Secrecy Capacity Analysis Over κ–μ Fading Channels: Theory and Applications

Secrecy Capacity Analysis Over κ–μ Fading Channels: Theory and Applications

Nidhi Bhargav, Simon L. Cotton, *Senior Member, IEEE*, and David E. Simmons

***Abstract*— In this paper, we consider the transmission of confidential information over a κ–μ fading channel in the presence of an eavesdropper who also experiences κ–μ fading. In particular, we obtain novel analytical solutions for the probability of strictly positive secrecy capacity (SPSC) and a lower bound of secure outage probability (SOP^L) for independent and non-identically distributed channel coefficients without parameter constraints. We also provide a closed-form expression for the probability of SPSC when the μ parameter is assumed to take positive integer values. Monte-Carlo simulations are performed to verify the derived results. The versatility of the κ–μ fading model means that the results presented in this paper can be used to determine the probability of SPSC and SOP^L for a large number of other fading scenarios, such as Rayleigh, Rice (Nakagami-*n*), Nakagami-*m*, One-Sided Gaussian, and mixtures of these common fading models. In addition, due to the duality of the analysis of secrecy capacity and co-channel interference (CCI), the results presented here will have immediate applicability in the analysis of outage probability in wireless systems affected by CCI and background noise (BN). To demonstrate the efficacy of the novel formulations proposed here, we use the derived equations to provide a useful insight into the probability of SPSC and SOP^L for a range of emerging wireless applications, such as cellular device-to-device, peer-to-peer, vehicle-to-vehicle, and body centric communications using data obtained from real channel measurements.**

***Index Terms*— Body centric communications, co-channel interference, device-to-device communications, fading channels, $\kappa - \mu$ fading, secrecy capacity, vehicular communications.**

I. Introduction

WITH the proliferation of smart devices, driven by applications such as the internet of things (IoT) [1], device-to-device communications (D2D) [2] and wearable sensors [3]–[5], privacy and security in wireless networking systems have once again been brought to the forefront. The wireless medium utilized by each of these applications has an inherent broadcast nature that makes it particularly susceptible to eavesdropping. Traditionally, these systems have attained secure communications by employing classical cryptographic techniques; e.g., RSA or AES [6]. Unfortunately, these algorithms are entirely disjoint from the physical nature of the wireless medium as they assume that the physical layer provides an error-free link. More recently, there has been growing interest in information-theoretic security that exploits the random nature of the wireless channel to guarantee the confidential transmission of messages [7]. It is widely believed that using this type of approach will provide the strictest form of security for physical layer communications [8].

The notion of perfect information-theoretic secrecy, i.e. $I(M; C) = 0$, where $I(\cdot; \cdot)$ denotes mutual information, M is the plane text message and C is its corresponding encryption, was first presented by Shannon [9]. These ideas were later developed by Wyner [10], in which he introduced the wiretap channel. Under the assumption that the wiretapper's channel is a probabilistically degraded version of the main channel, he studied the trade-off between the information rate and the achievable secrecy level for a wiretap channel and showed that it is possible to achieve a non-zero secrecy capacity. The secrecy capacity is defined as the largest transmission rate from the source to the destination, at which the eavesdropper is unable to obtain any information. Csiszár and Körner [11] later extended Wyner's work to non-degraded channels. Further developments were made in [12], where it was shown that it is possible to achieve secure communication in the presence of an eavesdropper over an additive white Gaussian noise (AWGN) channel provided the channel capacity of the legitimate user was greater than the eavesdropper's. The secrecy capacity was then shown to be equal to the difference between the two channel capacities.

The effect of fading on secrecy capacity was studied in [13]–[25]. Li *et al.* [13], Liang *et al.* [14] and Gopala *et al.* [15] characterized the secrecy capacity of ergodic fading channels and presented power and rate allocation schemes for secure communication. In [16] and [17], the secrecy capacity for multiple access and broadcast channels was considered. Barros and Rodrigues [18] showed that with signal fluctuation due to fading, information-theoretic security is achievable even when the eavesdropper's channel is of better average quality than that of the intended recipient. They analyzed the SOP and the outage secrecy capacity for Rayleigh fading channels when both the transmitter and the receiver are equipped with a single antenna in the presence of a solitary eavesdropping party. A similar analysis for a system consisting of a single antenna at the transmitter and multiple antennas

Manuscript received June 24, 2015; revised December 16, 2015 and March 7, 2016; accepted May 1, 2016. Date of publication May 10, 2016; date of current version July 12, 2016. This work was supported by the U.K. Royal Academy of Engineering, the Engineering and Physical Sciences Research Council under Grant References EP/H044191/1 and EP/L026074/1 and also by the Leverhulme Trust, UK through PLP-2011-061. The associate editor coordinating the review of this paper and approving it for publication was J. Yuan.

N. Bhargav and S. L. Cotton are with the Wireless Communications Laboratory, Institute of Electronics, Communications and Information Technology, Queen's University Belfast, Belfast BT3 9DT, U.K. (e-mail: nbhargav01@qub.ac.uk; simon.cotton@qub.ac.uk).

D. E. Simmons is with the Department of Engineering Science, University of Oxford, Oxford OX1 3PJ, U.K. (e-mail: david.simmons@eng.ox.ac.uk).

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/TCOMM.2016.2565580

at the receiver was presented in [19]. This was extended to multiple eavesdropping parties in [20] and over Nakagami-m fading channels in [21] and [22]. It was found that the SOP increases with the number of eavesdroppers and the average SNR of the eavesdropper. The outage secrecy capacity was found to increase with the Nakagami-m parameter, since an increase in m decreases the severity of fading in the channel. More recently, the secrecy characteristics of other commonly encountered fading models such as lognormal, Weibull and Rice have also been studied. For example, the probability of SPSC of lognormal fading channels was studied in [23], while the probability of SPSC and SOP^L of Weibull fading channels was investigated in [24]. In [25] a secrecy capacity analysis over Rice/Rice fading channels was conducted and the probability of non-zero secrecy capacity was determined.

While a number of important performance measures for κ-μ fading channels [26] have previously been developed such as energy detection based spectrum sensing [27]–[29] and outage probability analysis in interference-limited scenarios with restricted values of μ [29], to the best of the authors' knowledge the secrecy capacity of κ-μ fading channels has yet to be reported in the open literature. Due to the equivalency pointed out in [30], the results presented here will also have immediate applicability in the analysis of outage probability in cellular systems affected by co-channel interference (CCI) and background noise (BN), and the calculation of outage probability in interference-limited scenarios. Indeed the new equations proposed here provide an alternative, more general result than those presented in [29] (wherein the outage probability in interference-limited scenarios is restricted to particular values of the μ parameter) and allow the calculation of the relevant capacity formulations for arbitrary, real, positive values of the μ parameter. Motivated by this, we analyze the secrecy capacity of κ-μ fading channels in which we assume the eavesdropper to be passive and the channel state information (CSI) of the eavesdropper and the intended recipient are not available at the transmitter.

The main contributions of this paper are now listed as follows. Firstly, we derive novel analytical expressions for the probability of SPSC and SOP^L over *i.n.i.d.* κ-μ fading channels without any constraints on the channel parameters. Secondly, we provide an exact closed-form solution for the probability of SPSC over κ-μ fading channels when μ takes positive integer values. These expressions have been subsequently verified by reduction to known special cases and Monte-Carlo simulations. Thirdly and most importantly, because the κ-μ fading model [26] contains a number of other well-known fading models as special cases, the novel formulations presented in this paper unify the secrecy capacity of Rayleigh, Rice (Nakagami-n), Nakagami-m and One-Sided Gaussian fading channels, and their mixtures. Therefore they can be used to provide a useful insight into the secrecy capacity of eavesdropping scenarios which undergo generalized fading conditions. Fourthly, due to the known duality between the analysis of interference and eavesdropping [30], the utility of the results presented here extend well beyond their intended area of use. Put more precisely, they can also be used to analyze the outage probability in systems with CCI and BN, and the calculation of outage probability in interference-limited scenarios for κ-μ/κ-μ[1] fading channels. Finally, we provide important applications of these new results to estimate the probability of SPSC and SOP^L of a number of emerging wireless applications such as cellular device-to-device, peer-to-peer, vehicle-to-vehicle and body centric communications using data obtained from real channel measurements.

The remainder of this paper is organized as follows. Section II provides a brief overview of the κ-μ fading model. Section III explains the system model while Section IV provides the derivation of novel analytical and closed form expressions for the probability of SPSC and SOP^L. Section V discusses the secrecy capacity of the common fading models derived from the κ-μ fading model; this is followed by some numerical results. Section VI discusses some of the applications of this paper. Lastly, Section VII finishes the paper with some concluding remarks.

II. An Overview of the κ-μ Fading Model

The κ-μ fading model was originally conceived for modeling the small-scale variations of a fading signal under line-of-sight (LOS) conditions in homogeneous scattering environments [26]. The κ-μ fading signal is a composition of clusters of multipath waves with scattered waves of identical power with a dominant component of arbitrary power found within each cluster. Its received signal envelope, R, may be expressed in terms of the in-phase and quadrature components of the fading signal such that [26, eq. (6)]

$$R^2 = \sum_{i=1}^{\mu} (X_i + p_i)^2 + \sum_{i=1}^{\mu} (Y_i + q_i)^2 \tag{1}$$

where μ is the number of multipath clusters, X_i and Y_i are mutually independent Gaussian random processes with mean $E[X_i] = E[Y_i] = 0$ and variance $E\left[{X_i}^2\right] = E\left[{Y_i}^2\right] = \sigma^2$ (i.e., the power of the scattered waves in each of the clusters). Here p_i and q_i are the mean values of the in-phase and quadrature phase components of multipath cluster i and $d^2 = \sum_{i=1}^{\mu} {p_i}^2 + {q_i}^2$. Letting γ represent the instantaneous signal-to-noise-ratio (SNR) of a κ-μ fading channel, then its probability density function (PDF), $f_\gamma(\gamma)$, is obtained from the envelope PDF given in [26, eq. (11)] via a transformation of variables $\left(r = \sqrt{\gamma\ \hat{r}^2/\bar{\gamma}}\right)$ as

$$f_\gamma(\gamma) = \frac{\mu(1+\kappa)^{\frac{\mu+1}{2}}\,\gamma^{\frac{\mu-1}{2}}\,e^{\frac{-\mu(1+\kappa)\gamma}{\bar{\gamma}}}}{\kappa^{\frac{\mu-1}{2}}\,\bar{\gamma}^{\frac{\mu+1}{2}}\,e^{\mu\kappa}} I_{\mu-1}\left(2\mu\sqrt{\frac{\kappa(1+\kappa)\gamma}{\bar{\gamma}}}\right) \tag{2}$$

[1]Herein, it should be noted that we adopt the notation M/E to describe the fading conditions experienced by the main channel (M), and the eavesdropper (E). E.g. κ-μ/κ-μ indicates that the main and eavesdropper's channels are both subject to *i.n.i.d.* κ-μ fading. Due to the generality of the κ-μ fading model, M and E can be readily interchanged with the Rayleigh, Nakagami-m, Rice and One-sided Gaussian models which all appear as special cases of this fading model.

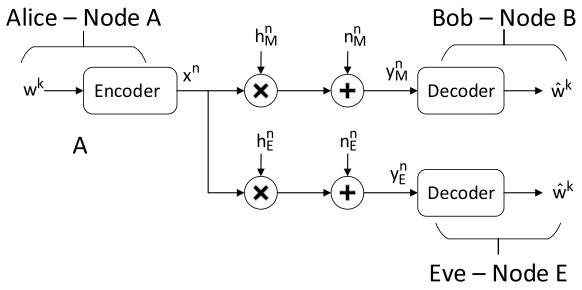

Fig. 1. The proposed system model.

where $\kappa > 0$ is the ratio of the total power of the dominant components (d^2) to the total power of the scattered waves ($2\mu\sigma^2$), $\mu > 0$ is related to the number of multipath clusters and is given by $\mu = \frac{\mathbb{E}^2(\gamma)(1+2\kappa)}{\mathbb{V}(\gamma)(1+\kappa)^2}$ where $\mathbb{E}(\cdot)$ and $\mathbb{V}(\cdot)$ denote the expectation and variance operators, respectively, $\bar{\gamma} = \mathbb{E}(\gamma)$, is the average SNR and $I_n(\cdot)$ is the modified Bessel function of the first kind and order n. As indicated in [26], it should be noted that the μ parameter can take non-integer values which can be due to the non-zero correlation between the in-phase and quadrature components of each cluster, non-zero correlation between the multipath clusters or non-Gaussian nature of the in-phase and quadrature components. The cumulative distribution function (CDF) of γ can be obtained from [26, eq. (3)] as

$$F_\gamma(\gamma) = 1 - Q_\mu\left[\sqrt{2\kappa\mu}, \sqrt{\frac{2(1+\kappa)\mu\gamma}{\bar{\gamma}}}\right] \tag{3}$$

where $Q_\cdot(\cdot,\cdot)$ is the generalized Marcum Q-function defined in [31, eq. (4.60)] as

$$Q_M(\alpha,\beta) = \frac{1}{\alpha^{M-1}}\int_\beta^\infty x^M e^{-\left(\frac{x^2+\alpha^2}{2}\right)} I_{M-1}(\alpha x)\,dx. \tag{4}$$

The κ-μ distribution is a generalized fading model which contains as special cases important distributions such as the Rice ($\mu = 1$; $\kappa = K$), Nakagami-m ($\kappa \to 0$; $\mu = m$), Rayleigh ($\mu = 1$; $\kappa \to 0$) and One-Sided Gaussian ($\mu = 0.5$; $\kappa \to 0$).

III. The System Model

Consider the system model of secure data transmission shown in Fig. 1. The legitimate transmitter, Alice (node A), wishes to communicate secretly with the legitimate receiver, Bob (node B), while a third party, Eve (node E), is attempting to eavesdrop. We assume that the main and eavesdropper's channels both experience κ-μ fading. Alice wishes to send a message, $w^k = [w(1), w(2)\ldots w(k)]$ to Bob. At the transmitter, the message w^k is encoded into a codeword, $x^n = [x(1), x(2)\ldots x(n)]$, for transmission over the channel. The signal received by Bob and Eve can be written as

$$y_M(i) = h_M(i)\,x(i) + n_M(i) \tag{5}$$
$$y_E(i) = h_E(i)\,x(i) + n_E(i) \tag{6}$$

where $h_M(i)$ and $h_E(i)$ are the quasi-static κ-μ fading coefficients of the main and the eavesdropper's channels, respectively (i.e., $h_M(i) = h_M \forall i$ and $h_E(i) = h_E \forall i$) and $n_M(i)$ and $n_E(i)$ are the zero-mean circularly symmetric complex Gaussian noise random variables with unit variance at Bob and Eve, respectively.

We assume that the fading coefficients of Bob and Eve's channels, although random, are constant during the transmission of an entire codeword and independent of each other. Letting P, N_M and N_E represent the average transmit power, noise power in the main channel, and noise power in the eavesdropper's channel respectively, then, the corresponding instantaneous SNR's at Bob and Eve are given by, $\gamma_M = \frac{P|h_M|^2}{N_M}$ and $\gamma_E = \frac{P|h_E|^2}{N_E}$, while the average SNR's are given by, $\bar{\gamma}_M = \frac{P\mathbb{E}(|h_M|^2)}{N_M}$ and $\bar{\gamma}_E = \frac{P\mathbb{E}(|h_E|^2)}{N_E}$. Now let us consider the channel components of Bob and Eve which are assumed to be *i.n.i.d.* random variables with parameters $\{\kappa_M, \mu_M, \bar{\gamma}_M\}$ and $\{\kappa_E, \mu_E, \bar{\gamma}_E\}$, respectively. The PDF's of γ_M and γ_E can be re-written from (2) as

$$f_{\gamma_M}(\gamma_M) = \frac{\mu_M(1+\kappa_M)^{\frac{\mu_M+1}{2}}\gamma_M^{\frac{\mu_M-1}{2}} e^{\frac{-\mu_M(1+\kappa_M)\gamma_M}{\bar{\gamma}_M}}}{\kappa_M^{\frac{\mu_M-1}{2}}\bar{\gamma}_M^{\frac{\mu_M+1}{2}} e^{\mu_M\kappa_M}} \times I_{\mu_M-1}\left(2\mu_M\sqrt{\frac{\kappa_M(1+\kappa_M)\gamma_M}{\bar{\gamma}_M}}\right) \tag{7}$$

$$f_{\gamma_E}(\gamma_E) = \frac{\mu_E(1+\kappa_E)^{\frac{\mu_E+1}{2}}\gamma_E^{\frac{\mu_E-1}{2}} e^{\frac{-\mu_E(1+\kappa_E)\gamma_E}{\bar{\gamma}_E}}}{\kappa_E^{\frac{\mu_E-1}{2}}\bar{\gamma}_E^{\frac{\mu_E+1}{2}} e^{\mu_E\kappa_E}} \times I_{\mu_E-1}\left(2\mu_E\sqrt{\frac{\kappa_E(1+\kappa_E)\gamma_E}{\bar{\gamma}_E}}\right). \tag{8}$$

Also, from (3) the CDF's of γ_M and γ_E can be written as

$$F_{\gamma_M}(\gamma_M) = 1 - Q_{\mu_M}\left[\sqrt{2\kappa_M\mu_M}, \sqrt{\frac{2(1+\kappa_M)\mu_M\gamma_M}{\bar{\gamma}_M}}\right] \tag{9}$$

$$F_{\gamma_E}(\gamma_E) = 1 - Q_{\mu_E}\left[\sqrt{2\kappa_E\mu_E}, \sqrt{\frac{2(1+\kappa_E)\mu_E\gamma_E}{\bar{\gamma}_E}}\right]. \tag{10}$$

IV. Secrecy Capacity in κ-μ Fading Channels

Here, we derive an analytical expression for the SOP^L. We also arrive at both an analytical and closed form expression for the probability of SPSC over κ-μ fading channels. In passive eavesdropping scenarios, where the CSI of the eavesdropper and the intended recipient are not available at the transmitter, perfect secrecy is not guaranteed. Hence, we are interested in calculating physical layer security metrics such as the probability of SPSC and SOP. For the system under consideration, the capacity of the main and the eavesdropper's channels are given by $C_M = \log_2(1+\gamma_M)$ and $C_E = \log_2(1+\gamma_E)$, respectively. From [8], we define the secrecy capacity, C_S, for one realization of the SNR pair (γ_M, γ_E) of the quasi-static complex fading wiretap channel as

$$C_S = \begin{cases} \log_2(1+\gamma_M) - \log_2(1+\gamma_E) & (\gamma_M > \gamma_E) \\ 0, & (\gamma_M \le \gamma_E) \end{cases} \tag{11}$$

A. SOP Analysis

The secrecy outage probability is the probability that the instantaneous secrecy capacity falls below a target secrecy rate R_S ($R_S \geq 0$) and is defined in [8] as

$$\mathcal{P}_{out}(R_S) = \mathbb{P}(C_S \leq R_S). \tag{12}$$

We now express R_S in terms of the threshold SNR, γ_{th}, related by $R_S = \log_2(1+\gamma_{th})$. Performing the necessary mathematical manipulations, we obtain

$$\mathcal{P}_{out}(\gamma_{th}) = \mathbb{P}\left[\gamma_M \leq (1+\gamma_{th})(1+\gamma_E) - 1\right] \tag{13}$$

which can then be expressed as

$$\begin{aligned}
&\mathcal{P}_{out}(\gamma_{th}) \\
&= \frac{\mu_E(1+\kappa_E)^{\frac{\mu_E+1}{2}}}{\kappa_E{}^{\frac{\mu_E-1}{2}}\overline{\gamma}_E{}^{\frac{\mu_E+1}{2}}e^{\mu_E\kappa_E}}\int_0^\infty \gamma_E{}^{\frac{\mu_E-1}{2}} \\
&\quad\times e^{\frac{-\mu_E(1+\kappa_E)\gamma_E}{\overline{\gamma}_E}} I_{\mu_E-1}\left(2\mu_E\sqrt{\frac{\kappa_E(1+\kappa_E)\gamma_E}{\overline{\gamma}_E}}\right) \\
&\quad\times\left(1 - Q_{\mu_M}\left(\sqrt{2\kappa_M\mu_M},\right.\right. \\
&\qquad\left.\left.\sqrt{\frac{2(1+\kappa_M)(\gamma_{th}+\gamma_{th}\gamma_E+\gamma_E)\mu_M}{\overline{\gamma}_M}}\right)\right)d\gamma_E.
\end{aligned} \tag{14}$$

Proof: See Appendix A. ∎

At present, due to the complicated form of the integral contained in (14) it is not possible to obtain a closed-form expression for the SOP, therefore, we derive the lower bound of SOP as follows [24]

$$\begin{aligned}
\mathcal{P}_{out}(\gamma_{th}) &= \mathbb{P}\left[\gamma_M \leq (1+\gamma_{th})(1+\gamma_E) - 1\right] \\
&\geq \mathrm{SOP}^L(\gamma_{th}) = \mathbb{P}\left[\gamma_M \leq (1+\gamma_{th})\gamma_E\right].
\end{aligned} \tag{15}$$

Now, using (8), (9) and (15) the lower bound of SOP is

$$\begin{aligned}
\mathrm{SOP}^L(\gamma_{th}) &= \frac{\mu_E(1+\kappa_E)^{\frac{\mu_E+1}{2}}}{\kappa_E{}^{\frac{\mu_E-1}{2}}\overline{\gamma}_E{}^{\frac{\mu_E+1}{2}}e^{\mu_E\kappa_E}}\int_0^\infty \gamma_E{}^{\frac{\mu_E-1}{2}} e^{\frac{-\mu_E(1+\kappa_E)\gamma_E}{\overline{\gamma}_E}} \\
&\quad\times I_{\mu_E-1}\left(2\mu_E\sqrt{\frac{\kappa_E(1+\kappa_E)\gamma_E}{\overline{\gamma}_E}}\right) \\
&\quad\times\left(1 - Q_{\mu_M}\left(\sqrt{2\kappa_M\mu_M},\right.\right. \\
&\qquad\left.\left.\sqrt{\frac{2(1+\kappa_M)(1+\gamma_{th})\gamma_E\mu_M}{\overline{\gamma}_M}}\right)\right)d\gamma_E.
\end{aligned} \tag{16}$$

The solution for (16) can be obtained via the following proposition.

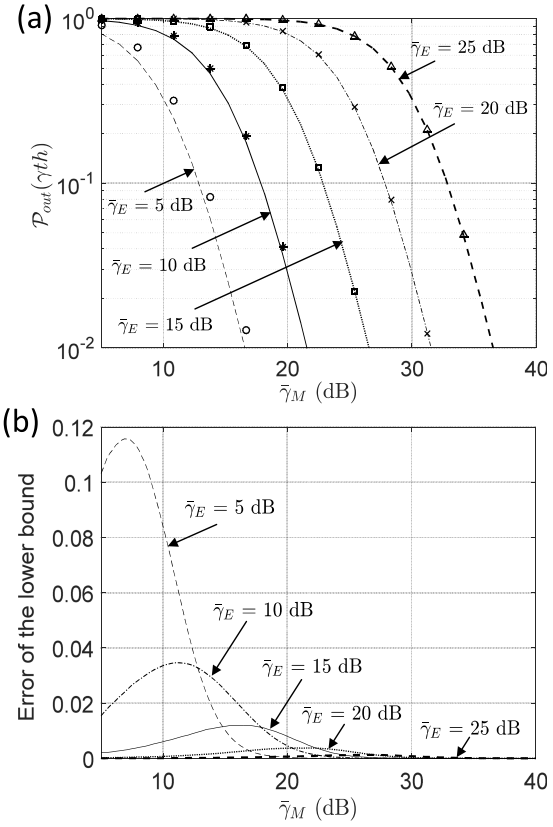

Fig. 2. (a) Comparison between the SOP and SOP^L. Lines represent (17) and markers represent simulation results for the SOP with $\gamma_{th} = 1.5$ dB. (b) Error of the lower bound versus $\bar{\gamma}_M$. In both figures $\kappa_M = 5$, $\kappa_E = 1.5$; $\mu_M = \mu_E = 2$.

Proposition 1: For the arbitrary real and positive μ_M, μ_E, κ_M and κ_E (16) can be evaluated as

$$\begin{aligned}
\mathrm{SOP}^L(\gamma_{th}) &= 1 - \frac{\beta_E{}^{\mu_E}}{e^{\alpha_E+\alpha_M}}\sum_{k=0}^{\infty}\sum_{l=0}^{\infty}\frac{(\alpha_E\beta_E)^k\alpha_M{}^l}{k!\,l!\,d\,\beta(c,d)} \\
&\quad\times\frac{(\beta_M(1+\gamma_{th}))^c}{(\beta_M(1+\gamma_{th})+\beta_E)^{c+d}} \\
&\quad\times {}_2F_1\left(1, c+d; d+1; \frac{\beta_E}{\beta_M(1+\gamma_{th})+\beta_E}\right)
\end{aligned} \tag{17}$$

where $a = 1/\bar{\gamma}_M$, $b = 1/\bar{\gamma}_E$, $c = \mu_M + l$, $d = \mu_E + k$, $\beta_M = (1+\kappa_M)a\mu_M$, $\beta_E = (1+\kappa_E)b\mu_E$, $\alpha_M = \kappa_M\mu_M$, $\alpha_E = \kappa_E\mu_E$, $\beta(c,d) = \frac{\Gamma(c)\Gamma(d)}{\Gamma(c+d)}$ is the Beta function and ${}_2F_1(\cdot\,,\cdot\,;\,\cdot\,;\,\cdot)$ is the Gauss hypergeometric function [32].

Proof: See Appendix B. ∎

Interestingly, by observing the second argument of $Q_{\cdot}(\cdot,\cdot)$ in (14) and (16), we see that, as $\bar{\gamma}_M$ grows large, the error of the lower bound will go to zero. Similarly, from (11) the same applies as $\bar{\gamma}_E$ grows large. To demonstrate this, we plot Figs. 2 (a) and (b). Fig. 2 (a) shows plots of $\mathcal{P}_{out}(\gamma_{th})$ and SOP^L as functions of $\bar{\gamma}_M$ for a range of $\bar{\gamma}_E$; while Fig. 2 (b) shows plots of the error between these two functions, again, as a function of $\bar{\gamma}_M$ for a range of $\bar{\gamma}_E$.

B. SPSC Analysis

In this subsection we examine the condition for the existence of strictly positive secrecy capacity. This occurs as a special case of the secrecy outage probability when the target secrecy rate, $R_S = 0$. According to [8] the probability of non-zero secrecy capacity is defined as

$$\mathcal{P}_0 = \mathbb{P}\left(C_S > 0\right) = \mathbb{P}\left(\gamma_M > \gamma_E\right). \tag{18}$$

In terms of the secrecy outage probability $\mathcal{P}_0$ is expressed as

$$\mathcal{P}_0 = 1 - \mathcal{P}_{out}\left(0\right) \tag{19}$$

Substituting $\gamma_{th} = 0$ in (14) and then using it in (19) the integral form of the probability of SPSC can be expressed as

$$\begin{aligned}\mathcal{P}_0 = {} & \frac{\mu_E(1+\kappa_E)^{\frac{\mu_E+1}{2}}}{\kappa_E{}^{\frac{\mu_E-1}{2}}\overline{\gamma}_E{}^{\frac{\mu_E+1}{2}}e^{\mu_E\kappa_E}}\int_0^\infty \gamma_E{}^{\frac{\mu_E-1}{2}}e^{\frac{-\mu_E(1+\kappa_E)\gamma_E}{\overline{\gamma}_E}} \\ & \times I_{\mu_E-1}\left(2\mu_E\sqrt{\frac{\kappa_E\left(1+\kappa_E\right)\gamma_E}{\overline{\gamma}_E}}\right) \\ & \times Q_{\mu_M}\left(\sqrt{2\kappa_M\mu_M}, \sqrt{\frac{2\left(1+\kappa_M\right)\mu_M\gamma_E}{\overline{\gamma}_M}}\right)d\gamma_E. \end{aligned} \tag{20}$$

The solution for (20) depends on the parameters μ_M and μ_E and is obtained via the following propositions.

Proposition 2: For the arbitrary real and positive μ_M and μ_E, (20) is evaluated by substituting $\gamma_{th} = 0$ in (17) and then using the obtained result in (19) as

$$\begin{aligned}\mathcal{P}_0 = {} & \frac{{\beta_E}^{\mu_E}}{e^{\alpha_E+\alpha_M}}\sum_{k=0}^{\infty}\sum_{l=0}^{\infty}\frac{(\alpha_E\beta_E)^k{\alpha_M}^l(\beta_M)^c}{k!\;l!\;d\;\beta\left(c,d\right)(\beta_M+\beta_E)^{c+d}} \\ & \times {}_2F_1\left(1, c+d; d+1; \frac{\beta_E}{\beta_M+\beta_E}\right)\end{aligned} \tag{21}$$

where $a = 1/\bar{\gamma}_M$, $b = 1/\bar{\gamma}_E$, $c = \mu_M + l$, $d = \mu_E + k$, $\beta_M = (1+\kappa_M)a\mu_M$, $\beta_E = (1+\kappa_E)b\mu_E$, $\alpha_M = \kappa_M\mu_M$, $\alpha_E = \kappa_E\mu_E$, $\beta(c,d) = \frac{\Gamma(c)\Gamma(d)}{\Gamma(c+d)}$ is the Beta function and ${}_2F_1(\cdot\,,\cdot\,;\,\cdot\,;\,\cdot)$ is the Gauss hypergeometric function [32].

Proposition 3: For integer values of μ_M and μ_E, an exact closed form solution for (20) is obtained as

$$\begin{aligned}\mathcal{P}_0 = {} & 1 - \acute{\mathcal{P}} + \exp\left(-\frac{A^2r + B^2r^{-1}}{2R}\right)\sum_{m=-\mu}^{\upsilon}\left(\frac{A}{Br}\right)^m I_m\left(\frac{AB}{R}\right) \\ & \times\left\{\sum_{k=1}^{\mu}\binom{\upsilon+k}{k+m}r^{\upsilon-k+1}R^{-\upsilon-k-1} - \sum_{j=1}^{\upsilon}\binom{j}{m}r^{j-1}R^{-j-1}\right\}\end{aligned} \tag{22}$$

where

$$\begin{aligned}\acute{\mathcal{P}} = {} & Q_1\left(\sqrt{\frac{A^2\acute{A}}{\acute{B}+\acute{A}}}, \sqrt{\frac{B^2\acute{B}}{\acute{B}+\acute{A}}}\right) - \left(\frac{\acute{B}}{\acute{B}+\acute{A}}\right) \\ & \times \exp\left(-\frac{A^2\acute{A}+B^2\acute{B}}{2\acute{B}+2\acute{A}}\right)I_0\left(\frac{\sqrt{A^2B^2\acute{A}\acute{B}}}{\acute{B}+\acute{A}}\right);\end{aligned}$$

$r = \sqrt{\frac{(1+\kappa_M)\mu_M a}{(1+\kappa_E)\mu_E b}}$; $A = \sqrt{2\kappa_E\mu_E}$; $B = \sqrt{2\kappa_M\mu_M}$; $\acute{A} = (1+\kappa_M)\,\mu_M a$; $\acute{B} = (1+\kappa_E)\,\mu_E b$; $\mu = \mu_E - 1$; $\upsilon = \mu_M - 1$; $a = \frac{1}{\bar{\gamma}_M}$; $b = \frac{1}{\bar{\gamma}_E}$ *and* $R = r + r^{-1}$.

Proof: See Appendix C. ∎

V. Special Cases and Numerical Results

In this section, we verify the novel analytical and closed-form expressions of the SOP^L and probability of SPSC derived above by first reducing the formulations to a number of known special cases and then, for the general case, performing Monte-Carlo simulations. We also use the formulations to provide a useful insight into the behavior of the SOP^L and SPSC as a function of the fading parameters of the legitimate and eavesdroppers channels.

A. Some Special Cases

As discussed previously, because of the generality of the κ-μ fading model the results presented here encompass the probability of SPSC and SOP^L for a wide range of fading channels.

1) Rice/Rice and Rayleigh/Rayleigh: To obtain the probability of SPSC for the case when both the main channel and eavesdropper's channel undergo Rician fading (i.e. a Rice/Rice fading scenario), we substitute $\mu_M = \mu_E = 1$ into (21) and/or (22) in which case these reduce to

$$\begin{aligned}\mathcal{P}_0 = {} & \frac{(1+\kappa_E)\,b}{e^{\kappa_E+\kappa_M}}\sum_{k=0}^{\infty}\sum_{l=0}^{\infty}\frac{\left(\kappa_E\left(1+\kappa_E\right)b\right)^k}{k!\Gamma\left(1+k\right)} \\ & \times\frac{(\kappa_M)^l}{l!\Gamma\left(1+l\right)}\frac{\left((1+\kappa_M)a\right)^{1+l}\Gamma\left(2+k+l\right)}{\left(1+k\right)\left(\left(1+\kappa_M\right)a+\left(1+\kappa_E\right)b\right)^{2+k+l}} \\ & \times {}_2F_1\left(1, 2+k+l; 2+k; \frac{\left(1+\kappa_E\right)b}{\left(1+\kappa_M\right)a+\left(1+\kappa_E\right)b}\right)\end{aligned} \tag{23}$$

and

$$\begin{aligned}\mathcal{P}_0 = {} & 1 - Q_1\left(\sqrt{\frac{2\kappa_E a\left(1+\kappa_M\right)}{b\left(1+\kappa_E\right)+a\left(1+\kappa_M\right)}}, \right. \\ & \left. \sqrt{\frac{2\kappa_M b\left(1+\kappa_E\right)}{b\left(1+\kappa_E\right)+a\left(1+\kappa_M\right)}}\right) \\ & + \left(\frac{b\left(1+\kappa_E\right)}{b\left(1+\kappa_E\right)+a\left(1+\kappa_M\right)}\right)e^{\left(-\frac{ak_E(1+\kappa_M)+b\kappa_M(1+\kappa_E)}{b(1+\kappa_E)+a(1+\kappa_M)}\right)} \\ & \times I_0\left(\frac{2\sqrt{ab\kappa_M\kappa_E\left(1+\kappa_E\right)\left(1+\kappa_M\right)}}{b\left(1+\kappa_E\right)+a\left(1+\kappa_M\right)}\right)\end{aligned} \tag{24}$$

which are in exact agreement with the result reported in [25, eq. (10)] and are illustrated visually in Fig. 3(a). Of course letting $\kappa_M = \kappa_E = 0$, then

$$\mathcal{P}_0 = \frac{\overline{\gamma}_M}{\overline{\gamma}_M + \overline{\gamma}_E} \tag{25}$$

which matches exactly with that given in [18, eq. (5)] for a Rayleigh/Rayleigh fading scenario.

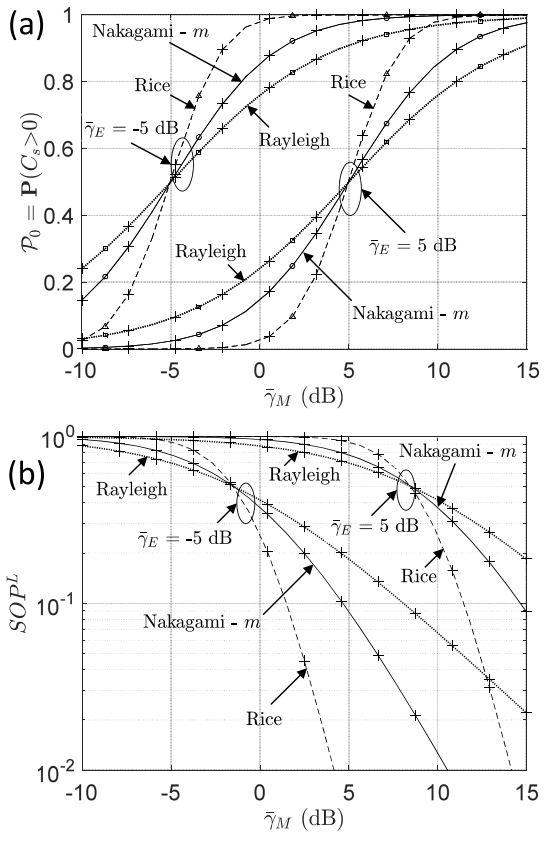

Fig. 3. (a) The probability of SPSC versus $\bar{\gamma}_M$. Triangle markers represent [25, eq. (10)] with $\kappa_a = 15$, $\kappa_b = 12$ for Rice; circle markers [21, eq. (8)] with $m = 2$; $N = 1$ for Nakagami-m and square markers [18, eq. (5)] for Rayleigh fading. (b) SOP^L versus $\bar{\gamma}_M$ with $\gamma_{th} = 1$ dB. Lines represent (21)/(22) in (a) and (17) in (b) for the special case of Rice ($\mu_M = \mu_E = 1$; $\kappa_M = 15$, $\kappa_E = 12$); Nakagami-m ($\kappa_M = \kappa_E \to 0$; $\mu_M = \mu_E = 2$) and Rayleigh fading ($\kappa_M = \kappa_E \to 0$; $\mu_M = \mu_E = 1$). Plus sign markers represent simulation results.

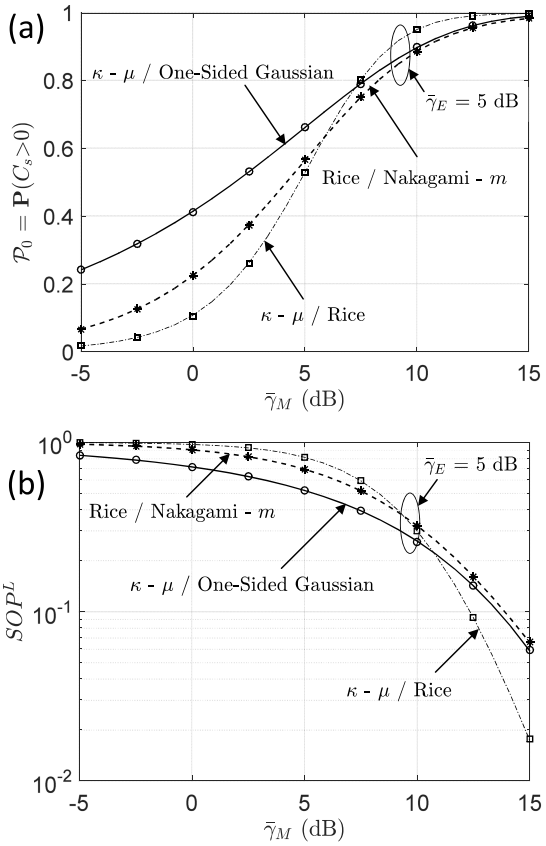

Fig. 4. (a) The probability of SPSC versus $\bar{\gamma}_M$ and (b) The lower bound of secrecy outage probability versus $\bar{\gamma}_M$ with $\gamma_{th} = 1$ dB. Both figures are obtained for the special case of κ-μ/One-Sided Gaussian ($\kappa_M = 4.5$; $\mu_M = 2$; $\kappa_E \to 0$; $\mu_E = 0.5$), Rice/Nakagami-m ($\kappa_M = 5$; $\mu_M = 1$; $\kappa_E \to 0$; $\mu_E = 1.2$) and κ-μ/Rice ($\kappa_M = 2.4$; $\mu_M = 3$; $\kappa_E = 4$; $\mu_E = 1$). Lines represent analytical results and markers represent simulations.

In a similar manner, substituting $\mu_M = \mu_E = 1$ in (17), we obtain the SOP^L for a Rice/Rice fading scenario as

$$\begin{aligned}\mathrm{SOP}^L(\gamma_{th}) &= 1 - \frac{(1+\kappa_E)\,b}{e^{\kappa_E+\kappa_M}} \sum_{k=0}^{\infty}\sum_{l=0}^{\infty} \frac{(\kappa_E(1+\kappa_E)\,b)^k {\kappa_M}^l}{k!l!\Gamma(1+k)\,\Gamma(1+l)} \\ &\times \frac{((1+\gamma_{th})(1+\kappa_M)\,a)^{1+l}\,\Gamma(2+k+l)}{(1+k)\,((1+\gamma_{th})(1+\kappa_M)\,a+(1+\kappa_E)\,b)^{2+k+l}} \\ &\times {}_2F_1\left(1, 2+k+l; 2+k; \frac{(1+\kappa_E)\,b}{(1+\gamma_{th})(1+\kappa_M)\,a+(1+\kappa_E)\,b}\right) \quad (26)\end{aligned}$$

It should be noted that the SOP or SOP^L for the case when both the main and the eavesdropper's channel undergo Rician fading has not been derived previously in the open literature. Of course letting $\kappa_M \to 0$ and $\kappa_E \to 0$ in (26), we obtain the SOP^L for a Rayleigh/Rayleigh fading scenario. The results presented here are in exact agreement with the simulated results and are visually illustrated in Fig. 3(b).

2) Nakagami-m/Nakagami-m: By letting $\kappa_M \to 0$ and $\kappa_E \to 0$ into (21) and/or (22), we obtain the probability of SPSC for the scenario where both the legitimate and non-legitimate users channels undergo Nakagami-m fading. As shown in Fig. 3(a), our results have been compared with that reported in [21, eq. (8)]. It should be noted that the expression proposed in [21, eq. (8)] is valid only for identical fading parameters of the main and the eavesdroppers channels and for integer values of the shape parameter, m (or equivalently μ when $\kappa \to 0$) when a single eavesdropper is considered whereas the equation proposed here is valid for any positive real value of the μ parameter. As shown in Fig. 3(a), for the case of integer μ_M and μ_E, the results presented here are in exact agreement with those presented in [21]. Similarly, letting $\kappa_M \to 0$ and $\kappa_E \to 0$ in (17), we obtain the SOP^L for a Nakagami-m/Nakagami-m fading scenario. Fig. 3(b) shows the lower bound of the secrecy outage probability versus $\bar{\gamma}_M$. It is seen that the numerical results are in exact agreement with the simulated ones.

3) Other Fading Scenarios: In a similar manner, the probability of SPSC and SOP^L for several different fading combinations, most of which have not previously been reported in the open literature, can be obtained through appropriate substitutions in (21), (22) and (17). Figs. 4 (a) and (b) show the shape of probability of SPSC and SOP^L for a selection of these scenarios, namely the κ-μ/One-Sided Gaussian, Rice/Nakagami-m and κ-μ/Rice.

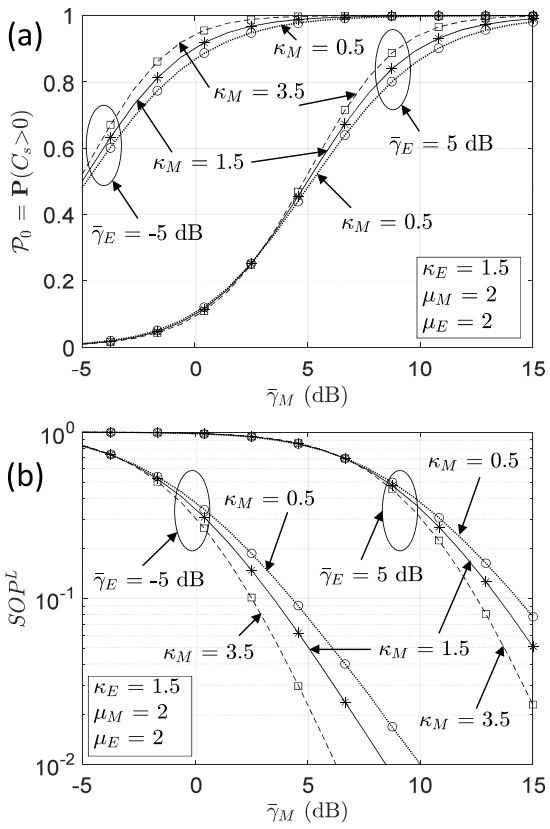

Fig. 5. (a) The probability of SPSC versus $\bar{\gamma}_M$ and (b) The lower bound of secrecy outage probability versus $\bar{\gamma}_M$ for γ_{th} = 1.5 dB. In both figures, $\kappa_E = 1.5$, $\mu_M = 2$ and $\mu_E = 2$. Lines represent analytical results and markers represent simulations.

B. Numerical Results

Here, we discuss the behavior of $\mathcal{P}_0$ and SOP^L as a function of the parameters $\{\kappa_M, \mu_M, \bar{\gamma}_M\}$ and $\{\kappa_E, \mu_E, \bar{\gamma}_E\}$. The results presented here have been verified through Monte-Carlo simulations. Two example profiles for the probability of SPSC and SOP^L are illustrated in Figs. 5 (a) and (b) with $\gamma_{th} = 0$ and 1.5 dB, respectively. These figures have been obtained when $\kappa_E = 1.5$ and $\mu_M = \mu_E = 2$.

From Figs. 5 (a) and (b), we observe that for a fixed $\bar{\gamma}_E$ the probability of SPSC increases and the secrecy outage probability decreases as $\bar{\gamma}_M$ increases. Since $\bar{\gamma}_M$ indicates the signal quality of the main channel, it is expected that improving this will lead to $\mathcal{P}_0$ being larger and SOP^L being smaller. From Fig. 5(a), we observe that the probability of SPSC is non-zero even when $\bar{\gamma}_M < \bar{\gamma}_E$. Furthermore, $\mathcal{P}_0$ increases as κ_M, the main channel's fading parameter, increases for fixed κ_E. From Fig. 5(b), we observe that for a fixed $\bar{\gamma}_M$, the SOP^L decreases as $\bar{\gamma}_E$ decreases. Additionally, we see that the SOP^L is negligibly affected by the main channels fading parameters for low values of $\bar{\gamma}_M$. Furthermore, for fixed κ_E, the SOP^L decreases as κ_M increases. Similar observations are made when κ_M, κ_E and μ_E are set and μ_M is varied.

VI. Applications of SPSC and SOP^L for Devices Operating in κ-μ Fading Channels

To illustrate the utility of the new equations proposed here, we now analyze the probability of SPSC and SOP^L for a number of emerging applications such as cellular device-to-device, body area network (BAN), peer-to-peer (P2P) and vehicle-to-vehicle (V2V) communications using channel data obtained from field trials. For all of the measurements conducted in this study, we considered a three node system which consisted of Alice which acted as the transmitter and also Bob and Eve which acted as the receivers. Each of the nodes: A, B and E, consisted of an ML5805 transceiver, manufactured by RFMD. The transceiver boards were interfaced with a PIC32MX which acted as a baseband controller and allowed the analog received signal strength (RSS) to be sampled with a 10-bit quantization depth. For all of the experiments conducted here, node A was configured to output a continuous wave signal with a power level of +17.6 dBm at 5.8 GHz while nodes B and E sampled the channel at a rate of 1 kHz. The antennas used by the transmitter and the receivers were +2.3 dBi sleeve dipole antennas (Mobile Mark model PSKN3-24/55S).

A. Device-to-Device Scenario

The first set of measurements considered cellular device-to-device communications channels operating at 5.8 GHz in an indoor environment located on the first floor of the ECIT building at Queen's University Belfast in the United Kingdom. The building mainly consists of metal studded dry walls with metal tiled floors covered with polypropylene-fiber, rubber backed carpet tiles, a metal ceiling with mineral fiber tiles and recessed louvered luminaries suspended 2.7 m above floor level. The D2D experiments were conducted in a large seminar room with dimensions of 7.92 m × 12.58 m × 2.75 m and contained a number of chairs, some desks constructed from medium density fiberboard, a projector and a white board. For these measurements, the antennas were housed in a compact acrylonitrile butadiene styrene (ABS) enclosure (107 × 55 × 20 mm). This setup was representative of the form factor of a smart phone which allowed the user to hold the device as they normally would to make a voice call. Each antenna was securely fixed to the inside of the enclosure using a small strip of Velcro®. The antennas were connected using low-loss coaxial cables to nodes A, B and E.

The experiment was performed when the room was unoccupied except for the test subjects holding the devices. As shown in Fig. 6(a), this particular scenario considered three persons carrying nodes A, B and E who were positioned at points X, Y and Z respectively. The three test subjects using nodes A, B and E were adult males of height 1.72 m, 1.84 m and 1.83 m; mass 80 kg, 92 kg and 74 kg, respectively. During the measurement trial, all three persons were initially stationary and had the hypothetical user equipment (UE) positioned at their heads. The persons at points Y and Z were then instructed to move around randomly within a circle of radius 0.5 m from their starting points while imitating a voice call. A total of 74763 samples of the received signal power were obtained and used for parameter estimation.

Figs. 7(a) and (b) show the empirical PDF of the signal envelope for Bob and Eve compared to the κ-μ PDF given in [26, eq. (11)] for the D2D channel measurements. All parameter estimates for the κ-μ fading model were

TABLE I

PARAMETER ESTIMATES FOR THE $\kappa - \mu$ FADING MODEL OBTAINED FROM THE FIELD MEASUREMENTS

Fading Channel	$\hat{\kappa}_M$	$\hat{\mu}_M$	$\hat{\bar{r}}_E$	$\hat{\kappa}_E$	$\hat{\mu}_E$	$\hat{\bar{r}}_E$
D2D	1.07	0.91	1.22	1.11	0.92	1.19
On-Body	2.92	0.75	1.17	3.60	0.67	1.17
P2P	8.03	2.6	1.00	18.09	2.31	1.01
V2V	5.02	0.70	1.04	7.17	0.60	1.03

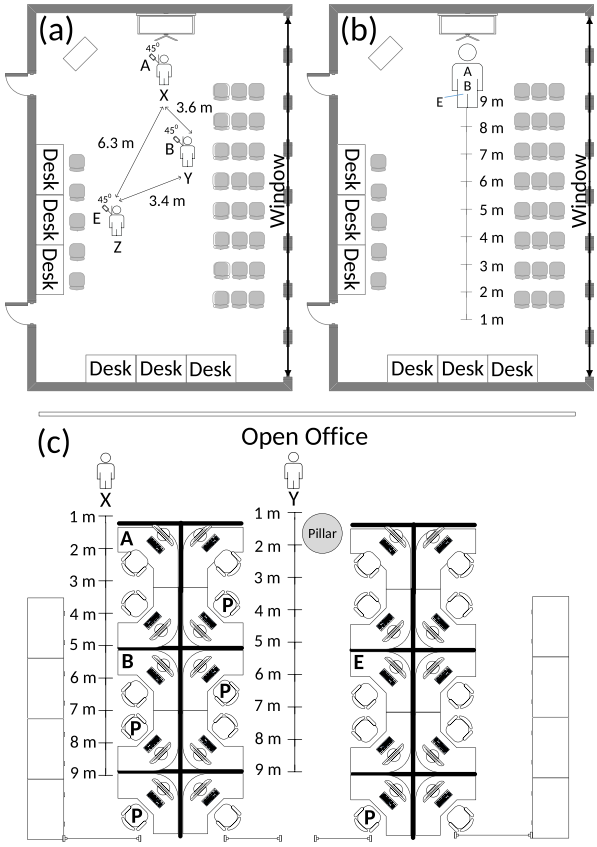

Fig. 6. Seminar room environment showing the position of nodes A, B and E for (a) D2D scenario and (b) on-body scenario, while (c) shows the open office environment with position of nodes A, B and E for P2P scenario. P indicates the locations at which people remained seated.

obtained using the `lsqnonlin` function available in the optimization toolbox of Matlab along with the κ-μ PDF given in [26, eq. (11)]. To compute the estimates, a set of lower and upper bounds for the κ - μ parameters are first defined,[2] and then some initial starting points for the parameters are chosen randomly and input into the Matlab function. The Matlab function then uses the Trust-Region-Reflective least squares algorithm [33], [34] to obtain the optimal points. This algorithm minimises a function $f(x)$ by approximating f with a simpler function q, that is given by the first two terms of the Taylor approximation to f at x. Optimization is then performed with respect to q within some neighbourhood N of x. Let $\acute{x}$ be the point obtained from this optimization procedure. If $f\left(\acute{x}\right) < f(x)$, the current point x is updated to $\acute{x}$ otherwise the point remains unchanged and the neighbourhood about x is shrunk. This is repeated until the optimal points are found. It should be noted that to remove the impact of any shadowing processes, which are not accounted for in the κ-μ fading model, the data sets were normalized to their respective local means prior to parameter estimation. To determine the window size for extraction of the local mean signal, the raw data was visually inspected and overlaid with the local mean signal for differing window sizes. For the D2D channel data, a smoothing window of 500 samples was used. As we can quite clearly see, from Figs. 7(a) and (b), the envelope PDF of the κ-μ fading model provides an excellent fit to the D2D data. To allow the reader to reproduce these plots, parameter estimates for all four measurement scenarios are given in Table I.

Using the parameter estimates obtained from the field trials, Figs. 7(c) and (d) depict the estimated probability of SPSC and SOP^L versus $\bar{\gamma}_E$ for selected values of $\bar{\gamma}_M$ for the measured D2D channel, respectively. In this instance, it can be seen that the estimates for κ of the main and eavesdropper's channels are comparable and also greater than 0, suggesting that a dominant component existed for both. We also observe that the parameter estimates for μ_M and μ_E are both quite close to 1, suggesting that a single multipath cluster contributes to the signal received by both node B and node E and thus this fading scenario is quite close to the Rician case.

Throughout the remainder of this paper, we adopt the following approach to analyse the secrecy metrics discussed in section IV. For all of the SPSC measurement scenarios, we perform our analysis when $\bar{\gamma}_M$ is fixed at 10 dB and for two different levels of P_0: 0.25 (25% SPSC level) and 0.5 (50% SPSC level), which are indicative of a relatively low and mid-range level of SPSC, respectively. Equivalently, for the secrecy outage probability performance metric, our analysis is carried out when $\bar{\gamma}_M$ is fixed at 10 dB and for two different levels of SOP^L: 0.75 (75% SOP^L level) and 0.5 (50% SOP^L level), which are representative of relatively high and mid-range levels of SOP^L. The SOP^L levels of 75% and 50% are equivalent to a secrecy reliability level[3] of 25% and 50%, respectively.

First, considering $\bar{\gamma}_M = 10$ dB in Fig. 7(c), we observe that if the eavesdropper can improve her average SNR from 5 dB to 10 dB, the probability of SPSC will decrease from 78% to 50%. Furthermore, to ensure an SPSC level of at least 25%, we find that the eavesdropper's average SNR must not exceed 14.4 dB. Likewise, to ensure an SPSC level of at least 50%, $\bar{\gamma}_E$ must not exceed 10 dB.

[2]For the parameter estimation process undertaken here, the κ and μ parameters were bounded according to the conditions: $0 \leq \kappa \leq 100$ and $0.01 \leq \mu \leq 5$.

[3]Here we define the secrecy reliability probability as $1 - SOP^L$.

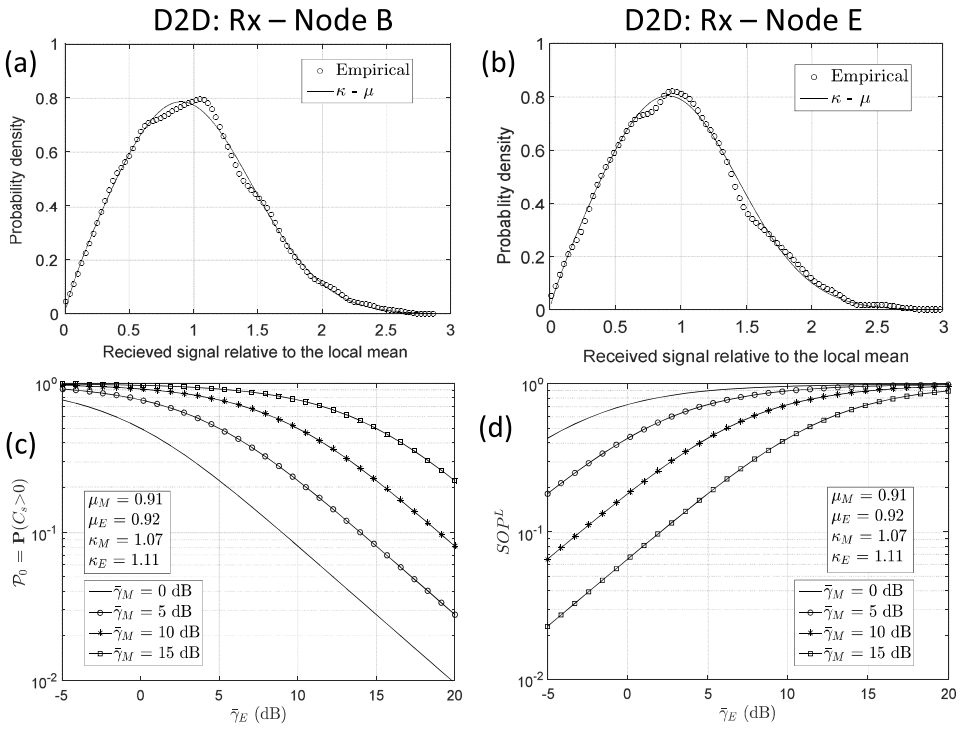

Fig. 7. Empirical envelope PDF of (a) node B and (b) node E compared to the κ-μ PDF given in [26, eq. (11)] while (c) and (d) show the probability of SPSC and SOP^L ($\gamma_{th} = 1.5$ dB) versus $\bar{\gamma}_E$ with selected values of $\bar{\gamma}_M$ for D2D channel measurements, respectively.

Next, consulting Fig. 7(d) with $\bar{\gamma}_M$ again equal to 10 dB, we find that an increase in the eavesdropper's average SNR from 5 dB to 10 dB causes the integrity of the channel between Alice and Bob to become increasingly compromised. This is evidenced by the increase in the secrecy outage probability which rises from 43% to 72%. For this fading environment, to ensure a secrecy reliability level of at least 25% or 50%, the eavesdropper's average SNR must not exceed 10.5 dB and 6.2 dB, respectively.

B. Body Area Network Scenario

The second set of measurements considered on-body communications channels operating at 5.8 GHz as found in body area networks. The experiment was performed in the same seminar room discussed above which was unoccupied except for the test subject on whom the on-body nodes were placed. For this scenario, to maximize coupling across the body surface, the antennas were mounted normal to the torso of an adult male of height 1.83 m and mass 74 kg. Node A was positioned at the front central chest region at a height of 1.42 m while nodes B and E were placed on the rear of the test subject at the central waist region at a height of 1.15 m and the right back-pocket at a height of 0.92 m, respectively. The measurements considered the case when the hypothetical BAN user walked along a straight line within the large room, covering a total distance of 9 m as shown in Fig. 6(b). For the BAN scenario, a total of 19260 samples of the received signal power were obtained and used for parameter estimation.

Figs. 8(a) and (b) show the empirical PDF of the signal envelope for Bob and Eve, again compared to the κ-μ PDF given in [26, eq. (11)]. Identical to the analysis of the D2D measurements, the optimum window size was determined from the raw channel data. In this case a smoothing window of 100 samples was used. Again, the κ-μ PDF was found to provide an excellent fit to the empirical data for both Bob and Eve. Interestingly for the BAN configuration considered here, the estimated κ parameter of the eavesdropper's channel was greater than that of the main channel, while for the estimated μ parameters, the converse situation was true (Table I).

Fig. 8(c) shows the probability of SPSC versus $\bar{\gamma}_E$ with selected values of $\bar{\gamma}_M$ for the measured BAN channel. With the main channel's average SNR fixed at 10 dB, we observe that increasing the average SNR of the eavesdropper's channel from 5 dB to 10 dB causes the probability of SPSC to significantly decrease from 82% to 50%. Moreover, to ensure an SPSC level of at least 25% or 50%, we find that the eavesdropper's average SNR must not exceed approximately 13.7 dB and 10 dB, respectively. Fig. 8(d) shows the SOP^L versus $\bar{\gamma}_E$ with selected values of $\bar{\gamma}_M$ for the measured BAN channel. With the main channel's average SNR fixed at 10 dB, we observe that if the average SNR of the eavesdropper is increased from 5 dB to 10 dB the SOP^L rises from 42% to 75%. Furthermore for this fading environment, it is also seen that the average SNR of the eavesdropper must not exceed 9.8 dB and 6.1 dB to ensure a secrecy reliability level of at least 25% or 50%, respectively.

C. Peer to Peer Scenario

The third set of measurements considered peer-to-peer communications channels operating at 5.8 GHz in an open office environment located on the first floor of the ECIT building at Queen's University Belfast in the United Kingdom. The office contained a number of chairs, metal storage spaces, doors

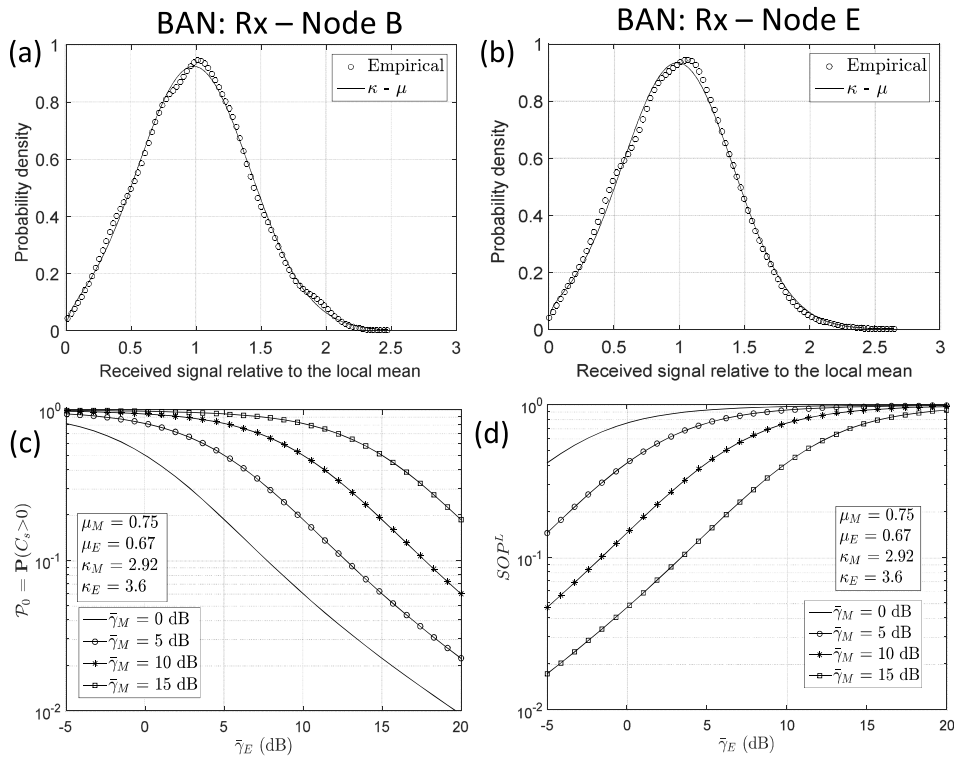

Fig. 8. Empirical envelope PDF of (a) node B and (b) node E compared to the κ-μ PDF given in [26, eq. (11)]. (c) and (d) show the probability of SPSC and SOP^L ($\gamma_{th} = 1.5$ dB) versus $\bar{\gamma}_E$ with selected values of $\bar{\gamma}_M$ for BAN channel measurements.

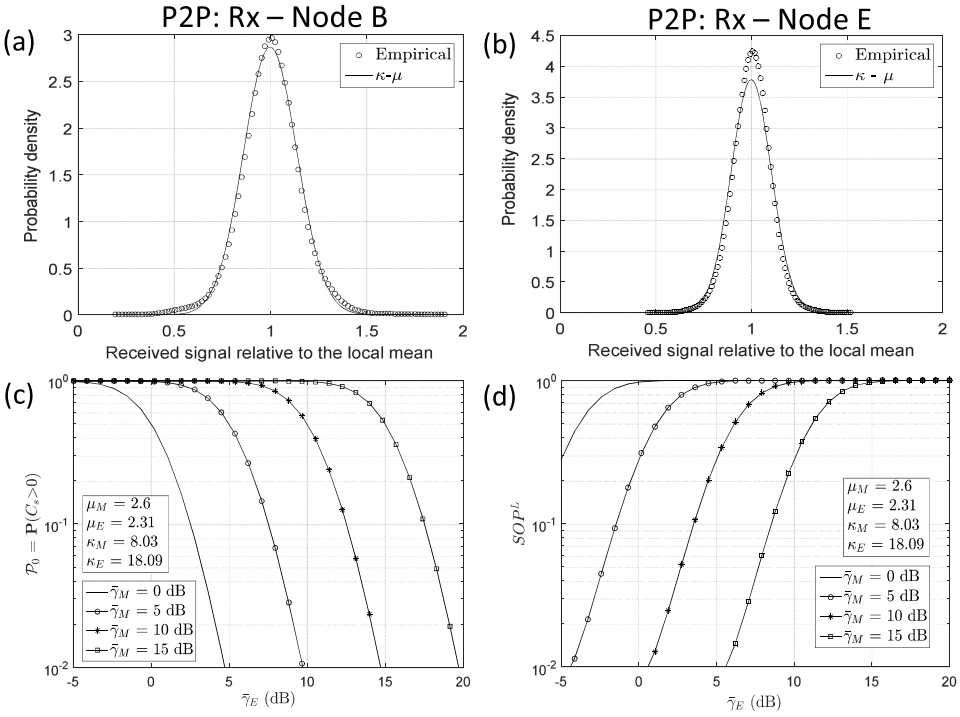

Fig. 9. Empirical envelope PDF of (a) node B and (b) node E compared to the κ-μ PDF given in [26, eq. (11)]. (c) and (d) show the probability of SPSC and SOP^L ($\gamma_{th} = 1.5$ dB) versus $\bar{\gamma}_E$ with selected values of $\bar{\gamma}_M$ for P2P channel measurements.

and desks constructed from medium density fibreboard. These desks were vertically separated by soft wooden partitions.

The experiment was performed with nodes A, B and E positioned on different desks in the open office with people seated at location's P as indicated in Fig. 6(c). During the measurement trial, two pedestrians initially stationary at points X and Y, walked simultaneously covering a distance of 9 m from their starting points, rotated clockwise and walked back

Fig. 10. Satellite view of measurement environment showing the position of nodes A, B and E for V2V scenario. The vehicle with node E remained parked on the side of the road and was oriented such that it faced directly towards node A. Arrows indicate the front of the car.

to their initial positions. The pedestrian at point X was an adult female of height 1.65 m and mass 53 kg while the pedestrian at point Y was an adult male of height 1.72 m and mass 80 kg. A total of 34464 samples of the received signal power were obtained and used for parameter estimation.

Figs. 9(a) and (b) show the empirical PDF of the signal envelope for Bob and Eve compared to the κ-μ PDF. An optimum window size was determined from the raw channel data and a smoothing window of 200 samples was used. It can be seen that the κ-μ PDF provides a very good fit to the measured data for both Bob and Eve. Figs. 9(c) and (d), show the probability of SPSC and SOP^L versus $\bar{\gamma}_E$ with selected values of $\bar{\gamma}_M$ for the measured P2P channel, respectively. It can be seen from these figures that the estimates for κ_M and κ_E are much greater than 0, suggesting that a dominant component exists for both. We also observe that the parameter estimates for μ_M and μ_E are both greater than 1, suggesting that multiple multipath clusters contribute to the signal received by both Bob and Eve. Furthermore, the κ and μ values measured for the P2P scenario were found to be much greater than the fading parameters measured for all other applications.

As before, considering the average SNR of the main channel to be equal to 10 dB in Fig. 9(c), we see that if the eavesdropper improves her average SNR from 5 dB to 10 dB, the probability of SPSC reduces from 98% to 50%. This steep decrease in P_0 is due to the estimated κ parameter of the eavesdropper's channel being much larger than that of the legitimate channel (see Table I). For the P2P application, to ensure an SPSC level of at least 25% we find that the eavesdropper's average SNR must not exceed 12.8 dB. Likewise, to ensure an SPSC level of at least 50%, $\bar{\gamma}_E$ must not exceed 10 dB. For the SOP, an increase in Eve's average SNR from 5 dB to 10 dB causes the channel between Alice and Bob to become increasingly susceptible to eavesdropping. Here, the secrecy outage probability increased from 30% to 96%. Furthermore, it can also be seen that the average SNR of the eavesdropper must not exceed 7.5 dB and 6.2 dB to ensure a secrecy reliability level of at least 25% or 50% for the legitimate channel, respectively.

D. Vehicle-to-Vehicle Scenario

The fourth set of measurements considered vehicle-to-vehicle communication channels operating at 5.8 GHz. The experiments were conducted in a business district environment in the Titanic Quarter of Belfast, United Kingdom. As shown in Fig. 10, the area consisted of a straight road with a number of office buildings nearby. For this particular scenario, nodes A, B and E were placed on the center of the dash boards of three different vehicles; namely, a Vauxhall (Opel in Europe) Zafira SRi, a Vauxhall Astra SRi and a Hyundai Getz. The initial positions of the vehicles are shown in Fig. 10. The measurements began when the vehicles that contained nodes A and B started approaching one another at a speed of 30mph. During these measurements the vehicle containing node E remained parked (with the driver still seated inside) on the side of the road as indicated in Fig. 10. It should be noted that all of the channel measurements made in this scenario were performed during off-peak traffic hours and were subject to perturbations caused by the driver, movement of the nearby pedestrians and other vehicular traffic. A total of 56579 samples of the received signal power were obtained and used for parameter estimation.

Figs. 11(a) and (b) show the empirical PDF of the signal envelope for Bob and Eve compared to the κ-μ PDF. Similar to the analysis of the D2D, P2P and BAN measurements, the optimum window size was determined from the raw channel data. The local mean for the V2V measurements was calculated over 200 samples. From these figures we can see that the PDF of the κ-μ fading model provides a very good approximation to the V2V data. From Table I, it can be seen that the estimates of κ for the main and the eavesdropper's channels are greater than 0 whilst the estimated μ parameters are less than 1, suggesting that a dominant component exists and that these channels suffer less from multipath caused by scattering. We also observe that the estimated κ parameter of the eavesdropper's channel was greater than that of the legitimate channel whilst the estimated μ parameter of the main channel was only marginally greater than that of the eavesdropper's channel.

Fig. 11(c) depicts the probability of SPSC versus $\bar{\gamma}_E$ with selected values of $\bar{\gamma}_M$ for the measured V2V channel. With $\bar{\gamma}_M = 10$ dB, it is seen that if the eavesdropper's average SNR is increased from 5 dB to 10 dB, the probability of SPSC is reduced from 86% to 48%. Furthermore, it can also be seen that this decrease in the probability of SPSC is higher than that experienced for the measured D2D and BAN channels for the same improvement in the average SNR of the eavesdropper's channel. For this application, to ensure an SPSC level of at least 25% or 50%, we find that the eavesdropper's average SNR must not exceed 12.8 dB and 10 dB, respectively. Equivalently, Fig. 11(d) depicts the probability of SOP^L versus $\bar{\gamma}_E$ with selected values of $\bar{\gamma}_M$ for the measured

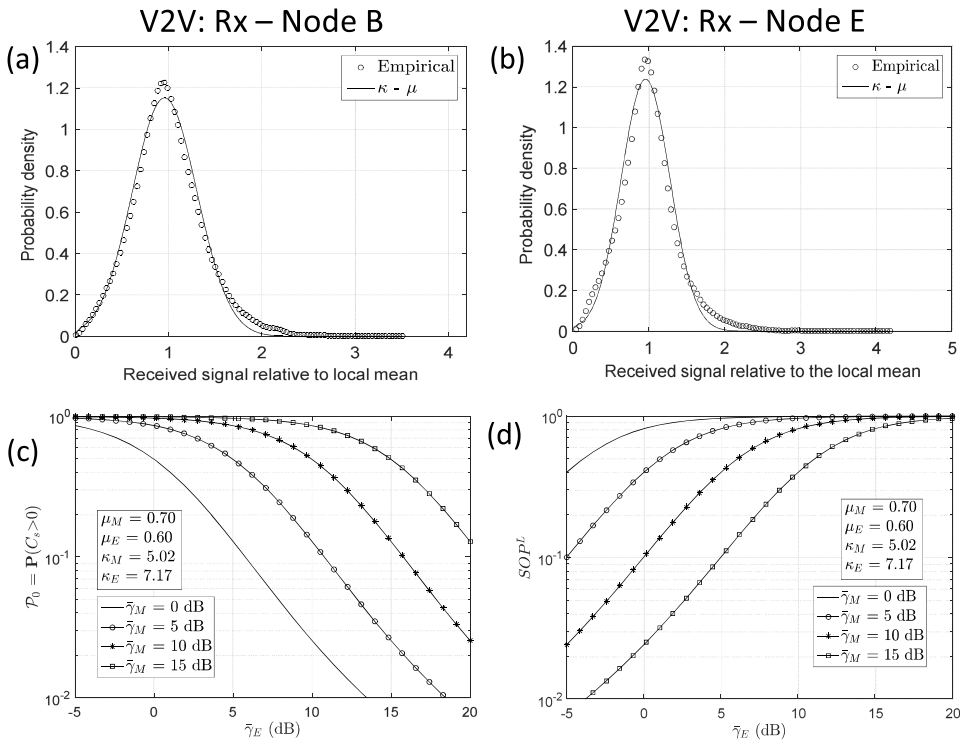

Fig. 11. Empirical envelope PDF of (a) node B and (b) node E compared to the κ-μ PDF given in [26, eq. (11)]. (c) and (d) show the probability of SPSC and SOP^L ($\gamma_{th} = 1.5$ dB) versus $\bar{\gamma}_E$ with selected values of $\bar{\gamma}_M$ for V2V channel measurements.

V2V channel. Again considering $\bar{\gamma}_M = 10$ dB, it is seen that if Eve is able to increase her average SNR from 5 dB to 10 dB, the secrecy outage probability is doubled. Since $\kappa_E > \kappa_M$, the legitimate channel becomes increasingly susceptible to eavesdropping as $\bar{\gamma}_E$ is increased. For the V2V application, it is also seen that the average SNR of the eavesdropper must not exceed 9 dB and 6.1 dB to ensure a secrecy reliability level of at least 25% or 50% for the Alice-Bob channel, respectively.

VII. Conclusion

Novel analytical and closed-form expressions for the probability of SPSC and SOP^L of the recently proposed κ-μ fading model have been presented. Specifically, the analytical expressions have been derived for $i.n.i.d.$ channel coefficients without parameter restrictions. We have also arrived at an exact closed form expression for the probability of SPSC for integer values of μ_M and μ_E. Based on these results we have provided a useful insight into the behavior of SPSC and SOP^L as a function of parameters $\{\kappa_M, \mu_M, \bar{\gamma}_M\}$ and $\{\kappa_E, \mu_E, \bar{\gamma}_E\}$. The analytical and closed form expressions have been validated through reduction to known special cases and Monte-Carlo simulations. As the κ-μ fading model is a very general statistical model that includes many well-known distributions, the new equations derived in this paper will find use in characterizing the secrecy performance of several different fading channels. Moreover, the results presented here will also find immediate application in the calculation of outage probability in wireless systems affected by CCI and BN, and the calculation of outage probability in interference-limited scenarios. Finally, we have illustrated the utility of the new formulations by investigating the probability of SPSC and SOP^L based on real channel measurements conducted for a diverse range of wireless applications such as cellular device-to-device, peer-to-peer, vehicle-to-vehicle and body centric fading channels. It is also worth highlighting that all of the expressions presented in this paper can be easily evaluated using functions available in mathematical software packages such as Mathematica and Matlab.

Appendix A
Proof of Equation (14)

From (13), we have

$$\begin{aligned}\mathcal{P}_{out}(\gamma_{th}) &= \mathbb{P}\left[\gamma_M \le (1+\gamma_{th})(1+\gamma_E) - 1\right] \\ &= \int_0^\infty f_{\gamma_E}(\gamma_E)\left[\int_0^{(\gamma_{th}+\gamma_{th}\gamma_E+\gamma_E)} f_{\gamma_M}(\gamma_M)\, d\gamma_M\right] d\gamma_E \\ &= \int_0^\infty f_{\gamma_E}(\gamma_E)\left[F_{\gamma_M}(\gamma_{th}+\gamma_{th}\gamma_E+\gamma_E)\right] d\gamma_E. \end{aligned} \tag{27}$$

Substituting (8) and (9) in (27) we obtain (14).

Appendix B
Proof of Proposition 1

An analytical expression for (16) can be derived by expressing the generalized Marcum Q-function and the modified

Bessel function of the first kind according to [35, eq. (16)] and [36] as follows:

$$Q_m(a,b) = \sum_{l=0}^{\infty} \frac{a^{2l}\Gamma\left(m+l, \frac{b^2}{2}\right)}{l!\Gamma(m+l)\,2^l e^{\frac{a^2}{2}}} \tag{28}$$

$$I_v(x) = \sum_{k=0}^{\infty} \frac{\left(\frac{x}{2}\right)^{v+2k}}{k!\Gamma(v+k+1)} \tag{29}$$

where $\Gamma(\cdot)$ is the gamma function, $\Gamma(\cdot,\cdot)$ is the incomplete gamma function. By substituting (28) and (29) in (16)

$$\begin{aligned} &SOP^L(\gamma_{th}) \\ &= \int_0^{\infty} \frac{\beta_E^{\frac{\mu_E-1}{2}}}{\alpha_E^{\frac{\mu_E-1}{2}} e^{\alpha_E}} \gamma_E^{\frac{\mu_E-1}{2}} e^{-\beta_E\gamma_E} \\ &\quad \times I_{\mu_E-1}\left(2\sqrt{\beta_E\alpha_E\gamma_E}\right) d\gamma_E - \sum_{k=0}^{\infty}\sum_{l=0}^{\infty} \frac{\left(\sqrt{\beta_E\alpha_E}\right)^{\mu_E-1+2k}}{k!l!\gamma(d)\,\gamma(c)\,e^{\alpha_M}} \\ &\quad \times \frac{\beta_E^{\frac{\mu_E-1}{2}}}{\alpha_E^{\frac{\mu_E-1}{2}} e^{\alpha_E}} \int_0^{\infty} \gamma_E^{d-1} e^{-\beta_E\gamma_E} \Gamma\left(c, \beta_M(1+\gamma_{th})\gamma_E\right) d\gamma_E \end{aligned} \tag{30}$$

where $a = 1/\bar{\gamma}_M$, $b = 1/\bar{\gamma}_E$, $c = \mu_M + l$, $d = \mu_E + k$, $\beta_M = (1+\kappa_M)a\mu_M$, $\beta_E = (1+\kappa_E)b\mu_E$, $\alpha_M = \kappa_M\mu_M$ and $\alpha_E = \kappa_E\mu_E$. Notably, the first integral in (30) is equivalent to 1 and the second integral is identical to [32, eq. (6.455)] given by

$$\begin{aligned} &\int_0^{\infty} x^{\mu-1} e^{-\beta x} \Gamma(v, \alpha x)\, dx \\ &= \frac{\alpha^v \Gamma(\mu+v)}{\mu(\alpha+\beta)^{\mu+v}} \\ &\quad \times {}_2F_1\left(1, \mu+v; \mu+1; \frac{\beta}{\alpha+\beta}\right) \\ &\quad [Re(\alpha+\beta) > 0, Re\ \mu > 0, Re(\mu+v) > 0]. \end{aligned} \tag{31}$$

Substituting these in (30) we obtain (17).

Appendix C
Proof of Proposition 3

From [37, eq. (2.5)], we have

$$\begin{aligned} \mathcal{P}_{\mu,v}(A,B;r) &= A^{-\mu}B^{-v}\int_0^{\infty} x^{\mu+1} e^{-\left(\frac{x^2+A^2}{2}\right)} I_{\mu}(Ax)\, dx \\ &\quad \times \int_0^{rx} y^{v+1} e^{-\left(\frac{y^2+B^2}{2}\right)} I_v(By)\, dy. \end{aligned} \tag{32}$$

Using the definition of the Marcum Q-function given in (4) in (32), we obtain

$$\begin{aligned} \mathcal{P}_{\mu,v}(A,B;r) &= 1 - A^{-\mu}\int_0^{\infty} x^{\mu+1} e^{-\left(\frac{x^2+A^2}{2}\right)} I_{\mu}(Ax) \\ &\quad \times Q_{v+1}(B, rx)\, dx. \end{aligned} \tag{33}$$

Now letting $x = \sqrt{\frac{2\mu_E(1+\kappa_E)\gamma_E}{\bar{\gamma}_E}}$ and performing the necessary transformation of variables we obtain

$$\begin{aligned} &\mathcal{P}_{\mu,v}(A,B;r) \\ &= 1 - A^{-\mu}e^{-\frac{A^2}{2}}\int_0^{\infty} 2^{\frac{\mu}{2}}\left(\frac{\mu_E(1+\kappa_E)}{\bar{\gamma}_E}\right)^{\frac{\mu}{2}+1} \\ &\quad \times \gamma_E^{\frac{\mu}{2}} e^{\frac{-\mu_E(1+\kappa_E)\gamma_E}{\bar{\gamma}_E}} I_{\mu}\left(A\sqrt{\frac{2\mu_E(1+\kappa_E)\gamma_E}{\bar{\gamma}_E}}\right) \\ &\quad \times Q_{v+1}\left(B, r\sqrt{\frac{2\mu_E(1+\kappa_E)\gamma_E}{\bar{\gamma}_E}}\right) d\gamma_E. \end{aligned} \tag{34}$$

Comparing (34) with (20) and with the appropriate variable substitutions (see Proposition 3), we obtain

$$\begin{aligned} &\mathcal{P}_{\mu,v}(A,B;r) \\ &= 1 - \frac{\mu_E(1+\kappa_E)^{\frac{\mu_E+1}{2}}}{\kappa_E^{\frac{\mu_E-1}{2}}\bar{\gamma}_E^{\frac{\mu_E+1}{2}} e^{\mu_E\kappa_E}} \int_0^{\infty} \gamma_E^{\frac{\mu_E-1}{2}} \\ &\quad \times e^{\frac{-\mu_E(1+\kappa_E)\gamma_E}{\bar{\gamma}_E}} I_{\mu_E-1}\left(2\mu_E\sqrt{\frac{\kappa_E(1+\kappa_E)\gamma_E}{\bar{\gamma}_E}}\right) \\ &\quad \times Q_{\mu_M}\left(\sqrt{2\kappa_M\mu_M}, \sqrt{\frac{2\mu_M(1+\kappa_M)\gamma_E}{\bar{\gamma}_M}}\right) d\gamma_E. \end{aligned} \tag{35}$$

$$\mathcal{P}_{\mu,v}(A,B;r) = 1 - \mathcal{P}_0. \tag{36}$$

From [37, eq. (3.16)], we have

$$\begin{aligned} \mathcal{P}_{\mu,v}(A,B;r) &= \mathcal{P}_{0,0}(A,B;r) + exp\left(-\frac{A^2r + B^2r^{-1}}{2R}\right) \\ &\quad \times \sum_{m=-\mu}^{v}\left(\frac{A}{Br}\right)^m I_m\left(\frac{AB}{R}\right) \\ &\quad \times \left\{\sum_{k=1}^{\mu}\binom{v+k}{k+m} r^{v-k+1} R^{-v-k-1} \right. \\ &\quad \left. - \sum_{j=1}^{v}\binom{j}{m} r^{j-1} R^{-j-1}\right\}. \end{aligned} \tag{37}$$

From [37, eq. (3.5)], we have

$$\begin{aligned} \mathcal{P}_{0,0}(A,B;r) &= Q\left(\frac{Ar}{\sqrt{1+r^2}}, \frac{B}{\sqrt{1+r^2}}\right) - \left(1+r^2\right)^{-1} \\ &\quad \times \exp\left[-\frac{A^2r^2+B^2}{2\left(1+r^2\right)}\right] I_0\left(\frac{ABr}{1+r^2}\right). \end{aligned} \tag{38}$$

Letting $\acute{\mathcal{P}} = \mathcal{P}_{0,0}(A,B;r)$ and combining (36), (37) and (38) we obtain (22). Note that [37] uses lower-case symbols (a, b) and we use upper-case symbols (A, B). This is because we define $a = \frac{1}{\bar{\gamma}_M}$ and $b = \frac{1}{\bar{\gamma}_E}$.

References

[1] O. Vermesan and P. Friess, *Internet of Things—From Research and Innovation to Market Deployment*. Aalborg, Denmark: River Publishers, 2014.

[2] S. L. Cotton, "Human body shadowing in cellular device-to-device communications: Channel modeling using the shadowed κ–μ fading model," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 1, pp. 111–119, Jan. 2015.

[3] S. L. Cotton and W. G. Scanlon, "An experimental investigation into the influence of user state and environment on fading characteristics in wireless body area networks at 2.45 GHz," *IEEE Trans. Wireless Commun.*, vol. 8, no. 1, pp. 6–12, Jan. 2009.

[4] S. L. Cotton and W. G. Scanlon, "Characterization and modeling of the indoor radio channel at 868 MHz for a mobile bodyworn wireless personal area network," *IEEE Antennas Wireless Propag. Lett.*, vol. 6, pp. 51–55, 2007.

[5] S. L. Cotton and W. G. Scanlon, "Indoor channel characterisation for a wearable antenna array at 868 MHz," in *Proc. IEEE Wireless Commun. Netw. Conf.*, vol. 4. Las Vegas, NV, USA, Apr. 2006, pp. 1783–1788.

[6] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[7] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[8] 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.

[9] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

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

[11] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

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

[13] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Proc. 44th. Allerton Conf. Commun. Control Comput.*, Monticello, IL, USA, Sep. 2006, pp. 841–848.

[14] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secrecy capacity region of fading broadcast channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 2007, pp. 1291–1295.

[15] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[16] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[17] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[18] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, USA, Jul. 2006, pp. 356–360.

[19] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Adelaide, SA, Australia, Sep. 2005, pp. 2152–2155.

[20] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 2007, pp. 1301–1305.

[21] M. Z. I. Sarkar, T. Ratnarajah, and M. Sellathurai, "Secrecy capacity of Nakagami-*m* fading wireless channels in the presence of multiple eavesdroppers," in *Proc. 43rd Asilomar Conf. Signals, Syst. Comput.*, Pacific Grove, CA, USA, Nov. 2009, pp. 829–833.

[22] M. Z. I. Sarkar and T. Ratnarajah, "On the secrecy mutual information of Nakagami-*m* fading SIMO channel," in *Proc. IEEE ICC*, Cape Town, South Africa, May 2010, pp. 1–5.

[23] X. Liu, "Secrecy capacity of wireless links subject to log-normal fading," in *Proc. 8th Int. ICST Conf. Commun. Netw. China (CHINACOM)*, Aug. 2012, pp. 167–172.

[24] X. Liu, "Probability of strictly positive secrecy capacity of the Weibull fading channel," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Atlanta, GA, USA, Dec. 2013, pp. 659–664.

[25] X. Liu, "Probability of strictly positive secrecy capacity of the Rician–Rician fading channel," *IEEE Wireless Commun. Lett.*, vol. 2, no. 1, pp. 50–53, Feb. 2013.

[26] M. D. Yacoub, "The κ–μ distribution and the η–μ distribution," *IEEE Antennas Propag. Mag.*, vol. 49, no. 1, pp. 68–81, Feb. 2007.

[27] P. C. Sofotasios, E. Rebeiz, L. Zhang, T. A. Tsiftsis, D. Cabric, and S. Freear, "Energy detection based spectrum sensing over κ–μ and κ–μ extreme fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 3, pp. 1031–1040, Mar. 2013.

[28] A. Annamalai, O. Olabiyi, S. Alam, O. Odejide, and D. Vaman, "Unified analysis of energy detection of unknown signals over generalized fading channels," in *Proc. 7th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Istanbul, Turkey, Jul. 2011, pp. 636–641.

[29] N. Y. Ermolova and O. Tirkkonen, "Laplace transform of product of generalized Marcum Q, Bessel I, and power functions with applications," *IEEE Trans. Signal Process.*, vol. 62, no. 11, pp. 2938–2944, Jun. 2014.

[30] G. Gomez, F. J. Lopez-Martinez, D. Morales-Jimenez, and M. R. McKay, "On the equivalence between interference and eavesdropping in wireless communications," *IEEE Trans. Veh. Technol.*, vol. 64, no. 12, pp. 5935–5940, Dec. 2015.

[31] M. K. Simon and M. Alouini, *Digital Communication Over Fading Channels*, 2nd ed. Wiley-Interscience, 2005.

[32] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. New York: Academic, 2007.

[33] J. E. Dennis, Jr., "Nonlinear least squares and equations," in *The State of the Art in Numerical Analysis*, D. Jacobs, Ed. San Diego, CA, USA: Academic, 1977, pp. 269–312.

[34] J. J. Moré and D. C. Sorensen, "Computing a trust region step," *SIAM J. Sci. Statist. Comput.*, vol. 4, no. 3, pp. 553–572, 1983.

[35] P. C. Sofotasios, T. A. Tsiftsis, Y. A. Brychkov, S. Freear, M. Valkama, and G. K. Karagiannidis, "Analytic expressions and bounds for special functions and applications in communication theory," *IEEE Trans. Inf. Theory*, vol. 60, no. 12, pp. 7798–7823, Dec. 2014.

[36] H. Bateman, *Higher Transcendental Functions*. New York, NY, USA: McGraw-Hill, 1953.

[37] R. Price, "Some non-central F-distributions expressed in closed form," *Biometrika*, vol. 51, nos. 1–2, pp. 107–122, 1964.

Nidhi Bhargav received the B.E. (Hons.) degree in telecommunications engineering from Visvesvaraya Technological University, Karnataka, India, in 2011, and the M.Sc. (Hons.) degree in wireless communications and signal processing from the University of Bristol, U.K., in 2012. She is currently pursuing the Ph.D. degree with Queen's University Belfast, U.K. Her research interests include physical layer security, and channel characterization and modeling for body-centric communications.

Simon L. Cotton (S'04–M'07–SM'14) received the B.Eng. degree in electronics and software from the University of Ulster, Ulster, U.K., in 2004, and the Ph.D. degree in electrical and electronic engineering from Queen's University Belfast, Belfast, U.K., in 2007. He is currently a Reader in wireless communications with the Institute of Electronics, Communications and Information Technology, Queen's University Belfast. He is also a Co-Founder and the Chief Technology Officer of ActivWireless Ltd., Belfast. He has authored or co-authored over 90 publications in major IEEE/IET journals and refereed international conferences, two book chapters, and two patents. His research interests are cellular device-to-device, vehicular, and body-centric communications. His other research interests include radio channel characterization and modeling and the simulation of wireless channels. He received the H. A. Wheeler Prize, in 2010, by the IEEE Antennas and Propagation Society for the best applications journal paper in the IEEE TRANSACTIONS ON ANTENNAS AND PROPAGATION in 2009. In 2011, he received the Sir George Macfarlane Award from the U.K. Royal Academy of Engineering in recognition of his technical and scientific attainment since graduating from his first degree in engineering.

David E. Simmons received the degree in mathematics from the University of Central Lancashire, in 2011, and the M.Sc. degree in communications engineering from the University of Bristol, U.K., in 2012. He is currently pursuing the D.Phil. degree with the University of Oxford, U.K., where his research has focused predominantly on amplify-and-forward relay networks. His research interests include information theory and communication theory. During his D.Phil. studies, he was a recipient of the Best Paper Award at the 23rd edition of EUCNC'14.