# On the Average Secrecy Outage Rate and Average Secrecy Outage Duration of Wiretap Channels with Rician Fading

Monir Abughalwa, Aymen Omri, and Mazen O. Hasna
Electrical Engineering Department, Qatar University

***Abstract*—In this paper, we study important physical layer security metrics over wiretap channels with Rician fading. We derive the average secrecy outage rate (ASOR) expression to quantify the average secrecy zero level crossing rate, and the expression of the average secrecy outage duration (ASOD), which measures (in second) how long in average the system remains in the secrecy outage status. Simulation results are conducted to confirm and discuss the theoretical derived expressions. The results show that maximum Doppler frequency shift and signal to noise ratio (SNR) at the eavesdropper are the main factors that affect the ASOR and ASOD.**

***Index Terms*—Average Secrecy Outage Duration, Average Secrecy Outage Rate, Rician Fading Channels, Secrecy Outage Probability, Wiretap Channels.**

## I. Introduction

Privacy and secure communications via wireless networks have taken special attentions in literature [1–4]. Indeed, because of the wireless communiction nature of broadcasting information, an unauthorized user can receive and decode the transmitted signals, via the wiretap channel, that may include highly personal and sensitive data. In general, cryptographic methods have been used to prevent unauthorized personnel from decoding the message. Those methods are based mainly on generating, exchanging, and employing cryptographic keys [3–5]. However, the key distribution and management present a big challenge in the presence of passive eavesdroppers, which can decode the encrypt wireless signals by using advanced computing power and resources [5]. Consequently, new efficient wireless security mechanisms that are not based on the overhead-heavy and coordination-intense cryptographic protocols are needed.

One of the emerging and promising solutions is physical layer security. This concept has been proposed to protect the legitimate users against eavesdroppers, without possibly the need of cryptographic methods [1], [3]. This can be done by exploiting the physical layer characteristics to improve the reliability and to offer secure communications even in the presence of eavesdroppers with unlimited computation ability [4], [6]. This concept was first introduced by Wyner [4], who laid the foundations of information theoretic security. He introduced the idea and the concept of a wiretap discrete memoryless channel and analyzed its inherent achievable secrecy rate capacity.
A lot of research work has been conducted to enhance the physical layer security in wireless communications. In [7], the Wyner's results for discrete memoryless wiretap channels have been extended to the Gaussian wiretap channel, where, the authors have shown that the secrecy capacity is the difference between the capacities of the main and wiretap channels. In [8–10] the authors have used the joint beamforming and jamming techniques to enhance the security communication systems. In [11], [12], the authors have presented the idea of artificial noise to improve the physical layer security. In [13–17], different cooperative schemes have been studied and investigated to confirm that cooperation can greatly improve the security.

Different physical layer security schemes have been analyzed in literature using mainly first order statistics, in particular the secrecy capacity and/or the secrecy outage probability, which have been traditionally the most commonly used security measures for wiretap channels [4], [10], [18], [19]. However, the dynamics of the performance of those systems require analysing higher order statistics metrics, for us to have better insight into their performance. For example, secrecy outage probability provides an idea about the fraction of fading realizations for which the channel can support a certain rate. However, it does not provide an idea on the average length (in terms of realizations) for which the channel cannot support secure communication. Mobility is another dimension where second order statistics come to play. In a scenario where transmitters, receivers, and eavesdroppers are on the move, we may need to check what speed results in what average secrecy outage duration, and hence the system may plan for specific measures in relocating or changing the speed of its components whenever applicable.

To the best of our knowledge, there is few published analytically works which addressed the impact of the fading statistics on the average outage rate, and the system outage duration. In particular, published analyt-

978-1-5386-2070-0/18/$31.00 ©2018 IEEE

ical work on the ASOR, and the ASOD of wireless communication systems over Rician fading channels is still not available in the literature.

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

- We derive the expression of the ASOR to evaluate the average secrecy zero level crossing rate for wireless communication systems over Rician fading channels.
- Based on the derived expressions of the secrecy outage probability, and the ASOR, we investigate the ASOD, during which the system remains in the secrecy outage status.

The rest of this paper is organized as follows. Section II describes the system and channel models. The performance analysis is detailed in Section III, where the expressions of the secrecy outage probability, the ASOR, and the ASOD are detailed and derived. In Section IV, the simulation results are presented to confirm and investigate the derived expressions. Finally, conclusions are drawn in Section V.

## II. System and Channel Models

In this section, we present the system and channel models, where a source (Alice) intends to send messages to a receiver (Bob), in the presence of an eavesdropper (Eve). The desired signal is received at both Bob and Eve, with additive white Gaussian noise (AWGN), where a perfect interference management is assumed. The received signal to noise ratios (SNRs) at Bob ($\gamma_{_B}$) and at Eve ($\gamma_{_E}$) are expressed as

$$\gamma_{_B} = \frac{\alpha_{_B}^2}{N_{_0}}, \tag{1}$$

and,

$$\gamma_{_E} = \frac{\alpha_{_E}^2}{N_{_0}}, \tag{2}$$

respectively, where, $\alpha_{_B}^2$ and $\alpha_{_E}^2$ are the total received desired signal power at Bob and at Eve, respectively, and $N_{_0}$ is the AWGN power.

The received signals are assumed to be subject to the Rician type of fading, where the corresponding general PDF of $\alpha_\chi$, $\forall\ \chi\ \in$ {B: Bob, E: Eve}, is expressed as [20]

$$p_{\alpha_\chi}(\alpha) = \frac{2(K_{_\chi}+1)\alpha}{\Omega_{_\chi}}\ \exp\left(-K_{_\chi} - \frac{(K_{_\chi}+1)\ \alpha^2}{\Omega_{_\chi}}\right) \times \mathrm{I}_0\left(2\ \alpha\ \sqrt{\frac{K_{_\chi}\ (K_{_\chi}+1)}{\Omega_{_\chi}}}\right), \tag{3}$$

with, $\mathrm{I}_0(.)$ is the zeroth-order modified Bessel function [21], $K_{_\chi}$ and $\Omega_{_\chi}$ are, respectively, the Rician factor and the average received power via the channel between Alice and $\chi$.

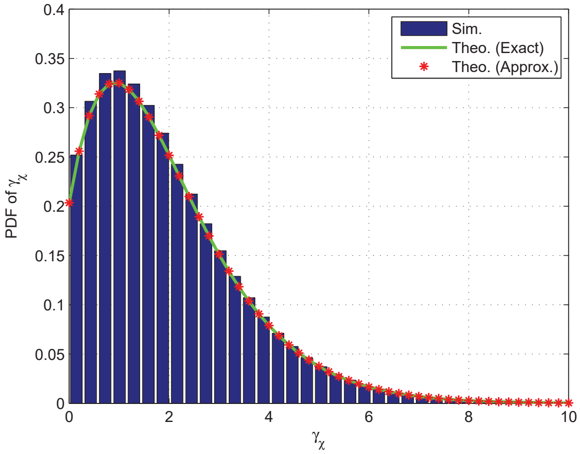

Fig. 1. Histogram for the PDF simulation of $\gamma_\chi$ as compared to the exact and approximate expressions in (5) and (6), respectively, with $\omega_\chi = 0$ dB, and $K_\chi = 1$.

It is known that the time derivative of the signal amplitude process, denoted by $\dot{\alpha}_{_\chi}$, is always independent of the signal amplitude, and the PDF expression of $\dot{\alpha}_{_\chi}$ is given by [20]

$$p_{\dot{\alpha}_{_\chi}}(\dot{\alpha}_{_\chi}) = \frac{1}{\sqrt{2\ \pi}\ \sigma_\chi}\ \exp\left(-\frac{\dot{\alpha}_{_\chi}^2}{2\ \sigma_\chi^2}\right), \tag{4}$$

where, $\sigma_\chi^2 = \pi^2 f_{_{\max}}^2 \Omega_{_\chi}/(K_{_\chi}+1)$, and $f_{_{\max}}$ is the maximum Doppler frequency shift.

Based on (1-3), the general PDF of $\gamma_\chi$, $\forall\ \chi\ \in \{B,\ E\}$, can be expressed as [20]

$$p_{\gamma_\chi}(\gamma) = \frac{K_{_\chi}+1}{\Omega_{_\chi}}\ \exp\left(-K_{_\chi} - \frac{(K_{_\chi}+1)\ \gamma}{\Omega_{_\chi}}\right) \times \mathrm{I}_0\left(\sqrt{\frac{K_{_\chi}\ (K_{_\chi}+1)\ \gamma}{\Omega_{_\chi}}}\right), \tag{5}$$

where, $\omega_{_\chi} = \Omega_{_\chi}/N_{_0}$ is the average received SNR at $\chi$.

To simplify the analytical derivations of the proposed security evaluation metrics, and based on the alternative expression of $\mathrm{I}_0(.)$ [21, Eq. (8.445)], a tight approximation of (5) is given by

$$p_{\gamma_\chi}(\gamma) \approx \frac{K_{_\chi}+1}{\Omega_{_\chi}}\ \exp\left(-K_{_\chi} - \frac{(K_{_\chi}+1)\ \gamma}{\Omega_{_\chi}}\right) \times \sum_{n=0}^{N}\left[\frac{K_{_\chi}(K_{_\chi}+1)}{\Omega_{_\chi}}\right]^n \frac{\gamma^n}{n!\ \Gamma(n+1)}, \tag{6}$$

where, $N >> 1$ is a large integer.

To confirm the accuracy of the approximate expression in (6), we present in Fig. 1 the histogram for simulating the PDF of $\gamma_\chi$ as well as the outputs of the exact and approximate PDF expressions in (5) and (6), respectively, with $\omega_\chi = 0$ dB, and $K_\chi = 1$. As shown in this figure, there is an excellent fit between the exact and the approximate expressions, where an average error of less than 2e$-$4 (for $N = 10$) is observed.

## III. Performances Analysis

### A. *Secrecy Outage Probability*

A secrecy outage can be defined as the event in which the secrecy capacity ($SC$) falls below zero, i.e., the secrecy capacity at Eve is larger or equal to that at Bob. Accordingly, the secrecy outage probability is written as follows

$$\begin{aligned} P_{out} &= \mathrm{P}\{SC < 0\} \\ &= \mathrm{P}\Big\{\big[\log_2(1+\gamma_B) - \log_2(1+\gamma_E)\big] < 0\Big\}. \end{aligned} \tag{7}$$

The final expression of $P_{out}$ is derived in Appendix A and is given by

$$\begin{aligned} P_{out} \approx \exp(-K_B) \sum_{n=0}^{N} \frac{K_B^n}{\Gamma(n+1)} \Bigg(1 - \exp(-K_E) \\ \times \sum_{m=0}^{n} \sum_{l=0}^{N} \binom{m+l}{l} \frac{K_E^n}{\Gamma(l+1)} \left[\frac{\omega_E}{\omega_B}\right]^m \left[1 + \frac{\omega_E}{\omega_B}\right]^{-m-l-1}\Bigg). \end{aligned} \tag{8}$$

### B. *Average Secrecy Outage Rate (ASOR)*

The secrecy outage rate is defined as the secrecy level crossing rate (SLCR) of the secrecy capacity $SC$ at level zero. Based on the definition of $SC$, the event of ($SC < 0$) is equivalent to the event of having $[r = \frac{\alpha_B}{\alpha_E} < 1]$. Consequently, $\mathfrak{R}$ is equivalent to the rate at which the process $r$ crosses downward the level 1. This LCR can be obtained from the general formula provided in [22]

$$\mathfrak{R} = \int_0^\infty \dot{r}\ p_{r,\dot{r}}(1,\dot{r})\ d\dot{r}, \tag{9}$$

where, $p_{r,\dot{r}}$ is the joint PDF of $r$ and $\dot{r}$, and which is given by [20]

$$\begin{aligned} p_{r,\dot{r}}(1,\dot{r}) = \int_0^\infty \int_{-\infty}^{\infty} \alpha_E^2\ p_{\alpha_B}(\alpha_E)\ p_{\dot{\alpha}_B}(\dot{r}\ \alpha_E + \dot{\alpha}_E) \\ \times p_{\alpha_E}(\alpha_E)\ p_{\dot{\alpha}_E}(\dot{\alpha}_E)\ d\dot{\alpha}_E\ d\alpha_E. \end{aligned} \tag{10}$$

By substituting (10) in (9), and based on the derivation details of the LCR in the case of the well known outage fading that is presented in [20], $\mathfrak{R}$ is expressed as follows

$$\begin{aligned} \mathfrak{R} = \frac{\sqrt{2\pi}\ f_{\max}\ \exp(-K_B - K_E)\ \sqrt{\lambda}}{1+\lambda} \\ \times \sum_{n=0}^{\infty} \frac{\Gamma(\frac{3}{2}+n)}{n!\ \Gamma(n+1)} \left[\frac{\lambda K_E}{1+\lambda}\right]^n {}_1\mathrm{F}_1\left(\frac{3}{2}+n;\ 1;\ \frac{K_B}{1+\lambda}\right), \end{aligned} \tag{11}$$

where, $\lambda = \omega_B(K_E+1)/[\omega_E(K_B+1)]$, and ${}_1\mathrm{F}_1(.;.;.)$ is the hypergeometric function [21].

### C. *Average Secrecy Outage Duration (ASOD)*

The ASOD is a measure to describe how long in average the system remains in the secrecy outage status. Mathematically speaking, and based on the definition of the average outage duration in [20], [22], the expression of ASOD is given by

$$\mathfrak{D} = \frac{P_{out}}{\mathfrak{R}}, \tag{12}$$

where, $P_{out}$ and $\mathfrak{R}$ are given by (8) and (11), respectively.

## IV. Numerical Results

In this section, numerical results are presented to confirm and discuss the derived analytical expressions. The conducted simulations are based on Monte Carlo simulation using MatLab software, where a channel object is used to represent Rice fading channels with a specific sampling time ($T_s$), a specific maximum Doppler frequency shift ($f_{\max}$), and a specific Rician factor $K_\chi$. Without loss of generality, the used simulation parameters are presented in the following table.

TABLE I
SIMULATION PARAMETERS

| Parameter | Value |
|---|---|
| *Simulation Time* [s] | 100 |
| $T_s$ [s] | $1e-4$ |
| $N_s$ | $1e6$ |
| $f_{\max}$ [Hz] | $5,\ 20,$ and $50$ |
| $\omega_B$ [dB] | $0:20$ |
| $\omega_E$ [dB] | $0,\ 10,$ and $20$ |
| $N$ | $10$ |

Fig. 2 presents the variation of secrecy capacity realizations versus time, with $K_B = K_E = 1$, $\omega_B = 10$

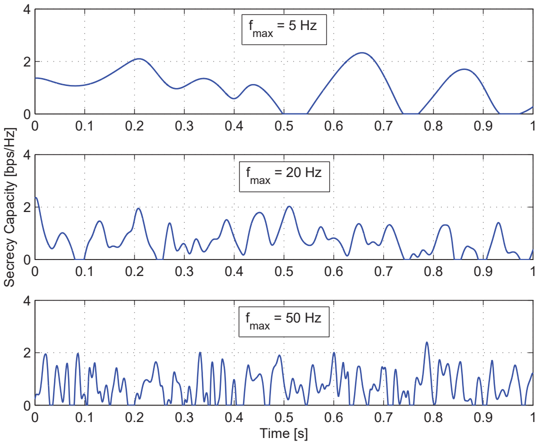

Fig. 2. Secrecy capacity realizations versus time, with $K_B = K_E = 1$, $\omega_B = 10$ dB, $\omega_E = 5$ dB, and different values of $f_{\max}$.

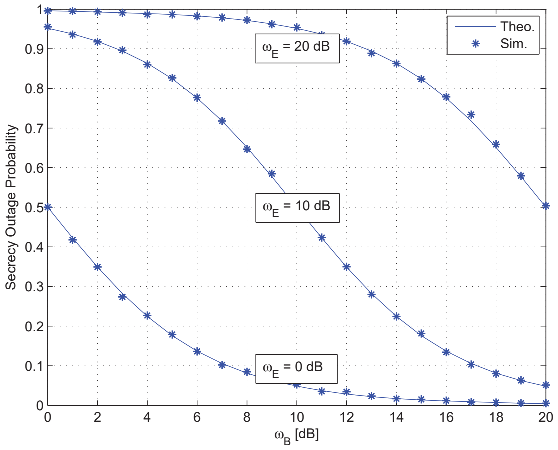

Fig. 3. Secrecy Outage Probability versus $\omega_B$, with $K_B = K_E = 2$, $f_m = 20$ Hz, and different values of $\omega_E$.

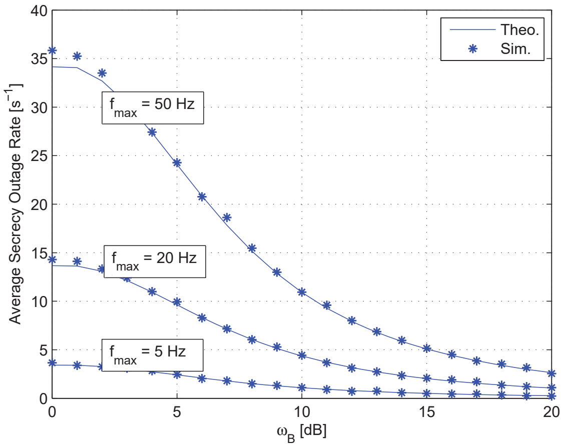

Fig. 4. Average secrecy outage rate versus $\omega_B$, with $K_B = K_E = 2$, $\omega_E = 0$ dB, and different values of $f_{\max}$.

dB, $\omega_E = 5$ dB, and different values of $f_{\max}$. In this figure, it is clear that the variation of the secrecy capacity increases with the increased values of $f_{\max}$. This is due to the fact that the channel coherence time is inversely proportional to $f_{\max}$, which results in fast fading channels between the different nodes in the network. Consequently, a fast variation of the secrecy capacity is observed, which increases the number of crossing the zero secrecy level.

The variation of the secrecy outage probability versus $\omega_B$ is presented in Fig. 3, with $K_B = K_E = 2$, $f_{\max} = 20$ Hz, and different values of $\omega_E$. As shown in this figure, the secrecy outage probability decreases with the increased values of $\omega_B$ and increases with the increased values of $\omega_E$. This is because, by increasing $\omega_B$, the secrecy capacity increases, which decreases the secrecy outage probability. In contrast, the increased values of $\omega_E$ decreases the secrecy capacity, and hence an increase in the secrecy outage probability is observed.

Fig. 4 presents the variation of the ASOR [or average secrecy level crossing rate] versus $\omega_B$, with $K_B = K_E = 2$, $\omega_E = 0$ dB, and different values of $f_{\max}$. As shown in this figure, the increased values of the maximum Doppler frequency shift $f_{\max}$ increases the ASOR. This is due to the fact that, as detailed for Fig. 1, the increased values of $f_{\max}$ results in fast fading channels between the different nodes in the network, and hence a fast variation of the secrecy capacity is observed, which increases the average secrecy level crossing rate.

In Fig. 5, the variation of the ASOD versus $\omega_B$ is presented, with $K_B = K_E = 1$, $f_m = 20$ Hz, and different values of $\omega_E$. Similar to the behavior of the secrecy outage probability, and different than the variation of the ASOR, the ASOD decreases with the increased values of $\omega_B$, and increases with the increased values of $\omega_E$. This is because, the ASOD is directly proportional to the secrecy outage probability and inversely proportional to the ASOR as defined in (12).

## V. Conclusion

In this paper, we have investigated the ASOR and the ASOD of wiretap Rician fading channels. The analytical expressions of the ASOR and the ASOD have been detailed and derived. Then, simulation results have been conducted to evaluate the analytical derived expressions, and to investigate the variations of the metrics under consideration in different scenarios. These results have shown the importance of those metrics for the evaluation of the physical layer security, and hence for the system design and deployment.

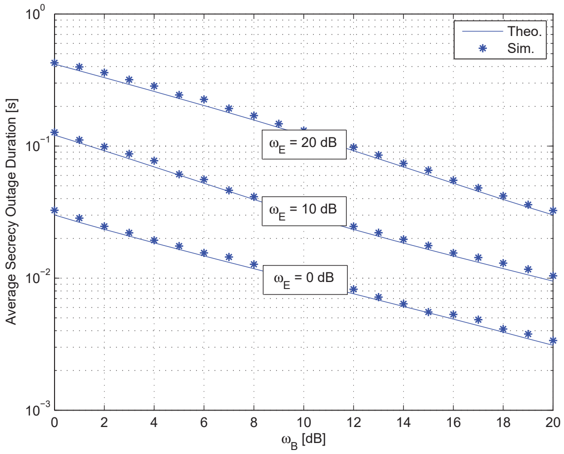

Fig. 5. Average Secrecy Outage Duration vs. $\omega_B$, with $K_B = K_E = 1$, $f_m = 20$ Hz, and different values of $\omega_E$.

## Appendix A
## Derivation of $P_{out}$

In this Appendix, we derive the expression of $P_{out}$. Based on (7), $P_{out}$ can be written as follows

$$\begin{aligned} P_{out} &= \mathrm{P}\left\{ \left[ \frac{1}{2}\log_2(1+\gamma_B) - \frac{1}{2}\log_2(1+\gamma_E) \right] <= 0 \right\} \\ &= \mathrm{P}\left\{ \gamma_B \ <= \ \gamma_E \right\} \\ &= \int_0^\infty \int_0^y p_{\gamma_B}(x)\, p_{\gamma_E}(y)\, dx\, dy. \end{aligned} \tag{13}$$

Based on the PDF approximate expression of $\gamma_B$ in (6), and on [21, Eq. (3.351.1)], the first integration, in (13), with respect to $x$ is evaluated, and the expression of $P_{out}$ is rewritten as

$$\begin{aligned} P_{out} \approx & \int_0^\infty \frac{K_B+1}{\omega_B}\ \exp(-K_B) \sum_{n=0}^{N} \left\{ \left[ \frac{K_B(K_B+1)}{\omega_B} \right]^n \right. \\ & \times \frac{1}{\Gamma(n+1)} \left( \left[ \frac{\omega_B}{K_B+1} \right]^{n+1} - \sum_{m=0}^{n} \frac{y^m}{m!}\ \exp\left( \frac{-y\,(K_B+1)}{\omega_B} \right) \right. \\ & \left. \left. \times \left[ \frac{\omega_B}{K_B+1} \right]^{n-m+1} \right) \right\} p_{\gamma_E}(y)\ dy. \end{aligned} \tag{14}$$

Now, by substituting the PDF expression of $\gamma_E$, which is given by (6), using [21, Eq. (3.351.3)], and carrying out some simplification steps, the final expression of $P_{out}$ is given by (8) on page 3.

## Acknowledgement

This publication was made possible by the sponsorship agreement in support of research and collaboration by Ooredoo, Doha, Qatar. The statements made herein are solely the responsibility of the authors.

## References

[1] Y. J. Tolossa, S. Vuppala, and G. Abreu, "Secrecy-Rate Analysis in Multitier Heterogeneous Networks Under Generalized Fading Model," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 101 – 110, 2017.

[2] H. M. Wang and X. G. Xia, "Enhancing Wireless Secrecy via Cooperation: Signal Design and Optimization," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 47–53, 2015.

[3] M. Bloch, M. Debbah, Y. Liang, Y. Oohama, and A. Thangaraj, "Special Issue on Physical-Layer Security," *Journal of Communications and Networks*, vol. 14, no. 4, pp. 349 – 351, 2012.

[4] A. D. Wyner, "The Wire-tap Channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355 – 1387, 1975.

[5] S. Iwata, T. Ohtsuki, and P. Y. Kam, "A Lower Bound on Secrecy Capacity for MIMO Wiretap Channel Aided by a Cooperative Jammer with Channel Estimation Error," *IEEE Access*, 2017.

[6] A. Salem and K. A. Hamdi, "Improving Physical Layer Security of AF Relay Networks via Beam-Forming and Jamming," *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*, 2016.

[7] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian Wire-Tap Channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[8] R. Negi and S. Goel, "Secret Communication Using Artificial Noise," *Vehicular Technology Conference (VTC)*, 2005.

[9] S. Goel and R. Negi, "Guaranteeing Secrecy Using Artificial Noise," *IEEE Transactions on Wireless Communications*, vol. 7, pp. 2180–2189, 2008.

[10] T. M. Hoang, T. Q. Duong, N-S. Vo, and C. Kundu, "Physical Layer Security in Cooperative Energy Harvesting Networks With a Friendly Jammer," *IEEE Wireless Communications Letters*, vol. 6, no. 2, pp. 174–177, 2017.

[11] X. Zhou and M. McKay, "Physical Layer Security with Artificial Noise: Secrecy Capacity and Optimal Power Allocation," *International Conference on Signal Processing Communications Systems (ICSPCS)*, 2009.

[12] W. Wang, K. C. Teh, and K. H. Li, "Artificial Noise Aided Physical Layer Security in Multi-Antenna Small-Cell Networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 6, pp. 1470–1482, 2017.

[13] K. Tourki and M. O. Hasna, "A Collaboration Incentive Exploiting the Primary-Secondary Systems Cross Interference for PHY Security Enhancement," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1346 – 1358, 2016.

[14] K. Tourki and M. O. Hasna, "Proactive Spectrum Sharing Incentive for Physical Layer Security Enhancement Using Outdated CSI," *IEEE Transactions on Wireless Communications*, vol. 15, no. 9, pp. 6273 – 6283, 2016.

[15] L. Hu, H. Wen, B. Wu, J. Tang, and F. Pan, "Adaptive Secure Transmission for Physical layer Security in Cooperative Wireless Networks," *IEEE Communications Letters*, vol. 21, no. 3, pp. 524–527, 2017.

[16] A. Petropulu L. Dong, Z. Han and H. Poor, "Improving Wireless Physical Layer Security Via Cooperating Relays," *IEEE Transactions on Signal Processing*, vol. 58, pp. 1875–1888, 2010.

[17] A. Petropulu J. Li and S. Weber, "On Cooperative Relaying Schemes for Wireless Physical Layer Security," *IEEE Transactions on Signal Processing*, vol. 59, pp. 4985–4997, 2011.

[18] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, "Secrecy Rate Optimizations for a MIMO Secrecy Channel With a Multiple-Antenna Eavesdropper," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 4, pp. 1678–1690, 2014.

[19] N. Bhargav, S. L. Cotton, and D. E. Simmons, "Secrecy Capacity Analysis Over k-mu Fading Channels: Theory and Applications," *IEEE Transactions on Communications*, vol. 64, no. 7, pp. 3011–3024, 2016.

[20] L. Yang and M. S. Alouini, "On the Average Outage Rate and Average Outage Duration of Wireless Communication Systems With Multiple Cochannel Interferers," *IEEE Transactions on Wireless Communications*, vol. 3, no. 4, pp. 1142 – 1153, 2004.

[21] I.S. Gradshteyn and I.M. Ryzhik, "Table of Integrals, Series, and Products," *Elsevier Inc.*, p. 1200, 2007.

[22] G. L. Stuber, *Principles of Mobile Communication*, 2nd ed. Norwell,MA: Kluwer, 2000.