ASTES

Advances in Science, Technology and Engineering Systems Journal
Vol. 2, No. 3, 384-388 (2017)
www.astesj.com
Special issue on Recent Advances in Engineering Systems

ASTES Journal
ISSN: 2415-6698

Security in SWIPT with Power Splitting Eavesdropper

Furqan Jameel*, Faisal, M Asif Ali Haider, Amir Aziz Butt

Department of Electrical Engineering, COMSATS Institute of Information Technology, Islamabad, Pakistan

ARTICLEINFO

Article history:
Received: 31 March, 2017
Accepted: 04 May, 2017
Online: 22 May, 2017

Keywords :
SWIPT
Secrecy Capacity
Weibull Fading
Power Splitting
Secrecy Performance
Weibull Shape Parameter

ABSTRACT

Simultaneous wireless information and power transfer (SWIPT) has drawn significant research interest in recent years. In this paper, we investigate the information theoretic secrecy of a SWIPT system under Weibull fading channel. To be specific, we analyze the information security in the presence of an energy harvesting and information decoding eavesdropper. All links are subjected to Weibull fading which is more complex than traditional Rayleigh fading. Moreover, we derive closed-form expressions for the probability of strictly positive secrecy capacity and the ergodic secrecy capacity. We evaluate the effect of Weibull shape parameter and power splitting factor on the secrecy performance of SWIPT system. Numerical and simulation results are provided to demonstrate that our findings are instantly applicable on the design of wireless power networks.

1 Introduction

Most of the conventional electrical energy transfer takes palace with the help of conductors between power source and load. However, in case of wireless power transfer (WPT), the transmission of energy from source to load takes place without interconnecting conductors. In other words, this simply means that WPT allows transfer of energy without wires [1]. In WPT, a power source connected to a wireless transmitter conveys the energy wirelessly across an intervening space to once or more wireless receivers. At the receiving end, electromagnetic energy is again converted to electrical current which can be stored and used by the device. Since most wireless devices are powered either through power cables or battery replacement, which limits the scalability, sustainability, and mobility of wireless communications [2]. In practice, wireline charging and battery replacement may be infeasible under some conditions; for instance, it is very difficult to replace the battery of implanted medical devices in human bodies. Besides, wireline charging and battery renewal shortens working period of wireless mobile devices. The WPT technique becomes appealing since it can be used to wirelessly charge the devices in hazardous conditions.

In this context, simultaneous transfer of power and information is emerging as one of the most promising technique to increase the lifetime of wireless devices [2]. However, provisioning of security over a Simultaneous wireless information and power transfer (SWIPT) system has remained a daunting task due to the broadcast nature of wireless networks. Traditional cryptographic techniques are not suitable for SWIPT because they require complex hardware and consume large amounts of energy that are typically not affordable by wireless devices. Moreover, an eavesdropper with unlimited computing power may still decipher these techniques using brute-force attack. In this context, Physical Layer Security (PLS) has emerged as an attractive solution for securing wireless transmissions by exploiting the wireless channel characteristics [3]. The PLS techniques such as artificial noise generation and cooperative relaying are not suitable for day to day wireless devices due to the latters limited energy resources.

Weibull distribution was studied by authors in [4] to understand the effect of small scale fading (SSF) in outdoor environment for 800/900 MHz frequency band. The authors in [5] performed channel measurements for indoor channels and found Weibull distribution to conform closely with measurements for less than 10 dB of fading variations. In [6] the authors found the Weibull model to be a good fit for the SSF in narrow-band channel measurements for wireless body area networks. Authors in [7] and [8]investigated the SSF for 5 and 10-GHz band and proposed to use the Weibull distribution with its parameter β taking values between 1.77 to 3.9 to perfectly match the measurement curves. Authors in [9] measured the wireless channel based on pedestrians movement in a forest environment for 5-GHz band. These measure-

*Furqan Jameel, COMSATS Institute of Information Technology,Islamabad, 44000, Pakistan, Email: furqanjamil01@yahoo.com

https://dx.doi.org/10.25046/aj020349

ments suggested that Weibull distribution can be used to specify amplitude fading in a forest environment.

Despite this importance, a handful of studies have investigated Weibull fading from security point of view. Moreover, most of the existing work in SWIPT security is limited to analysis of Rayleigh fading which is a special case of Weibull fading. In this regard, it is pertinent to note that this paper is an extension of our previous work [10], where expressions of optimal power splitting and time switching were derived under Weibull fading. However, this paper evaluates the secrecy performance of SWIPT system under the influence of Weibull fading. Here, we provide closed-form expressions of probability of strictly positive secrecy capacity and ergodic secrecy capacity in the presence of power splitting eavesdropper. Additionally, we evaluate the impact of power splitting factor and Weibull parameter β, on determining the overall secrecy of information in SWIPT system.

The rest of this paper is organized as follows. System model is provided in Sec. 2; Sec. 3 contains derivation of the SPSC probability and Secrecy capacity under Weibull fading. In Sec. 4 numerical results are discussed. Finally, in Sec. 5, conclusions are highlighted.

2 System Model

A downlink SWIPT system is assumed which consists of a Base Station (BS) and an information receiving node S in the presence of an energy harvesting and information decoding node represented as E, as shown in Figure 1. BS conveys information to S and transfers energy to E during a single scheduling slot. Energy harvesting node is assumed to store energy from received radio signal. The BS, node S and eavesdropper E are equipped with single antenna. Antennas in all the network entities are assumed to be experiencing statistically independent flat Weibull fading. Moreover, we assume quasi-static fading to incorporate the effect of fading during each block of time. The BS is assumed to have channel state information (CSI) for the channels to node S. Being part of the coverage range of the BS, the energy harvesting node can act as a potential eavesdropper. It is assumed that eavesdropper uses power splitting (PS) scheme [1] to incorporate the process of energy harvesting and information decoding. According to PS, signal is divided into two streams for with ratio ρ and $(1-\rho)$for information decoding and energy harvesting, respectively; where $0 \leq \rho \leq 1$.

When BS transmits its signal s to S with power P; the received signal at S can be expressed as

$$y_m = \sqrt{\frac{P}{P_{Loss,s}}} h_m s + n_m, \tag{1}$$

where h_m represents the main channel between BS and S with $|h_m|$ being Weibull-distributed. Furthermore, n_m represents the zero mean additive white Gaussian noise (AWGN) with variance N_0 due to the receiver electronics at node S. $P_{Loss,s} = \frac{(4\pi)^2 d_s^{\gamma}}{G_t G_r \lambda^2}$ is the path loss at main link, d_s is the distance between BS and S. γ is the path loss exponent, G_t and G_r are transmitting and receiving antenna gains. Since the transmission from BS is also picked up by the eavesdropper, the signal received at the eavesdropper is given as

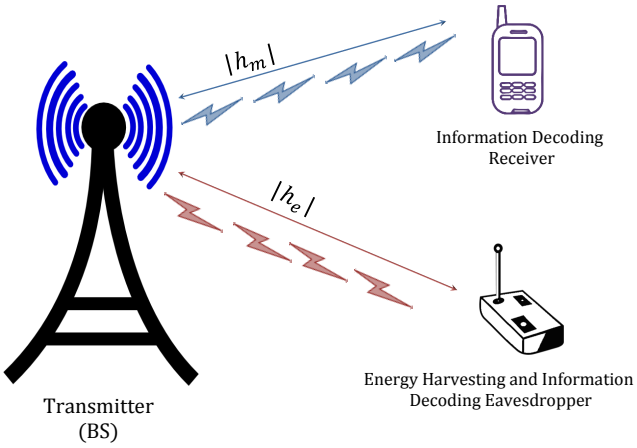

Figure 1. System Model.

$$y_e = \sqrt{\rho}\left(\sqrt{\frac{P}{P_{Loss,e}}} h_e s + n_e \right) + z, \tag{2}$$

where n_e is the AWGN at eavesdropper, h_e represents the channel between BS and eavesdropper with $|h_e|$ being Weibull-distributed. Also, $P_{Loss,e} = \frac{(4\pi)^2 d_e^{\gamma}}{G_t G_r \lambda^2}$ is the path loss at wiretap link, d_e is the distance between BS and E and n_e represents the zero mean additive white Gaussian noise (AWGN) with same variance as N_0 . z is the signal processing noise which is modeled as AWGN with zero mean and variance σ.

Then the instantaneous signal-to-noise ratio (SNR) at S for the received signal is written as

$$x_m = \frac{|h_m|^2 P}{P_{Loss,s} N_0}. \tag{3}$$

The instantaneous signal-to-noise ratio (SNR) at eavesdropper for the received signal is

$$x_e = \frac{\rho |h_e|^2 P}{P_{Loss,e} N_0 \left(\rho + \frac{\sigma^2}{N_0}\right)}. \tag{4}$$

Since main and wiretap link are subjected to Weibull fading, therefore, the Probability Density Function (PDF) and Cumulative Distribution Function (CDF) of the SNR of received signal at S and E is given by

$$f_{X_a}(x_a) = \beta_a \left(\frac{\Gamma\left(1+\frac{1}{\beta_a}\right)}{\bar{x}_a} \right)^{\beta_a} x_a^{\beta_a - 1} \times e^{-\left(\frac{\Gamma\left(1+\frac{1}{\beta_a}\right) x_a}{\bar{x}_a} \right)^{\beta_a}}. \tag{5}$$

$$F_{X_a}(x_a) = 1 - e^{-\left(\frac{\Gamma\left(1+\frac{1}{\beta_a}\right)x_a}{\bar{x}_a}\right)^{\beta_a}}, \quad (6)$$

where $a \in (m,e)$ for main and wiretap link, β_a represents the Weibull shape parameter and $\Gamma(.)$ is the well-known Gamma function. The channel capacity for both main and wiretap link can be written as $C_m = \log_2(1+x_m)$ and $C_e = \log_2(1+x_e)$, respectively [11]. Now, the positive difference between main link capacity and wiretap link capacity is called the secrecy capacity which is expressed as [12]

$$C_{\text{sec}} = [C_m - C_e]^+. \quad (7)$$

3 Analysis of Secrecy Performance

In this section, we will derive closed form expression of probability of SPSC and Ergodic Secrecy Capacity.

3.1 Probability of Strictly Positive Secrecy Capacity (SPSC)

Let us now derive an expression for the probability of strictly positive secrecy capacity (SPSC) which is the probability that the secrecy capacity is greater than zero. Mathematically it is written as

$$\Pr(C_{\text{sec}} > 0) = \Pr\left[\log_2\left(\frac{1+x_m}{1+x_e}\right) > 0\right]. \quad (8)$$

$$\Pr(C_{\text{sec}} > 0) = \Pr(x_m > x_e). \quad (9)$$

The above expression can be written as

$$\Pr(C_{\text{sec}} > 0) = \int_0^\infty \int_{x_e}^\infty f_{X_m,X_e}(x_m,x_e)dx_m dx_e, \quad (10)$$

where $f_{X_m,X_e}(x_m,x_e)$ is the joint PDF, which can be decomposed by using independence of x_m, x_m. Consequently (10) can be written as

$$\begin{aligned}\Pr(C_{\text{sec}} > 0) &= \int_0^\infty \int_{x_e}^\infty f_{X_m}(x_m) f_{X_e}(x_e)dx_m dx_e \\ &= \int_0^\infty f_{X_e}(x_e)[1 - F_{X_m}(x_e)]dx_e. \end{aligned} \quad (11)$$

Using the definition of CDF of a random variable Y we can write

$$F_Y(y) = \Pr(Y < y) = \int_{-\infty}^{y} f(t)dt. \quad (12)$$

Replacing values from (5) and (6) in (11) we can write above equation as

$$\begin{aligned}Pr(C_{\text{sec}} > 0) = \beta_e \left(\frac{\Gamma(1+\frac{1}{\beta_e})}{\bar{x}_e}\right)^{\beta_e} \times \int_0^\infty x_e^{\beta_e - 1} e^{-\left(\frac{\Gamma(1+\frac{1}{\beta_e})x_e}{\bar{x}_e}\right)^{\beta_e}} \\ \times e^{-\left(\frac{\Gamma\left(1+\frac{1}{\beta_m}\right)x_e}{\bar{x}_m}\right)^{\beta_m}} dx_e, \end{aligned} \quad (13)$$

where $\bar{x}_m = \frac{\Omega_s}{P_{Loss,s}}$ and $\bar{x}_e = \frac{\rho\Omega_e}{(P_{Loss,e}(\rho+\sigma^2/N_0))}$; also Ω_s and Ω_e is the average SNR of main and wiretap link, respectively.

Assuming $\beta_e = \beta_m = \beta$ and substituting $u = \left(\frac{\Gamma\left(1+\frac{1}{\beta_e}\right)x_e}{x_e}\right)^{\beta_e}$ in (10), we can solve integral as

$$\Pr(C_{\text{sec}} > 0) = \frac{(\bar{x}_m)^\beta}{(\bar{x}_m)^\beta + (\bar{x}_e)^\beta}, \quad (14)$$

3.2 Ergodic Secrecy Capacity (C)

Another measure of interest is the ergodic secrecy capacity. It is defined as the average of secrecy rate over x_m and x_e. It can be mathematically written as

$$\begin{aligned} C &= \mathbf{E}\{[\log_2(1+x_m) - \log_2(1+x_e)]^+\} \\ &= \int_0^\infty \underbrace{\int_0^{x_m} [\log_2(1+u) - \log(1+v)] f_{x_e}(v)dv}_{\mathcal{G}} f_{x_m}(u)du \end{aligned} \quad (15)$$

Using integration by parts, the above expression can be simplified as

$$\begin{aligned}\mathcal{G} &= \log_2(1+u)F_{x_e}(u) - \left[\log_2(1+u)F_{x_e}(u) - \frac{1}{\ln 2} \right. \\ &\quad \left. \times \int_0^u \frac{1}{1+v} F_{x_e}(v)dv\right] \\ &= \frac{1}{\ln 2}\int_0^u \frac{F_{x_e}(v)}{1+v}dv. \end{aligned} \quad (16)$$

Replacing (16) in (15) and by changing the order of integration, we get

$$\begin{aligned} C &= \frac{1}{\ln 2}\int_0^\infty \frac{F_{x_e}(v)}{1+v}\left[\int_v^\infty f_{x_m}(v)du\right]dv \\ &= \frac{1}{\ln 2}\int_0^\infty \frac{F_{x_e}(v)}{1+v}[1 - F_{x_m}(v)]dv. \end{aligned} \quad (17)$$

After replacing (6) for $\beta_e = \beta_m = \beta$ in (17) and performing some algebraic manipulations, we obtain

$$\begin{aligned} C = \frac{1}{\ln 2}\int_0^\infty \frac{1}{1+x_e} e^{-\left(\frac{\Gamma\left(1+\frac{1}{\beta}\right)x_e}{\bar{x}_m}\right)^\beta} - \frac{e^{-\frac{(\bar{x}_m)^\beta + (\bar{x}_e)^\beta}{(\bar{x}_m\bar{x}_e)^\beta}}}{1+x_e} \\ \times e^{-2\left(\Gamma(1+\frac{1}{\beta})x_e\right)^\beta} dx_e. \end{aligned} \quad (18)$$

Above equation contains single integral which can be readily solved using computational software packages such as MATHEMATICA and MATLAB.

4 Numerical Results

In the following section we provide some numerical results along with discussion on the above analysis. Unless mentioned otherwise, the simulation parameters along with their respective values are provided in Table 1.

S No.	Simulation Parameter	Value
1.	Path loss at Main Link $P_{Loss,s}$	0 dB
2.	Path loss at Wiretap Link $P_{Loss,e}$	0 dB
3.	Power splitting factor ρ	0.8
4.	Weibull shaper parameter β	2
5.	Noise at main/ wiretap link	- 60 dB
6.	Channel realizations	10^6

Table 1. Simulation Parameters

Figure 2 shows the SPSC probability plotted against $\bar{x}_m$ for different values of $\bar{x}_e$. It is vividly clear from the figure that probability of SPSC increases with the increase in $\bar{x}_m$. It is because with the increase in $\bar{x}_m$ the channel capacity of the main link increases which resultantly increases the SPSC probability. Moreover, it is also evident from the graph that increase in x_e, decreases the probability of SPSC. In addition to this, we can observe that for the same values of $\bar{x}_m$, $\bar{x}_e$ and $P_{Loss,e}$, the probability of SPSC significantly decreases with the increase in $P_{Loss,s}$. Furthermore, we observe that the impact of decrease in $P_{Loss,s}$ is more significant for larger values of $\bar{x}_e$ as compared to smaller $\bar{x}_e$. It can also be seen that the simulation results closely coincide with the analytical results which proves the accuracy of our analysis.

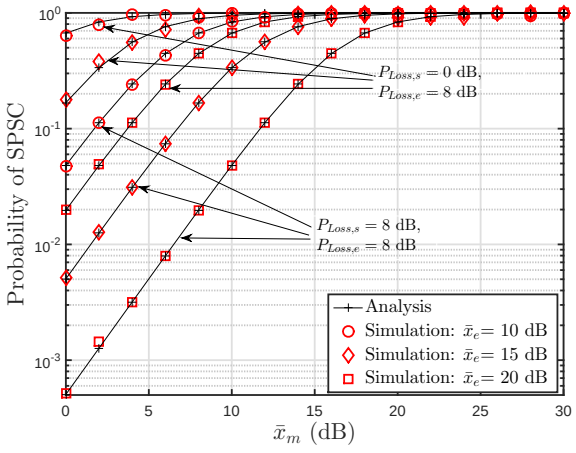

Figure 2. SPSC probability plotted as a function of $\bar{x}_m$.

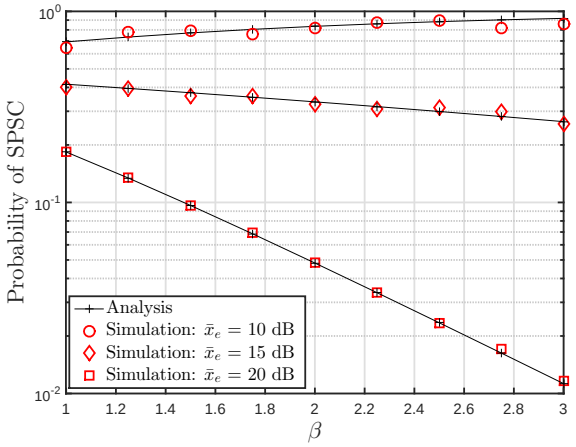

Figure 3. SPSC probability against Weibull shape parameter β.

Figure 3 plots SPSC probability as a function of Weibull shape parameter β. It is observed from the figure that the SPSC probability increases with the increase in β until main links SNR is equal or greater than eavesdroppers SNR. However, when $\bar{x}_m < \bar{x}_e$ then the probability of SPSC decreases with increase in β. Additionally, this effect is more significant for large values of $\bar{x}_e$ as compared to small values.

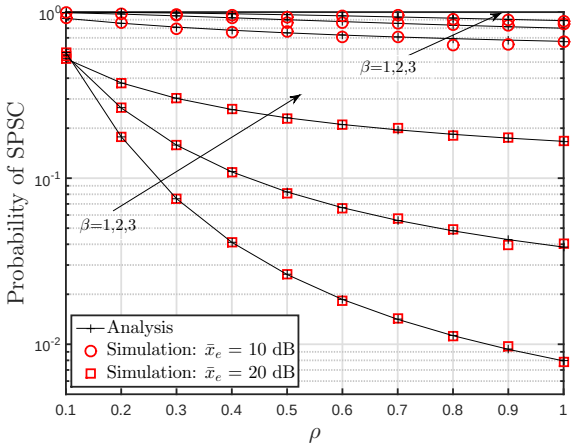

Figure 4. Probability of SPSC vs power splitting factor ρ.

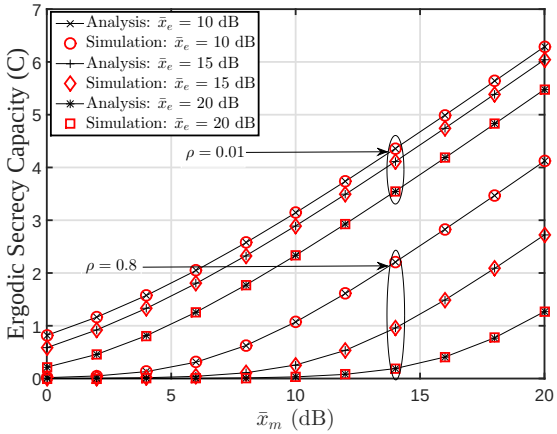

Figure 5. Ergodic secrecy capacity as a function of $\bar{x}_m$.

Figure 4 gives the SPSC probability as a function of ρ for different values of $\bar{x}_e$. It can be observed from the figure that for the increasing values of ρ the probability of SPSC decreases. It is due to the fact that larger values of ρ indicate that more power at the eavesdropper is being used for information decoding which results into reduction in the secrecy capacity. Furthermore, the reduction in probability of SPSC is more significant at higher values of eavesdroppers SNR. Additionally, it can be seen from the plot that influence of β increases with the increase in ρ and $\bar{x}_e$.

Finally, Figure 5 illustrates the achievable secrecy capacity as a function of increasing values of main links average SNR. It is well established by now that the increase in $\bar{x}_m$ increases the secrecy capacity. It is noteworthy that for a specific value of $\bar{x}_m = 12$ dB and $\bar{x}_e = 10 \rightarrow 20$ dB, the secrecy capacity increases from 3 to 3.8 for $\rho = 0.01$, whereas, secrecy capacity increases from 0.1 to 1.8 for $\rho = 0.8$. This result is shows that secrecy capacity varies rapidly for higher values of ρ as compared to lower ones.

5 Conclusion

In this article we have analyzed the performance of SWIPT system from the perspective of physical layer security. We have derived the closed-form expression for probability of SPSC. We have characterized the effect of Weibull shape parameter in SPSC. Our results also demonstrate the significance of power splitting factor on the confidentiality of information. Finally, we evaluated the impact of power splitting factor on ergodic secrecy capacity while varying the Weibull shape parameter. These findings can be of utility for ensuring data security for wireless communication.

Conflict of Interest The authors declare no conflict of interest.

References

[1] X. Zhou, R. Zhang and C. K. Ho, "Wireless information and power transfer: Architecture design and rate-energy tradeoff", IEEE Trans. Commun., vol. 61, no. 11, pp. 4754-4767, 2013.

[2] L. R. Varshney, Transporting information and energy simultaneously, in Proc. I EEE Int. Symp. Inform. Theory (ISIT), Toronto, pp. 16121616, 2008.

[3] Y. Zou, J. Zhu, X. Wang and V. C. M. Leung, "Improving physical-layer security in wireless communications using diversity techniques," in IEEE Network, vol. 29, no. 1, pp. 42-48, Jan.-Feb. 2015.

[4] N. S. Adawi et al., Coverage prediction for mobile radio systems operating in the 800/900 MHz frequency range, IEEE Transactions on Vehicular Technology, vol. 37, pp. 372, 1988.

[5] H. Hashemi, The indoor radio propagation channel, Proceedings of IEEE, vol. 81, pp. 943968, 1993.

[6] D. Smith, J. Zhang, L. Hanlen, D. Miniutti, D. Rodda, and B. Gilbert, A Simulator for the Dynamic On-body Area Propagation Channel, in IEEE International Symposium on Antennas and Propagation Society, pp. 14, 2009.

[7] I. Sen, D. W. Matolak, Vehicle-vehicle channel models for the 5-GHz band, IEEE Transactions on Intelligent Transportation Systems, vol. 9, no. 2, p. 235 - 245, 2008.

[8] Q. Wu, D. W. Matolak, and I. Sen, 5-GHz-band vehicle-to-vehicle chan-nels: Models for multiple values of channel bandwidth, IEEE Transactions on Vehicular Technology, vol. 59, no. 5, pp. 26202625, 2010.

[9] D. W. Matolak, F.-C. Yang, and H. B. Riley, Short range forest channel modeling in the 5 GHz band, in Proceedings of 6th European Conference on Antennas Propagation, Prague, Czech Republic, pp. 33373341, 2012.

[10] F. Jameel, A. Ali and R. Khan, "Optimal time switching and power splitting in SWIPT," 2016 19th International Multi-Topic Conference (INMIC), Islamabad, 2016, pp. 1-5.

[11] A. D. Wyner, The wire-tap channel, Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, 1975.

[12] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, Wireless information theoretic security, IEEE Transactions on Information Theory, vol.54, no.6, pp.25152534, 2008.