International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 10-No.3 (2024) pp. 381-387
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Secrecy Rate Maximization for Symbiotic Radio Network with Relay-Obstacle

Muhammed Yusuf ONAY*

Hitit University, Engineering Faculty, Department of Electrical-Electronics Engineering, 19030, Corum-Turkiye
*** Corresponding Author Email:** muhammedyusufonay@hitit.edu.tr - **ORCID:** 0000-0002-4984-5421

Article Info:

DOI: 10.22399/ijcesen.413
Received : 09 August 2024
Accepted : 20 August 2024

Keywords

Sixth generation
Secrecy rate
Relay
Symbiotic radio network
Eavesdropper

Abstract:

The idea that everything can communicate with each other with high bit rate and low latency is the main goal for next generation communication systems. In this context, allocating spectrum resources and providing energy to each device that can communicate is a big problem. In order to develop different techniques in this regard, symbiotic radio networks (SRNs) have been proposed in the literature. In SRN, devices transmit information to the same receiver by using the communication infrastructure together. However, this situation may create a security problem. In this paper, SRN with relay-obstacle is proposed to test physical layer security (PLS). This model is the first approach that maximizes the secrecy rate of SRN by using the ambient radio frequency resource in the presence of relay-obstacle. There are two different clusters in the system model and each cluster contains a device, a relay and an obstacle. An eavesdropper (ED) overhearing to the signals transmitted by the relays and is blocked by a cooperative jammer. The proposed system model is mathematically modeled and the secrecy rate expression is maximized over the time parameters. In the numerical analysis, the advantages of using the channel symbiotically compared to the nonsymbiotic scenario where the energy harvest-then-transmit (HTT) protocol is used in the literature are evaluated in terms of the reflection coefficient, noise power, signal transmission power and quality of service (QoS) of the devices and its superiority is revealed.

1. Introduction

Sixth generation (6G) technology, which has the potential to open the doors of a world where everything can communicate with each other, aims for much faster bit transmission and secure communication with low latency [1]. In this context, SRN is one of the paradigms put forward in the literature [2-4]. In SRN, models are presented in which the devices in the system use the communication infrastructure together to transmit information to the same receiver and each device reaches its own communication target. The critical issue here is that instead of allocating a separate spectrum resource to the devices, the same resources are used in a mutualistic relationship. Thus, the need for spectrum resources is minimized. Although cognitive radio networks (CRNs) are used to solve this problem in the literature [5], SRN has many advantages. First, information is transmitted to the same receiver in SRN. Thus, a single receiver is sufficient in the system. Second, the performance of the subsystems using the spectrum source of the main system may change the operating time of the main system. This situation provides main system parameters under the control of the subsystem instead of the subsystem having to comply with the operating conditions of the main system. Thus, having adjustable parameters of the system according to the environmental conditions can keep the performance of the system under control [6].

Another issue that needs to be analyzed for SRN is the energy supply to the devices. The backscatter communication technique has the potential to overcome the energy problem for next generation communication systems [7]. In this technique, the signal coming from the ambient radio frequency source to the device is passively backscattered back to the receiver with the antenna impedance mismatch. Since the device does not need its own radio frequency generator, it does not consume serious energy. This allows communication with low power. In [8], only backscattering is used to transmit bits to the receiver. However, it is

observed in the obtained results that the bit transmission rate remained low. For this reason, energy harvesting technique is included in the existing systems [9]. This technique, in which the device harvests energy with the signals in the environment without using an external battery, increased the bit transmission rate.

Studies conducted in the literature have particularly aimed to increase the bit transmission rates of devices. However, secure communication within the scope of 6G is a subject that researchers should focus more on. In particular, the shared use of the communication infrastructure by devices makes the system vulnerable to interventions that can be made from the outside [10]. In addition, the symbiotic relationship between the devices is damaged and the performance of the system decreases. The aim of the secrecy rate for phsical layer security considered in secure communication is to maximize the difference between the number of bits sent by the devices to the gateway and the number of bits leaked to the ED that overhears on the system [11].

In this paper, the secrecy rate is maximized for SRN with relay-obstacle within the PLS framework. The proposed system model is the first approach to maximize the secrecy rate for a relay-obstacle SRN using an ambient radio frequency source. Unlike [12-14], it is considered that there is no direct link between the device and the gateway. Since there may be obstacles between the terminals in real-life applications, this makes the system performance more realistic [15]. The system, consists of a source (such as a TV tower, like [6, 7, 16]) that emits signals into the environment, two different clusters, a gateway as a receiver, an ED that overhears signals transmitted by users in the system, and a cooperative jammer. While cluster 1 consists of device 1 (D_1) and relay 1 (R_1) and an obstacle, cluster 2 consists of device 2 (D_2), relay 2 (R_2), and an obstacle. Using relays is a preferred method in communication systems in the presence of an obstacle. Since there is no direct connection from D_1-D_2 to the gateway due to the obstacle, the relays serve to transmit information. Unlike [15, 16], each relay and device in the clusters has the ability to perform both backscatter communication and active data transmission. The cooperative jammer in the system, unlike [17, 18], serves to both reduce the signal-to-noise (SNR) value of ED and to be an energy source for the R_1 and R_2. After the proposed system model is expressed with mathematical equations, the secrecy rate equation is found. Then, the optimization problem is maximized with certain constraints. By means of computer simulations, the advantages of using the channel as symbiotic compared to the nonsymbiotic scenario in the literature where the HTT protocol is used are evaluated and the performance is tested according to the changes in different parameters in the system and the results are shown graphically.

The main contributions of this paper can be listed as follows:

1. The proposed system model is the first approach to maximize the secrecy rate for a relay-obstacle SRN using ambient radio frequency resources.
2. In order to be more realistic in real-life applications, an obstacle is considered between the device and the gateway and the secrecy rate expression is derived.
3. It is considered that each relay and device in the system has the capacity to perform both backscatter communication and active data transmission.
4. The cooperative jammer degrades the signal quality in the ED by generating artificial noise.
5. The advantages of using the channel symbiotically compared to nonsymbiotic scenarios in the literature where the HTT protocol is used are tested for different system parameters.

2. Proposed System Model

The system model with relay-obstacle designed and the time frame of this system are shown in Fig. 1 and Fig. 2, respectively. There are two different clusters in the system model, and each cluster has a device, a relay, and an obstacle. The source is considered as an ambient radio frequency (e.g., TV tower). The source transmits its information to the gateway for γ_1 duration. D_1 and D_2 help the source to reach the number of bits it needs to send faster. In the SRN, there is no direct link because there is an obstacle in the channel between D_1-D_2 and the gateway. Therefore, R_1 and R_2 are used in the system. During the γ_1^a period, cluster 1 is active and the signal coming from the source to D_1 is delivered to the gateway using the backscatter technique with the help of R_1. During γ_1^b, cluster 2 is active and the signal coming from the source to D_2 is transmitted to the gateway using the backscatter technique with the help of R_2. Since the two clusters are responsible for transmitting the source's information to the gateway at different times, interference at the gateway is prevented. In the period $\gamma_1 = \gamma_1^a, +\gamma_1^b$, a symbiotic communication based on backscatter communication is established by adopting the time switching protocol (TSP).

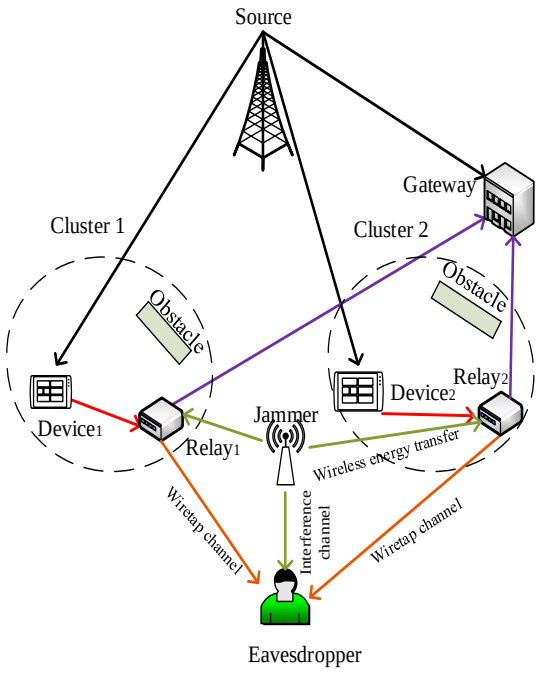

Figure 1. *System model.*

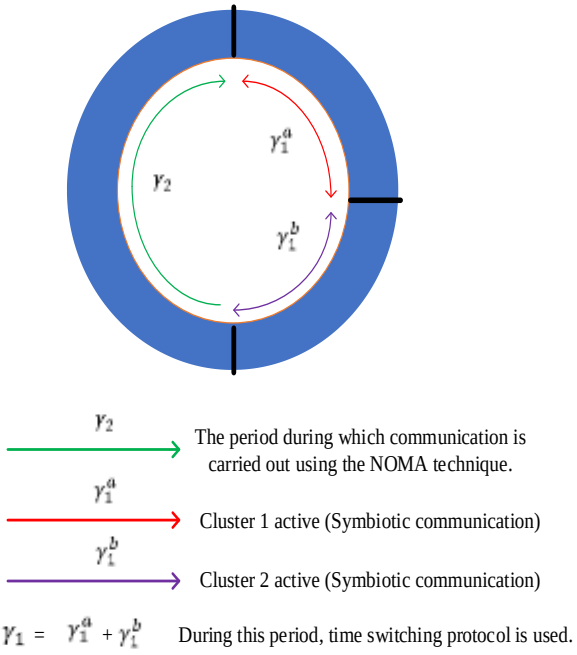

Figure 2. *Time frame for system model.*

Thus, D_1-R_1 and D_2-R_2 passively transmit the source's information to the gateway. At the end of γ_1 period, the source reaches the number of bits it needs to send to the gateway and becomes passive. This means that the gateway will now work as the receiver of cluster 1-2. R_1 and R_2 harvest energy from the surrounding signals and actively transmit their information to the gateway simultaneously with the non-orthogonal multiple access (NOMA) technique for γ_2 period. In this system where the secrecy rate is maximized, the ED, which tries to capture information from both the source and R_1-R_2 over the wiretap channel during the whole period, is prevented by the artificial noise emitted by the cooperative jammer. The jammer is also considered as an energy source for R_1 and R_2.

The number of bits reaching the gateway in γ_1 time is found with the formula below [19, 20].

$$C_{\gamma_1} = \gamma_1^a \log_2\left(1+\frac{P_s g_{S-D_1} g_{D_1-R_1} g_{R_1-G} \beta_{D_1} \beta_{R_1}}{N_0}\right) + \gamma_1^b \log_2\left(1+\frac{P_s g_{S-D_2} g_{D_2-R_2} g_{R_2-G} \beta_{D_2} \beta_{R_2}}{N_0}\right) + \gamma_1 \log_2\left(1+\frac{P_s g_{S-G}}{N_0}\right) \quad (1)$$

where β_{D_1}, β_{R_1}, β_{D_2} and β_{R_2} are the reflection coefficients for D_1, R_1, D_2 and R_2, respectively. P_s is the source signal transmission power. The channel is modeled as additive white gaussian noise (AWNG) and the noise power is N_0. g_{S-D_1}, $g_{D_1-R_1}$, g_{R_1-G}, g_{S-G}, g_{j-R_1}, g_{j-R_2}, g_{S-R_1}, g_{S-R_2}, g_{S-D_2}, $g_{D_2-R_2}$, g_{R_2-G}, g_{R_1-ED}, g_{R_2-ED}, g_{S-ED}, g_{j-ED} represent the channel gain between source-D_1, D_1-R_1, R_1-gateway, source-gateway, jammer-R_1, jammer-R_2, source-R_1, source-R_2, source-D_2, D_2-R_2, R_2-gateway, R_1-ED, R_2-ED, source-ED, jammer-ED respectively. In Fig. 3, a decode-forwarding (DF) protocol is designed for relays that transmit bits to the gateway with active data transmission for γ_2 duration. For cluster 1, the parameter that determines how long R_1 will decode or forward is the time splitting factor α_1, while for cluster 2 this parameter is α_2 (α_1, $\alpha_2 \in (0,1)$). The number of bits transmitted to the gateway in period γ_2 when the communication is performed with the NOMA technique is as follows [16].

$$C_{\gamma_2} = \gamma_2(1-\alpha_1)\log_2\left(1+\frac{P_{R_1} g_{R_1-G}}{N_0 + P_{R_2} g_{R_2-G}}\right) + \gamma_2(1-\alpha_2)\log_2\left(1+\frac{P_{R_2} g_{R_2-G}}{N_0}\right) \quad (2)$$

Since the source is idle during the γ_2 time, the number of bits transmitted between the source and the gateway is not included in Equation 2. The energy harvested by R_1 and R_2 in the proposed system network is found by the following equations respectively.

$$E_{R_1} = P_s g_{S-R_1} \gamma_1 + P_j g_{j-R_1}(\gamma_1+\gamma_2) + P_s g_{S-D_1} g_{D_1-R_1} \beta_{D_1} \gamma_1^a \quad (3)$$

$$E_{R_2} = P_s g_{S-R_2} \gamma_1 + P_j g_{j-R_2}(\gamma_1+\gamma_2) + P_s g_{S-D_2} g_{D_2-R_2} \beta_{D_2} \gamma_1^b \quad (4)$$

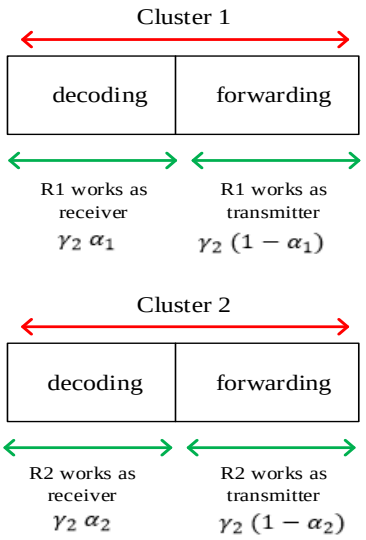

Figure 3. *Decode-forwarding protocol design for SRN in* γ_2.

As can be seen from Equations 3 and 4, R_1 and R_2 harvest energy source signal, jammer signal and from the backscattered signals of the devices. In active data communication, the signal power transmitted to the receiver by R_1 and R_2 at time γ_2 can be found by the following expressions, respectively.

$$P_{R_1} = \frac{E_{R_1} - P_c^b \gamma_2 \alpha_1}{\gamma_2 (1-\alpha_1)} \tag{5}$$

$$P_{R_2} = \frac{E_{R_2} - P_c^b \gamma_2 \alpha_2}{\gamma_2 (1-\alpha_2)} \tag{6}$$

P_c^b is the power consumed by the relay during the decoding process in γ_2 time. Since simple techniques are used in passive backscatter communication during γ_1 time, the energy consumed is neglected. The number of bits leaked by R_1, R_2 and the source to the ED over the wiretap channel for γ_1 duration is found as follows.

$$\begin{aligned} C_{ED}^1 = {} & \gamma_1^a \log_2\left(1+\frac{P_s g_{S-D_1} g_{D_1-R_1} g_{R_1-ED} \beta_{D_1} \beta_{R_1}}{N_0 + P_j g_{j-ED}}\right) \\ & + \gamma_1^b \log_2\left(1+\frac{P_s g_{S-D_2} g_{D_2-R_2} g_{R_2-ED} \beta_{D_2} \beta_{R_2}}{N_0 + P_j g_{j-ED}}\right) \\ & + \gamma_1 \log_2\left(1+\frac{P_s g_{S-ED}}{N_0 + P_j g_{j-ED}}\right) \end{aligned} \tag{7}$$

The number of bits leaked by R_1, R_2 and the source to the ED over the wiretap channel for γ_2 duration is found as follows.

$$\begin{aligned} C_{ED}^2 = {} & \gamma_2 (1-\alpha_1) \log_2\left(1+\frac{P_{R_1} g_{R_1-ED}}{N_0 + P_j g_{j-ED}}\right) \\ & + \gamma_2 (1-\alpha_2) \log_2\left(1+\frac{P_{R_2} g_{R_2-ED}}{N_0 + P_j g_{j-ED}}\right) \end{aligned} \tag{8}$$

In the channel capacity expressions in Equation 7 and Equation 8, the situation where the jammer creates interference in the ED is taken into account. The total number of bits acquired by the ED is expressed as $C_{ED} = C_{ED}^1 + C_{ED}^2$. In symbiotic radio network with relay-obstacle, considering the number of bits reaching the ED over the wiretap channel, the secrecy rate in terms of physical layer security is expressed by the following equation.

$$C_{\text{sec}} = (C_{\gamma_1} + C_{\gamma_2} - C_{ED})^+ \tag{9}$$

where $(x)^+ = \max(x, 0)$. This paper aims to maximize the secrecy rate. Therefore, we can write our optimization problem with various constraints as follows.

$$\max_{\gamma_1^a, \gamma_1^b, \gamma_2} C_{\text{sec}} \rightarrow s.t. \begin{cases} \sum_{i=1}^{2} \gamma_i \le 1 \\ \gamma_1^a, \gamma_1^b, \gamma_2 \ge 0, \\ \gamma_1^a + \gamma_1^b = \gamma_1 \\ 0 < \alpha_1, \alpha_2 < 1 \\ C_{\gamma_1} \ge C_1^+ \\ C_{\gamma_2} \ge C_2^+ \end{cases} \tag{10}$$

In Equation 10, we maximize the secrecy rate of the system over the time parameters. The first constraint indicates that a full period cannot exceed 1 s by normalizing it. The second constraint guarantees that the variables are not negative. The $C_{\gamma_1} \ge C_1^+$ constraint indicates the quality of service (QoS) the source and expresses that the number of bits that the source should transmit is at least C_1^+. The $C_{\gamma_2} \ge C_2^+$ constraint indicates the QoS cluster 1-2 and expresses that the total number of bits that the relays should transmit is at least C_2^+.

3. Results and Discussions

Computer simulation results for the proposed system model are given in this section. In the results, the following numerical values are used unless otherwise stated: P_s = 17 kW, P_j=300 W, $\beta_{D_1} = \beta_{R_1} = \beta_{D_2} = \beta_{R_2}$= 0.7, T = 1 s, $N_0 = 10^{-6}$ W, P_c^b = 0.1 mW, $\alpha_1 = \alpha_2$ = 0.5, C_1^+ = 15 bps/Hz,

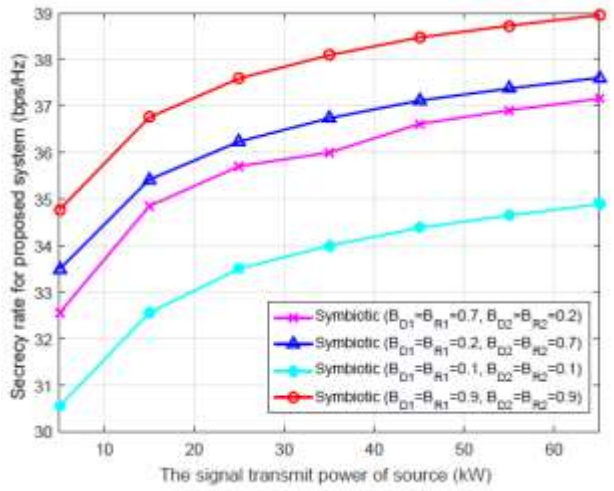

Figure 4. *Secrecy rate variation with respect to P_S under different reflection coefficients.*

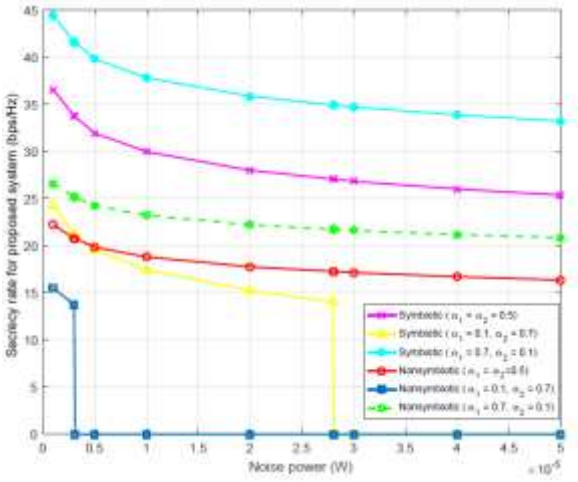

Figure 5. *Secrecy rate variation with respect to noise power under different time splitting factor.*

$C_2^+ = 5$ bps/Hz, $g_{S-D_1} = 0.05$, $g_{D_1-R_1} = 0.3$, $g_{R_1-G} = 0.04$, $g_{S-G} = 0.1$, $g_{j-R_1} = 0.08$, $g_{j-R_2} = 0.08$, $g_{S-R_1} = 0.05$, $g_{S-R_2} = 0.05$, $g_{S-D_2} = 0.05$, $g_{D_2-R_2} = 0.3$, $g_{R_2-G} = 0.04$, $g_{R_1-ED} = 0.02$, $g_{R_2-ED} = 0.02$, $g_{S-ED} = 0.03$, $g_{j-ED} = 0.2$. Channel gains are modeled as quasi-static flat fading to remain constant over a period. It is also assumed that there is a signal attenuation depending on the distance [6].

Fig.4 shows the change of secrecy rate with respect to P_s under different reflection coefficient values. Although the increase of P_s improves the system performance, the secrecy rate increase rate is slowed down by ED since the number of bits transmitted over the wiretap channel also augments. For low values of P_s, the rate of increase of C_{sec} is high, while for high values of P_s, the rate of increase of C_{sec} is slower. In addition, the effects of different values of the reflection coefficient, which can be adjusted by utilizing the antenna impedance mismatch of the devices and relays, on the system performance are shown. According to Equation 1, the increase in the reflection coefficient increases the capacity of the system. Therefore, the situation where the reflection coefficient is the highest for all users gives the best performance of the system. The $\beta_{D_1} = \beta_{R_1} = \beta_{D_2} = \beta_{R_2} = 0.1$ case is the scenario where the symbiotic relationship between the source and cluster 1-2 is weak and has the worst performance.

The change of secrecy rate according to noise power is shown under different time splitting factor in Fig. 5. The increase in noise power reduces the system performance according to Equations 1-2. The nonsymbiotic scenario is the $\beta_{D_1} = \beta_{R_1} = \beta_{D_2} = \beta_{R_2} = 0$ situation where cluster 1-2 does not assist in the transmission of source information but only transmits information for γ_2 duration using the energy HTT protocol. This system is known as the wireless powered communication model in the literature [7]. When system analyzed under the same parameter values, it is seen that cluster 1-2 and the source terminal transmitting information to the gateway using the same communication protocol (symbiotically) is more advantageous than the non-symbiotic case. In symbiotic ($\alpha_1 = 0.1$, $\alpha_2 = 0.7$), the system performance is 0 because the $C_{\gamma_1} \geq C_1^+$ and $C_{\gamma_2} \geq C_2^+$ constraints cannot be met after the value of $N_0 = 28x10^{-6}$, while in nonsymbiotic ($\alpha_1 = 0.1$, $\alpha_2 = 0.7$), this value is seen after at $N_0 = 3x10^{-6}$. Setting $\alpha_2 = 0.1$ means that R_2 allocates more time for data transmission in the DF protocol. Thus, it needs to harvest more energy in time γ_1. As time γ_1 increases, the number of bits sent by the source to the gateway increases from the expression $\gamma_1 \log_2(1 + (P_s g_{S-G})/N_0)$. This result shows us that the secrecy rate is higher for low values of α_2 under the change of noise power. $\alpha_1 = 0.1$, $\alpha_2 = 0.7$ increases the forwarding time of R_1. In the $\gamma_2 (1 - \alpha_1) \log_2 \left(1 + (P_{R_1} g_{R_1-G})/(N_0 + P_{R_2} g_{R_2-G})\right)$ expression in Equation 2, due to the interference caused by NOMA, the number of transmitted bits will be less. This causes the secrecy rate to be low.

In Fig. 6, the performance of the proposed system model is examined with respect to the jammer signal power and compared with the nonsymbiotic scenario. In the nonsymbiotic scenario where the antennas of all users in the system work with impedance matching, cluster 1-2 does not help the main system in bit transmission and waits for its turn to transmit its information to the gateway. The decrease of P_j reduces the system performance for both cases. In the proposed system, the jammer

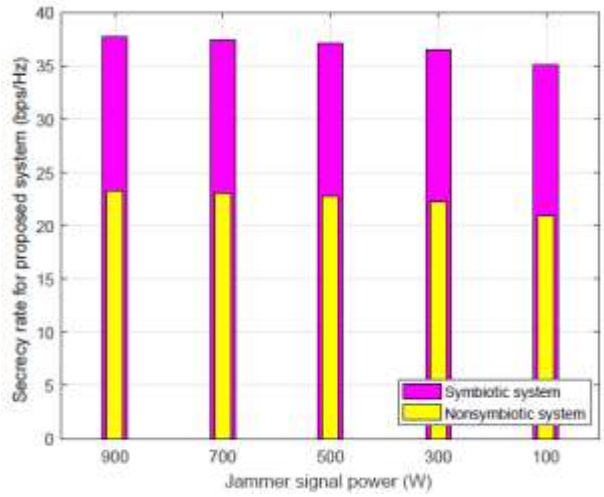

Figure 6. *Change of the secrecy rate for two different cases according to the jammer signal power.*

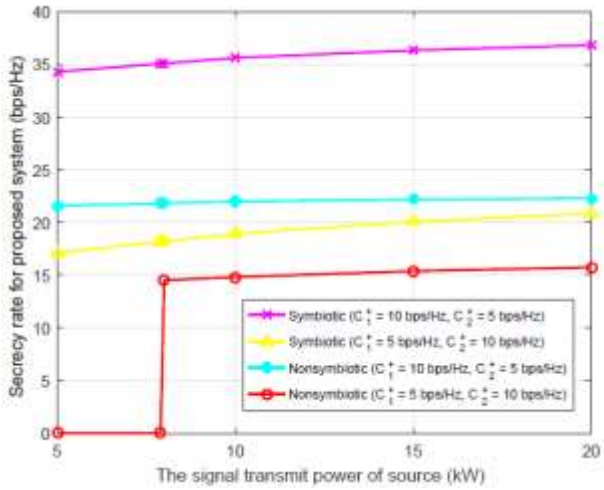

Figure 7. *Secrecy rate according to the change of P_S under different C_1^+ and C_2^+ constraints.*

works in cooperation with the relays and sends artificial noise to ED. The decrease of P_j reduces the harvested energy according to Equations 3 and 4. This reduces the number of bits sent to the gateway according to the channel capacity expression in Equation 2. In addition, the jammer reduces the SNR value of ED, causing C_{sec} to increase. Although the contribution of the jammer to the system performance in the given range seems to be small, it ensures the performance of the system by keeping it above a certain value with the interference it creates to the ED. As a result, designing the system as symbiotic gives better performance than the nonsymbiotic scenario.

The secrecy rate according to the change of P_s under different C_1^+ and C_2^+ values is shown in Fig. 7. The best performance is obtained in the symbiotic scenario, where the number of bits that the main system have to send is high. The worst performance is observed in the nonsymbiotic scenario, where the number of bits that cluster 1-2 sent to the gateway in their communication protocols is kept high for γ_2 duration. Setting C_2^+ to a high value reduces the number of bits the source sends during γ_1. Therefore, case ($C_1^+ = 5$ bps/Hz and $C_2^+ = 10$ bps/Hz) has lower performance than case ($C_1^+ = 10$ bps/Hz and $C_2^+ = 5$ bps/Hz) in the same scenario. For nonsymbiotic ($C_1^+ = 10$ bps/Hz and $C_2^+ = 5$ bps/Hz) scenario, C_{sec} = 21.57 bps/Hz is obtained at P_s = 5 kW, while C_{sec} = 22.27 bps/Hz is found at P_s = 20 kW. Augmenting P_s caused a small increase in the secrecy rate. For nonsymbiotic ($C_1^+ = 5$ bps/Hz and $C_2^+ = 10$ bps/Hz) scenario, the secrecy rate of the system is taken as 0 since the constraints in Equation 10 could not be met at values smaller than P_s = 8 kW.

4. Conclusions

In this paper, for an SRN with relay-obstacle, the secrecy rate is maximized. The proposed system model is the first approach to maximize the secrecy rate for an SRN in the presence of a relay-obstacle by using ambient radio frequency source. The system consists of a source that propagates signals to the environment, two different clusters, a gateway as a receiver, an ED that overhears to the signals transmitted by the users in the system, and a cooperative jammer. Cluster 1 consists of D_1 and R_1 and the obstacle, while cluster 2 consists of D_2, R_2 and the obstacle. Since there is no direct link from D_1-D_2 to the gateway due to the obstacle, relays act as information forwarding. The proposed system model is expressed in mathematical equations and the channel capacity is maximized over time parameters for secrecy rate. Through computer simulations, the advantages of using the channel symbiotically are evaluated compared to the nonsymbiotic scenario in the literature where the HTT protocol is used, and the results are shown graphically by testing the performance according to the variation of different parameters in the system. In future work, we will consider the system as a model with more than two clusters and analyze the secrecy rate of the system.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper

- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Funding information:** The authors declare that there is no funding to be acknowledged.

- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Dangi, R., Choudhary, G., Dragoni, N., Lalwani, P., Khare, U., & Kundu, S. (2023, December). 6G Mobile Networks: Key Technologies, Directions, and Advances. In *Telecom* 4(4);836-876. DOI: 10.3390/telecom4040037

[2] Janjua, M. B., & Arslan, H. (2023). A survey of symbiotic radio: methodologies, applications, and future directions. *Sensors*, *23*(5), 2511 DOI: 10.3390/s23052511

[3] Long, R., Liang, Y. C., Guo, H., Yang, G., & Zhang, R. (2019). Symbiotic radio: A new communication paradigm for passive Internet of Things. *IEEE Internet of Things Journal*, *7*(2), 1350-1363. DOI: 10.1109/JIOT.2019.2954678

[4] Liang, Y. C., Long, R., Zhang, Q., & Niyato, D. (2022). Symbiotic communications: Where marconi meets darwin.*IEEE Wireless Communications*, 29(1), DOI:144-150. 10.1109/MWC.101.2100132

[5] Akyildiz, I. F., Lee, W. Y., Vuran, M. C., & Mohanty, S. (2008). A survey on spectrum management in cognitive radio networks. *IEEE Communications magazine*, *46*(4), 40-48. DOI: 10.1109/MCOM.2008.4481339

[6] Onay, M. Y. (2024). Dynamic Time Allocation Based Physical Layer Security for Jammer-Aided Symbiotic Radio Networks. *Radioenginering*, *33*(3), 443. DOI: 10.13164/re.2024.0442

[7] Hoang, D. T., Niyato, D., Wang, P., Kim, D. I., & Han, Z. (2017). Ambient backscatter: A new approach to improve network performance for RF-powered cognitive radio networks. *IEEE Transactions on Communications*, *65*(9), 3659-3674. DOI: 10.1109/TCOMM.2017.2710338

[8] Liu, V., Parks, A., Talla, V., Gollakota, S., Wetherall, D., & Smith, J. R. (2013). Ambient backscatter: Wireless communication out of thin air. *ACM SIGCOMM computer communication review*, *43*(4), 39-50. DOI: 10.1145/2534169.2486015

[9] Srivastava, A., & Kaur, G. (2023). Cooperation and energy harvesting based spectrum sensing schemes for green cognitive radio networks. *Transactions on Emerging Telecommunications Technologies*, *34*(3), e4714. DOI: 10.1002/ett.4714

[10] Furqan, H. M., Solaija, M. S. J., Türkmen, H., & Arslan, H. (2021). Wireless communication, sensing, and REM: A security perspective. *IEEE Open Journal of the Communications Society*, *2*, 287-321. DOI: 10.1109/OJCOMS.2021.3054066

[11] Solaija, M. S. J., Salman, H., & Arslan, H. (2022). Towards a unified framework for physical layer security in 5G and beyond networks. *IEEE Open Journal of Vehicular Technology*, *3*, 321-343. DOI: 10.1109/OJVT.2022.3183218

[12] Yang, H., Ding, H., Elkashlan, M., Li, H., & Xin, K. (2023). A novel symbiotic backscatter-NOMA system. *IEEE Transactions on Vehicular Technology*, *72*(8), 11006-11011. DOI: 10.1109/TVT.2023.3259687

[13] Nimi, T., & Babu, A. V. On the physical layer security performance of full- duplex cooperative NOMA system with multiple eavesdroppers, imperfect SIC and hardware imperfections. *Internet Technology Letters*, e513. DOI: 10.1002/itl2.513

[14] Li, X., Jiang, J., Wang, H., Han, C., Chen, G., Du, J., ... & Mumtaz, S. (2023). Physical layer security for wireless-powered ambient backscatter cooperative communication networks. *IEEE Transactions on Cognitive Communications and Networking*, *9*(4), 927-939. DOI: 10.1109/TCCN.2023.3270425

[15] Li, D. (2020). Backscatter communication via harvest-then-transmit relaying. *IEEE Transactions on Vehicular Technology*, *69*(6), 6843-6847. DOI: 10.1109/TVT.2020.2991227

[16] Onay, M. Y., & Ertug, O. (2023). Ambient Backscatter Communication Based Cooperative Relaying for Heterogeneous Cognitive Radio Networks. *Radioengineering*, *32*(2). DOI: 10.13164/re.2023.0236

[17] Dursun, Y., Wang, K., & Ding, Z. (2022). Secrecy sum rate maximization for a MIMO-NOMA uplink transmission in 6G networks. *Physical Communication*, *53*, 101675. DOI: 10.1016/j.phycom.2022.101675

[18] Hema, P. P., & Babu, A. V. (2024). Full- duplex jamming for physical layer security improvement in NOMA- enabled overlay cognitive radio networks. *Security and Privacy*, *7*(3), e371. DOI: 10.1002/spy2.371

[19] Onay, M. Y., & ERTUĞ, Ö. (2023, July). Performance Analysis under Signal Jammer in Relay Aided Ambient Backscatter Cognitive Radio Networks. In *2023 31st Signal Processing and Communications Applications Conference (SIU)* (pp. 1-4). IEEE.

[20] Sun, J., Zhang, S., & Chi, K. (2021). Optimal time allocation for throughput maximization in backscatter assisted wireless powered communication networks. *IET Communications*, *15*(12), 1620-1631.