On the Effect of Random Power Availability in Wireless Power Transfer Systems with Physical Layer Security

Antonio Tarrías-Muñoz[1,2], Juan Manuel Romero-Jerez[1], F. Javier López-Martínez[2]
antoniotarriasm@uma.es, romero@dte.uma.es, fjlopezm@ic.uma.es
[1]Dpto. de Tecnología Electrónica, Universidad de Málaga.
[2]Dpto. de Ingeniería de Comunicaciones, Universidad de Málaga.
Campus de Teatinos s/n, ETSI Telecomunicación, 29071 Málaga.

***Abstract*—In this paper, we evaluate the performance of wireless powered communication systems from a physical layer security perspective. Our aim is to determine under which conditions the random power availability due to wireless power transmission using a dedicated power beacon impacts the maximum secrecy rate, compared to its deterministic counterpart. We also investigate the effect of line-of-sight condition on the system performance. Analytical expressions are derived for some specific scenarios, which are combined with Monte Carlo simulations. We see that under a moderate line-of-sight condition in the wireless power transfer link, the secrecy performance is barely affected.**

I. Introduction

Traditionally, the provision of security in communications has been focused in software encryption techniques, which are in continuous development due to the huge evolution of processors and their computing capabilities [1]. These cryptographic techniques usually rely on upper-layer operation, being the physical layer usually not taken into consideration. For the latter case, the pioneering work by Shannon [2] on communication security from an information-theoretic perspective proved that secure communication was attainable regardless of the computing power of malicious eavesdroppers. However, this work remained as a rather unpractical reference for decades [3]. This idea, for which the term physical layer security was later coined, has gained momentum in the last years in the context of wireless communications [4]. The random fluctuations inherent to wireless fading channels are known to enable the secure transmission of information over a wireless link in the presence of an external eavesdropper.

In a different context, there is a need for extending the battery lifetimes and reducing operational costs associated to the deployment of wireless sensor networks that enable the Internet of Things (IoT) paradigm [5]. Wireless power transfer (WPT) [6, 7] is being considered as a potential solution to provide remote nodes with the required energy for operation, by wirelessly conveying energy from dedicated power beacons. The need for security in IoT applications opens the door to the use of physical layer techniques in this WPT scenario. Indeed, some authors have tackled this problem [8], although its inherent analytical complexity does not facilitate understanding the interplay between the different parameters from a system design perspective.

In this paper, we investigate to what extent secure wireless communications from a physical layer perspective are feasible, in the context of wireless powered communications. Specifically, we consider a wireless communication system on which a legitimate transmitter harvests energy for its operation from a remote power beacon, and then uses it to transmit information to a legitimate receiver, in the presence of an external eavesdropper that observes the communication. The outage probability of secrecy capacity and the average secrecy rate are evaluated, and compared to those of a conventional device with unlimited battery used for benchmarking purposes.

II. System Model

A. Reference System Set-up

We first consider a system set-up where a legitimate user (Alice) wants to communicate with another legitimate user (Bob) over a wireless fading channel. At the same time, a non-legitimate user (Eve) is capable of eavesdropping on Alice-Bob's transmissions due to the broadcast nature of wireless transmissions. The system is depicted in Fig. 1.

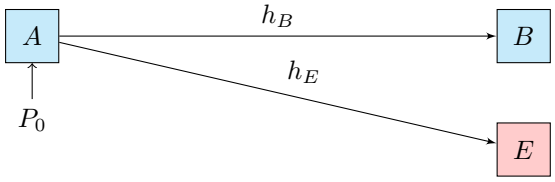

Fig. 1. Initial System Set-up

In the figure, P_0 is the available power at Alice's transmitter, which is assumed to be constant, and h_B and h_E are in charge of modeling the random effects of multipath fading over the transmitted signal. Without loss of generality, we consider normalized fading channel coefficients so that, $\mathbb{E}\{|h_B|^2\} = \mathbb{E}\{|h_E|^2\} = 1$, where $\mathbb{E}\{\cdot\}$ is the expectation operator. We also assume that the desired (between Alice and Bob) and eavesdropped (between Alice and Eve) channels are independent quasi-static fading channels, (i.e. constant during the transmission of given codeword, yet independent between codewords), and that both receivers are affected by additive white Gaussian noise (AWGN).

With these definitions, the instantaneous signal-to-noise ratio (SNR) at Bob's receiver is given by:

$$\gamma_B = \frac{P_0 (d_B)^{-\alpha}}{N_0} |h_B|^2 = \overline{\gamma}_B \, |h_B|^2 \tag{1}$$

where $\overline{\gamma}_B = \frac{P_0 (d_B)^{-\alpha}}{N_0}$ is the average SNR at Bob, d_B is the distance between A and B, α is the path loss exponent and N_0 is the noise power. In the same way, at Eve's receiver the instantaneous SNR is given by:

$$\gamma_E = \frac{P_0 (d_E)^{-\alpha}}{N_0} |h_E|^2 = \overline{\gamma}_E \, |h_E|^2 \tag{2}$$

and the average SNR is $\overline{\gamma}_E = \frac{P_0 (d_E)^{-\alpha}}{N_0}$, where d_E is the now the distance between A and E, α is the path-loss exponent, and N_0 is the noise power. For notational simplicity and without loss of generality, we assume the same values for α and N_0 at both receivers. Because the following analysis will be made as a function of $\overline{\gamma}_B$ and $\overline{\gamma}_E$, the effect of the former parameters as well as the distances between nodes are embedded within the average SNRs.

B. Wireless Power Transmission Set-up

Let us now consider a modification of the reference system model in Fig. 1, where now a dedicated power beacon (PB) is used to convey energy to Alice. As we can see in Fig. 2, the energy transmission between PB and A is made through a wireless channel denoted as h_P, which is independent of h_B and h_E, with $\mathbb{E}\{|h_P|^2\} = 1$.

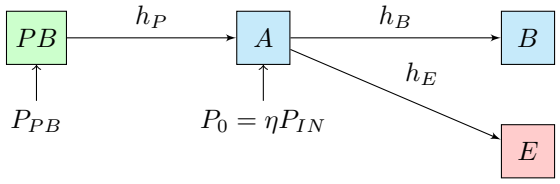

Fig. 2. Wireless power transfer-based system set-up

In Fig. 2, we define P_{PB} as the available power at PB, and denote as P_{IN} the input power at Alice's receiver. The coefficient η is the energy harvesting (EH) conversion efficiency. For the sake of tractability, we assume a linear EH model for Alice as in [8]. In this situation, the instantaneous SNR at Bob and Eve's receivers are given, respectively, by:

$$\gamma'_B = \overline{\gamma}'_B \left|h_B\right|^2 \left|h_P\right|^2, \tag{3}$$

$$\gamma'_E = \overline{\gamma}'_E \left|h_E\right|^2 \left|h_P\right|^2, \tag{4}$$

and their average values can be written as:

$$\overline{\gamma}'_B = \frac{P_{PB}\eta (d_B d_{PB-A})^{-\alpha}}{N_0}, \tag{5}$$

$$\overline{\gamma}'_E = \frac{P_{PB}\eta (d_E d_{PB-A})^{-\alpha}}{N_0}, \tag{6}$$

where d_{PB-A} denotes the distance between the PB and Alice. Note that according to (3) and (4), a product channel arises naturally in the definitions of the instantaneous SNRs. By inspecting (1), (2), (5) and (6), we see that P_{PB} needs to be designed in order to provide the same average P_O at the harvester output as in the reference case, in order to ensure a target average SNR at Bob. This will be the case in our analysis, i.e. $\overline{\gamma}'_B = \overline{\gamma}_B$ and $\overline{\gamma}'_E = \overline{\gamma}_E$ with a proper design of the power beacon transmit power P_{PB}.

III. Secrecy Capacity Metrics

A. General definitions

According to Shannon's definition, channel capacity is the maximum achievable transmission rate (bits/s) that can be attained, with the condition of being error-free. In the following, and without loss of generality, we will use capacity definitions per bandwidth unit, i.e. $C = \log_2(1+\gamma)$. Similarly, the secrecy capacity C_S is defined as the maximum achievable transmission rate that can be attained under two conditions: being error-free for the desired link, and being secure in the sense of the eavesdropper being unable to decode the information. With this definition, and in the absence of fading, we have $C_S = C_B - C_E > 0$ [4, eq. (4)]:

$$C_S = \begin{cases} \log_2(1+\gamma_B) - \log_2(1+\gamma_E) & \gamma_B \geq \gamma_E \\ 0 & \gamma_B < \gamma_E \end{cases} \tag{7}$$

Inspection of (7) reveals that a secure rate does not exist in the event that the SNR at Bob is worse than the SNR at Eve. However, when channel fading comes into play, it is possible that such condition is met for the instantaneous SNR even though the average SNR at Bob is lower than the average SNR at Eve. With this in mind, and depending on whether Eve's channel state information is available at Alice or not, two secrecy metrics are conventionally used to characterize the physical layer security performance in wireless channels: the average secrecy capacity (ASC) and the outage probability of secrecy capacity (OPSC).

The ASC can be obtained (as indicated in [9, eq. (12)]) by averaging the instantaneous secrecy capacity in (7) over all possible fading states, yielding:

$$\overline{C_S} = \log_2(e) \int_0^\infty [1 - F_{\gamma_B}(x)] \frac{F_{\gamma_E}(x)}{1+x}\, \mathrm{d}x \tag{8}$$

where $F_\gamma(\cdot)$ is the cumulative distribution function (CDF) for the intended SNRs (γ_B and γ_E, respectively).

Similarly, the OPSC is defined as the probability that the maximum secrecy information rate is less than a required threshold secrecy information rate R_{th}, and can be computed as [11]

$$\Pr\{C_S \leq R_{th}\} = \int_0^\infty F_{\gamma_B}\left(2^{R_{th}} - 1\right) f_{\gamma_E}(x)\, \mathrm{d}x \tag{9}$$

where $f_\gamma(\cdot)$ is the probability density function (PDF) of γ.

B. Scenario under analysis

We aim to determine the effect of random power availability at Alice because of the channel fading at the h_P link, using the above definitions for the secrecy metrics. Because of the inherent LOS nature of the WPT link, we model the random fluctuations at h_P using the Rician (Rice) distribution [10]. As for the channel fading at the information links h_B and h_E, we will use different combinations of the Rician and Rayleigh distributions in order to encompass LOS and non-LOS conditions. We will refer to these cases as X-Y, denoting X the fading distribution for h_B and Y the fading distribution for h_E. From (3) and (4), and defining $g_P = |h_P|^2$, we can write $\gamma'_B = \gamma_B g_P$ and $\gamma'_E = \gamma_E g_P$. Hence, when conditioning to a specific value of g_P, the secrecy metrics are those of the case of having a deterministic power availability at Alice, only that the average SNRs at Bob and Eve are now scaled by g_P. Hence, we can solve the set-up in Section II-B by using the solution of the set-up in Section II-A, and then average over all possible states of the random variable g_P using

$$f_{g_P}(g) = (K_P+1)\, e^{(-g(K_P+1)-K_P)} I_0\left(2\sqrt{g\, K_P(K_P+1)}\right), \tag{10}$$

where $I_0(\cdot)$ is the modified Bessel function of the first kind and order zero, and K_P is the Rician K factor for the WPT

link accounting for the amount of power conveyed through the LOS component, with respect to the NLOS power. This can be formally stated as $\overline{C_S} = \mathbb{E}\{C_S|g_P\}$ for the ASC metric and $\Pr\{C_S \leq R_{th}\} = \mathbb{E}\{\Pr\{C_S \leq R_{th}\}|g_P\}$ for the OPSC.

Analytical solutions for the OPSC in the Rayleigh-Rayleigh, Rayleigh-Rice and Rice-Rayleigh cases are either available in [4] or can be deduced using the approach in [11].They are not explicitly shown here for the sake of brevity. Similarly, the ASC in the Rayleigh-Rayleigh case is also given in [4]; as for the rest of cases, analytical solutions are very complicated [9] to be averaged out over (10). Therefore, we will use the tight asymptotic approximation recently proposed in [12] in order to approximate the average secrecy capacity $\overline{C}_S$ as the difference between the average capacities of the desired and eavesdropper's links in the high-SNR regime:

$$\overline{C}_S|_{\uparrow\overline{\gamma}_B} \approx \overline{C}_B - \overline{C}_E. \tag{11}$$

With these considerations, we will describe the Rayleigh-Rayleigh as an example of how the analytical evaluation of the performance metrics of interest can be carried out when conditioning to g_P. In this situation, we have [4]

$$P(C_S|g_P \leq R_{th}) = 1 - \frac{\overline{\gamma}_B}{\overline{\gamma}_B + 2^{R_{th}}\overline{\gamma}_E} e^{-\frac{2^{R_{th}}-1}{\overline{\gamma}_B}} \tag{12}$$

$$\overline{C}_S|g_P = \mathcal{F}(\overline{\gamma}_B) - \mathcal{F}\left(\frac{\overline{\gamma}_B\overline{\gamma}_E}{\overline{\gamma}_B + \overline{\gamma}_E}\right), \tag{13}$$

with $\mathcal{F}(x) = \log_2(e)e^{\frac{1}{x}}E_1(x^{-1})$, and $E_1(\cdot)$ is the exponential integral function [13, eq. 8.211]. Now, replacing $\overline{\gamma}_B \to \overline{\gamma}_B g_P$ and also $\overline{\gamma}_E \to \overline{\gamma}_E g_P$, the desired performance metrics are obtained as:

$$P(C_S \leq R_{th}) = 1 - \frac{\overline{\gamma}_B/\overline{\gamma}_E}{\overline{\gamma}_B/\overline{\gamma}_E + 2^{R_{th}}} \int_0^\infty e^{-\frac{2^{R_{th}}-1}{g\overline{\gamma}_B}} f_{g_P}(g)dg \tag{14}$$

$$\overline{C}_S = \int_0^\infty \left[\mathcal{F}(\overline{\gamma}_B g) - \mathcal{F}\left(\frac{\overline{\gamma}_B g}{\overline{\gamma}_B/\overline{\gamma}_E + 1}\right)\right] f_{g_P}(g)dg, \tag{15}$$

and

$$\overline{C}_S|_{\uparrow\overline{\gamma}_B} \approx \int_0^\infty \left[\mathcal{F}(\overline{\gamma}_B g) - \mathcal{F}(\overline{\gamma}_E g)\right] f_{g_P}(g)dg, \tag{16}$$

IV. Numerical Results

After the definition of the secrecy capacity metrics given in the previous Section, we now provide numerical results of their evaluation in several scenarios of interest. Theoretical expressions have been used to reproduce the secrecy performance metrics in the following figures, and Monte Carlo simulations have been performed in all instances to double-check the validity of the theoretical results. We first evaluate the reference scenario given in Section II-A, in order to determine the effect of LOS propagation in the desired and eavesdropper's links. This will be quantified through the Rician K parameters denoted as K_B and K_E, respectively. When either of these parameters equals zero, that corresponds to the Rayleigh case, i.e. NLOS scenario.

In Fig. 3, we evaluate the ASC in different scenarios as K_E and K_B vary. We consider two different values for $\overline{\gamma}_E = \{5, 15\}$ dB to enable a clearer representation of the ASC curves. The AWGN case is included as a reference. We see that because of the independent fluctuation of the wireless links due to fading, it is possible to achieve a non-zero secrecy capacity when $\overline{\gamma}_B$ is lower than $\overline{\gamma}_E$. We also see that when $\overline{\gamma}_B$ takes low values (i.e., in the low-SNR regime), NLOS channels achieve a better secrecy rate than their LOS counterparts. This is due to the fact that larger fluctuations associated to NLOS fading cause that the instantaneous SNR of Bob may be above the instantaneous SNR of Eve with a higher probability. However, in the high-SNR regime the situation is just the opposite. In general terms, LOS channels achieve better secrecy capacities than their NLOS counterparts. In this situation, and because of the asymptotic behavior predicted by (11), we see that a larger secrecy capacity is achieved when the fading severity is reduced in the desired link (i.e. stronger LOS), and when the fading severity grows in the eavesdropper's link (i.e., the Rayleigh case). We see that the ASC in such case exceeds that of the AWGN case.

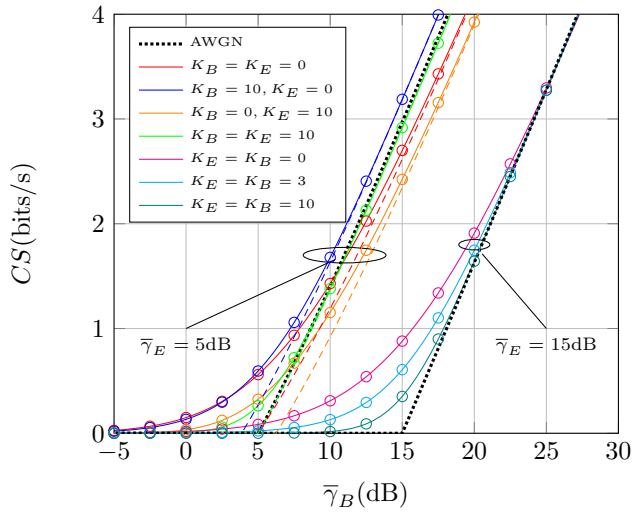

Fig. 3. Average secrecy capacity vs. average SNR at Bob, for different values of K_E, K_B and $\overline{\gamma}_E$. Solid lines correspond to the theoretical exact results using (8), dashed lines are the asymptotic results using (11) and markers represent Monte Carlo simulations. AWGN case is included as a reference (dotted black lines).

We now evaluate the OPSC in Fig. 4 for different choices of K_B and K_E. Parameter values are $\overline{\gamma}_E = 5$ dB and $R_{th} = 3$ bits/s. At first glance, we see that the OPSC mainly depends on K_B, whereas the dependence on K_E is of lesser relevance. For instance, in order to achieve a target OPSC of 10^{-1}, we need $\Delta \approx 5$ dB less for $K_B = 10$ than in the NLOS case ($K_B = 0$). However, we see that the effect of changing K_E is minor, and practically irrelevant when $K_B = 0$. In the low-SNR regime, we see than the influence of the fading severity through parameters K_B and K_E is reverted, because of the same reasons indicated when evaluating the ASC in Fig. 3.

Having now determined the effects of K_B and K_E on the system performance for the reference case, we now investigate the effect of the random fluctuation in the WPT link on the system performance. Fig. 5 compares the performance of the WPT (solid lines) vs. the baseline case (dashed lines), for different LOS conditions in the WPT link: NLOS ($K_P = 0$) and LOS ($K_P = 10$). We see that when a LOS condition is considered for the WPT link, the performance loss is negligible compared to the reference case. As the WPT LOS condition vanishes, the performance loss becomes now evi-

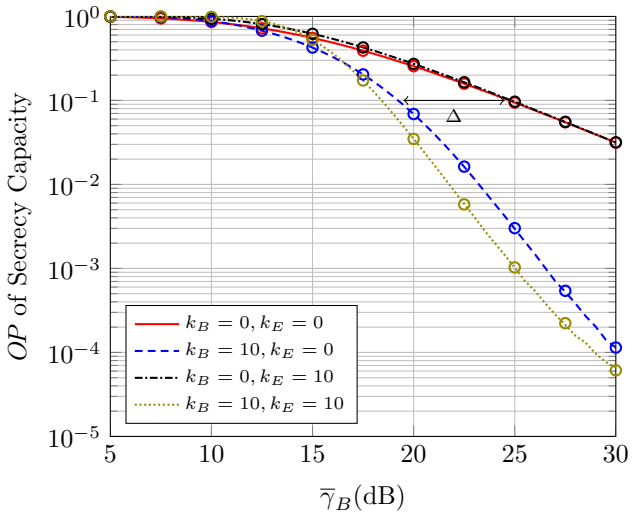

Fig. 4. Outage probability of secrecy capacity, vs. average SNR at Bob, for different values of K_E, K_B and $\overline{\gamma}_E$. Solid lines correspond to the theoretical results with (9) and markers represent Monte Carlo simulations.

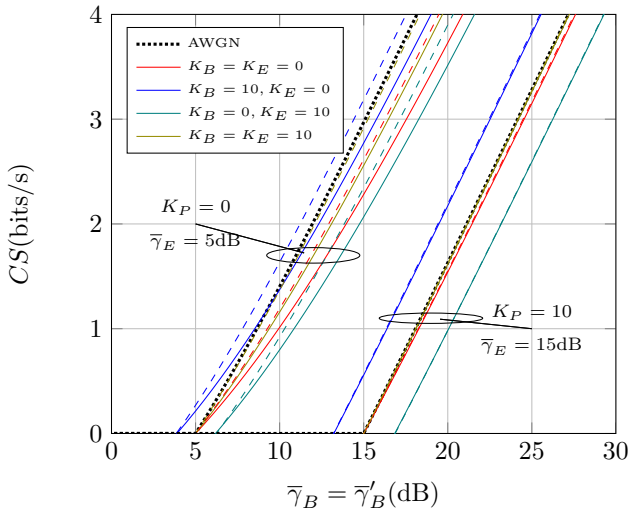

Fig. 5. Average secrecy capacity vs. average SNR at Bob, for different values of K_E, K_B and $\overline{\gamma}_E$. Solid lines correspond to the asymptotic results using (16) (i.e. wireless PB), dashed lines are the asymptotic results using (11) (i.e. no wireless PB). AWGN case is included as a reference (dotted black lines).

dent: e.g., for a target ASC of 3 bits/s, we need approximately 1 dB more of SNR than in the reference case (i.e. without PB). Monte Carlo simulations are not included in the figure for the sake of clarity, although the correctness of the results has been verified. The effect of a LOS WPT link on the OPSC metric is also negligible as observed in Fig. 6. In fact, the distribution of the WPT channel becomes almost irrelevant when $K_B = 0$.

V. Conclusions

We investigated the impact of the random fluctuations and the LOS condition in a wireless power transfer set-up with physical layer security constraints. Results show that as long as the wireless power link has strong LOS, the impact on the system performance is limited, and especially in those cases on which the legitimate link is NLOS. Future extensions of this work will quantify the impact of non-linear energy harvesting on the physical layer security.

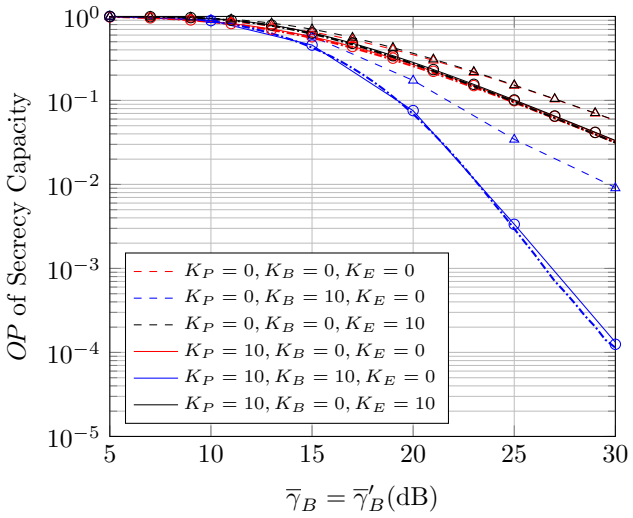

Fig. 6. Outage probability of secrecy capacity, vs. average SNR at Bob, for different values of K_E, K_B and $\overline{\gamma}_E$. Solid ($K_P = 10$) and dashed ($K_P = 0$) lines correspond to the theoretical results after averaging (9) with (10) (i.e. wireless PB), dashdotted lines are obtained from (9) (i.e. no PB), and markers represent Monte Carlo simulations for the wireless PB case. $R_{th} = 3$ bits/s.

Acknowledgements

This was was funded by the Spanish Government (Ministerio de Economia y Competitividad) through grant TEC2017-TEC2017-87913-R and the "Becas Colaboración con departamentos" program. This work has also been supported by Universidad de Málaga-Campus de Excelencia Internacional Andalucía Tech, Plan Propio de Investigación.

References

[1] W. Stallings, *Cryptography and Network Security, 4/E.* Pearson Education India, 2006.

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

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

[4] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless Information-Theoretic Security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[5] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[6] P. Grover and A. Sahai, "Shannon meets Tesla: Wireless information and power transfer," in *2010 IEEE International Symposium on Information Theory*, June 2010, pp. 2363–2367.

[7] M. M. Rana, W. Xiang, E. Wang, X. Li, and B. J. Choi, "Internet of Things Infrastructure for Wireless Power Transfer Systems," *IEEE Access*, vol. 6, pp. 19 295–19 303, 2018.

[8] X. Jiang, C. Zhong, X. Chen, T. Q. Duong, T. A. Tsiftsis, and Z. Zhang, "Secrecy Performance of Wirelessly Powered Wiretap Channels," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3858–3871, Sep. 2016.

[9] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical Layer Security of Maximal Ratio Combining in Two-Wave With Diffuse Power Fading Channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 2, pp. 247–258, Feb 2014.

[10] M. K. Simon and M.-S. Alouini, *Digital communication over fading channels*. John Wiley & Sons, 2005, vol. 95.

[11] J. M. Romero-Jerez, G. Gomez, and F. J. Lopez-Martinez, "On the outage probability of secrecy capacity in arbitrarily-distributed fading channels," in *Proceedings of European Wireless 2015; 21th European Wireless Conference*, May 2015, pp. 1–6.

[12] J. Moualeu, D. B. da Costa, F. J. Lopez-Martinez, W. Hamouda, T. M. Ngatched, and U. Dias, "Transmit Antenna Selection in Secure MIMO Systems over α-μ Fading Channels," *under review*, 2019.

[13] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. Academic Press, 2007.