{N})}(0) = 1 - \sum_{k=0}^{mL_{\mathrm{AB}}-1} \frac{\left(\frac{\omega_{\mathrm{B}}}{m}\right)^{k+1-mL_{\mathrm{AB}}} \binom{mL_{\mathrm{AB}}+mL_{\mathrm{AE}}-2-k}{mL_{\mathrm{AE}}-1}}{\left(\frac{m}{\omega_{\mathrm{E}}}\right)^{mL_{\mathrm{AB}}-k-1} \left[1+\frac{\omega_{\mathrm{E}}}{\omega_{\mathrm{B}}}\right]^{mL_{\mathrm{AB}}+mL_{\mathrm{AE}}-1-k}}. \quad (14)$$

Continuing with this special case and assuming further that ($m = L_{\mathrm{AB}} = L_{\mathrm{AE}} = 1$), which refers to the case where all channels suffer from Rayleigh fading, and all nodes are equipped with one antenna only, $P_{\mathrm{out}}^{(\mathrm{N})}(0)$ reduces to

$$P_{\mathrm{out}}^{(\mathrm{N})}(0) = \frac{\omega_{\mathrm{E}}}{\omega_{\mathrm{B}} + \omega_{\mathrm{E}}}, \quad (15)$$

which is in agreement with the derived expression in [34]. From this equation, we can remark that the secrecy outage probability increases with ω_{E} and is inversely proportional to ω_{B}. In addition, for large values of $\omega_{\mathrm{E}} (>> \omega_{\mathrm{B}})$, this probability converges to one, which is expected.

2) Interference Limited Systems: For an interference limited system, and based on (3), (4), and (9), the expression of the secrecy outage probability is written as

$$\begin{aligned} P_{\mathrm{out}}^{(\mathrm{I})}(\xi_{\mathrm{th}}) &= \mathrm{P}\left\{\left[\log_2(1+\lambda_{\mathrm{B}}) - \log_2(1+\lambda_{\mathrm{E}})\right] \le \xi_{\mathrm{th}}\right\} \\ &= \mathrm{P}\left\{\alpha_{\mathrm{AB}}^2 \le \alpha_{\mathrm{IB}}^2\left[2^{\xi_{\mathrm{th}}}(1+\lambda_{\mathrm{E}}) - 1\right]\right\} \\ &= \int_0^\infty \int_0^\infty \int_0^{y[2^{\xi_{\mathrm{th}}}(1+v)-1]} p_{\alpha_{\mathrm{AB}}^2}(x)\ p_{\alpha_{\mathrm{IB}}^2}(y)\ p_{\lambda_{\mathrm{E}}}(v)\mathrm{d}x\mathrm{d}y\mathrm{d}v, \end{aligned} \quad (16)$$

where, $p_{\alpha_{\mathrm{AB}}^2}$ and $p_{\alpha_{\mathrm{IB}}^2}$ are the PDFs of α_{AB}^2 and α_{IB}^2, respectively, and $p_{\lambda_{\mathrm{E}}}$ is the PDF of λ_{E}. As the ratio of two independent Gamma random variables is a Beta prime random variable [37], and based on (5), the PDF of λ_{E} is expressed as

$$p_{\lambda_{\mathrm{E}}}(\lambda_{\mathrm{E}}) = \frac{\left(\frac{\lambda_{\mathrm{E}}}{\Omega_{\mathrm{E}}}\right)^{mL_{\mathrm{AE}}-1} \left(1+\frac{\lambda_{\mathrm{E}}}{\Omega_{\mathrm{E}}}\right)^{-mL_{\mathrm{AE}}-mL_{\mathrm{IE}}}}{\Omega_{\mathrm{E}}\ \mathfrak{B}(mL_{\mathrm{AE}}, mL_{\mathrm{IE}})}, \quad (17)$$

where, $\Omega_{\mathrm{E}} = \frac{\Omega_{\mathrm{AE}}}{\Omega_{\mathrm{IE}}}$, and $\mathfrak{B}$ is the Beta function [38, eq. $8.380-1$].

The final exact form expression of $P_{\mathrm{out}}^{(\mathrm{I})}(\xi_{\mathrm{th}})$ is derived in Appendix B and is given by (18), shown on the top of the next page, where $\Omega_{\mathrm{B}} = \frac{\Omega_{\mathrm{AB}}}{\Omega_{\mathrm{IB}}}$, $\rho_{\mathrm{B}} = mL_{\mathrm{AB}} + mL_{\mathrm{AB}}$, $\rho_{\mathrm{E}} = mL_{\mathrm{AE}} + mL_{\mathrm{AE}}$, and ${}_2\mathcal{F}_1$ is the Gauss hypergeometric function [38, eq. $9.14-1$].

For the special case of ($\xi_{\mathrm{th}} = 0$), the expression of $P_{\mathrm{out}}^{(\mathrm{I})}(0)$ is given by

$$\begin{aligned} P_{\mathrm{out}}^{(\mathrm{I})}(0) &= 1 - \frac{\Omega_{\mathrm{B}}^{mL_{\mathrm{AE}}}\ \Omega_{\mathrm{E}}^{-mL_{\mathrm{AE}}}}{\mathfrak{B}(mL_{\mathrm{AE}}, mL_{\mathrm{IE}})} \sum_{k=0}^{mL_{\mathrm{AB}}-1} \left\{ \binom{\rho_{\mathrm{B}}-2-k}{mL_{\mathrm{IB}}-1} \right. \\ &\quad \times \mathfrak{B}\left(mL_{\mathrm{AB}} + mL_{\mathrm{AE}} - 1 - k, mL_{\mathrm{IB}} + mL_{\mathrm{IE}}\right) \\ &\quad \left. \times {}_2\mathcal{F}_1\left(\rho_{\mathrm{E}}, mL_{\mathrm{AB}} + mL_{\mathrm{AE}} - 1 - k;\ \rho_{\mathrm{B}} + \rho_{\mathrm{E}} - 1 - k; 1 - \frac{\Omega_{\mathrm{B}}}{\Omega_{\mathrm{E}}}\right)\right\}, \end{aligned} \quad (19)$$

which simplifies further in the single antenna Rayleigh case (i.e. $m = L_{\mathrm{AB}} = L_{\mathrm{AE}} = L_{\mathrm{IB}} = L_{\mathrm{IE}} = 1$) to

$$P_{\mathrm{out}}^{(\mathrm{I})}(0) = 1 - \frac{\Omega_{\mathrm{B}}}{2\ \Omega_{\mathrm{E}}}\ {}_2\mathcal{F}_1\left(2,\ 1;\ 3;\ 1 - \frac{\Omega_{\mathrm{B}}}{\Omega_{\mathrm{E}}}\right). \quad (20)$$

Similar to (15), it is clear that the secrecy outage probability, in the case of interference limited systems with those specific parameters, is proportional to Ω_{E} and is inversely proportional to Ω_{B}.

C. Average Secrecy Outage Rate (ASOR)

The average secrecy outage rate is defined as the average secrecy level crossing rate of the instantaneous secrecy capacity SC at level ξ_{th}, i.e., it quantifies the expected number of downward crossings per second of the secrecy capacity, which is variable in time. at a threshold level ξ_{th}. The ASOR for the two systems under consideration are derived as follows:

1) Noise Limited Systems: For a noise limited system, and based on the definition of SC, the event of ($SC \le \xi_{\mathrm{th}}$) is equivalent to the event of having $\left[r = \frac{\alpha_{\mathrm{AB}}}{\sqrt{N_0}} \le \sqrt{2^{\xi_{\mathrm{th}}}(1+\gamma_{\mathrm{E}}) - 1}\right]$. Consequently, the ASOR, denoted as $\mathfrak{R}^{(\mathrm{N})}(\xi_{\mathrm{th}})$, is equivalent to the rate at which the process r crosses downward the level $r_{\mathrm{th}} (= \sqrt{2^{\xi_{\mathrm{th}}}(1+\gamma_{\mathrm{E}}) - 1})$. Based on the general formula provided in [39], the ASOR can be written as

$$\mathfrak{R}^{(\mathrm{N})}(\xi_{\mathrm{th}}) = \int_0^\infty \int_0^\infty \dot{r}\ p_r(r_{\mathrm{th}})\ p_{\dot{r}}(\dot{r})\ p_{\gamma_{\mathrm{E}}}(y)\ \mathrm{d}\dot{r}\ \mathrm{d}y, \quad (21)$$

where, p_r and $p_{\dot{r}}$ are the PDFs of r and $\dot{r}$, respectively. Based on (6) and (7), the expressions of those PDFs are given by

$$p_r(r) = \left(\frac{m}{\omega_{\mathrm{B}}}\right)^m \frac{2\ r^{2m-1}}{\Gamma(m)} \exp\left(-\frac{m}{\omega_{\mathrm{B}}}r^2\right), \quad (22)$$

and,

$$p_{\dot{r}}(\dot{r}) = \frac{\sqrt{N_0}}{\sqrt{2\ \pi}\ \sigma_{\mathrm{AB}}} \exp\left(-\frac{N_0\dot{r}^2}{2\ \sigma_{\mathrm{AB}}^2}\right), \quad (23)$$

where, $\sigma_{\mathrm{AB}}^2 = \pi^2 f_{\max}^2(\Omega_{\mathrm{B}}/m)$. Based on (21-23), the final expression of $\mathfrak{R}^{(\mathrm{N})}(\xi_{\mathrm{th}})$ is derived in Appendix C and is given by (24), shown on the top of the next page, where x_n and

$$P_{\text{out}}^{(\text{N})}(\xi_{\text{th}}) = 1 - \exp\Big(\frac{-m}{\omega_{\text{B}}}\big[2^{\xi_{\text{th}}}-1\big]\Big) \sum_{k=0}^{mL_{\text{AB}}-1} \sum_{n=0}^{mL_{\text{AB}}-1-k} \frac{\big(\frac{\omega_{\text{B}}}{m}\big)^{k+1-mL_{\text{AB}}} \binom{n+mL_{\text{AE}}-1}{n}\ 2^{\xi_{\text{th}}(mL_{\text{AB}}-1-k)}\big[1-2^{-\xi_{\text{th}}}\big]^{mL_{\text{AB}}-k-n-1}}{\big(\frac{m}{\omega_{\text{E}}}\big)^{n}\ (mL_{\text{AB}}-k-n-1)!\ \big[1+\frac{\omega_{\text{E}}}{\omega_{\text{B}}}2^{\xi_{\text{th}}}\big]^{n+mL_{\text{AE}}}}. \tag{13}$$

$$P_{\text{out}}^{(\text{I})}(\xi_{\text{th}}) = 1 - \frac{\Omega_{\text{B}}^{mL_{\text{IB}}}\ \Omega_{\text{E}}^{-mL_{\text{AE}}}}{2^{\xi_{\text{th}}mL_{\text{IB}}}\ \mathfrak{B}(mL_{\text{AE}}, mL_{\text{IE}})} \sum_{k=0}^{mL_{\text{AB}}-1} \sum_{n=0}^{mL_{\text{AB}}-1-k} \Bigg\{ \frac{\binom{\rho_{\text{B}}-2-k}{mL_{\text{IB}}-1}\ \binom{mL_{\text{AB}}-1-k}{n}\ \big[1-2^{-\xi_{\text{th}}}\big]^{mL_{\text{AB}}-1-k-n}}{\big[1-2^{-\xi_{\text{th}}}(1-\Omega_{\text{B}})\big]^{\rho_{\text{B}}-mL_{\text{AE}}-k-n-1}}$$
$$\times \mathfrak{B}\Big(n+mL_{\text{AE}}, \rho_{\text{B}}+mL_{\text{IE}}-n-1-k\Big)\ {}_2\mathcal{F}_1\Bigg(\rho_{\text{E}}\ ,\ n+mL_{\text{AE}}\ ;\ \rho_{\text{B}}+\rho_{\text{E}}-1-k\ ;\ 1-\frac{\big[1-2^{-\xi_{\text{th}}}(1-\Omega_{\text{B}})\big]}{\Omega_{\text{E}}}\Bigg)\Bigg\}. \tag{18}$$

$$\mathfrak{R}^{(\text{N})}(\xi_{\text{th}}) \approx \frac{\sqrt{2\pi}\ f_{\max}\ \exp\Big(-\frac{m}{\omega_{\text{B}}}\big[2^{\xi_{\text{th}}}-1\big]\Big)\Big(\frac{m}{\omega_{\text{B}}}\Big)^{mL_{\text{AB}}}}{\Gamma(mL_{\text{AB}})\ \Gamma(mL_{\text{AE}})\ 2^{-\xi_{\text{th}}(2mL_{\text{AB}}-1)}\Big(\frac{m}{\omega_{\text{E}}}\Big)^{-mL_{\text{AE}}}} \sum_{n=1}^{N} \Bigg\{ \frac{w_n\ x_n^{mL_{\text{AE}}-1}}{[x_n+1-2^{-\xi_{\text{th}}}]^{-mL_{\text{AB}}+\frac{1}{2}}} \exp\Bigg(-x_n\Big[\frac{m2^{\xi_{\text{th}}}}{\omega_{\text{B}}}+\frac{m}{\omega_{\text{E}}}-1\Big]\Bigg)\Bigg\}. \tag{24}$$

w_n are the n^{th} abscissa (root) and weight of the N^{th} order Laguerre polynomial, respectively.

For the special case of ($\xi_{\text{th}} = 0$), the expression can be derived in an exact form, as shown in Appendix C, and is given by

$$\mathfrak{R}^{(\text{N})}(0) = \frac{\sqrt{2\pi}\ f_{\max}\ \Gamma(mL_{\text{AB}}+mL_{\text{AE}}-\frac{1}{2})\Big[\frac{\omega_{\text{B}}}{\omega_{\text{E}}}\Big]^{mL_{\text{AE}}-\frac{1}{2}}}{\Gamma(mL_{\text{AB}})\ \Gamma(mL_{\text{AE}})\ \Big[1+\frac{\omega_{\text{B}}}{\omega_{\text{E}}}\Big]^{mL_{\text{AB}}+mL_{\text{AE}}-1}}. \tag{25}$$

Now, simplifying further with ($m = L_{\text{AB}} = L_{\text{AE}} = 1$), the expression of $\mathfrak{R}^{(\text{N})}(0)$ reduces to

$$\mathfrak{R}^{(\text{N})}(0) = \frac{\pi\ f_{\max}\ \sqrt{\frac{\omega_{\text{B}}}{\omega_{\text{E}}}}}{\sqrt{2}\ \Big(1+\frac{\omega_{\text{B}}}{\omega_{\text{E}}}\Big)}. \tag{26}$$

2) Interference Limited Systems: For interference limited systems, the event of ($SC \le \xi_{\text{th}}$) is equivalent to the event of having $\Big[\beta = \frac{\alpha_{\text{AB}}}{\alpha_{\text{IB}}} \le \sqrt{2^{\xi_{\text{th}}}(1+\lambda_{\text{E}})-1}\Big]$. Consequently, $\mathfrak{R}^{(\text{I})}(\xi_{\text{th}})$ is equivalent to the rate at which the process β crosses downward the level $\beta_{\text{th}}(= \sqrt{2^{\xi_{\text{th}}}(1+\lambda_{\text{E}})-1})$. This ASOR can be obtained from the general formula provided in [39] as follows

$$\mathfrak{R}^{(\text{I})}(\xi_{\text{th}}) = \int_0^{\infty}\int_0^{\infty} \dot{\beta}\ p_{\beta,\dot{\beta}}(\beta_{\text{th}}, \dot{\beta})\ p_{\lambda_{\text{E}}}(v)\text{d}\dot{\beta}\ \text{d}v, \tag{27}$$

where, $p_{\beta,\dot{\beta}}$ is the joint PDF of β, and $\dot{\beta}$.

The final expression of $\mathfrak{R}^{(\text{I})}(\xi_{\text{th}})$ is derived in Appendix D and is given by (28), shown on the bottom of the next page.

For the special case of ($\xi_{\text{th}} = 0$), the expression of $\mathfrak{R}^{(\text{I})}(0)$ is derived in Appendix D as well, and is given by the following exact form

$$\mathfrak{R}^{(\text{I})}(0) = \frac{\sqrt{2\pi}\ f_{\max}\ \Omega_{\text{B}}^{mL_{\text{AE}}}\ \Gamma(\rho_{\text{B}}-\frac{1}{2})}{\Omega_{\text{E}}^{mL_{\text{AE}}}\ \Gamma(mL_{\text{AB}})\ \Gamma(mL_{\text{IB}})\ \mathfrak{B}(mL_{\text{AE}}, mL_{\text{IE}})}$$
$$\times \mathfrak{B}\Big(mL_{\text{AB}}+mL_{\text{AE}}-\frac{1}{2}, mL_{\text{IB}}+mL_{\text{IE}}-\frac{1}{2}\Big)$$
$$\times {}_2\mathcal{F}_1\Big(\rho_{\text{E}},\ mL_{\text{AB}}+mL_{\text{AE}}-\frac{1}{2};\ \rho_{\text{B}}+\rho_{\text{E}}-1;\ 1-\frac{\Omega_{\text{B}}}{\Omega_{\text{E}}}\Big). \tag{29}$$

For the single antenna Rayleigh case ($m = L_{\text{AB}} = L_{\text{AE}} = L_{\text{IB}} = L_{\text{IE}} = 1$), the expression of $\mathfrak{R}^{(\text{I})}(0)$ is given by the following simpler expression

$$\mathfrak{R}^{(\text{I})}(0) = \frac{87\sqrt{2\pi}\ f_{\max}\ \Omega_{\text{B}}}{250\ \Omega_{\text{E}}}\ {}_2\mathcal{F}_1\Big(2,\ \frac{3}{2};\ 3;\ 1-\frac{\Omega_{\text{B}}}{\Omega_{\text{E}}}\Big). \tag{30}$$

D. Average Secrecy Outage Duration (ASOD)

The ASOD is a measure [in seconds] to describe how long in average the system remains in the secrecy outage status. Mathematically speaking, and based on the definition of the average outage duration in [26] and [39], the ASOD is expressed as

$$T(\xi_{\text{th}}) = \frac{P_{\text{out}}(\xi_{\text{th}})}{\mathfrak{R}(\xi_{\text{th}})}. \tag{31}$$

Based on (31), and the derived expressions of SOP and ASOD, the average secrecy outage duration can be evaluated for noise limited and interference limited systems of interest.

For the specific case of ($\xi_{\text{th}} = 0$, $m = L_{\text{AB}} = L_{\text{AE}} = 1$), the expression of ASOD for noise limited and interference limited systems are given by

$$T^{(\text{N})}(0) = \frac{1}{\pi\ f_{\max}}\ \sqrt{\frac{2\ \omega_{\text{E}}}{\omega_{\text{B}}}}, \tag{32}$$

TABLE I
SIMULATION PARAMETERS

Parameter	Value
Simulation Time [s]	100
Sampling Time (T_s) [s]	$1e-4$
Number of Channel Samples (N_s)	$1e6$
ξ_{th} [bps/Hz]	0, and 1
f_{max} [Hz]	10, 50, and 100
ω_B | Ω_B [dB]	0 : 20
ω_E | Ω_E [dB]	0, 10, and 20
Order of Laguerre Polynomial (N)	50

and,

$$T^{(\mathrm{I})}(0) = \frac{250\ \Omega_{\mathrm{E}} - 125\Omega_{\mathrm{B}}\ {}_2\mathcal{F}_1\left(2,\ 1;\ 3;\ 1-\frac{\Omega_{\mathrm{B}}}{\Omega_{\mathrm{E}}}\right)}{87\sqrt{2\pi}\ f_{\max}\ \Omega_{\mathrm{B}}\ {}_2\mathcal{F}_1\left(2,\ \frac{3}{2};\ 3;\ 1-\frac{\Omega_{\mathrm{B}}}{\Omega_{\mathrm{E}}}\right)}, \quad (33)$$

respectively. Based on (32) and (33), and for equal values of $\omega_{\mathrm{B}}(\Omega_{\mathrm{B}})$ and $\omega_{\mathrm{E}}(\Omega_{\mathrm{E}})$, the hypergeometric function, in (33), reduces to 1. Consequently, the ASOD depends in this case on the maximum Doppler shift only (which is related to the mobility and the channel variation in time) for both noise limited and interference limited systems. This is expected as the parameters of Bob and Eve are the same (in terms of average power and diversity order).

In the next section, we will try to draw more insights on the derived expressions for both systems under consideration.

IV. NUMERICAL RESULTS

In this section, and using Monte Carlo simulation in MatLab, numerical results are presented to confirm and discuss the derived analytical expressions for noise limited and interference limited systems. Without loss of generality, the main parameters used in our simulations are presented in Table I.

The accuracy of the derived analytical expressions are confirmed by the conducted simulation results that are presented in the following different figures.

A. Noise Limited Systems:

In this subsection, we present and discuss the numerical results for noise limited systems.

In Fig. 2, the variation of secrecy capacity realizations, which is essentially the difference in the realizations of the main and wiretap channels, versus time for a noise limited system, with $m = 2$, $\omega_{\mathrm{B}} = 10$ dB, $f_{\max} = 10$ Hz, $\xi_{\mathrm{th}} = 1$, and different values of ω_{E} are presented. As shown in this figure, the secrecy capacity decreases with the increased values of ω_{E} (which is evident from the region of the curve below ξ_{th}. This is because, by increasing ω_{E}, the level of the instantaneous capacity at the eavesdropper channel increases,

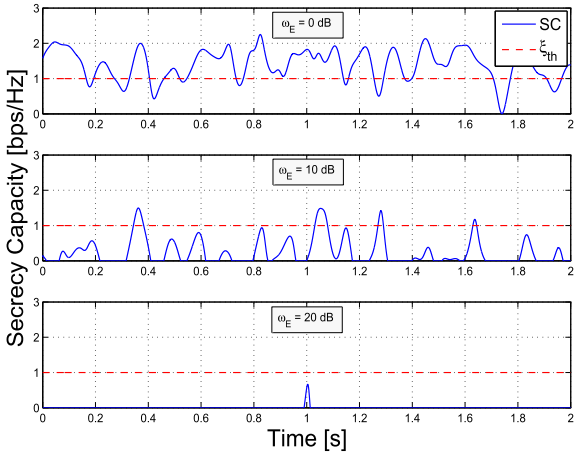

Fig. 2. Secrecy capacity realizations versus time for a noise limited system, with $m = 2$, $L_{\mathrm{AB}} = 2$, $L_{\mathrm{AE}} = 2$, $\omega_{\mathrm{B}} = 10$ dB, $f_{\max} = 10$ Hz, $\xi_{\mathrm{th}} = 1$, and different values of ω_{E}.

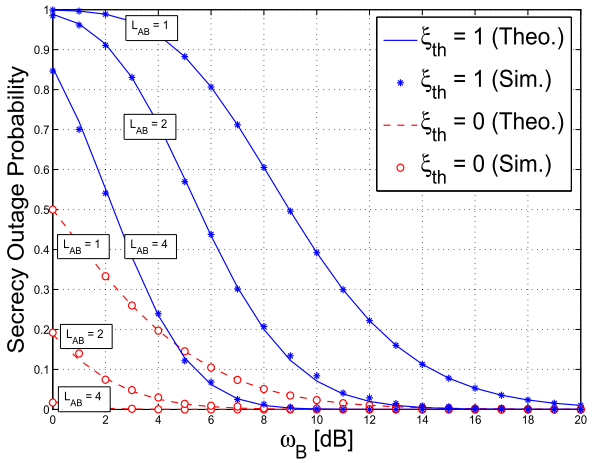

Fig. 3. Secrecy outage probability versus ω_{B} for a noise limited system, with $m = 2$, $L_{\mathrm{AE}} = 1$, $\omega_{\mathrm{E}} = 0$ dB, $f_{\max} = 10$ Hz, and different values of L_{AB} and ξ_{th}.

which results in a decrease of the secrecy capacity of the legitimate communications channels.

Fig. 3 presents the variation of the secrecy outage probability versus ω_{B} for a noise limited system, with $m = 2$, $L_{\mathrm{AE}} = 1$, $\omega_{\mathrm{E}} = 0$ dB, $f_{\max} = 10$ Hz, and different values of L_{AB} and ξ_{th}. It is clear that the secrecy outage probability decreases with the increased values of L_{AB} and ω_{B}. This is due to the fact that the increased values of L_{AB} and ω_{B} enhances the SNR at Bob, which decreases the secrecy outage probability. Also, and as expected, it is shown in this figure that the secrecy outage probability decreases with the decreased values of ξ_{th} for all values of L_{AB}. Consequently, systems requiring larger secrecy thresholds need to employ higher diversity order to maintain the same outage performance.

$$\mathfrak{R}^{(\mathrm{I})}(\xi_{\mathrm{th}}) \approx \frac{\sqrt{2\pi}\ \Gamma(\rho_{\mathrm{B}} - \frac{1}{2})\ f_{\max}\ \Omega_{\mathrm{B}}^{mL_{\mathrm{IB}}-\frac{1}{2}}\ \Omega_{\mathrm{E}}^{mL_{\mathrm{IE}}}}{2^{\xi_{\mathrm{th}}(2mL_{\mathrm{IB}}-1)}\Gamma(mL_{\mathrm{AB}})\ \Gamma(mL_{\mathrm{IB}})\ \mathfrak{B}(mL_{\mathrm{AE}}, mL_{\mathrm{IE}})} \sum_{n=1}^{N} \frac{w_n\ x_n^{mL_{\mathrm{AE}}-1}\left[x_n + 1 - 2^{-\xi_{\mathrm{th}}}\right]^{mL_{\mathrm{AB}}-\frac{1}{2}}\ \exp(x_n)}{\left[x_n + \Omega_{\mathrm{E}}\right]^{\rho_{\mathrm{E}}}\left[x_n + 1 - 2^{-\xi_{\mathrm{th}}}(1-\Omega_{\mathrm{B}})\right]^{\rho_{\mathrm{B}}-1}}. \quad (28)$$

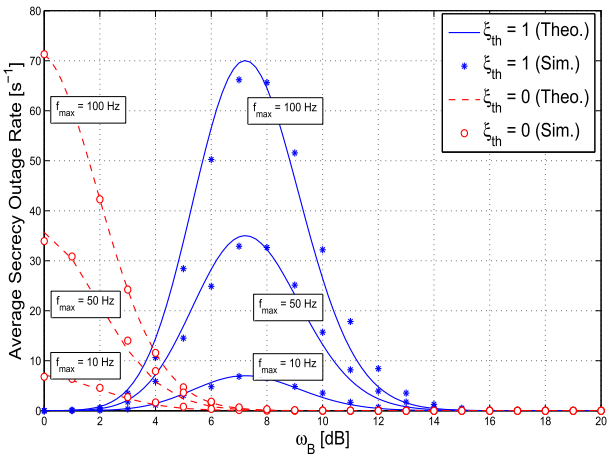

Fig. 4. Average secrecy outage rate versus ω_B for a noise limited system, with $m = 4$, $L_{AB} = 2$, $L_{AE} = 2$, $\omega_E = 0$ dB, and different values of f_{max} and ξ_{th}. (For $N = 50$, the Laguerre evaluation results in an average error less than $1e-2$ compared to the numerical evaluation of the integrations, using MatLab software.).

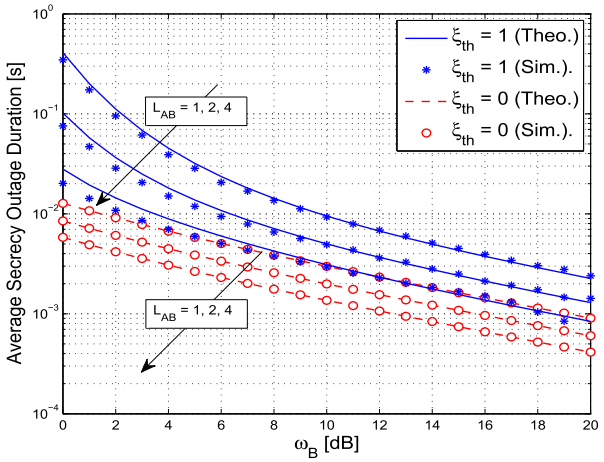

Fig. 5. Average secrecy outage duration versus ω_B for a noise limited system, with $m = 1$, $L_{AE} = 1$, $\omega_E = 0$ dB, $f_{max} = 50$ Hz, and different values of L_{AB} and ξ_{th}.

Fig. 4 presents the variation of the average secrecy outage rate [or average secrecy level crossing rate] versus ω_B for a noise limited system, with $m = 4$, $L_{AB} = 2$, $L_{AE} = 2$, $\omega_E = 0$ dB, and different values of f_{max} and ξ_{th}. As shown in this figure, for $\xi_{th} = 0$ and $\xi_{th} = 1$, the increased values of the maximum Doppler frequency shift f_{max} (which reflects nodes moving at higher speed) increase the average secrecy outage rate. This is due to the fact that the channel coherence time is inversely proportional to f_{max}, which results in fast fading channels between the different nodes in the network. Consequently, a fast variation of the secrecy capacity is observed, which increases the average secrecy level crossing rate. It is clear also that for $\xi_{th} = 1$, which refers to the case where the system has higher requirements in terms of secrecy outage, and for a given value of f_{max}, the ASOR curves have maximum values. This is because, for small values of ω_B, the instantaneous secrecy capacity is mostly below the threshold with occasional crossing upward, while at large values of ω_B, the instantaneous secrecy capacity is mostly above the threshold with occasional crossing downward.

In Fig. 5, the variation of the average secrecy outage duration versus ω_B for a noise limited system is presented, with $m = 1$, $L_{AE} = 1$, $\omega_E = 0$ dB, $f_{max} = 50$ Hz, and different values of L_{AB} and ξ_{th}. Similar to the behavior of the secrecy outage probability, the average secrecy outage duration decreases with the increased values of Ω_B and L_{AB}. This is because, the average secrecy outage duration is directly proportional to the secrecy outage probability as defined in Eq. (31).

Fig. 6 presents the average secrecy outage duration for a noise limited system, with $m = 2$, $\omega_B = \omega_E = 10$ dB, $f_{max} = 10$ Hz, $\xi_{th} = 0$, and different diversity orders on the main and wiretap channels (L_{AB} and L_{AE}). As shown in this figure, the average secrecy outage duration increases with the increased values of L_{AE} and decreases with the increased values of L_{AB}. This is due to the fact that the increase of the diversity order at Eve enhances the corresponding capacity,

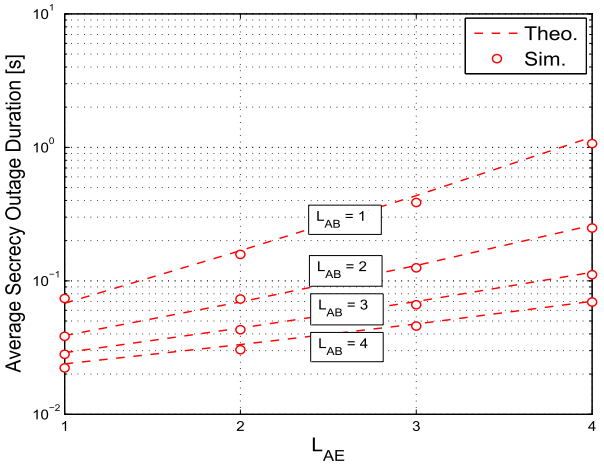

Fig. 6. Average secrecy outage duration versus L_{AE} for a noise limited system, with $m = 2$, $\omega_B = \omega_E = 10$ dB, $f_{max} = 10$ Hz, $\xi_{th} = 0$, and different values of L_{AB}.

which results in an increase of the secrecy outage probability, and hence an increase of the average secrecy outage duration can be observed. In contrast, the increased values of L_{AB} enhances the SNR at Bob, which decreases the secrecy outage probability as well as the average secrecy outage duration. We note also the diminishing effect in reducing the ASOD as we increase L_{AB} for a fixed L_{AE}, which is a natural diversity behavior.

Fig. 7 presents a comparison between the average secrecy outage duration and the well known average fade duration [26]–[28], for a noise limited system, with $m = 2$, $N_A = 1$, $N_B = N_E = 2$, $f_{max} = 10$ Hz, $\xi_{th} = 0$, fading threshold equal to 5 dB, and different values of ω_B and ω_E. The figure shows clearly the advantage of the proposed metric over current available metrics in the literature. While average fade duration gives an important insight on the main channel, it fails to reflect the level of secrecy of the system, and presents generally optimistic values (lower than expected) on the duration of "bad" intervals of the channel.

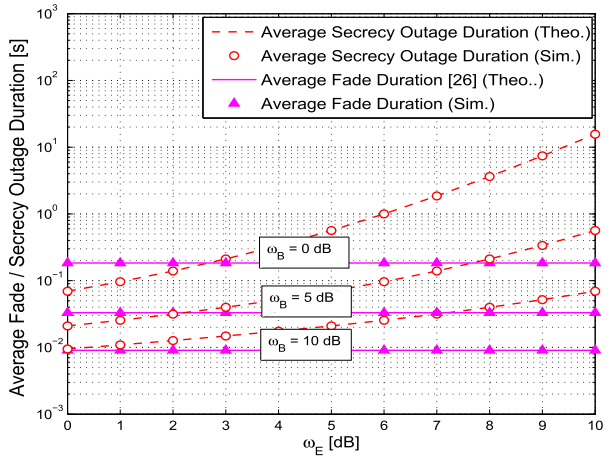

Fig. 7. Comparison between the average secrecy outage duration and the average fade duration, for a noise limited system, with $m = 2$, $N_{\rm A} = 1$, $N_{\rm B} = N_{\rm E} = 2$, $f_{\max} = 10$ Hz, $\xi_{\rm th} = 0$, fading threshold equal to 5 dB, and different values of ω_B and ω_E.

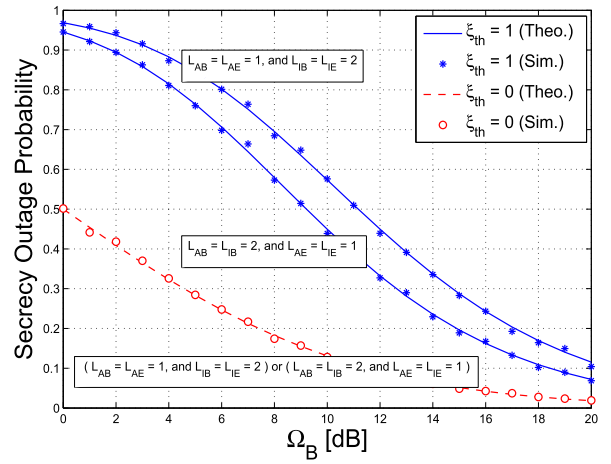

Fig. 8. Secrecy outage probability versus $\Omega_{\rm B}$ for an interference limited system, with $m = 1$, $\Omega_{\rm E} = 0$ dB, $f_{\max} = 10$ Hz, and different values of $L_{\rm AB}$, $L_{\rm IB}$, $L_{\rm AE}$, $L_{\rm IE}$, and $\xi_{\rm th}$.

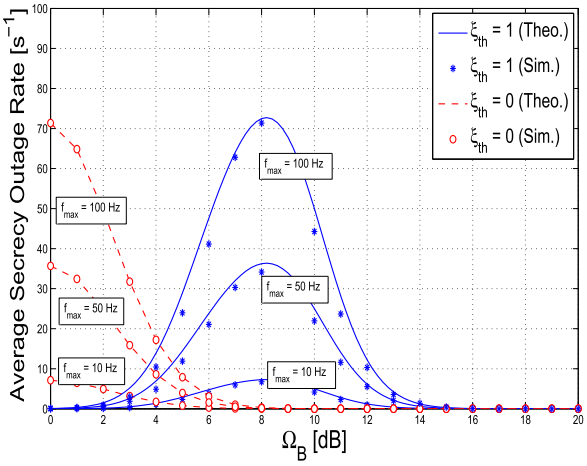

Fig. 9. Average secrecy outage rate versus $\Omega_{\rm B}$ for an interference limited system, with $m = 4$, $L_{\rm AB} = 4$, $L_{\rm AE} = 4$, $L_{\rm IB} = 3$, $L_{\rm IE} = 3$, $\Omega_{\rm E} = 0$ dB, and different values of $f_{\max}$ and $\xi_{\rm th}$.

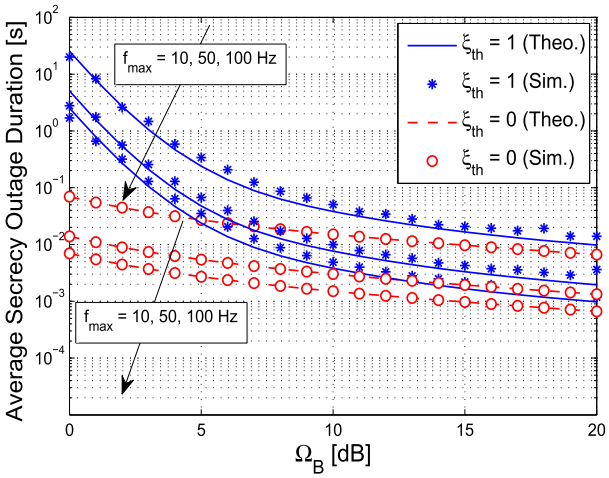

Fig. 10. Average secrecy outage duration versus $\Omega_{\rm B}$ for an interference limited system, with $m = 2$, $L_{\rm AB} = 2$, $L_{\rm AE} = 2$, $L_{\rm IB} = 2$, $L_{\rm IE} = 2$, $\Omega_{\rm E} = 0$ dB, and different values of $f_{\max}$ and $\xi_{\rm th}$.

B. Interference Limited Systems:

For interference limited systems, and without loss of generality, the conducted numerical results are also based on the simulation parameters in Table I.

The variation of the secrecy outage probability versus $\Omega_{\rm B}$ for an interference limited system is presented in Fig. 8, with $m = 1$, $\Omega_{\rm E} = 0$ dB, $f_{\max} = 10$ Hz, and different values of $L_{\rm AB}$, $L_{\rm IB}$, $L_{\rm AE}$, $L_{\rm IE}$, and $\xi_{\rm th}$. As shown in this figure, for $\xi_{\rm th} = 1$, having a higher diversity order on the Alice-Bob link has more positive impact on the system performance than receiving interference signals of the same order at Eve. This is simply because the interference source affects both Eve and Bob. However, for $\xi_{\rm th} = 0$, increasing the diversity order on the Alice-Bob link has the same impact on the system performance as the increase of the diversity of interference signals with the same order. This is because, for $\xi_{\rm th} = 0$, and based on (3), (4), and (16), the secrecy outage probability is directly proportional to $(L_{\rm AB} L_{\rm IE})$. Hence, for fixed values of $L_{\rm AE}$, $L_{\rm IB}$, $\Omega_{\rm B}$, and $\Omega_{\rm E}$, the simulation scenario of ($L_{\rm AB} = L_{\rm AE} = 1$ and $L_{\rm IB} = L_{\rm IE} = 2$) presents the same performance in term of the secrecy outage probability as the simulation scenario of ($L_{\rm AB} = L_{\rm IB} = 2$ and $L_{\rm AE} = L_{\rm IE} = 1$). Based on this, systems requiring higher secrecy thresholds for their outage tolerance need to invest resources in increasing the diversity order on the main link, rather than relying on having large interference levels that might affect the eavesdropper.

Fig. 9 presents the variation of the average secrecy outage rate versus $\Omega_{\rm B}$ for an interference limited system, with $m = L_{\rm AB} = L_{\rm AE} = 4$, $L_{\rm IB} = L_{\rm IE} = 3$, $\Omega_{\rm E} = 0$ dB, and different values of $f_{\max}$ and $\xi_{\rm th}$. Similar to the average secrecy outage rate behavior for noise limited systems, the increased values of $f_{\max}$, in this scenario, increases the average secrecy outage rate. This is because, as detailed before, increasing $f_{\max}$ results in fast variation of the secrecy capacity, and hence an increases of the average secrecy level crossing rate can be observed.

The variation of the average secrecy outage duration versus $\Omega_{\rm B}$ is presented in Fig. 10, with $m = L_{\rm AB} = L_{\rm AE} =$

$L_{\text{IB}} = L_{\text{IE}} = 2$, $\Omega_{\text{E}} = 0$ dB, and different values of $f_{\max}$ and ξ_{th}. As shown in this figure, for the different values of ξ_{th}, the average secrecy outage duration decreases with the increased values of $f_{\max}$. This is because, as detailed for Fig. 9, by increasing $f_{\max}$, the average secrecy outage rate increases, which decreases the average secrecy outage duration. Consequently, systems operating in fast mobility environments should consider optimizing their design based on the expected strength of the wiretap channel to avoid working in secrecy outage regions for extended times, or to suffer from frequent secrecy capacity drops, even with shorter periods on average.

V. Conclusion

In this paper, an analytical methodology for the security evaluation of wireless communication systems with diversity in wiretap channels has been proposed and evaluated, where two important physical layer security metrics have been introduced, and the corresponding analytical expressions have been derived for Nakagami-m fading channels. Based on that, numerical simulations have been conducted to evaluate the analytical results and to investigate the variations of the new metrics in different scenarios. These results have shown the importance of the proposed second order statistics metrics for the evaluation of the physical layer security dynamics. Specifically, communication security dropping rates and average outage regions are essentially affected by the diversity order at the receivers, and the maximum Doppler frequency shift. The results show that systems with high secrecy requirements should invest in increasing the diversity order of the main link.

Appendix A
Derivation of $P_{\text{out}}^{(\text{N})}$ for Noise Limited Systems

In this Appendix, we present the derivation of the secrecy outage probability expression in the case of a noise limited system.

Based on (10), $P_{\text{out}}^{(\text{N})}$ can be written as

$$P_{\text{out}}^{(\text{N})}(\xi_{\text{th}}) = \int_0^{\infty} \int_0^{2^{\xi_{\text{th}}}(1+y)-1} p_{\gamma_{\text{B}}}(x)\, p_{\gamma_{\text{E}}}(y)\, \mathrm{d}x\, \mathrm{d}y, \quad (34)$$

By using the PDF expression of γ_{B} in (11), and the integration by parts [38, eq. $3.351-1$.[8]], (34) can be rewritten as follows

$$\begin{aligned} P_{\text{out}}^{(\text{N})}(\xi_{\text{th}}) = {} & \frac{m^{mL_{\text{AB}}}}{\omega_{\text{B}}^{mL_{\text{AB}}}\ \Gamma(mL_{\text{AB}})} \\ & \times \int_0^{\infty} \Bigg[\exp\Big(-\frac{m[2^{\xi_{\text{th}}}(1+y)-1]}{\omega_{\text{B}}}\Big) \\ & \times \sum_{k=0}^{mL_{\text{AB}}-1} \frac{(-1)^k k! \binom{mL_{\text{AB}}-1}{k} \left(\frac{-\omega_{\text{B}}}{m}\right)^{k+1}}{[2^{\xi_{\text{th}}}(1+y)-1]^{-mL_{\text{AB}}+1+k}} \\ & + \left(\frac{\omega_{\text{B}}}{m}\right)^{mL_{\text{AB}}} (mL_{\text{AB}}-1)! \Bigg]\ p_{\gamma_{\text{E}}}(y)\ \mathrm{d}y. \end{aligned} \quad (35)$$

Now, by substituting the PDF expression of γ_{E} in (35), and by using the equality ($\Gamma(\text{N}) = (n-1)!$), the expression of $P_{\text{out}}^{(\text{N})}$ becomes

$$\begin{aligned} P_{\text{out}}^{(\text{N})}(\xi_{\text{th}}) = {} & 1 - \frac{m^{mL_{\text{AB}}}\ m^{mL_{\text{AE}}} \exp\Big(-\frac{m[2^{\xi_{\text{th}}}-1]}{\omega_{\text{B}}}\Big)}{\omega_{\text{B}}^{mL_{\text{AB}}}\ \omega_{\text{E}}^{mL_{\text{AE}}} \Gamma(mL_{\text{AB}})\ \Gamma(mL_{\text{AE}})} \\ & \times \sum_{k=0}^{mL_{\text{AB}}-1} \Bigg\{ k! \binom{mL_{\text{AB}}-1}{k} \left(\frac{\omega_{\text{B}}}{m}\right)^{k+1} 2^{\xi_{\text{th}}(mL_{\text{AB}}-1-k)} \\ & \times \int_0^{\infty} \frac{y^{mL_{\text{AE}}-1} \exp\Big(-\Big[\frac{m}{\omega_{\text{E}}} + \frac{m2^{\xi_{\text{th}}}}{\omega_{\text{B}}}\Big]y\Big)}{\Big[y+1-2^{-\xi_{\text{th}}}\Big]^{-mL_{\text{AB}}+1+k}}\ \mathrm{d}y \Bigg\}. \end{aligned} \quad (36)$$

By using the following finite sum in [38, eq. 1.111]

$$(a+y)^N = \sum_{n=0}^{N} \binom{N}{n} a^{N-n} y^n, \quad (37)$$

(36) can be rewritten as

$$\begin{aligned} & P_{\text{out}}^{(\text{N})}(\xi_{\text{th}}) \\ & = 1 - \frac{m^{mL_{\text{AB}}}\ m^{mL_{\text{AE}}} \exp\Big(-\frac{m[2^{\xi_{\text{th}}}-1]}{\omega_{\text{B}}}\Big)}{\omega_{\text{B}}^{mL_{\text{AB}}}\ \omega_{\text{E}}^{mL_{\text{AE}}} \Gamma(mL_{\text{AB}})\ \Gamma(mL_{\text{AE}})} \\ & \quad \times \sum_{k=0}^{mL_{\text{AB}}-1} \Bigg\{ k! \binom{mL_{\text{AB}}-1}{k} \left(\frac{\omega_{\text{B}}}{m}\right)^{k+1} 2^{\xi_{\text{th}}(mL_{\text{AB}}-1-k)} \\ & \quad \times \sum_{n=0}^{mL_{\text{AB}}-1-k} \Big\{ \binom{mL_{\text{AB}}-1-k}{n} \Big[1-2^{-\xi_{\text{th}}}\Big]^{mL_{\text{AB}}-1-k-n} \\ & \quad \times \int_0^{\infty} y^{mL_{\text{AE}}-1+n} \exp\Big(-\Big[\frac{m}{\omega_{\text{E}}} + \frac{m2^{\xi_{\text{th}}}}{\omega_{\text{B}}}\Big]y\Big)\ \mathrm{d}y \Big\} \Bigg\}. \end{aligned} \quad (38)$$

Based on [38, eq. $3.351-3$], the integration in (38) is evaluated, and $P_{\text{out}}^{(\text{N})}(\xi_{\text{th}})$ is expressed as

$$\begin{aligned} & P_{\text{out}}^{(\text{N})}(\xi_{\text{th}}) \\ & = 1 - \frac{m^{mL_{\text{AB}}}\ m^{mL_{\text{AE}}} \exp\Big(-\frac{m[2^{\xi_{\text{th}}}-1]}{\omega_{\text{B}}}\Big)}{\omega_{\text{B}}^{mL_{\text{AB}}}\ \omega_{\text{E}}^{mL_{\text{AE}}} \Gamma(mL_{\text{AB}})\ \Gamma(mL_{\text{AE}})} \\ & \quad \times \sum_{k=0}^{mL_{\text{AB}}-1} \Bigg\{ k! \binom{mL_{\text{AB}}-1}{k} \left(\frac{\omega_{\text{B}}}{m}\right)^{k+1} 2^{\xi_{\text{th}}(mL_{\text{AB}}-1-k)} \\ & \times \sum_{n=0}^{mL_{\text{AB}}-1-k} \frac{\binom{mL_{\text{AB}}-1-k}{n} \Big(n+mL_{\text{AE}}-1\Big)!}{\Big[1-2^{-\xi_{\text{th}}}\Big]^{k+n+1-mL_{\text{AB}}} \Big[\frac{m}{\omega_{\text{E}}} + \frac{m2^{\xi_{\text{th}}}}{\omega_{\text{B}}}\Big]^{n+mL_{\text{AE}}}} \Bigg\}. \end{aligned} \quad (39)$$

After some simplifications, the final exact closed form expression of $P_{\text{out}}^{(\text{N})}(\xi_{\text{th}})$ is given by (13) on the top of page 5.

Appendix B
Derivation of $P_{\text{out}}^{(\text{I})}$ for Interference Limited Systems

In this Appendix, we derive the expression of the secrecy outage probability for interference limited systems.

Based on (16), $P_{\text{out}}^{(\text{I})}$ is written as

$$P_{\text{out}}^{(\text{I})}(\xi_{\text{th}}) = \int_0^\infty \int_0^\infty \int_0^{y[2^{\xi_{\text{th}}}(1+v)-1]} p_{\alpha_{\text{AB}}^2}(x)\ \ p_{\alpha_{\text{IB}}^2}(y) \times p_{\lambda_{\text{E}}}(v)\ \text{d}x\text{d}y\text{d}v, \quad (40)$$

By using the PDF expression of α_{AB}^2, which is given by (5), and [38, eq. $3.351-1.^8$], (40) can be rewritten as follows

$$\begin{aligned} P_{\text{out}}^{(\text{I})}(\xi_{\text{th}}) &= \frac{m^{mL_{\text{AB}}}}{\Omega_{\text{AB}}^{mL_{\text{AB}}}\ \Gamma(mL_{\text{AB}})} \int_0^\infty \int_0^\infty \Bigg[\exp\Big(-\frac{my[2^{\xi_{\text{th}}}(1+v)-1]}{\Omega_{\text{AB}}}\Big) \\ &\times \sum_{k=0}^{mL_{\text{AB}}-1} \frac{(-1)^k k! \binom{mL_{\text{AB}}-1}{k} (y[2^{\xi_{\text{th}}}(1+v)-1])^{mL_{\text{AB}}-1-k}}{(\frac{-m}{\Omega_{\text{AB}}})^{k+1}} \\ &+ \Big(\frac{\Omega_{\text{AB}}}{m}\Big)^{mL_{\text{AB}}} (mL_{\text{AB}}-1)! \Bigg]\ p_{\alpha_{\text{IB}}^2}(y)\ p_{\lambda_{\text{E}}}(v)\ \text{d}y\ \text{d}v. \quad (41) \end{aligned}$$

By substituting the PDF expression of α_{IB}^2 in (41), and using the equality ($\Gamma(\text{N}) = (n-1)!$), the expression of $P_{\text{out}}^{(\text{I})}$ becomes

$$\begin{aligned} P_{\text{out}}^{(\text{I})}(\xi_{\text{th}}) &= 1 - \frac{m^{mL_{\text{AB}}}\ m^{mL_{\text{IB}}}}{\Omega_{\text{AB}}^{mL_{\text{AB}}}\ \Omega_{\text{IB}}^{mL_{\text{IB}}}\ \Gamma(mL_{\text{AB}})\ \Gamma(mL_{\text{IB}})} \\ &\times \int_0^\infty \int_0^\infty \exp\Big(-y\Big[\frac{m[2^{\xi_{\text{th}}}(1+v)-1]}{\Omega_{\text{AB}}} + \frac{m}{\Omega_{\text{IB}}}\Big]\Big) \\ &\times \sum_{k=0}^{mL_{\text{AB}}-1} y^{mL_{\text{IB}}+mL_{\text{AB}}-2-k} \Big(\frac{\Omega_{\text{AB}}}{m}\Big)^{k+1}\ k!\ \binom{mL_{\text{AB}}-1}{k} \\ &\times \Big[2^{\xi_{\text{th}}}(1+v)-1\Big]^{mL_{\text{AB}}-1-k} p_{\lambda_{\text{E}}}(v)\ \text{d}y\ \text{d}v. \quad (42) \end{aligned}$$

Based on [38, eq. $3.351-3$], the second integration in (42), with respect to y is evaluated, yielding

$$\begin{aligned} P_{\text{out}}^{(\text{I})}(\xi_{\text{th}}) &= 1 - \frac{m^{mL_{\text{AB}}}\ m^{mL_{\text{IB}}}}{\Omega_{\text{AB}}^{mL_{\text{AB}}}\ \Omega_{\text{IB}}^{mL_{\text{IB}}}\ \Gamma(mL_{\text{AB}})\ \Gamma(mL_{\text{IB}})} \\ &\times \Big(\frac{\Omega_{\text{AB}}}{m}\Big)^{mL_{\text{AB}}} (mL_{\text{AB}}-1)! - \frac{m^{mL_{\text{IB}}}}{\Omega_{\text{IB}}^{mL_{\text{IB}}}\ \Gamma(mL_{\text{IB}})} \\ &\times \int_0^\infty \sum_{k=0}^{mL_{\text{AB}}-1} \frac{(mL_{\text{IB}}+mL_{\text{AB}}-2-k)! \Big(\frac{\Omega_{\text{AB}}}{m}\Big)^{k+1} k! \binom{mL_{\text{AB}}-1}{k}}{\Big[\frac{m[2^{\xi_{\text{th}}}(1+v)-1]}{\Omega_{\text{AB}}} + \frac{m}{\Omega_{\text{IB}}}\Big]^{mL_{\text{IB}}+mL_{\text{AB}}-1-k}} \\ &\times \Big[2^{\xi_{\text{th}}}(1+v)-1\Big]^{mL_{\text{AB}}-1-k} p_{\lambda_{\text{E}}}(v)\ \text{d}v. \quad (43) \end{aligned}$$

By substituting (17) in (43), the expression of $P_{\text{out}}^{(\text{I})}(\xi_{\text{th}})$ can be rewritten as

$$\begin{aligned} P_{\text{out}}^{(\text{I})}(\xi_{\text{th}}) &= 1 - \frac{m^{mL_{\text{AB}}} m^{mL_{\text{IB}}} \Big(\frac{1}{\Omega_{\text{E}}}\Big)^{mL_{\text{AE}}}}{\Omega_{\text{AB}}^{mL_{\text{AB}}}\ \Gamma(mL_{\text{AB}}) \Omega_{\text{IB}}^{mL_{\text{IB}}}\ \Gamma(mL_{\text{IB}}) \mathfrak{B}(mL_{\text{AE}}, mL_{\text{IE}})} \\ &\times \sum_{k=0}^{mL_{\text{AB}}-1} (mL_{\text{IB}}+mL_{\text{AB}}-2-k)! \Big(\frac{\Omega_{\text{AB}}}{m}\Big)^{k+1} k! \binom{mL_{\text{AB}}-1}{k} \\ &\times \int_0^\infty \frac{\Big[2^{\xi_{\text{th}}}(1+v)-1\Big]^{mL_{\text{AB}}-1-k}\ v^{mL_{\text{AE}}-1}}{\Big[\frac{m[2^{\xi_{\text{th}}}(1+v)-1]}{\Omega_{\text{AB}}} + \frac{m}{\Omega_{\text{IB}}}\Big]^{mL_{\text{IB}}+mL_{\text{AB}}-1-k} \Big(1+\frac{v}{\Omega_{\text{E}}}\Big)^{mL_{\text{AE}}+mL_{\text{IE}}}} \\ &\times \text{d}v. \quad (44) \end{aligned}$$

By using the equality ($\Gamma(\text{N}) = (n-1)!$), and after some simplifications, (44) can be simplified to

$$\begin{aligned} P_{\text{out}}^{(\text{I})}(\xi_{\text{th}}) &= 1 - \frac{\Omega_{\text{B}}^{mL_{\text{IB}}}\ \Omega_{\text{E}}^{mL_{\text{IE}}}}{\mathfrak{B}(mL_{\text{AE}}, mL_{\text{IE}})} \sum_{k=0}^{mL_{\text{AB}}-1} \binom{mL_{\text{IB}}+mL_{\text{AB}}-2-k}{mL_{\text{IB}}-1} \\ &\times \int_0^\infty \frac{2^{-\xi_{\text{th}} mL_{\text{IB}}} \Big[v+1-\frac{1}{2^{\xi_{\text{th}}}}\Big]^{mL_{\text{AB}}-1-k}\ v^{mL_{\text{AE}}-1}}{\Big[v+1-\frac{1-\Omega_{\text{B}}}{2^{\xi_{\text{th}}}}\Big]^{mL_{\text{IB}}+mL_{\text{AB}}-1-k} \Big(v+\Omega_{\text{E}}\Big)^{mL_{\text{AE}}+mL_{\text{IE}}}}\ \text{d}v. \quad (45) \end{aligned}$$

By using the finite sum [38, eq. 1.111], and carrying out some simplification steps, (45) can be written as

$$\begin{aligned} P_{\text{out}}^{(\text{I})}(\xi_{\text{th}}) &= 1 - \frac{\Omega_{\text{B}}^{mL_{\text{IB}}}\ \Omega_{\text{E}}^{mL_{\text{IE}}}}{\mathfrak{B}(mL_{\text{AE}}, mL_{\text{IE}})} \sum_{k=0}^{mL_{\text{AB}}-1} \binom{mL_{\text{IB}}+mL_{\text{AB}}-2-k}{mL_{\text{IB}}-1} \\ &\times 2^{-\xi_{\text{th}} mL_{\text{IB}}} \sum_{n=0}^{mL_{\text{AB}}-1-k} \binom{mL_{\text{AB}}-1-k}{n} [1-2^{-\xi_{\text{th}}}]^{mL_{\text{AB}}-1-k-n} \\ &\times \int_0^\infty \frac{v^{n+mL_{\text{AE}}-1}}{\Big[v+1-\frac{1-\Omega_{\text{B}}}{2^{\xi_{\text{th}}}}\Big]^{mL_{\text{IB}}+mL_{\text{AB}}-1-k} \Big(v+\Omega_{\text{E}}\Big)^{mL_{\text{AE}}+mL_{\text{IE}}}} \\ &\times \text{d}v. \quad (46) \end{aligned}$$

Based on [38, eq. 3.197], the integration in (46) is evaluated and the final exact form expression of $P_{\text{out}}^{(\text{I})}(\xi_{\text{th}})$ is given by (18) on the top of page 5.

Appendix C
Derivation of $\mathfrak{R}^{(\text{N})}$ for Noise Limited Systems

For a noise limited system, the expression of ASOR, $\mathfrak{R}^{(\text{N})}(\xi_{\text{th}})$, is derived as follows.

Based on (21), $\mathfrak{R}^{(\text{N})}(\xi_{\text{th}})$ is given by

$$\mathfrak{R}^{(\text{N})}(\xi_{\text{th}}) = \int_0^\infty \int_0^\infty \dot{r}\ p_r(r_{\text{th}})\ p_{\dot{r}}(\dot{r})\ p_{\gamma_{\text{E}}}(y)\ \text{d}\dot{r}\ \text{d}y, \quad (47)$$

By substituting the expression of $p_{\dot{r}}$ of (23) in (47), $\mathfrak{R}^{(\text{N})}(\xi_{\text{th}})$ can be written as

$$\begin{aligned} \mathfrak{R}^{(\text{N})}(\xi_{\text{th}}) &= \int_0^\infty p_r(r_{\text{th}})\ p_{\gamma_{\text{E}}}(y) \\ &\times \int_0^\infty \frac{\sqrt{N_0}\ \dot{r}}{\sqrt{2\ \pi}\ \sigma_{\text{AB}}}\ \exp\Big(-\frac{N_0 \dot{r}^2}{2\ \sigma_{\text{AB}}^2}\Big)\ \text{d}\dot{r}\ \text{d}y, \quad (48) \end{aligned}$$

After evaluating the integration with respect to $\dot{r}$, (48) yields to

$$\mathfrak{R}^{(\text{N})}(\xi_{\text{th}}) = \frac{\sigma_{\text{AB}}}{\sqrt{2\ \pi}} \int_0^\infty p_r(r_{\text{th}})\ p_{\gamma_{\text{E}}}(y)\ \text{d}y, \quad (49)$$

Now, by using the expression of p_{r} in (22), the expression of $p_{\gamma_{\mathrm{E}}}$ in (12), and the expression of σ_{χ} that is given after Eq. (7), $\mathfrak{R}^{(\mathrm{N})}(\xi_{\mathrm{th}})$ is rewritten as

$$\mathfrak{R}^{(\mathrm{N})}(\xi_{\mathrm{th}}) = \frac{\sqrt{2\pi}\ f_{\max}\ \exp\Big(-\frac{m}{\omega_{\mathrm{B}}}\big[2^{\xi_{\mathrm{th}}}-1\big]\Big)\Big(\frac{m}{\omega_{\mathrm{B}}}\Big)^{mL_{\mathrm{AB}}}}{\Gamma(mL_{\mathrm{AB}})\ \Gamma(mL_{\mathrm{AE}})\ 2^{-\xi_{\mathrm{th}}(2mL_{\mathrm{AB}}-1)}\Big(\frac{m}{\omega_{\mathrm{E}}}\Big)^{-mL_{\mathrm{AE}}}} \times \int_0^{\infty} \frac{y^{mL_{\mathrm{AE}}-1}}{\big[y+1-2^{-\xi_{\mathrm{th}}}\big]^{-mL_{\mathrm{AB}}+\frac{1}{2}}} \times \exp\left(-x_n\left[\frac{m2^{\xi_{\mathrm{th}}}}{\omega_{\mathrm{B}}}+\frac{m}{\omega_{\mathrm{E}}}\right]\right)\mathrm{d}y. \tag{50}$$

By applying the Laguerre theorem [40], the average ASOR expression is given by (24) on the top of page 5.

For the special case of ($\xi_{\mathrm{th}} = 0$), and based on (50), the expression of $\mathfrak{R}(0)$ can be further simplified to

$$\mathfrak{R}^{(\mathrm{N})}(0) = \frac{\sqrt{2\pi}\ f_{\max}\ \Big(\frac{m}{\omega_{\mathrm{B}}}\Big)^{mL_{\mathrm{AB}}}}{\Gamma(mL_{\mathrm{AB}})\ \Gamma(mL_{\mathrm{AE}})\Big(\frac{m}{\omega_{\mathrm{E}}}\Big)^{-mL_{\mathrm{AE}}}} \times \int_0^{\infty} y^{mL_{\mathrm{AE}}+mL_{\mathrm{AB}}-\frac{3}{2}} \exp\left(-x_n\left[\frac{m}{\omega_{\mathrm{B}}}+\frac{m}{\omega_{\mathrm{E}}}\right]\right)\mathrm{d}y. \tag{51}$$

Based on [38, eq. $3.351-3$], the integration in (51) is evaluated, and the final expression of $\mathfrak{R}^{(\mathrm{N})}(0)$ is given by the exact form (25).

Appendix D
Derivation of $\mathfrak{R}^{(\mathrm{I})}$ for Interference Limited Systems

Based on (27), the expression of ASOR for an interference limited system is derived as follows

$$\mathfrak{R}^{(\mathrm{I})}(\xi_{\mathrm{th}}) = \int_0^{\infty}\int_0^{\infty} \dot{\beta}\ p_{\beta,\dot{\beta}}(\beta_{\mathrm{th}},\dot{\beta})\ p_{\lambda_{\mathrm{E}}}(v)\ \mathrm{d}\dot{\beta}\ \mathrm{d}\lambda_{\mathrm{E}}, \tag{52}$$

The expression of $p_{\beta,\dot{\beta}}$ is given by [26]

$$p_{\beta,\dot{\beta}}(\beta_{\mathrm{th}},\dot{\beta}) = \int_0^{\infty}\int_{-\infty}^{\infty} \alpha_{\mathrm{IB}}^2\ p_{\alpha_{\mathrm{AB}}}(\beta\ \alpha_{\mathrm{IB}})\ p_{\dot{\alpha}_{\mathrm{AB}}}(\dot{\beta}\ \alpha_{\mathrm{IB}}+\beta\ \dot{\alpha}_{\mathrm{IB}}) \times p_{\alpha_{\mathrm{IB}}}(\alpha_{\mathrm{IB}})\ p_{\dot{\alpha}_{\mathrm{IB}}}(\dot{\alpha}_{\mathrm{IB}})\ \mathrm{d}\dot{\alpha}_{\mathrm{IB}}\ \mathrm{d}\alpha_{\mathrm{IB}}. \tag{53}$$

By substituting (53) in (52), and based on the derivation details of the LCR in the case of the well know outage probability that is presented in [26], $\mathfrak{R}^{I}(\xi_{\mathrm{th}})$ can be expressed as follows

$$\mathfrak{R}^{I}(\xi_{\mathrm{th}}) = \frac{\sqrt{2\pi}\Gamma(mL_{\mathrm{AB}}+mL_{\mathrm{IB}}-\frac{1}{2})f_{\max}}{\Gamma(mL_{\mathrm{AB}})\ \Gamma(mL_{\mathrm{IB}})} \times \int_0^{\infty} p_{\lambda_{\mathrm{E}}}(v)\frac{\Omega_{\mathrm{B}}^{mL_{\mathrm{IB}}-\frac{1}{2}}\big[2^{\xi_{\mathrm{th}}}\big(1+v\big)-1\big]^{mL_{\mathrm{AB}}-\frac{1}{2}}}{\Big[2^{\xi_{\mathrm{th}}}\big(1+v\big)-1+\Omega_{\mathrm{B}}\Big]^{mL_{\mathrm{AB}}+mL_{\mathrm{IB}}-1}}\mathrm{d}v. \tag{54}$$

By substituting the PDF expression of v, given by (17), in (54), $\mathfrak{R}^{I}(\xi_{\mathrm{th}})$ is expressed as

$$\mathfrak{R}^{(\mathrm{I})}(\xi_{\mathrm{th}}) = \frac{\sqrt{2\pi}\ \Gamma(mL_{\mathrm{AB}}+mL_{\mathrm{IB}}-\frac{1}{2})\ f_{\max}\ \Omega_{\mathrm{B}}^{mL_{\mathrm{IB}}-\frac{1}{2}}\ \Omega_{\mathrm{E}}^{mL_{\mathrm{IE}}}}{2^{\xi_{\mathrm{th}}(2mL_{\mathrm{IB}}-1)}\Gamma(mL_{\mathrm{AB}})\ \Gamma(mL_{\mathrm{IB}})\ \mathfrak{B}(mL_{\mathrm{AE}},mL_{\mathrm{IE}})} \times \int_0^{\infty} \frac{v^{mL_{\mathrm{AE}}-1}\ \big[v+1-2^{-\xi_{\mathrm{th}}}\big]^{mL_{\mathrm{AB}}-\frac{1}{2}}}{\Big(v+\Omega_{\mathrm{E}}\Big)^{mL_{\mathrm{AE}}+mL_{\mathrm{IE}}}\Big[v+1-2^{-\xi_{\mathrm{th}}}\big(1-\Omega_{\mathrm{B}}\big)\Big]^{mL_{\mathrm{AB}}+mL_{\mathrm{IB}}-1}}\mathrm{d}v. \tag{55}$$

By applying the Laguerre theorem, the ASOR expression is given by (28).

For the special case of ($\xi_{\mathrm{th}} = 0$), and based on (55), the expression of $\mathfrak{R}^{(\mathrm{I})}(0)$ is rewritten as

$$\mathfrak{R}^{(\mathrm{I})}(0) = \frac{\sqrt{2\pi}\ \Gamma(mL_{\mathrm{AB}}+mL_{\mathrm{IB}}-\frac{1}{2})\ f_{\max}\ \Omega_{\mathrm{B}}^{mL_{\mathrm{IB}}-\frac{1}{2}}\ \Omega_{\mathrm{E}}^{mL_{\mathrm{IE}}}}{\Gamma(mL_{\mathrm{AB}})\ \Gamma(mL_{\mathrm{IB}})\ \mathfrak{B}(mL_{\mathrm{AE}},mL_{\mathrm{IE}})} \times \int_0^{\infty} \frac{v^{mL_{\mathrm{AB}}+mL_{\mathrm{AE}}-\frac{3}{2}}}{\Big[v+\Omega_{\mathrm{E}}\Big]^{mL_{\mathrm{AE}}+mL_{\mathrm{IE}}}\ \Big[v+\Omega_{\mathrm{B}}\Big]^{mL_{\mathrm{AB}}+mL_{\mathrm{IB}}-1}}\mathrm{d}v. \tag{56}$$

Based on [38, eq. 3.197], the integration in (56) is evaluated, and the final expression of $\mathfrak{R}^{(\mathrm{I})}(0)$ is given by the exact form (29) in page 5.

References

[1] T. M. Hoang, T. Q. Duong, N.-S. Vo, and C. Kundu, "Physical layer security in cooperative energy harvesting networks with a friendly jammer," *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 174–177, Apr. 2017.

[2] S. Iwata, T. Ohtsuki, and P.-Y. Kam, "A lower bound on secrecy capacity for MIMO wiretap channel aided by a cooperative jammer with channel estimation error," *IEEE Access*, vol. 5, pp. 4636–4645, Mar. 2017.

[3] Y. J. Tolossa, S. Vuppala, and G. Abreu, "Secrecy-rate analysis in multitier heterogeneous networks under generalized fading model," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 101–110, Feb. 2017.

[4] H.-M. Wang and X.-G. Xia, "Enhancing wireless secrecy via cooperation: Signal design and optimization," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 47–53, Dec. 2015.

[5] W. K. Harrison and S. W. McLaughlin, "Tandem coding and cryptography on wiretap channels: EXIT chart analysis," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun./Jul. 2009, pp. 1939–1943.

[6] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[7] O. O. Koyluoglu and H. El Gamal, "Polar coding for secure transmission and key agreement," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1472–1483, Oct. 2012.

[8] M. Bloch, M. Debbah, Y. Liang, Y. Oohama, and A. Thangaraj, "Special issue on physical-layer security," *J. Commun. Netw.*, vol. 14, no. 4, pp. 349–351, Aug. 2012.

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

[10] A. Salem and K. A. Hamdi, "Improving physical layer security of AF relay networks via beam-forming and jamming," in *Proc. IEEE 84th Veh. Technol. Conf. (VTC)-Fall*, Sep. 2016, pp. 1–5.

[11] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[12] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE 62nd Veh. Technol. Conf. (VTC-Fall)*, Sep. 2005, pp. 1906–1910.

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

[14] X. Zhou and M. McKay, "Physical layer security with artificial noise: Secrecy capacity and optimal power allocation," in *Proc. Int. Conf. Signal Process. Commun. Syst. (ICSPCS)*, Sep. 2009, pp. 1–5.
[15] W. Wang, K. C. Teh, and K. H. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1470–1482, Jun. 2017.
[16] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4347–4362, Nov. 2015.
[17] K. Tourki and M. O. Hasna, "A collaboration incentive exploiting the primary-secondary systems' cross interference for PHY security enhancement," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1346–1358, Dec. 2016.
[18] K. Tourki and M. O. Hasna, "Proactive spectrum sharing incentive for physical layer security enhancement using outdated CSI," *IEEE Trans. Wireless Commun.*, vol. 15, no. 9, pp. 6273–6283, Sep. 2016.
[19] L. Hu, H. Wen, B. Wu, J. Tang, and F. Pan, "Adaptive secure transmission for physical layer security in cooperative wireless networks," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 524–527, Mar. 2017.
[20] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
[21] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.
[22] W. Wang, K. C. Teh, and K. H. Li, "Relay selection for secure successive AF relaying networks with untrusted nodes," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2466–2476, Nov. 2016.
[23] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 63, no. 4, pp. 1678–1690, May 2014.
[24] N. Bhargav, S. L. Cotton, and D. E. Simmons, "Secrecy capacity analysis over κ-μ fading channels: Theory and applications," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3011–3024, Jul. 2016.
[25] O. Gungor, C. E. Koksal, and H. El Gamal, "On secrecy outage capacity of fading channels under relaxed delay constraints," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2013, pp. 2024–2028.
[26] L. Yang and M. S. Alouini, "On the average outage rate and average outage duration of wireless communication systems with multiple cochannel interferers," *IEEE Trans. Wireless Commun.*, vol. 3, no. 4, pp. 1142–1153, Jul. 2004.
[27] A. Olutayo, H. Ma, J. Cheng, and J. F. Holzman, "Level crossing rate and average fade duration for the Beaulieu-Xie fading model," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 326–329, Jun. 2017.
[28] X. Dong and N. C. Beaulieu, "Average level crossing rate and average fade duration of selection diversity," *IEEE Commun. Lett.*, vol. 5, no. 10, pp. 396–398, Oct. 2001.
[29] L. Yang, M. O. Hasna, and M. S. Alouini, "Average outage duration of multihop communication systems with regenerative relays," *IEEE Trans. Wireless Commun.*, vol. 4, no. 4, pp. 1366–1371, Jul. 2005.
[30] L. Yang and M.-S. Alouini, "Level crossing rate over multiple independent random processes: An extension of the applicability of the Rice formula," *IEEE Trans. Wireless Commun.*, vol. 6, no. 12, pp. 4280–4284, Dec. 2007.
[31] K. Otani, K. Daikoku, and H. Omori, "Burst error performance encountered in digital land mobile radio channel," *IEEE Trans. Veh. Technol.*, vol. VT-30, no. 4, pp. 156–160, Nov. 1981.
[32] Z. Cao and Y.-D. Yao, "Definition and drivation of level crossing rate and average fade duration in an interference-limited environment," in *Proc. IEEE 54th Veh. Technol. Conf. (VTC-Fall)*, Oct. 2001, pp. 1608–1611.
[33] M. Patzold and F. Laue, "Level-crossing rate and average duration of fades of deterministic simulation models for Rice fading channels," *IEEE Trans. Veh. Technol.*, vol. 48, no. 4, pp. 1121–1129, Jul. 1999.
[34] 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.
[35] X. Chen, X. Chen, and T. Liu, "A unified performance optimization for secrecy wireless information and power transfer over interference channels," *IEEE Access*, vol. 5, pp. 12726–12736, Jul. 2017.
[36] D. B. Rawat, T. White, S. Parwez, C. Bajracharya, and M. Song, "Evaluating secrecy outage of physical layer security in large-scale MIMO wireless communications for cyber-physical systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1987–1993, Dec. 2017.
[37] N. Balakrishnan N. L. Johnson, and S. Kotz, *Continuous Univariate Distributions*, vol. 2, 2nd ed. Hoboken, NJ, USA: Wiley, 1995.
[38] D. Zwillinger, *Table of Integrals, Series, and Products*, 8th ed. San Diego, CA, USA: Academic, 2014.
[39] G. L. Stuber, *Principles of Mobile Communication*, 4th ed. New York, NY, USA: Springer, 2017.
[40] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables*. New York, NY, USA: Dover, 1965.

Aymen Omri (M'13) received the telecommunication engineering degree from the Academy of Aviation, Tunisia, in 2007, and the M.Res. and Ph.D. degrees in telecommunications from the Engineering National School of Tunis, Tunis El Manar University, Tunisia, in 2009 and 2012.

From 2010 to 2012, he was a Research Assistant with the Electrical Engineering Department, Qatar University, Qatar, where he is currently a Post-Doctoral Researcher. His research interests include modeling, design, and performance analysis of wireless communication systems. His current research interests include device-to-device communications, UAV-based networks, and the fifth generation wireless communication networks.

Mazen O. Hasna (S'94–M'03–SM'07) received the B.S. degree from Qatar University, Doha, Qatar, in 1994, the M.S. degree from the University of Southern California at Los Angeles, Los Angeles, CA, USA, in 1998, and the Ph.D. degree from the University of Minnesota Twin Cities, Minneapolis, MN, USA, in 2003, all in electrical engineering. In 2003, he joined the Department of Electrical Engineering, Qatar University, where he is currently an Associate Professor.

His research interests include the general area of digital communication theory and its application to the performance evaluation of wireless communication systems over fading channels. His current specific research interests include cooperative communications, UAV-based networks, physical layer security, and FSO/RF hybrid networks.