Thu Dau Mot University Journal of Science
ISSN 2615 - 9635
journal homepage: ejs.tdmu.edu.vn

Simulating the physical layer security performance of underlay cognitive energy-harvesting relay radio networks

by ***Do Dac Thiem*** *(Thu Dau Mot University)*

Article Info*: Received April 4th, 2023, Accepted May 15th, 2023, Available online June 15th, 2023*
Corresponding author: *thiemdd@tdmu.edu.vn*
https://doi.org/10.37550/tdmu.EJS/2023.02.397

ABSTRACT

This article analyzes the security performance of underlay cognitive energy-harvesting relay radio networks (UCEHRRN) through the Monter-Carlo simulation results. The results clarify the influence of critical operating parameters on the security performance of the system. Furthermore, the security capabilities of UCEHRRN have been compared with those of the live transmission system. Moreover, many results show that the security performance of the system is significantly improved. Analysis of the results also shows that UCEHRRN is especially effective when the direct transmission system cannot achieve security due to objective reasons such as path loss, severe fading, and shadowing.

Keywords: *energy-harvesting relay, physical layer security, security performance*

1. Introduction

Security plays a very important role in information systems. Typically, information security is implemented at the upper layers of the OSI open system model through the design of cryptographic protocols. However, with advances in new hardware technology, achieving secure communication based on cryptographic protocols alone is not enough. Because of this, the new paradigm of secure communication shifts towards implementing security at the physical layer. By exploiting the space-time characteristics of wireless channels, physical layer security can be well applied to cognitive radio networks. The physical layer security of cognitive radio networks offers outstanding features of high data and strong information security. Therefore, research on the physical layer security of cognitive energy-harvesting relay radio networks to improve security performance is very necessary. This is the main reason for this article.

2. Related studies

There have been many studies that have analyzed the security performance of energy-harvesting direct transmission cognitive radio networks (Srivastava & Singh, 2022; Ding et al., 2019; Singla et al., 2018; Singh et al., 2016; Liu et al., 2016) and some works (Raghuwanshi et al., 2016; Benedict et al., 2017; Hieu et al., 2018; Khuong & Thiem, 2020) have analyzed the security performance of underlay cognitive energy-harvesting relay radio networks. Specifically, the authors (Raghuwanshi et al., 2016) have investigated UCRNWEH in which the unlicensed relay performs decoding and forwarding. Its power consumption is harvested from radio frequency signals of the unlicensed transmitter and the licensed transmitter, the relay transmits messages as direct communication, which is unreliable. In addition, the relay node adopts the power division method to harvest energy. However, the authors (Raghuwanshi et al., 2016) presented only the simulation results of SOP. The problem in (Raghuwanshi et al., 2016) has been revisited in (Benedict et al., 2017) with distinct aspects in which the relay node performs amplification and forwarding operations and harvests energy from the unpowered transmitter signals. based on the time division method. To further improve security, the authors (Hieu et al., 2018) have suggested choosing a multi-hop forwarding link that gives the greatest spectral efficiency. However, the authors (Hieu et al., 2018) relied on source generators to ensure the energy-harvesting energy for the relay nodes by the time division method. Furthermore, the authors (Hieu et al., 2018) merely performed an analysis of the probability of disconnection at the wiretapper and receiver. In (Khuong & Thiem, 2020), this analysis was proposed to evaluate the decoding trade-off in the UCEHRRN when an unlicensed relay node only harvests energy in the transmitter's radio frequency signals. be licensed. The wiretapping decoding trade-off is represented by the relationship between the probability that the target receiver and the wiretapper recover the message from the failed transmitter. From an information theory point of view, SOP analysis is more important than wiretapping-decryption analysis. Accordingly, SOP analysis should be performed to assess the security capabilities of UCEHRRN before actual implementation. The authors (Ngoc et al., 2021) have analyzed the security for underlay cognitive selective energy-harvesting relay radio networks. Note that all studies (Raghuwanshi et al., 2016; Benedict et al., 2017; Hieu et al., 2018; Khuong & Thiem, 2020; Ngoc et al., 2021) only considered UCEHRRN under the limitation of threshold interference power and limit of peak transmit power over Rayleigh fading channels. From the above survey results, SOP analysis for UCEHRRN with Nakagami-m fading channels (Guo & Feng, 2019) is extremely necessary. Note that the authors (Lei et al., 2017) performed SOP analysis for cognitive networks with Nakagami-*m* fading channels but did not study energy harvesting. The article (Khuong & Thiem, 2019) analyzed the security performance of underlay cognitive energy-gathering relay radio networks over Nakagami-m fading channels. However, (Khuong & Thiem, 2019) did not compare the security performance of the direct transmission model. Therefore, this article analyzes the security performance of underlay

cognitive energy-harvesting relay radio networks over Nakagami-m fading channels and compares it with the secure performance of the direct transmission model.

3. System model

Figure 1 illustrates underlay cognitive energy-harvesting relay radio networks. In which, the source transmitter (S) transmits legitimate information to the destination receiver (D). This process can be stolen by wiretapping devices (W) and interfere with the reception of the licensed receiver (L).

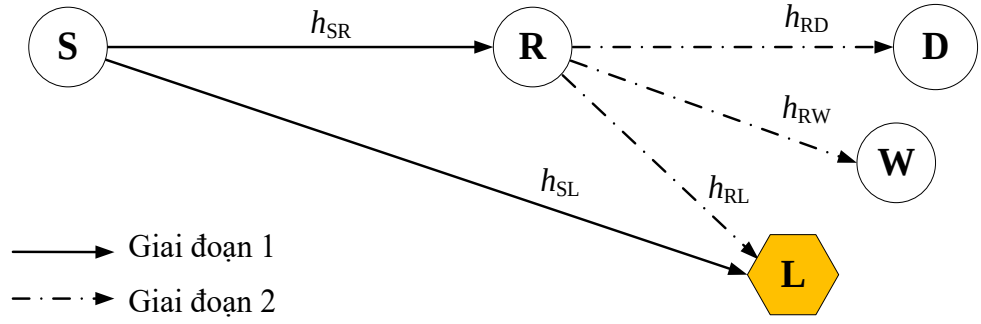

Figure 1. UCEHRRN model

Assuming channels are independent and have a Nakagami- *m* distribution. In there, h_{SR}, h_{SL}, h_{RD}, h_{RW}, and h_{RL} are the transmission channel coefficients between pairs of nodes S-R, S-L, R-D, R-W, and R-L, respectively.

Due to undesired causes (e.g., heavy path-loss, severe fading, and shadowing), D receives a signal of S that is not strong enough for successful decoding. Therefore, S requires a relay node (R), located between S and D, to help forward S's message to D. So, two phases are required for communication from S to D as shown in Figure 2 (a).

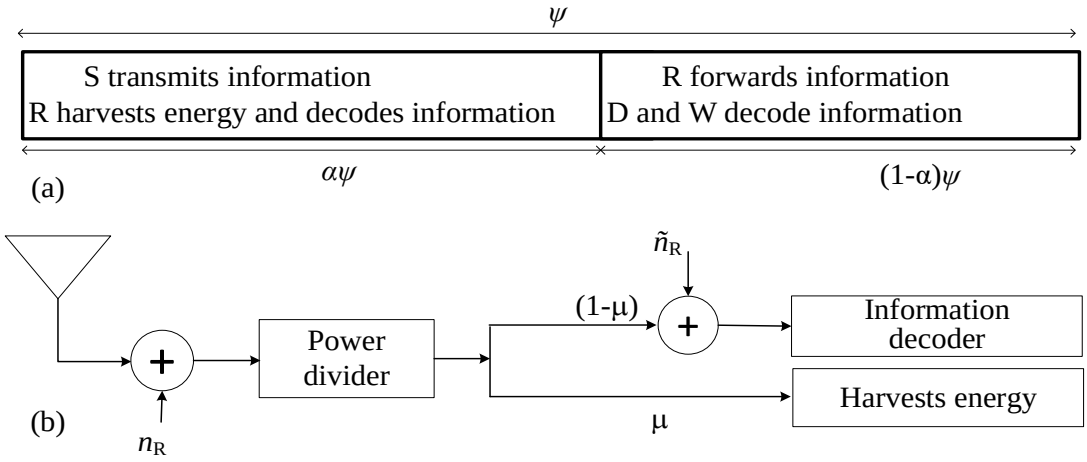

Figure 2. Phases and signal processing at the relay

To optimize the security performance, the duration of the two phases can be different. Phase 1 of $\alpha\psi$ and phase 2 of $(1-\alpha)\psi$, where $0<\alpha<1$ is the time percentage parameter and ψ is the time to finish transmitting the message from S to D. Phase 1 is used for S to transmit information to R, and phase 2 is for R to forward received information to D. To avoid noise gain of the gain and forward operation, choose R to operate in the decode and forward manner. Furthermore, R is capable of being self-powered by harvesting radio wave energy. To save system resources, R uses a power division method as shown in Figure 2(b) to harvest energy. This method divides the received signal at R into two different power parts with different powers which are represented by the power percentage. The first one μ is for harvesting the energy and the other $(1-\mu)$ is for restoring the sender's message and that the message decoder consumes the negligible amount of power for its operation. In phase 1, S does the communication message while R processes the signal received from S. Therefore, the received signal at R is as follows:

$$q_{\mathrm{R}} = h_{\mathrm{SR}}\sqrt{P_{\mathrm{S}}}t_S + n_{\mathrm{R}} \quad (1)$$

where P_{S} is transmit power of S, t_S is S's unit transmit power symbol, and $n_{\mathrm{R}} \sim \mathrm{CN}\left(0,\sigma_{\mathrm{R}}^2\right)$ is the noise generated by the receiving antenna at R. Because the model operates under the underlay mechanism, S's transmit power must comply with the limitations of the threshold interfering power (I_{t}) and the maximum transmit power (P_{Sm}), ensuring that S does not interfere with L (Bouanani et al., 2023), that is, S's maximum transmit power, P_{Sm} determined by the hardware, i.e $P_{\mathrm{S}} \le P_{\mathrm{Sm}}$. Accordingly, these two limits establish S's transmit power:

$$P_{\mathrm{S}} \le \min\left(P_{\mathrm{Sm}}, \frac{I_{\mathrm{t}}}{\left|h_{\mathrm{SL}}\right|^2}\right) \quad (2)$$

Signal q_{R} obtained at R according to Figure 2 (b), divided into two parts. The first part $\sqrt{\mu}q_{\mathrm{R}}$ to harvest energy and the second part $\sqrt{(1-\mu)}q_{\mathrm{R}}$ to recover S's message.

The energy that R harvests is given by:

$$E_{\mathrm{R}} = \eta\Xi_{t_S,n_{\mathrm{R}}}\left\{\left|\sqrt{\mu}\right|^2 q_{\mathrm{R}}\right\}\alpha\psi = \eta\mu\left(P_{\mathrm{S}}\left|h_{\mathrm{SR}}\right|^2 + \sigma_{\mathrm{R}}^2\right)\alpha\psi \quad (3)$$

where η (with $0 < \eta < 1$) is the energy conversion efficiency at R.

The duration of period 2 is $(1-\alpha)\psi$ so that the energy consumed by R in phase 2 is given by:

$$H_{\mathrm{R}} = \frac{E_{\mathrm{R}}}{(1-\alpha)\psi} = \frac{\eta\alpha\mu}{1-\alpha}\left(P_{\mathrm{S}}\left|h_{\mathrm{SR}}\right|^2 + n_{\mathrm{R}}\right) \quad (4)$$

The information decoder input in Figure 2(b) is represented as:

$$\tilde{q}_{\mathrm{R}} = \sqrt{(1-\mu)} q_{\mathrm{R}} + \tilde{n}_{\mathrm{R}} \quad (5)$$

where $\tilde{n}_{\mathrm{R}} \sim \mathcal{CN}\left(0, \tilde{\sigma}_{\mathrm{R}}^2\right)$ is the noise that caused by the passband-to-baseband signal conversion.

Embedding (1) in (5), we can rewrite (5) as:

$$\tilde{q}_{\mathrm{R}} = \sqrt{(1-\mu) P_{\mathrm{S}}} h_{\mathrm{SR}} t_{\mathrm{S}} + \sqrt{(1-\mu)} n_{\mathrm{R}} + \tilde{n}_{\mathrm{R}} \quad (6)$$

From (6), the signal-to-noise ratio at R is determined as follows:

$$\theta_{\mathrm{R}} = \frac{(1-\mu) P_{\mathrm{S}} \left| h_{\mathrm{SR}} \right|^2}{(1-\mu)\sigma_{\mathrm{R}}^2 + \tilde{\sigma}_{\mathrm{R}}^2} = \frac{P_{\mathrm{S}} \left| h_{\mathrm{SR}} \right|^2}{\bar{\sigma}_{\mathrm{R}}^2} \quad (7)$$

in there $\bar{\sigma}_{\mathrm{R}}^2 = \sigma_{\mathrm{R}}^2 + \dfrac{\tilde{\sigma}_{\mathrm{R}}^2}{1-\mu}$ (8)

R can obtain channel capacity $\Lambda_{\mathrm{R}} = \alpha \log_2\left(1+\theta_{\mathrm{R}}\right)$ bit/s/Hz, where the factor α is due to the duration of the 1st phase $\alpha\psi$. Based on information analysis, R correctly recovers S's message because its channel capacity is larger than the given effective spectrum Λ_1, i.e. $\Lambda_{\mathrm{R}} \geq \Lambda_1$. That is, t_{S} successfully recovered at R if $\theta_{\mathrm{R}} \geq \theta_1$ in $\theta_1 = 2^{\Lambda_1/\alpha} - 1$.

In phase 2, the relay transmits power P_{R} and sends a message t_{R}, is also the correct recovery S's message (i.e., $\theta_{\mathrm{R}} \geq \theta_1$ and $t_{\mathrm{R}} = t_{\mathrm{S}}$). If this condition is not satisfied, it is in standby mode. Thus, D and W receive the following signals, respectively:

$$q_{\mathrm{D}} = \begin{cases} h_{\mathrm{RD}} \sqrt{P_{\mathrm{R}}} t_{\mathrm{R}} + n_{\mathrm{D}} & , \theta_{\mathrm{R}} \geq \theta_1 \\ n_{\mathrm{D}} & , \theta_{\mathrm{R}} < \theta_1 \end{cases} \quad (9)$$

and $q_{\mathrm{W}} = \begin{cases} h_{\mathrm{RW}} \sqrt{P_{\mathrm{R}}} t_{\mathrm{R}} + n_{\mathrm{W}} & , \theta_{\mathrm{R}} \geq \theta_1 \\ n_{\mathrm{W}} & , \theta_{\mathrm{R}} < \theta_1 \end{cases}$ (10)

where $n_{\mathrm{W}} \sim \mathcal{CN}\left(0, \sigma_{\mathrm{W}}^2\right)$ and $n_{\mathrm{D}} \sim \mathcal{CN}\left(0, \sigma_{\mathrm{D}}^2\right)$ are the additive disturbances generated by the receiving antenna at W and D respectively. Since R operates in underlay cognitive radio networks, the transmit power of R is P_{R} given by:

$$P_{\mathrm{R}} = \min\left(H_{\mathrm{R}}, \frac{I_{\mathrm{t}}}{\left| h_{\mathrm{RL}} \right|^2} \right) \quad (11)$$

According to (9) and (10), the SNR at D and W are, respectively:

$$\theta_{\mathrm{D}}=\begin{cases}\dfrac{\left|h_{\mathrm{RD}}\right|^{2}P_{\mathrm{R}}}{\sigma_{\mathrm{D}}^{2}} & ,\theta_{\mathrm{R}}\geq\theta_{1}\\ 0 & ,\theta_{\mathrm{R}}<\theta_{1}\end{cases} \quad (12)$$

and $\theta_{\mathrm{W}}=\begin{cases}\dfrac{\left|h_{\mathrm{RW}}\right|^{2}P_{\mathrm{R}}}{\sigma_{\mathrm{W}}^{2}} & ,\theta_{\mathrm{R}}\geq\theta_{1}\\ 0 & ,\theta_{\mathrm{R}}<\theta_{1}\end{cases}$ (13)

W and D can be achieved channel capacities as follows:

$$C_{\mathrm{W}}=(1-\alpha)\log_{2}(1+\theta_{\mathrm{W}}) \quad (14)$$

and $C_{\mathrm{D}}=(1-\alpha)\log_{2}(1+\theta_{\mathrm{D}})$ (15)

In (14) and (15), the duration of tphase 2 is $(1-\alpha)\psi$, resulting in a pre-logarithmic factor of $(1-\alpha)$.

By definition, the secrecy capacity of the system is the difference between the trusted channel capacity R-D and the wiretapping channel capacity R-W:

$$C_{\mathrm{Sec}}=\left[C_{\mathrm{D}}-C_{\mathrm{W}}\right]^{+}=\begin{cases}(1-\alpha)\left[\log_{2}\dfrac{1+\theta_{\mathrm{D}}}{1+\theta_{\mathrm{W}}}\right]^{+} & ,\theta_{\mathrm{R}}\geq\theta_{1}\\ 0 & ,\theta_{\mathrm{R}}<\theta_{1}\end{cases} \quad (16)$$

which $[x]^{+}$ performed for $\max(x,0)$.

According to information theory, SOP is a formula used to calculate the probability of the secrecy capacity (C_{Sec}) is less than given security level (C_{0}). Accordingly, the SOP formula of UCEHRRN .

$$\mathrm{S}(C_{0})=\Pr\{C_{\mathrm{Sec}}<C_{0}\} \quad (17)$$

This section analyzes the security performance of UCEHRRN through the SOP parameter. Whereby the security performance is large when SOP is small, and vice versa. During operation, the relay node R in the middle of S and D, it is capable of receiving information from S and forwarding it to D. To obtain survey data, assuming the coordinates of S, D, R, W and L are randomly given and fixed at $(0.0,\ 0.5)$, $(0.8,\ 0.5)$, $(d,\ 0.5)$, $(0.9,\ 1.0)$, and $(0.8,\ 0.2)$; the channel loss exponent considered in this work is chosen as $\tau=4$; the power conversion efficiency, $\eta=0.8$; the additive noise variances are assumed to be equal, and the fading severity of channels is also assumed to be equal for integer values ($m=1,\ 2,\ 3$).

4. Results and discussion

Using Matlab to write Monte-Carlo simulation programs, the legends "No Relay" represent the SOP of the system going straight from S to D, and the legends "Relay" represent the SOP for the system pass through the relay button R. Comparing "No Relay" and "Relay", we see that the security performance is significantly improved when forwarding through the R node .

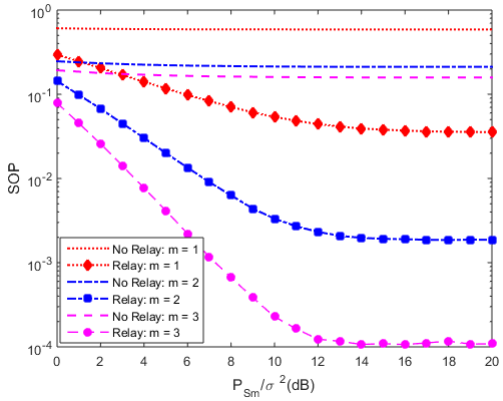

Figure 3. SOP according to P_{Sm}/σ^2

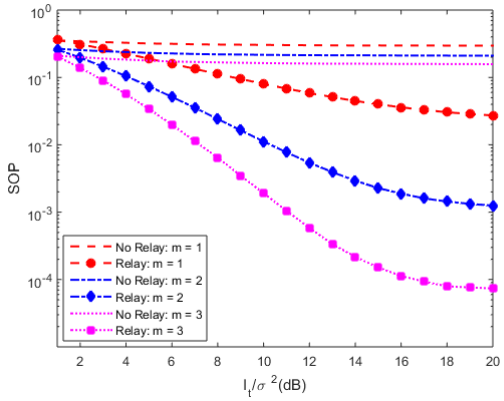

Figure 4. SOP according to I_t/σ^2

Figure 3 shows the SOP of UCEHRRN according to the ratio of the maximum transmit power to noise variance P_{Sm}/σ^2 given $I_t/\sigma^2 = 16$ dB, $\alpha = 0.6$, $d = 0.6$, $\mu = 0.7$, $L_1 = 0.4$ bit/s/Hz and $C_0 = 0.2$ bit/s/Hz. This result shows that the security performance of the system increases as it P_{Sm}/σ^2 increases. This is obvious because increasing P_{Sm}/σ^2 support for R has a better chance to capture more power in the transport signal S and correctly recover S's message, ultimately reducing the SOP in phase 2. However, SOP becomes constant at large values of P_{Sm}/σ^2. The constant SOP is due to the power allocation of R and S, where the power of R and S does not depend on P_{Sm}/σ^2 at large value P_{Sm}/σ^2, leaving the SOP unchanged. In addition, this result also shows that the SOP decreases when the fading severity is small (large *m*) as the SOP is small as expected.

Figure 4 illustrates the SOP of UCEHRRN according to the ratio I_t/σ^2 when giving the same parameters as the previous section, except for $P_{Sm}/\sigma^2 = 18$ dB. The results also shown that the security performance is improved when increasing I_t/σ^2 at small value ranges and unchanged at large value ranges. These results are interpreted as due to the power distribution of R and S, same as in the previous section. Furthermore, SOP decreases with less severity.

Given the same parameters as in Figure 4 except for $I_t/\sigma^2 = 16$ dB, Figure 5 shows SOP according to the given security level C_0. The results show that security performance is

degraded with increasing C_0. This makes perfect sense because for fixed system parameters, the network only achieves a certain level of security. Therefore, C_0 the higher it is, the more the event stops. Furthermore, security performance is improved with less severity.

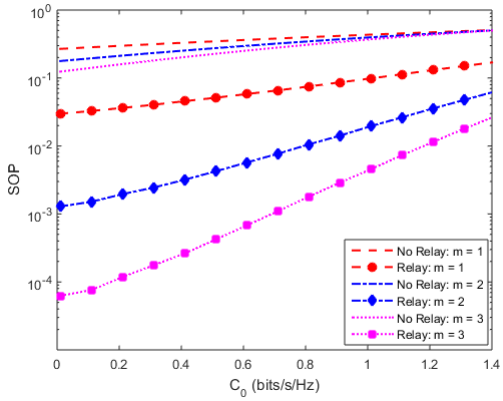

Figure 5. SOP according to C_0

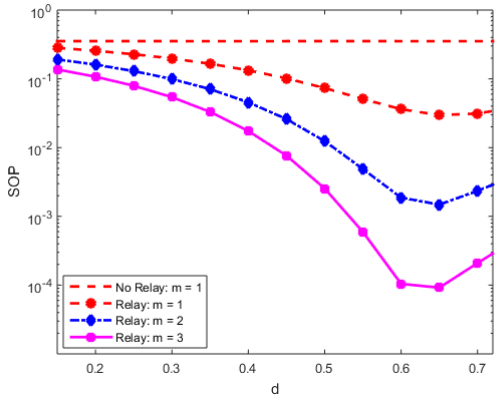

Figure 6. SOP according to d

Figure 6 illustrates the SOP of the UCEHRRN according to the S-R distance (d) when given $P_{\mathrm{Sm}}/\sigma^2 = 18\,\mathrm{dB}$, $I_t/\sigma^2 = 16\,\mathrm{dB}$, $\alpha = 0.6$, $\mu = 0.7$, $\Lambda_1 = 0.4$ bit/s/Hz and $C_0 = 0.2$ bit/s/Hz. Note that when R recovers the incorrect S's information (i.e. large S-R distance) or R forwards recovered information to D unreliable (i.e. large R-D distance), the shutdown security action occurs. Accordingly, an optimal forwarding location balances the possibility that R can correctly recover S's message and the possibility that R can forward S's recovered message to D to minimize SOP. Figure 6 illustrates this reasoning, wherein, security performance is optimized when distances from S to R are $d_{opt} = 0.68,\ 0.66,\ 0.64$ respectively $m = 1,\ 2,\ 3$. Furthermore, this result also shows that small fading severity improves security performance. In addition, this result shows that the SOP of the system with R is smaller than the SOP of the direct transmission system.

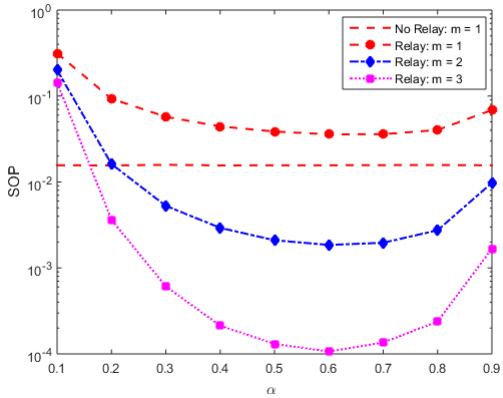

Figure 7. SOP according to α

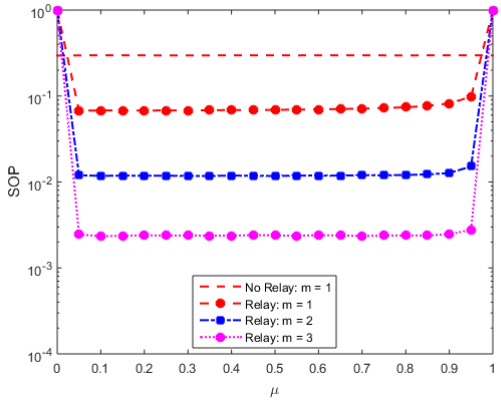

Figure 8. SOP according to μ

Figure 7 shows the SOP according to the time percentage parameter α given $P_{\mathrm{Sm}}/\sigma^2 = 18\,\mathrm{dB}$, $I_t/\sigma^2 = 16\,\mathrm{dB}$, $d = 0.5$, $\mu = 0.7$ and $\Lambda_1 = 0.4$ bit/s/Hz and $C_0 = 0.2$ bit/s/Hz,. The results also show that there exists an optimal value α (for example $\alpha_{opt} = 0.70, 0.65, 0.60$ respectively $m = 1, 2, 3$ as illustrated in Figure 6) for the best security performance exists, the presence of which α_{opt} is understood as follows: Increase the value α of prolongation of phase 1; therefore, R harvests more energy and recovers the message of S more accurately. However, the increase α also reduces the secrecy capacity in phase 2, making the secrecy capacity decrease. Therefore, to get α optimal, it is necessary to balance the time of the two phases for the best security. In addition, this result shows that the SOP of the direct transmission system does not depend on α (which is a constant) and that the SOP is larger than the SOP of the direct transmission system only occurs when the transmission channels are forward (S-R, R-D) suffers from heavy fading ($m = 1$). This is explained by the fact that the relay system has to spend some time on harvesting energy, so the channel capacity is reduced, leading to an increase in SOP. However, when the direct channel is heavy fading ($m = 1$), since R is a relay device in between S and D, it is possible to select the coordinates of R so that the forwarding channels only suffer from lighter fading ($m = 2, 3$) combined with adjustment to get the ratio α in suitable range, then the SOP of the system is smaller than the SOP of the direct transmission system, ie, the performance of the system is improved.

Figure 8 illustrates the SOP of UCRNWEHR according to the power percentage parameter μ when given $P_{\mathrm{Sm}}/\sigma^2 = 18\,\mathrm{dB}$, $I_t/\sigma^2 = 16\,\mathrm{dB}$, $\alpha = 0.6$, $d = 0.5$, $\Lambda_1 = 0.4$ bit/s/Hz and $C_0 = 0.2$ bit/s/Hz. This result shows that there exists an optimal μ value (for example, $\mu_{\mathrm{opt}} = 0.08,\ 0.09,\ 0.10$ respectively $m = 1, 2, 3$ as illustrated in Figure 8) makes the best security performance available. The presence of μ_{opt} is explained as follows: An increase of μ creates more opportunities for R to harvest higher energy; therefore, R increases signal reception quality in phase 2, ultimately improving security. However, the increase μ also reduces the power for the message decoder, thereby reducing the possibility that R correctly recovers S‘s message, and leads to an increased probability of security stopping at phase 2. Therefore, it is necessary to trade off the communication reliability of R and S to get μ_{opt}. Furthermore, this result also shows that the security performance is enhanced when the fading severity is smaller.

Figure 9 illustrates the SOP of UEHRRN according to the given spectral efficiency parameter Λ_1 when given $P_{\mathrm{Sm}}/\sigma^2 = 18\,\mathrm{dB}$, $I_t/\sigma^2 = 16\,\mathrm{dB}$, $\alpha = 0.6$, $\mu = 0.7$, $d = 0.6$ and $C_0 = 0.2$ bit/s/Hz. The figure also shows that SOP increases by Λ_1 which means security performance decreases. This shows that, because Λ_1 is higher, the probability that R successfully recovers S’s message is lower, leading to reduced security performance. Furthermore, the security performance increases when the severity is low.

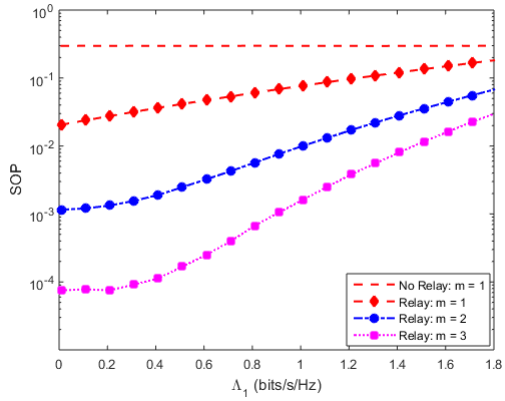

Figure 9. *SOP according to* Λ_1

5. Conclusion

Analysis results have provided insights into physical layer security under the influence of system operating parameters such as the maximum transmit power, the threshold interference power, the given security level, the energy harvesting time ratio, the power split ratio, the transition distance, and the spectrum efficiency. In addition, the results show that the security performance of both systems will increase when the fading severity of the channels is low. Furthermore, the results have shown that the physical layer security performance of UCEHRRN increases significantly with the security performance of the direct transmission system when choosing suitable S-R distance.

References

Benedict et al. (2017). Secrecy analysis of a cognitive radio network with an energy harvesting AF relay. *n Proc. the WiSPNET Chennai, India*, (pp. 1358–1624).

Bouanani et al. (2023). On the Secrecy Analysis of Dual-Hop SWIPT-Based Multi-Source Underlay Cognitive Radio Networks. *in IEEE Transactions on Cognitive Communications and Networking, 9*(1), 114-129.

Ding et al. (2019). The security-reliability trade-off of multiuser scheduling-aided energy harvesting cognitive radio networks. *IEEE Trans. on Commun, 67*(6), 3890–3904.

Guo & Feng. (2019). Joint relay and eavesdropper selection strategy against multiple eavesdroppers over Nakagami- m fading channels in cooperative decode-and-forward relay networks. *IEEE Access, 7*, 37980–37988.

Hieu et al. (2018). Performance enhancement for harvest-to-transmit cognitive multi-hop networks with best path selection method under presence of eavesdropper. *in Proc. the ICACT Chuncheon-si Gangwon-do, Korea*, (pp. 323–328).

Khuong & Thiem. (2019). Security Analysis for Underlay Cognitive Network with Energy Scavenging Capable Relay over Nakagami-m Fading Channels,". *Wireless Communications and Mobile Computing.*

Khuong & Thiem. (2020). Eavesdropping-decoding compromise in spectrum sharing paradigm with ES-capable AF relay. *Wireless Netw 26*, 1937–1948.

Lei et al. (2017). On secrecy outage of relay selection in underlay cognitive radio networks over nakagami- m fading channels. *IEEE Transactions on Cognitive Communications and Networking , 3*(4), 614–627.

Liu et al. (2016). Secure D2D communication in large-scale cognitive cellular networks: a wireless power transferodel. *IEEE Trans. on Commun, 64*(1), 329–342.

Ngoc et al. (2021). Security Analysis of Relay Selection in Energy Scavenging-based Cognitive Networks. *2021 International Conference on Advanced Technologies for Communications (ATC),*, (pp. 94-98). Ho Chi Minh City, Vietnam.

Raghuwanshi et al. (2016). Secrecy performance of a dual hop cognitive relay network with an energy harvesting relay. *in Proc. the ICACCI Jaipur, India*, (pp. 1622–1627).

Singh et al. (2016). Secrecy outage of a simultaneous wireless information and power transfer cognitive radio system. *IEEE Wire. Commun. Letters, 5*(3), 288–291.

Singla et al. (2018). A Survey on Energy Harvesting Cognitive Radio Networks,. *2018 6th Edition of International Conference on Wireless Networks & Embedded Systems (WECON), Rajpura, India*, (pp. 6-10).

Srivastava & Singh. (2022). Review On Resource Allocation For Energy Harvesting- Cognitive Radio Networks. *Journal of East China University of Science and Technology, 65*(4), 20–30.