PHYSICAL LAYER INFORMATION SECURITY IN ENERGY HARVESTING UNDERLAY COGNITIVE RADIO NETWORKS

Do Dac Thiem[(1)], Duong Thi Kim Chi[(1)]

(1) Thu Dau Mot University
Corresponding author: thiemdd@tdmu.edu.vn

DOI: 10.37550/tdmu.EJS/2024.02.562

Article Info

Volume: 6
Issue: 02
June 2024
Received:
Accepted:
Page No: 324-330

Abstract

This article investigates the physical layer security (PLS) performance in Energy Harvesting Underlay Cognitive Radio Networks (EHUCRN). Firstly, the article examines the impact of parameters such as primary transmitter power, interference power threshold, and expected security level on EHUCRN's Secrecy Outage Probability (SOP). Then, based on the findings, the article evaluates the PLS performance of the system. The results indicate that increasing the primary transmitter power reduces the PLS performance while raising the interference power threshold improves PLS performance. Furthermore, increasing the expected security level decreases the PLS performance. Additionally, the percentage of energy harvesting time increases within a small range, resulting in an increasing PLS performance up to a peak value. However, if this percentage continues to increase within a large range, the PLS gradually decreases. Moreover, the results demonstrate that the PLS performance in EHUCRN is low due to relatively high SOP values.

Keywords: cognitive radio networks, energy harvesting, physical layer security, secrecy outage probability

1. Introduction

The creation of the Cognitive Radio Networks (CRN) has solved the problem of spectrum scarcity and better-supported applications that require high bandwidth in new-generation wireless communications. Furthermore, the recently developed Radio Frequency Energy Harvesting (RF-EH) technique is considered a solution to provide energy for wireless users (Ding et al., 2019; Moloudian et al., 2024). Energy harvesting can be performed by using a rectifier circuit to convert the RF signals into direct current (DC) electricity, which charges the battery for future signal processing (Yela et al., 2017). Power splitting and time switching are two typical energy harvesting methods (Zhao et al., 2017). Previously, RF-EH was not widely used due to severe signal degradation at high-frequency transmission. However, the latest advances in wireless access, including large antenna arrays, small cells, millimeter waves, etc., have improved the signal loss problem, attracting more attention to energy harvesting (Huang & Zhou, 2015; Shi et al., 2023; Kumawat et al., 2023; Sharma & Gautam, 2023). Furthermore, technological advancements in low-power electronics continuously reduce the energy consumption for wireless communication. Therefore, energy harvesting, even with low power levels, can sufficiently support the operation of wireless users. Consequently, RF energy harvesting has the potential for widespread deployment in modern wireless access networks (Mouapi, 2022; Bito et al., 2017). Hence, this paper examines SOP in energy harvesting underlay cognitive radio networks to gain insight into physical layer security performance under the influence of system operating parameters. The results of this paper answer two questions: 1. How do system operating parameters affect the physical layer security performance of EHUCRN? 2. How secure is the system's physical layer information?

1.1. Research Methodology

Firstly, the paper employs a synthesis method to systematize related research works. Next, the paper proposes a system model and utilizes the Monte Carlo simulation method to obtain the SOP of the system. Finally, the paper evaluates the PLS of the model based on illustrative results.

1.2. Key Contributions

The paper analyzes and evaluates the PLS performance of the EHUCRN through fading Rayleigh channels. The novelty of the paper lies in considering the simultaneous impact of multiple parameters such as the maximum transmit power of the secondary transmitter, interference power threshold, and noise power.

2. System Model

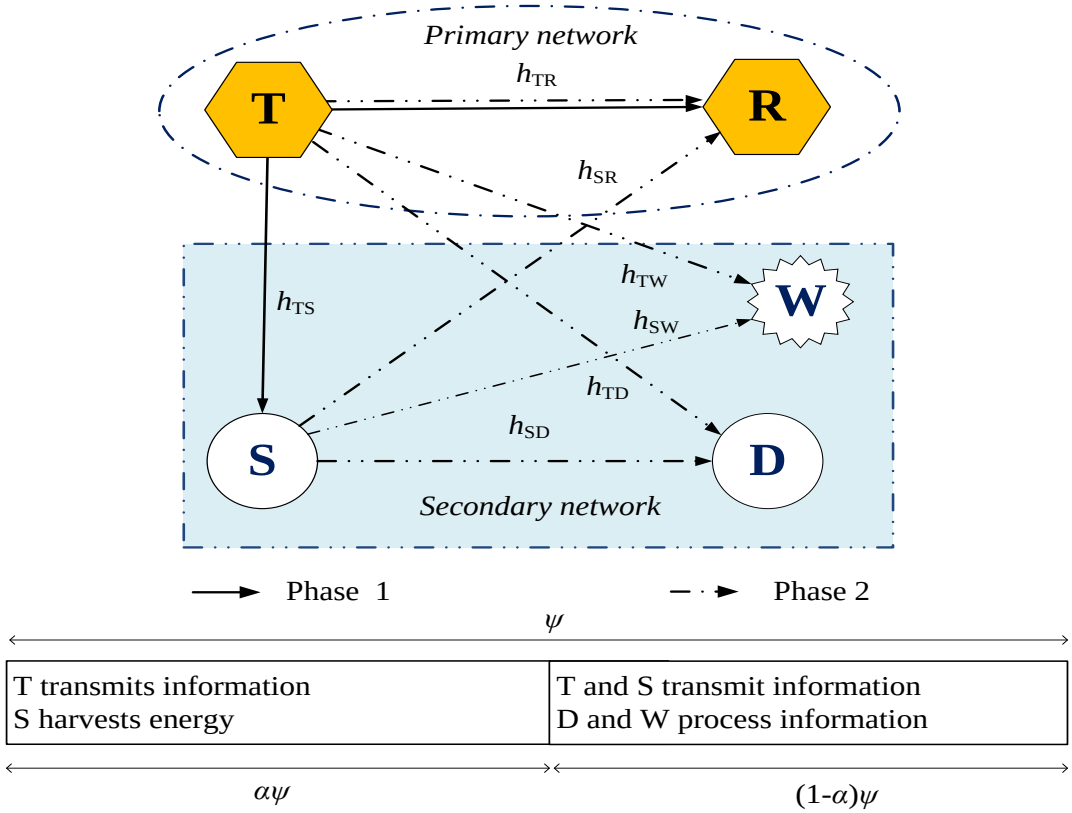

Figure 1. EHUCRN system model

The system model of energy harvesting underlay cognitive radio networks is depicted in Figure 1. The EHUCRN consists of a primary network with a primary transmitter (T) and a primary receiver (R), coexisting with a secondary network comprising a secondary transmitter (S), a secondary receiver (D), and an eavesdropper (W). It should be noted that S is assumed to be able to harvest energy from T to operate.

In the system model, h_{tr} is the channel coefficient, where $t \in \{\mathrm{T}, \mathrm{S}\}$ and $r \in \{\mathrm{S}, \mathrm{R}, \mathrm{D}, \mathrm{W}\}$. h_{TS}, h_{TR}, h_{SD}, h_{SW}, h_{SR}, h_{PD}, h_{TW} represent the channel coefficients of the node pairs $\mathrm{T} \to \mathrm{S}$, $\mathrm{T} \to \mathrm{R}$, $\mathrm{S} \to \mathrm{D}$, $\mathrm{S} \to \mathrm{W}$, $\mathrm{S} \to \mathrm{R}$, $\mathrm{T} \to \mathrm{D}$, $\mathrm{T} \to \mathrm{W}$, respectively. Assuming all channels are subject to Rayleigh fading, the channel gain is denoted as $g_{tr} = |h_{tr}|^2$ and the fading power $\rho_{tr} = \Xi_{g_{tr}}\{g_{tr}\}$ is modeled as $\rho_{tr} = d_{tr}^{-\tau}$. Here, the model takes into account the interference from the primary transmitter, with a limited interference power threshold. Additionally, the system model assumes that all end nodes have a single antenna and perform energy harvesting based on time-switching techniques.

The total duration of a complete cycle ψ is divided into two phases. Phase 1 has a duration of $\alpha\psi$ (with being the percentage of energy harvesting time $0<\alpha<1$). During phase 1, S harvests energy from the primary transmitter's RF signal. Phase 2 has a duration $(1-\alpha)\psi$. In phase 2, S utilizes the energy harvested in phase 1 to transmit legitimate information to D, which is eavesdropped by W. In this case, the energy that S can harvest in phase 1 is given by:

$$E_S = \eta\left(P_T g_{TS} + \sigma_S^2\right)\alpha\psi \quad (1)$$

where $\sigma_S^2 = \sigma^2$ is the noise variance at S, P_T is the transmit power of T, and η is the energy harvesting efficiency.

The maximum transmit power of S in phase 2 is:

$$P_{Sm} = \frac{E_S}{(1-\alpha)\psi} = Ag_{TS} + B \quad (2)$$

where

$$A = \eta\alpha P_{Sm} / (1-\alpha) \quad (3)$$

$$B = \eta\alpha\sigma^2 / (1-\alpha) \quad (4)$$

S operates in Underlay Cognitive Radio Networks, so the transmit power P_S must satisfy the constraints on the maximum transmit power and interference power threshold. In other words, P_S must satisfy:

$$P_S = \min\left(P_{Sm}, \frac{I_t}{g_{SR}}\right) \quad (5)$$

where I_t is the interference power threshold that R can tolerate.

In phase 2, S transmits legitimate information to D while T transmits information to R. Therefore, S introduces interference to R, and T introduces interference to D. The received signals at D and W are, respectively:

$$y_D = h_{SD}\sqrt{P_S}x_S + h_{TD}\sqrt{P_T}x_T + n_D \quad (6)$$

and

$$y_W = h_{SW}\sqrt{P_S}x_S + h_{TW}\sqrt{P_T}x_T + n_W \quad (7)$$

Where and P_S are the transmit powers of T and S, respectively; $\sqrt{P_T}x_T$ and $\sqrt{P_S}x_S$ are the transmitted signals of T and S, respectively; and n_D and n_W are the AWGN noises at D and W, respectively. These noises are modeled as complex circularly symmetric Gaussian random variables with zero mean and variances σ^2, $n_D \sim \mathrm{CN}\left(0,\sigma^2\right)$ and $n_W \sim \mathrm{CN}\left(0,\sigma^2\right)$ respectively. It should be noted that in the investigated works, the interference from S to R is often neglected, as in (Law et al., 2017) and the referenced literature therein. Therefore, with the consideration of interference from the primary network in the calculation of SOP, this paper provides a more comprehensive approach for previously published works.

From (6) and (7), we can calculate the SINR at D and W, respectively:

$$\Phi_D = \frac{P_S\left|h_{SD}\right|^2}{P_T\left|h_{TD}\right|^2 + \sigma^2} = \frac{P_S g_{SD}}{P_T g_{TD} + \sigma^2} \quad (8)$$

and

$$\Phi_W = \frac{P_S |h_{SW}|^2}{P_T |h_{TW}|^2 + \sigma^2} = \frac{g_{SW}}{P_T g_{TW} + \sigma^2} \quad (9)$$

According to information theory, the transmission channel capacity and are respectively:

$$C_D = (1-\alpha)\log_2(1+\Phi_D) \quad (10)$$

and

$$C_W = (1-\alpha)\log_2(1+\Phi_W) \quad (11)$$

where $(1-\alpha)$ appearing in (10) and (11) is because the duration of phase 2 is $(1-\alpha)\psi$.

The secrecy capacity is defined as the difference in capacity between the main transmission channel and the eavesdropping channel. Therefore, the secrecy capacity of EHUCRN is:

$$\begin{aligned} C_{Sec} &= \max\{C_D - C_W, 0\} \\ &= (1-\alpha)\max\left\{\log_2\left(\frac{1+\Phi_D}{1+\Phi_W}\right), 0\right\}. \end{aligned} \quad (12)$$

By definition, EHUCRN's secrecy outage probability formula is determined as follows:

$$S(C_0) = \Pr(C_{Sec} < C_0) \quad (13)$$

where C_0 is expected security level.

3. Results and discussion

To have data for illustrating the secrecy outage probability in EHUCRN, assume that nodes are at random coordinates as follows: T(0.5,1); R(1, 1); S(0.1, 0.1; D(0.6, 0.1); W(0.9, 0.8) and Rayleigh fading channels. Using Matlab software to write a Monte-Carlo simulation program with the number of realizations of the channel 10^6 and the transmission loss $\tau = 3$.

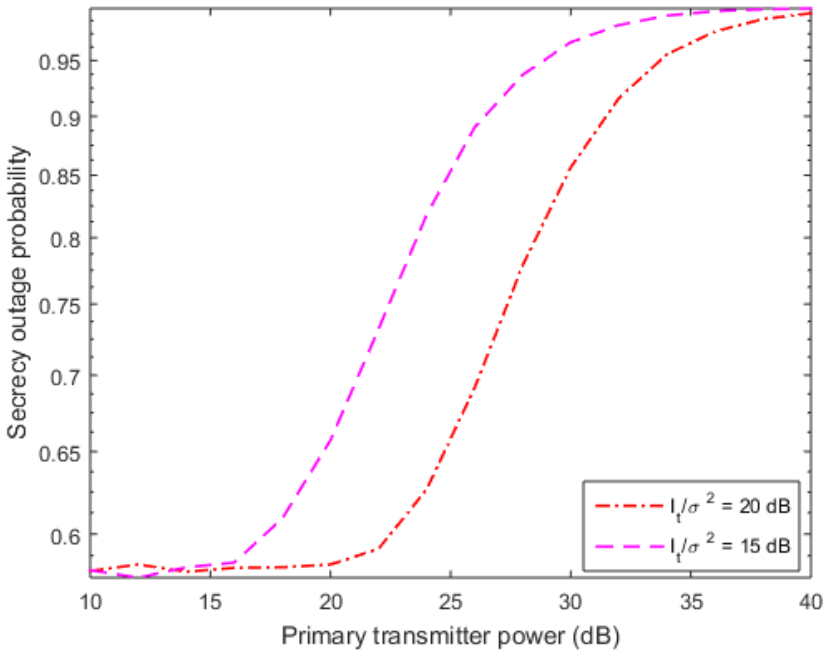

Figure 2. EHUCRN SOP according to P_T / σ^2

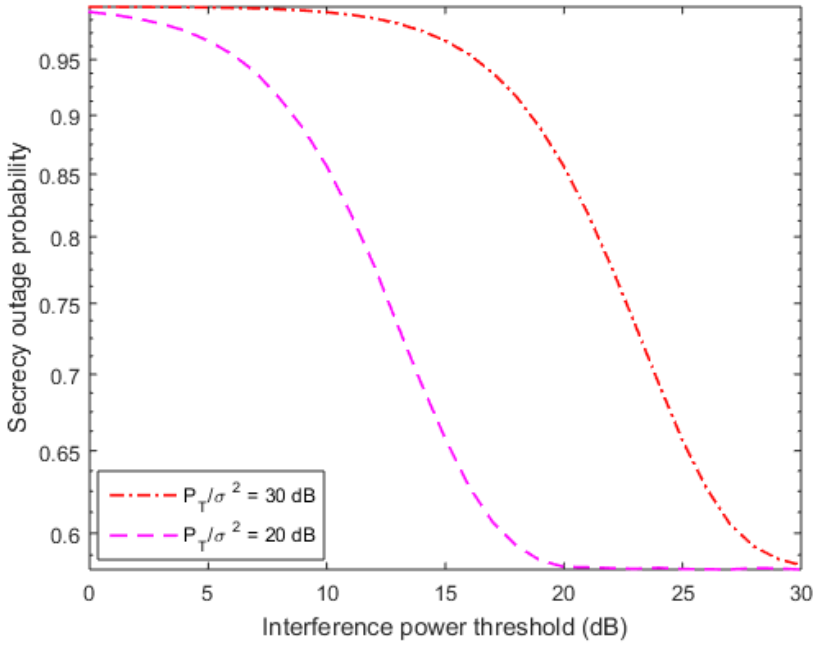

Figure 3. EHUCRN SOP according to

Figure 2 plots the secrecy outage probability in EHUCRN according to ratio primary transmitter power to noise variance given dB , , bit/s/Hz. The results show that as the SOP increases , the security performance decreases. This is explained because increasing the harvesting energy of S increases, but this causes more interference to machines D and W. Because increasing the energy harvesting cannot compensate for the amount of interference, the secrecy outage probability is proportional to Additionally, this figure also shows that SOP is higher when is smaller.

Figure 3 shows the secrecy outage probability in EHUCRN according to ratio interference power threshold to noise variance given dB, , bit/s/Hz. When increased, SOP decreases, enhancing security performance. This increase is explained by the fact that the increase allows the receiver to withstand more interference, thereby increasing the power of the transmitter S and thus improving security. Additionally, the figure shows that the probability of security is higher when is larger.

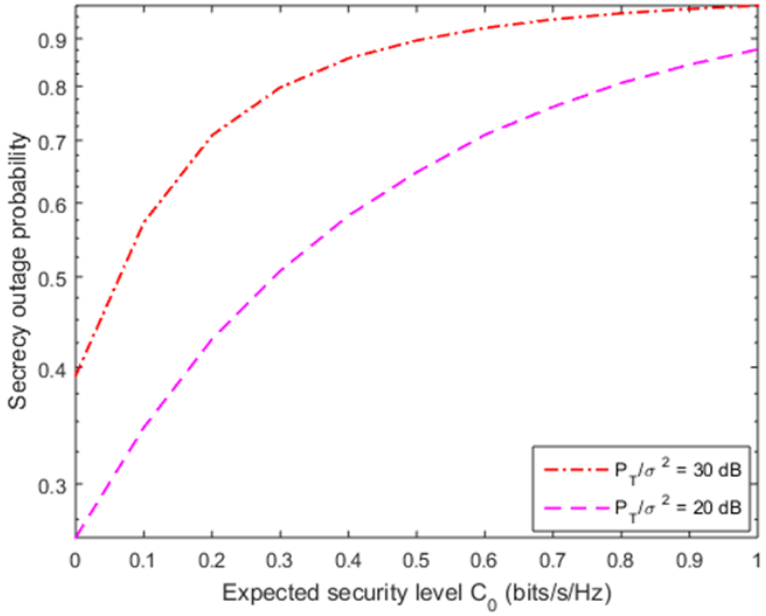

Figure 4. EHUCRN SOP according to

Figure 4 shows the secrecy outage probability in EHUCRN according to the expected security level given dB, dB. The results show that an expected security level is higher, the SOP increases. This is explained because with a certain set of parameters, SOP will reach a certain value, so when security requirements are higher, the probability of stopping security is higher.

Figure 5 represents SOP in EHUCRN according to the time division factor given dB, dB, bít/s/Hz.The results show that the security performance can achieve the best value if an appropriate is chosen. The reason is that increasing the value of can improve the energy harvesting process and harvest more energy in the first phase when increasing the transmit power of S but decreasing in the second phase. Therefore, an appropriate value of is chosen to both harvest energy in the first phase and achieve the desired energy in the second phase, leading to the lowest security outage probability.

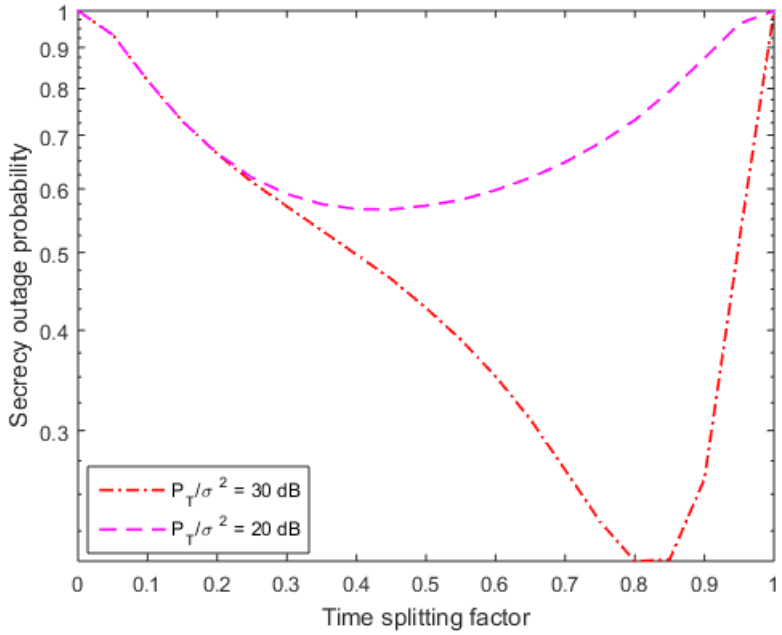

Figure 5. EHUCRN SOP according to α

4. Conclusion

The article has surveyed the physical layer security performance in the energy harvesting underlay cognitive radio network. The results have shown that: i) increasing the primary transmitter power tends to decrease the physical layer security performance; ii) increasing the expected security level leads to a decrease in PLS performance; iii) increasing the interference power threshold can enhance the PLS performance; iv) increasing the percentage of energy harvesting time within a small range gradually improves the PLS performance, reaching a maximum but increasing the percentage within a large range, the PLS performance decreases. Furthermore, when the primary transmitter operates at a relatively low power, the PLS performance in EHUCRN can be achieved by adjusting the appropriate system parameters. On the other hand, the secondary transmitter needs some time in each cycle to harvest energy, which means the time for information transmission is reduced. The result can lead to increased SOP. Additionally, the results indicate that the physical layer security performance in EHUCRN is highly limited.

References

Bito J. et al (2017). *Millimeter-wave ink-jet printed RF energy harvester for next-generation flexible electronics. Proc*. IEEE Wireless Power Transfer Conference (WPTC). Taipei, Taiwan, pp. 1-4, doi: 10.1109/WPT.2017.7953871.

Ding X. et al. (2019). The security reliability tradeoff of multiuser scheduling aided energy harvesting cognitive radio networks. *IEEE Transactions on Communications*, *67*(6), 3890-3904. https://doi.org/10.1109/TCOMM.2019.2904258.

Huang K., and Zhou X. (2015). Cutting the last wires for mobile communications by microwave power transfer. *IEEE Communications Magazine*, *53*(6), pp. 86-93. doi: 10.1109/MCOM.2015.7120022.

Kumawat Y., Shukla S.,Verma D., and Rathore P. S. (2023). *Wireless Energy Harvesting and Transfer: A Comprehensive Review of Recent Developments*. IEEE Renewable Energy and Sustainable E-Mobility Conference (RESEM), Bhopal, India, pp. 1-4, doi: 10.1109/RESEM57584.2023.10236286.

Law K. L., Masouros C., and Pesavento M. (2017). Transmit Precoding for Interference Exploitation in the Underlay Cognitive Radio Z-channel. IEEE Transactions on Signal Processing, *65*(14), pp. 3617-3631, https://doi.org/10.1109/TSP.2017.2695448.

Moloudian G. et al. (2024), RF Energy Harvesting Techniques for Battery-Less Wireless Sensing, Industry 4.0, and Internet of Things: A Review. *IEEE Sensors Journal*, *24*(5), pp. 5732-5745, doi: 10.1109/JSEN.2024.3352402.

Mouapi A. (2022). Radiofrequency Energy Harvesting Systems for Internet of Things Applications: A Comprehensive Overview of Design Issues. *Sensors,22*(21), 8088. https://doi.org/10.3390/s22218088.

Sharma N. and Gautam S. (2023). *Optimizing RIS-assisted Wireless Communication Systems with Non-Linear Energy Harvesting*. International Conference on Energy, Power and Environment: Towards Flexible Green Energy Technologies (ICEPE), Shillong, India, pp. 1-5, doi: 10.1109/ICEPE57949.2023.10201582.

Shi Y., Cui X., Qi L., Zhang X., Li X., and Shen H. (2023). A Novel Energy Harvesting Method for Online Monitoring Sensors in HVdc Overhead Line. *IEEE Transactions on Industrial Electronics*, *70*(2), pp. 2139-2143, Feb. doi: 10.1109/TIE.2022.3158028.

Yela A. L. et al. (2017). *A triple-band bow-tie rectenna for RF energy harvesting without matching network. Proc*. IEEE Wireless Power Transfer Conference (WPTC), Taipei, Taiwan, pp. 1-4. doi:10.1109/WPT.2017.7953809

Zhao N. et al. (2017). Exploiting interference for energy harvesting: A survey, research issues, and challenges. *IEEE Access,* vol. 5, pp. 10403-10421. doi: 10.1109/ACCESS.2017.2705638.