Physical Layer Security in the Presence of Interference

Dimitrios S. Karas, *Member, IEEE*, Alexandros-Apostolos A. Boulogeorgos, *Member, IEEE*, George K. Karagiannidis, *Fellow, IEEE*, and Arumugam Nallanathan, *Fellow, IEEE*

***Abstract*—We evaluate and quantify the joint effect of fading and multiple interferers on the physical-layer (PHY) security of a system consisted of a base-station (BS), a legitimate user, and an eavesdropper. To this end, we present a novel closed-form expression for the secrecy outage probability, which takes into account the fading characteristics of the wireless environment, the location and the number of interferers, as well as the transmission power of the BS and the interference. The results reveal that the impact of interference should be seriously taken into account in the design and deployment of a wireless system with PHY security.**

***Index Terms*—Interference, Secrecy Outage Probability, Physical layer security.**

I. Introduction

Physical layer (PHY) security has received significant attention in the last years, since it can provide reliable and secure communication by employing the fundamental characteristics of the transmission medium, such as multi-path fading [1], [2]. As a result, a great amount of effort was put in analyzing the performance of such systems. Scanning the open literature, most of the related works have neglected the impact of interference and fading on the security performance of wireless systems. However, in modern heterogeneous wireless enviroments, interference is an inevitable key factor for the communication system's performance [3].

The above mentioned scenarios motivated a general investigation of the effect of interference on the security performance of wireless systems [4], [5]. Specifically, a scenario where two independent confidential messages are transmitted to their respective receivers (RXs), which interfere with each other was examined in [6]. In this work, the equivocation rate at the eavesdropper was used as a metric to ensure mutual information-theoretic secrecy. Furthermore, in [7], the problem of security in the presence of interference was examined from a similar point of view, where two transmitters (TXs) sent two messages to a cognitive RX, who should be able to decode both messages, and a non-cognitive RX, which is able to decode only one message, while the other is kept secret. Moreover, in [8], a system that consisted of a primary TX-RX pair, as well as a number of secondary transceivers, and a single eavesdropper, was examined. However, in [8], the impact of multipath fading was neglected. In [9], the secrecy capacity was investigated for a cognitive radio system with security based on artificial noise, assuming full channel state information (CSI) knowledge for the legitimate RX's channel, and partial CSI for the eavesdropper's channel. Finally, the impact of interference on multi-user scheduling transmission schemes was investigated in [10] and [11]. However, in these works the fading characteristics of the interference channels were not taken into consideration.

To the best of the authors' knowledge, the joint effect of interference and fading in PHY security has not been addressed in the open technical literature. Motivated by this, in this paper, we examine PHY security for a system, where a TX aims to communicate securely with a legitimate RX, in the presence of an eavesdropper. The signals transmitted by an arbitrary number of base-stations (BSs) cause interference in the signals received by the legitimate RX and the eavesdropper. All TXs and RXs are assumed to be equipped with a single antenna. Also, all wireless links are subject to Rayleigh fading, and statistical CSI is assumed for all channels. To this end, a closed-form expression for the secrecy outage probability (SOP) is derived.

II. System and signal model

We consider the downlink scenario in a wireless network that consists of a BS, which aims to transmit a confidential message to a legitimate user, in the presence of an eavesdropper, and M other BSs, which operate in the same frequency band, i.e., they are interferers. For convenience, in what follows, we will refer to the BS as Alice (A), the legitimate user as Bob (B), and the eavesdropper as Eve (E).

The baseband equivalent signals received by B and E can be respectively obtained as

$$y_B = h_B x + \sum_{i=1}^{M} h_{Bi} x_i + n_B, \tag{1}$$

$$y_E = h_E x + \sum_{i=1}^{M} h_{Ei} x_i + n_E, \tag{2}$$

where x denotes the transmitted signal by A, and x_i denotes the transmitted signal by the i-th interferer. Also, n_B and n_E are zero-mean complex Gaussian random variables (RVs) that models the additive white Gaussian noise (AWGN), with power spectral density N_0 at both B's and E's RXs. Moreover, the baseband equivalent channel between A and B is denoted by h_B, while the one between A and E by h_E. The baseband equivalent channels between the i-th interferer and B are denoted by h_{Bi}, whereas those between the i-th interferer

D. S. Karas, A.-A. A. Boulogeorgos, and G. K. Karagiannidis are with the Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, Greece (e-mail: {dkaras, ampoulog, geokarag}@auth.gr).

A. Nallanathan is with the Department of n the Department of Informatics at King's College London, UK (e-mail: arumugam.nallanathan@kcl.ac.uk)

and E by h_{Ei}. Due to the distance, $d_{\mathcal{X}}$, between A and node $\mathcal{X} \in \{B, E\}$, the channel gain can be expressed as in [12], $h_{\mathcal{X}} = \frac{g_{\mathcal{X}}}{\sqrt{1+d_{\mathcal{X}}^{\alpha}}}$, where $g_{\mathcal{X}}$ and α denote the fading channel and the path loss coefficients, respectively. Similarly, the channel gain between the i-th interferer and node $\mathcal{X}$ is given by $h_{\mathcal{X}i} = \frac{g_{\mathcal{X}i}}{\sqrt{1+d_{\mathcal{X}i}^{\alpha}}}$, where $\mathcal{X} \in \{B, E\}$, while $g_{\mathcal{X}i}$ denotes the fading channel coefficient, and $d_{\mathcal{X}i}$ denotes the distance between the i-th interferer and node $\mathcal{X}$. Note that $g_{\mathcal{X}}$ and $g_{\mathcal{X}i}$ are zero-mean complex Gaussian RVs with variance equals 1. Hence, $|g_{\mathcal{X}}|^2$ and $|g_{\mathcal{X}i}|^2$ follow Rayleigh distribution.

Based on (1) and (2), the instantaneous signal to interference and noise ratio (SINR) at B and E can be expressed as

$$\gamma_{\mathcal{X}} = \frac{\frac{E_s}{1+d_{\mathcal{X}}^{\alpha}}|g_{\mathcal{X}}|^2}{N_0 + \sum_{i=1}^{M} |g_{\mathcal{X}i}|^2 \frac{E_{si}}{1+d_{\mathcal{X}i}^{\alpha}}}, \tag{3}$$

where E_s represents the energy of the signal transmitted by Alice, while E_{si} represents the energy of the signal transmitted by the i-th interferer.

III. Secrecy Outage Probability

In this section, we evaluate the SOP, which is defined as the probability that the secrecy capacity is lower than a target secrecy rate, r_s, i.e., $P_o(r_s) = Pr\left(C_B - C_E \le r_s\right)$, or

$$P_o(r_s) = Pr\left(\log_2\left(\frac{\gamma_B+1}{\gamma_E+1}\right) \le r_s\right), \tag{4}$$

where $C_B = \log_2\left(\gamma_B + 1\right)$ and $C_E = \log_2\left(\gamma_E + 1\right)$ denote the capacity of A-B and A-E links, respectively.

Theorem 1. *The SOP can be expressed in closed form as in* (5)*, given at the top of the next page. In* (5)*,*

$$K = \frac{1}{\tilde{\gamma}_B}2^{-r_s} + \frac{1}{\tilde{\gamma}_E}, \tag{6}$$

$$L_{Bi} = \frac{E_s - (1+d_B^{\alpha})b_{Bi}}{(1+d_B^{\alpha})2^{r_s}b_{Bi}}, \tag{7}$$

$$L_{Ej} = \frac{E_s - (1+d_E^{\alpha})b_{Ej}}{(1+d_E^{\alpha})b_{Ej}}, \tag{8}$$

while $\tilde{\gamma}_B = \frac{E_s}{(1+d_B^{\alpha})N_0}$ *and* $\tilde{\gamma}_E = \frac{E_s}{(1+d_E^{\alpha})N_0}$. *Also,* $\Xi_{\mathcal{X}}(i)$, $\mathcal{X} \in \{B, E\}$ *is defined in [13, Eqs. (8) and (9)][1] and* $\mathcal{E}i(\cdot)$ *is the exponential integral function defined in [15, Eq. (5.1.4)].*

Proof: Please refer to the Appendix. ■

Theorem 1 reveals that the SOP does not only depend on the characteristics of the links between A and B/E, but also on the characteristics of the links between the interferers and B/E, as well as the number of interferers. In other words, Theorem 1 quantifies the importance of taking into account the impact of interference in PHY security.

IV. Numerical Results and Discussion

In this section, we evaluate and illustrate the joint effect of fading and interference on the performance of wireless systems with PHY security. Unless otherwise stated, we assume that the distance between Alice and Bob is 2.5 m, while the distance between Alice and Eve is 25 m. Also, there are three interfering BSs, and their normalized distances from Bob are 10, 20 and 25, whereas their corresponding normalized distances from Eve are 15, 10 and 5. In all cases, the target secrecy rate r_s is expressed in bit/s/Hz. Moreover, it is assumed that the signals transmitted by the interferers have equal energy, denoted by E_{sI}.

Fig. 1 depicts the SOP as a function of E_s/N_0 for different values of r_s and E_{sI}/N_0, and $\alpha = 3$. We observe that the SOP decreases as E_s/N_0 increases. Furthermore, for given E_s/N_0 and E_{sI}/N_0, higher rates lead to higher values of the SOP. Also, in the examined scenario, in the low E_s/N_0 regime, low values for the SOP are achieved if the interferers have low E_{sI}/N_0. On the other hand, in the high E_s/N_0 regime, low values of the SOP are achieved if the interferers have high E_{sI}/N_0.

In Fig. 2, the SOP is illustrated as a function of r_s for different values of E_s/N_0 and α. We observe that, regardless of the values of E_s/N_0 and α, as r_s increases, the SOP also increases. Furthermore, for given r_s and α, the increase of E_s/N_0 results in lower values for the SOP. On the other hand, the impact of α on the SOP is not as straightforward. For fixed E_s/N_0, $\alpha = 4$ yields the highest SOP in almost all the r_s regime. However, the SOP for $\alpha = 2$ is higher than for $\alpha = 3$ when $E_s/N_0 = 40$ dB, while the SOP for $\alpha = 3$ is higher than for $\alpha = 2$ when $E_s/N_0 = 20$ dB or $E_s/N_0 = 30$ dB. This behavior indicates the dependence of the secrecy performance on the spatial placement of the elements of the system as well as the pathloss parameters.

Fig. 3 demonstrates the SOP as a function of E_{sI}/N_0 for different values of r_s and E_s/N_0, and $\alpha = 3$. Regardless of the values of E_{sI}/N_0 and E_s/N_0, it can be seen that for given E_{sI}/N_0 and E_s/N_0, as r_s increases, the SOP also increases. However, for given r_s, higher values of E_s/N_0 lead to a lower SOP. Moreover, it is observed that as E_{sI}/N_0 changes, the behavior of the SOP is not straightforward. Specifically, in some cases we observe that as E_{sI}/N_0 increases, the SOP decreases until a certain point, and increases afterwards. This is expected, because the interferers are, on average, closer to Eve than to Bob. Therefore, an increase in E_{sI} is more beneficial to Bob than to Eve. However, as E_{sI} increases, the energy of the signal received by Bob from Alice becomes smaller compared to the energy received from the interferers. Therefore, the capacity of the Alice-Bob and Alice-Eve channels tend to zero, and so does the secrecy capacity, leading to higher values of the SOP.

Next, we present the impact of interference on PHY security for different positions of Eve. We assume that Alice, Bob and the interferers are placed at fixed locations, while Eve can be placed at 1 m intervals on a staight line that goes through Alice and Bob, up to 20 m from Alice. Also, in this scenario, $E_{sI}/N_0 = 35$ dB and $\alpha = 3$. In Fig. 4, we observe that, for a fixed r_s, when d_E increases, the SOP decreases. Moreover, we observe that, for fixed E_s/N_0 and d_E, higher values r_s lead to a higher SOP. In all cases, when Eve moves further from Alice and closer to the interferers, the SOP decreases.

Finally, we investigate the impact of the number of interfering BSs on the SOP. Fig. 5 depicts the SOP as a function of E_s/N_0 for different values of r_s and M. Also, it was

[1]Note that there is a typo in [13, Eqs. (8)]. The correct expression is provided in [14].

$$P_o(r_s) = 1 - \frac{E_s N_0}{2^{r_s}(1+d_B^{\alpha})} e^{\left(\frac{1}{\tilde{\gamma}_B}+\frac{1}{\tilde{\gamma}_E}\right)} \times \sum_{i=1}^{M}\sum_{j=1}^{M} \frac{\Xi_B(i)\Xi_E(j)}{b_{Bi}b_{Ej}} \Bigg(\frac{\tilde{\gamma}_E e^{-K}}{(L_{Ej}-1)(L_{Bi}-L_{Ej})} - \frac{K\tilde{\gamma}_E e^{L_{Ej}K}\mathcal{E}i\left(-\left(L_{Ej}+1\right)K\right)}{(L_{Bi}-L_{Ej})} + \frac{\tilde{\gamma}_E e^{L_{Bi}K}\mathcal{E}i\left(-\left(L_{Bi}+1\right)K\right)}{L_{Bi}-L_{Ej}} - \frac{\tilde{\gamma}_E e^{L_{Ej}K}\mathcal{E}i\left(-\left(L_{Ej}+1\right)K\right)}{L_{Bi}-L_{Ej}} + \frac{e^{KL_{Bi}}\mathcal{E}i\left(-(1+L_{Bi})K\right)}{L_{Ej}-L_{Bi}} - \frac{e^{KL_{Ej}}\mathcal{E}i\left(-(1+L_{Ej})K\right)}{L_{Ej}-L_{Bi}} \Bigg). \quad (5)$$

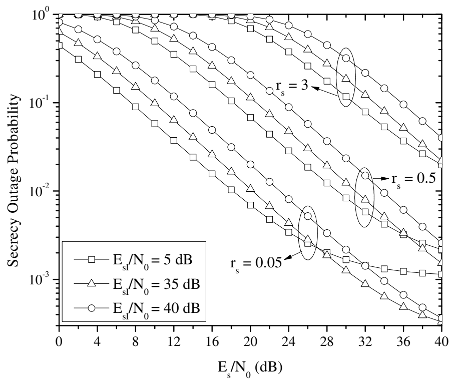

Fig. 1: SOP against E_s/N_0 for different values of r_s and E_{sI}/N_0.

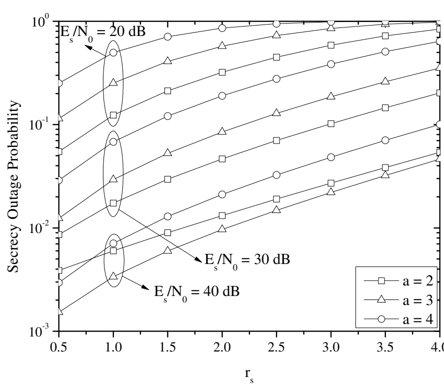

Fig. 2: SOP against r_s for different values of α and E_s/N_0.

assumed that $E_{sI}/N_0 = 25dB$ and $\alpha = 3$. The distance between Alice-Bob and Alice-Eve was $d_B = 1$ m and $d_E = 10$ m, respectively. It was assumed that the locations of Alice, Bob, Eve, and the interfering BSs are collinear, and all other elements are on the same side of the line, as defined by Alice's location. The distance of the first interfering BS from Alice was 15 m, and each consecutive BS was placed 1 m closer

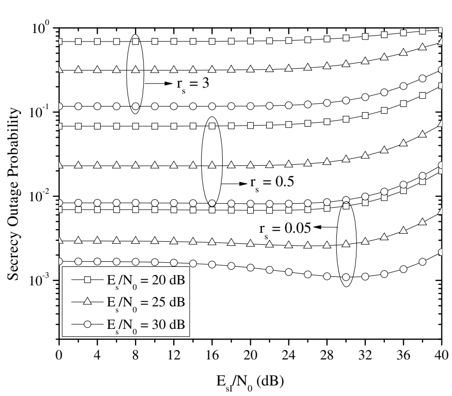

Fig. 3: SOP against E_{sI} for different values of r_s and E_s/N_0.

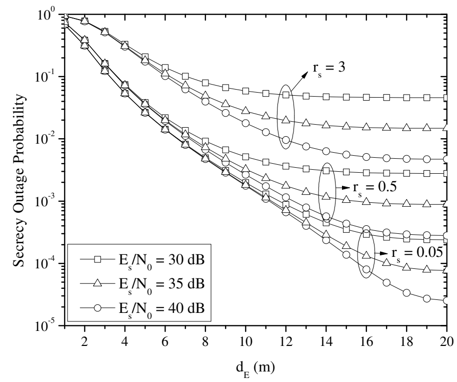

Fig. 4: SOP against d_E for different values of r_s and E_s/N_0.

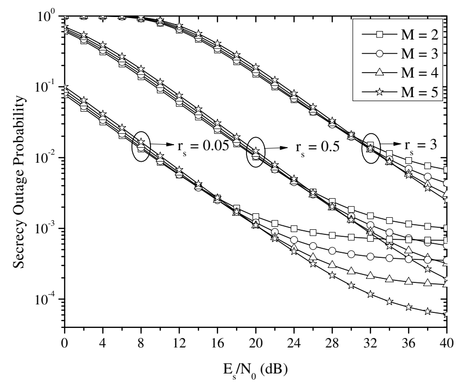

Fig. 5: SOP against E_s/N_0 for different values of M and r_s.

to Alice. We observe that, as the value of E_s/N_0 increases, the SOP decreases. In the low E_s/N_0 regime, a lower number of interferers leads to a lower SOP, but in the high E_s/N_0 regime, a larger number of interferers leads to a lower SOP. These results indicate the need to take into consideration the number of interfering BSs in the evaluation of PHY security in a wireless system.

Appendix
Proof of Theorem 1

The SOP can be expressed as $P_o(r_s) = P_r\left(\frac{X}{Y} \leq 2^{r_s}\right)$. where $X = \gamma_B + 1$ and $Y = \gamma_E + 1$. In order to evaluate the SOP, we first evaluate the cumulative distribution function (CDF) of the SNR at Bob and Eve, which can be obtained as

$$F_{\gamma_{\mathcal{X}}}(x) = \int_{N_0}^{\infty} F_A(yx) f_B(y) dy, \quad (9)$$

where $F_{A_{\mathcal{X}}}(x)$ is the CDF of the RV $A_{\mathcal{X}}$, which is given by $A_{\mathcal{X}} = \frac{E_s}{1+d_{\mathcal{X}}^{\alpha}}|g_{\mathcal{X}}|^2$, while $f_{B_{\mathcal{X}}}(x)$ is the probability density function (PDF) of the RV $B_{\mathcal{X}}$, which can be expressed as $B_{\mathcal{X}} = N_0 + \sum_{i=1}^{M} |g_{\mathcal{X}i}|^2 \frac{E_{si}}{1+d_{\mathcal{X}i}^{\alpha}}$. Notice, that $A_{\mathcal{X}}$ and $B_{\mathcal{X}}$ are independent RVs.

Based on [16], $A_{\mathcal{X}}$ follows Rayleigh distribution with CDF given by $F_{A_{\mathcal{X}}}(x) = 1 - e^{-\frac{1+d_{\mathcal{X}}^{\alpha}}{E_s}x}$. Moreover, since $B_{\mathcal{X}}$ is a weighted sum of Rayleigh distributed RVs, it distribution can be obtained as in [13], and its PDF can be expressed as

$$f_{B_{\mathcal{X}}}(x) = \sum_{i=1}^{M} \frac{\Xi_{\mathcal{X}}(i)}{b_{\mathcal{X}i}} e^{\frac{x-N_0}{b_{\mathcal{X}i}}}, \tag{10}$$

where $b_{\mathcal{X}i} = \frac{E_{si}}{2(1+d_{\mathcal{X}i}^{\alpha})}$. The expressions for b_{Bi} and b_{Ei} are used in the definitions of $\Xi_B(i)$ and $\Xi_E(i)$, respectively. Next, by substituting (10) into (9), and after some simplifications, we obtain

$$F_{\gamma_{\mathcal{X}}}(x) = 1 - \sum_{i=1}^{M} \frac{\Xi_{\mathcal{X}}(i)}{b_{\mathcal{X}i}} \int_{N_0}^{\infty} e^{\left(-\frac{1+d_{\mathcal{X}}^{\alpha}}{E_s}yx - \frac{y-N_0}{b_{\mathcal{X}i}}\right)} dy. \tag{11}$$

By evaluating the integral in (11), we obtain

$$F_{\gamma_{\mathcal{X}}}(x) = 1 - \sum_{i=1}^{M} \frac{E_s \Xi_{\mathcal{X}}(i) e^{-\frac{(1+d_{\mathcal{X}}^{\alpha})N_0 x}{E_s}}}{E_s + (1+d_{\mathcal{X}}^{\alpha}) b_{\mathcal{X}i} x}. \tag{12}$$

Next, the CDFs of X can be derived as $F_X(x) = F_{\gamma_B}(x-1)$, or equivalently

$$F_X(x) = 1 - \sum_{i=1}^{M} \frac{\Xi_B(i) E_s e^{-\frac{(1+d_B^{\alpha})N_0(x-1)}{E_s}}}{E_s + (1+d_B^{\alpha}) b_{Bi}(x-1)}. \tag{13}$$

Additionally, the PDF of Y can be derived as $f_Y(x) = \frac{dF_{\gamma_E}(x-1)}{dx}$ which, after some algebraic manipulations, can be rewritten as

$$\begin{aligned} f_Y(x) &= (1+d_E^{\alpha}) e^{-\frac{(1+d_E^{\alpha})N_0(x-1)}{E_s}} \\ &\times \sum_{i=1}^{M} \Xi_E(i) \left(\frac{E_s b_{Ei}}{\left(E_s + b_{Ei}(1+d_E^{\alpha})(x-1)\right)^2} \right. \\ &\left. + \frac{N_0}{E_s + b_{Ei}(1+d_E^{\alpha})(x-1)} \right). \end{aligned} \tag{14}$$

Since X and Y are independent RV, the SOP can be obtained as

$$P_o(r_s) = \int_1^{\infty} F_X(2^{r_s}x) f_Y(x) dx. \tag{15}$$

By substituting (13) and (14) into (15), and after some mathematical manipulations, we get

$$\begin{aligned} P_o(r_s) = 1 - \sum_{i=1}^{M}\sum_{j=1}^{M} \frac{E_s N_0 \Xi_B(i) \Xi_E(j) e^{\left(\frac{1}{\tilde{\gamma}_B} + \frac{1}{\tilde{\gamma}_E}\right)}}{2^{r_s} b_{Bi} b_{Ej}(1+d_B^{\alpha})} \\ \times \left(\tilde{\gamma}_E \mathcal{I}_1 + \mathcal{I}_2\right), \end{aligned} \tag{16}$$

where $\mathcal{I}_1$ and $\mathcal{I}_2$ can be respectively expressed as

$$\mathcal{I}_1 = \int_1^{\infty} \frac{e^{-Ky}}{(L_{Bi}+y)(L_{Ej}+y)^2} dy \tag{17}$$

and

$$\mathcal{I}_2 = \int_1^{\infty} \frac{e^{-Ky}}{(L_{Bi}+y)(L_{Ej}+y)} dy. \tag{18}$$

By setting $z = y - 1$ into (17) and (18) and after some basic algebraic manipulations and the use of [17, Eq.8.359.1], (17) can be rewritten as

$$\begin{aligned} \mathcal{I}_1 = &\frac{e^{-K}}{(L_{Ej}-1)(L_{Bi}-L_{Ej})} - \frac{K e^{L_{Ej}K} \mathcal{E}i\left(-(L_{Ej}+1)K\right)}{L_{Bi}-L_{Ej}} \\ &+ \frac{e^{L_{Bi}K}\mathcal{E}i(-(L_{Bi}+1)K)}{L_{Bi}-L_{Ej}} - \frac{e^{L_{Ej}K}\mathcal{E}i(-(L_{Ej}+1)K)}{L_{Bi}-L_{Ej}} \end{aligned} \tag{19}$$

$$\mathcal{I}_2 = \frac{e^{KL_{Bi}}\mathcal{E}i(-(1+L_{Bi})K)}{L_{Ej}-L_{Bi}} - \frac{e^{KL_{Ej}}\mathcal{E}i(-(1+L_{Ej})K)}{L_{Ej}-L_{Bi}}. \tag{20}$$

Finally, by substituting (19) and (20) into (16), we obtain (5). This concludes the proof.

References

[1] D. B. Ha, T. Q. Duong, D. D. Tran, H. J. Zepernick, and T. T. Vu, "Physical layer secrecy performance over Rayleigh/Rician fading channels," in *International Conference on Advanced Technologies for Communications*, Oct. 2014, pp. 113–118.

[2] D. Karas, A. A. Boulogeorgos, and G. Karagiannidis, "Physical layer security with uncertainty on the location of the eavesdropper," *IEEE Wireless Commun. Lett.*, vol. PP, no. 99, pp. 1–1, 2016.

[3] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[4] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, Mar. 2014.

[5] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proc. IEEE*, vol. 103, no. 10, pp. 1814–1825, Oct. 2015.

[6] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, p. 2493, 2507 2008.

[7] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdu, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604–619, Feb. 2009.

[8] Z. Shu, Y. Yang, Y. Qian, and R. Q. Hu, "Impact of interference on secrecy capacity in a cognitive radio network," in *IEEE Global Telecommunications Conference (GLOBECOM)*, Dec. 2011, pp. 1–6.

[9] V. D. Nguyen, T. M. Hoang, and O. S. Shin, "Secrecy capacity of the primary system in a cognitive radio network," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3834–3843, Aug. 2015.

[10] Y. Jiang, J. Zhu, and Y. Zou, "Secrecy outage analysis of multi-user cellular networks in the face of cochannel interference," in *IEEE 14th International Conference on Cognitive Informatics Cognitive Computing (ICCI*CC)*, Jul. 2015, pp. 441–446.

[11] Y. Zou, X. Li, and Y. C. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 2222–2236, Nov. 2014.

[12] Z. Ding, Z. Yang, P. Fan, and H. V. Poor, "On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users," *IEEE Signal Process. Lett.*, vol. 21, no. 12, pp. 1501–1505, Dec. 2014.

[13] G. K. Karagiannidis, N. C. Sagias, and T. A. Tsiftsis, "Closed-form statistics for the sum of squared nakagami-m variates and its applications," *IEEE Trans. Commun.*, vol. 54, no. 8, pp. 1353–1359, Aug. 2006.

[14] A.-A. A. Boulogeorgos, N. D. Chatzidiamantis, and G. K. Karagiannidis, "Spectrum sensing with multiple primary users over fading channels," *IEEE Commun. Lett.*, vol. 20, no. 7, pp. 1457–1460, Jul. 2016.

[15] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*. New York: Dover Publications, 1965.

[16] A. Papoulis and S. Pillai, *Probability, Random Variables, and Stochastic Processes*, ser. McGraw-Hill series in electrical engineering: Communications and signal processing. Tata McGraw-Hill, Jan. 2002.

[17] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 6th ed. New York: Academic, 2000.