Dynamic Time Allocation Based Physical Layer Security for Jammer-Aided Symbiotic Radio Networks

Muhammed Yusuf ONAY

Dept. of Electrical and Electronics Engineering, Faculty of Engineering, University of Hitit, Corum, Turkey

muhammedyusufonay@hitit.edu.tr

Submitted March 25, 2024 / Accepted June 6, 2024 / Online first June 24, 2024

Abstract. *Symbiotic Radio Networks (SRNs) have emerged as an important communication protocol to solve the increasing energy demand and spectrum resource shortage. However, the low bit rates of the devices working in SRNs during backscatter communication, where the surrounding radio frequency resources are used by subsystems different from the main system, make SRNs very vulnerable to external attacks such as eavesdropping and jamming. To solve this problem, the Physical Layer Security (PLS) for SRNs with Signal Emitter (SE), user, jammer, receiver and eavesdropper (ED) is analyzed. While the SE conveys its information to the receiver, the user assists the SE in part of the time period and transmits its information to the receiver in the other part. While ED is overhearing SE and user's information over the wiretap channel, the jammer is trying to prevent ED with the signal it emits. This model, in which the secrecy rate is maximized over time parameters, is the first approach in which PLS analysis is carried out in the presence of a cooperative jammer when the perfect/imperfect Successive Interference Cancellation (SIC) technique is used at the receiver. Numerical results show that the existence of a symbiotic relationship between the user and the SE increases the secrecy rate of the system compared to the non-symbiotic situation. Moreover, adopting the perfect SIC technique at the receiver without energy constraint at the user resulted in a significant increase in PLS performance compared to the imperfect SIC under energy constraint.*

Keywords

Symbiotic radio networks, sixth generation (6G), physical layer security, eavesdropper, jammer, imperfect successive interference cancellation

1. Introduction

Sixth generation (6G) is a technology that has the potential to improve the quality of life by designing communication network structures that are secure and enable communication anywhere in the world [1]. Approaches in the literature on 6G systems aim to realize communication protocols where a large number of devices can transfer data with each other at high data rate and with low latency [2], [3]. The Internet of Things (IoT), which directs this development with 6G technology and is highly emphasized by researchers, has increased the need for energy and spectrum resources with the increase in service demands in the network [4]. It is inevitable that the devices, which are expected to reach 125 billion by 2030, will consume high power with active data transmission. In addition, it is very difficult to allocate spectrum resources to these devices to transmit signals [5].

SRNs have emerged as an important paradigm for devices to use the available spectrum by designing communication protocols based on efficient resource sharing and time allocation scheme, supporting massive IoT connections that will solve the mentioned problems [6]. The aim of SRNs, where users in the communication network share resources in a mutual symbiotic relationship, is to ensure that both the main user and other users using the signal source of the main user reach their target in their own communication protocol. In order to solve the spectrum limitation problem, in some models put forward in IoT networks, the system is considered as a cognitive radio network, and in addition to the primary receiver of the base station (primary transmitter), secondary receiver of the user (secondary transmitter) is included in the system [7], [8]. This situation increases the system cost. Moreover, in this type of cognitive radio model, the performance of the system is highly dependent on the primary channel parameters (such as idle period), while in SRN, the control of system variables can be adjusted by the user [9], [10].

One of the most emphasized topics within the scope of 6G technology, which allows SRN devices to transmit information to the receiver with low power and without the need for an external energy source, is the backscatter communication and energy harvesting technique [3]. Backscatter devices in SRNs, which do not have a high-power radio frequency signal generator, backscatter the incoming signal to the receiver by taking advantage of the impedance mismatch. In this method, where simple modulation techniques are used, passive communication is achieved with low energy. The fact that the backscattering device only transmits information passively does not meet the goals set within the scope of 6G. Therefore,

DOI: 10.13164/re.2024.0442

the energy harvesting technique using surrounding signals, which will enable the user to perform active data transmission as well as backscatter communication without requiring an external energy source, is highly preferred in SRNs.

The use of surrounding radio frequency resources by subsystems different from the main system and the low bit rates of the devices during backscatter communication make SRNs very vulnerable to attacks such as unwanted signals from the outside, eavesdropping and jamming [11]. This creates a security problem in SRNs and damages the symbiotic relationship between the base station and the user. Cryptography-based authentication and encryption methods used to ensure information security in traditional active radio communications have high computational complexity. Such methods with high energy consumption are not particularly suitable for SRNs where low-power secure communication is targeted [12]. To overcome the problem, PLS has been proposed [13], [14]. PLS is used as an alternative to traditional cryptography methods in this type of wireless communication [15].

The main purpose of PLS is to maximize the secrecy rate, which is defined as the difference of the total number of bits sent to the receiver over the main channel and the number of bits reaching the ED via the wiretap channel [16]. In SRNs, if the propagation capacity of the main channel consisting of base station-receiver and user-receiver exceeds that of the wiretap channel, the confidential information to be transmitted to the receiver can be perfectly delivered to the receiver at a bit rate other than zero. Thus, ED cannot overhear any information intended to be transmitted to the receiver and system security is ensured. In most of the approaches in the literature regarding PLS, users are considered to have a single antenna. Although multiple antenna technology is used to increase the secrecy rate in next-generation communication systems, the existence of small-sized devices with low power and low complexity in SRNs makes the use of a single antenna more common [17–19]. In [20] where PLS is analyzed, the jammer in the network prevents ED from accessing confidential information by reducing its Signal-to-Noise Ratio (SNR) value. In the considered system, the user only actively transmits data. Additionally, two different receivers are allocated to the system. In [21], physical layer security due to the structural design of the user was examined for the wirelessly powered ambient backscatter communication system. In the system where a non-linear energy harvesting technique is used, PLS performance and secrecy outage probability are derived and performance analysis is tested. In another article, capacity analysis has been derived under the sensitivity constraint, which is based on the circuit sensitivity in the user infrastructure for SRN [22]. It has been discussed in the literature that collaborative approaches in which Jammer reduces the SNR value of ED together with the users in the network, and it is accepted that the receiver uses the perfect SIC method to obtain the information again [23], [24]. The authors, who introduced a Utility-Based model in symbiotic radio-supported Internet of Things Networks, analyzed the system regarding resource sharing [25]. In [26], an SRN model consisting of base station, user, receiver and ED device was designed. Perfect SIC was used in the study where the secrecy rate value was tried to be found by optimizing the user's reflection coefficient and the system's power allocation factor. In another study, the authors proposed a symbiotic network with multiple users and used a time allocation scheme to improve energy efficiency in the network [27]. For next generation communication systems where there are multiple users, the Non-Orthogonal Multiple Access (NOMA) technique allows efficient use of the frequency spectrum in scenarios where data transmission is made simultaneously [7]. In [28], the authors maximize the secrecy sum rate under the constraint of total transmission power and quality of service in a Multiple-Input Multiple-Output (MIMO) system. The original non-convex problem using the NOMA technique was transformed into concave sub-problems using the first-order Taylor approach. NOMA has been shown to perform better compared to some benchmarks. In [29], the authors test the physical layer security of primary and secondary users in the cognitive radio network using the NOMA technique in the presence of an external passive eavesdropper. To improve the secrecy outage probability performance, target nodes operate in full-duplex mode and generate signals towards the eavesdropper. Performance analysis for jamming-assisted and non-jamming-assisted scenarios is given in comparative numerical analyses.

In this article, PLS is examined for an SRN with the SE, user, jammer, receiver and ED. The proposed model is the first approach in which PLS analysis is performed using the perfect/imperfect SIC technique in SRN, in the presence of a hybrid user capable of backscatter communication and a cooperative jammer, by taking advantage of the existing radio frequency signal. The user helps the SE to transmit information towards the receiver for a period of time α_1. The signals sent from the user and the SE reach the receiver simultaneously using the NOMA technique. During α_2, the SE interrupts signal transmission and the user sends its own information to the receiver using traditional communication techniques. It is assumed that the SIC technique is used at the receiver. In the model where the secrecy rate is maximized, unlike [23] and [24], system performance is analyzed for two scenarios under perfect/imperfect SIC and energy constraint. While the system in [29] is designed as a cognitive radio network and PLS analysis is performed, the system proposed in this article is modeled as an SRN and one receiver is used. The SE is not a radio frequency source specifically allocated to the SRN, but can be considered as a TV tower or FM base station with high signal transmission power broadcasting in the environment. While there is no jammer in [21], our model has a cooperative jammer. Moreover, the jammer is considered as an energy source for the user, unlike [28] and [29], in addition to its task of reducing the SNR value of ED. The first scenario is the model where the perfect SIC technique is used at the receiver. Unlike [20, 21, 28, 29], the user can perform both backscattering and traditional communication. Like [21], in the first scenario, there is no energy limitation

for the system. The second scenario is a model where the imperfect SIC technique is used at the receiver and the energy constraint for the user is taken into account as in [20]. Although the energy constraint makes the problem considered more complex, it makes the proposed system more practical. Both scenarios are considered comparatively under certain constraints, and the secrecy rate is maximized in the proposed dynamic time allocation scheme. Numerical results show that having a symbiotic relationship between the user and the SE increases the secrecy rate of the system compared to the non-symbiotic situation. The adoption of the perfect SIC technique at the receiver without energy constraint at the user results in a significant increase in PLS performance compared to the imperfect SIC under energy constraint. In addition, the perfect SIC technique is generally adopted in system models where PLS analysis is performed. In this system model, the performance difference that occurs when the imperfect SIC technique is used at the receiver is given comparatively in the simulation results. The main contributions of this article are summarized as follows:

1. In order to solve the problem of SRNs being vulnerable to external attacks such as eavesdropping and jamming, a system model with SE that propagates radio frequency signals to the environment has been proposed and PLS has been analyzed.

2. This system model, in which the secrecy rate is maximized over the time parameters, is the first approach in which PLS analysis for SRNs is performed in the presence of a cooperative jammer using the perfect/imperfect SIC technique at the receiver.

3. Since cryptography-based authentication and encryption methods used to ensure information security in traditional active radio communication have high computational complexity, the approach implemented in the proposed system can be used as an alternative to traditional cryptography methods in next generation wireless communication.

4. Unlike the cognitive radio network models in [7] and [20], where there are two receivers and the user's performance is highly dependent on the primary channel parameters (such as idle time), this model proposed as SRN has a single receiver and the control of system variables can be adjusted by the user.

5. The existence of a symbiotic relationship between the user and the SE increases the secrecy rate of the system compared to the non-symbiotic case. This means that the system achieves a higher bit rate compared to [30] and [31], which only adopted the wireless powered communication model. Moreover, it is an important contribution to the literature that the adoption of perfect SIC technique in the receiver without energy constraint in the user causes a significant increase in PLS performance compared to imperfect SIC under energy constraint.

The remaining sections of this article are presented as follows: In Sec. 2, the system model is examined, and the proposed dynamic time allocation scheme is given. In Sec. 3, the system model is analyzed in two different scenarios and transformed into an optimization problem. In Sec. 4, simulation results are obtained and the results are interpreted. Finally, conclusions and future work are presented in Sec. 5.

2. System Model

The system model and dynamic time allocation scheme are shown in Figs. 1 and 2, respectively. In this model, the SE transmits the information to its receiver in α_1 time. The user helps the SE to transmit the information of the signal emitter to the receiver during α_1. The user, which acts as a relay for the α_1, also harvests energy from the SE and charges its battery with wireless energy. The SE, which reaches the minimum number of bits it must transmit to the receiver, remains inactive for the second period of the time scheme, α_2. The user operates the energy collected during α_1 for α_2 by evaluating the time when the SE is inactive. The user, which transmits its information to the receiver at high signal transmission power through traditional communication during the α_2 period, does not create any interference between the SE and the receiver. The ED in the system model works continuously for full period in the dynamic time allocation scheme and overhears to the information of both the user and the SE. The jammer in the system prevents the ED from receiving information by reducing the SNR value in the ED with the signal it sends. The jammer signal is also used by the user to harvest energy. System channels consist of the wiretap channel (between SE-ED and user-ED), the energy harvesting channel (between user-jammer), and the jamming channel (between jammer-ED). The total signal received by ED is given as follows:

$$y_E = y_S g_{S\text{-}E} + y_u g_{U\text{-}E} + y_j g_{j\text{-}E} + w \tag{1}$$

where the signal sent by the SE is y_S and the signal sent by the jammer is y_j. In $y_S = \sqrt{P_S} S_S(t)$, $y_j = \sqrt{P_j} S_j(t)$, the information sent by the SE is $S_S(t)$ and the signal transmission power is $\sqrt{P_S}$, the information sent by the jammer is $S_j(t)$ and the signal transmission power is $\sqrt{P_j}$. The signal transmission power of SE and jammer are given in the following equations, respectively:

$$\begin{aligned} E\left[|y_S(t)|^2\right] &= P_S, \\ E\left[\left|y_j(t)\right|^2\right] &= P_j. \end{aligned} \tag{2}$$

The channel gain is named as between SE and ED, between user and ED, between jammer and ED as $g_{S\text{-}E}$, $g_{U\text{-}E}$, $g_{j\text{-}E}$, respectively. $w(t)$ is a additive white gaussion noise with zero mean and variance σ_E^2. The signal transmitted by the user can be evaluated for two different situations:

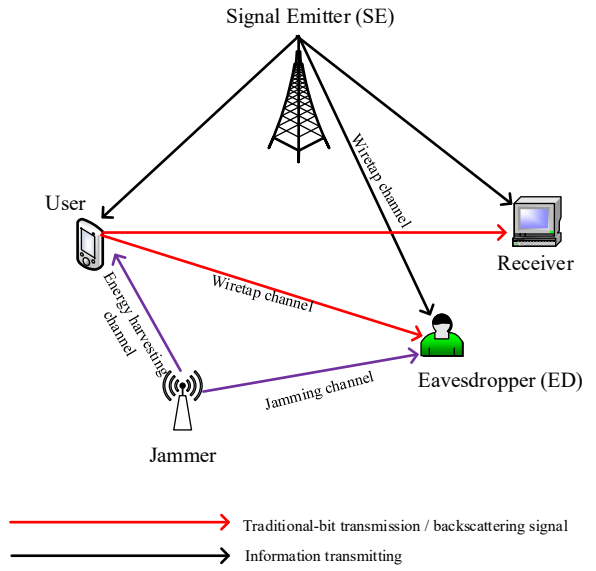

Fig. 1. The system model.

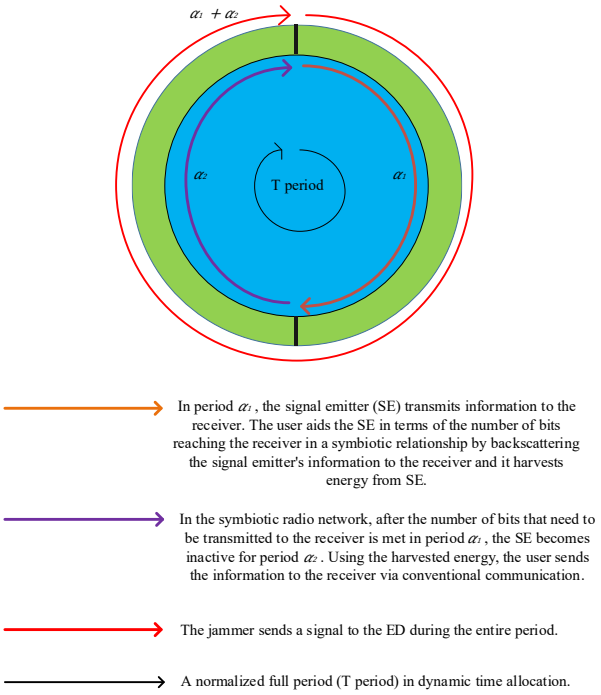

Fig. 2. Dynamic time allocation scheme.

$$y_{\mathrm{u}} = \begin{cases} \sqrt{P_{\mathrm{S}}\,\epsilon} S_{\mathrm{S}}(t)\; g_{\mathrm{S\text{-}U}}\; x_{\mathrm{u}}, & \text{backscatter signal} \\ \sqrt{P_{\mathrm{a}}}\, x_{\mathrm{u}}, & \text{bit transmission} \end{cases} \tag{3}$$

where x_{u} is user's signal. While the SE and the user transmit information to the receiver, the jammer simultaneously sends its signal to the ED. The user harvests energy from the jammer's signal for time T. Therefore, while the jammer is an energy source for the user, it also functions to disrupt the signal obtained by the ED. Power reflection coefficient $\epsilon \in (0, 1]$ is a term that determines how much of the signal coming from the SE will be backscattered and how much will go to the energy harvesting circuit. P_{a} is the signal transmission power of the user during information transmission via conventional communication in period α_2. It is assumed that the user and the SE know the jammer signal very well and in this cooperative structure the jammer only interferes with ED [20].

3. Problem Formulation

Two different scenarios are considered in the system model. In the first scenario, it is assumed that there is no energy constraint for the user, considering that there is perfect SIC at the receiver. In the second scenario, it is assumed that the user is operating under energy constraint, considering that there is a imperfect SIC at the receiver. The secrecy rate is formulated for both cases.

3.1 Scenario 1: Under Perfect SIC and No-Energy Constraint

The upper bound of shannon channel capacity for the receiver is given by the following equation:

$$R_a = \alpha_1 \log_2\left(1 + \frac{P_{\mathrm{S}}\,|g_{\mathrm{S\text{-}R}}|^2}{\sigma_{\mathrm{R}}^2}\right) + \alpha_1 \log_2\left(1 + \frac{P_{\mathrm{S}}\,\epsilon\,|g_{\mathrm{U\text{-}R}}\,g_{\mathrm{S\text{-}U}}|^2\,a}{\sigma_{\mathrm{R}}^2}\right) + \alpha_2 \log_2\left(1 + \frac{P_{\mathrm{a}}\,|g_{\mathrm{U\text{-}R}}|^2}{\sigma_{\mathrm{R}}^2}\right) \tag{4}$$

where $a \in (0, 1]$ is the performance gap reflecting the real modulation, $g_{\mathrm{S\text{-}R}}$ is the channel gain between the SE and the receiver, $g_{\mathrm{S\text{-}U}}$ is the channel gain between the SE and the user, $g_{\mathrm{U\text{-}R}}$ is the channel gain between the user and the receiver. The noise power at the receiver is considered as σ_{R}^2. Since only the user is active during α_2, there is no interference at the receiver. However, the SE and the user transmit signals simultaneously during α_1 and interference is taken into account at the receiver. In the NOMA technique, we assumed that there is an $g_{\mathrm{S\text{-}R}} > (g_{\mathrm{S\text{-}U}}\; g_{\mathrm{U\text{-}R}})$ relationship between channel gains to guarantee system performance [32]. In the proposed system, there are only two terminals transmitting at the same time, and the SE and the user transmit signals at different power levels. While the SE is a base station that continues its current broadcast in the environment, the signal reaching the receiver from the user has been experienced to channel attenuation twice and its portion multiplied by ϵ reaches the receiver and $P_{\mathrm{S}}|g_{\mathrm{S\text{-}R}}|^2 > P_{\mathrm{S}}\,\epsilon\,|g_{\mathrm{S\text{-}U}} g_{\mathrm{U\text{-}R}}|^2 a$.

In the R_a, let's define the number of bits transmitted to the receiver in time α_1 as $R_a^{(1)}$, and the number of bits transmitted to the receiver in time α_2 as $R_a^{(2)}$.

$$R_a^{(1)} = \alpha_1 \log_2\left(1 + \frac{P_{\mathrm{S}}\,|g_{\mathrm{S\text{-}R}}|^2}{\sigma_{\mathrm{R}}^2}\right) + \alpha_1 \log_2\left(1 + \frac{P_{\mathrm{S}}\,\epsilon\,|g_{\mathrm{U\text{-}R}}\,g_{\mathrm{S\text{-}U}}|^2\,a}{\sigma_{\mathrm{R}}^2}\right), \quad (5)$$

$$R_a^{(2)} = \alpha_2 \log_2\left(1 + \frac{P_{\mathrm{a}}\,|g_{\mathrm{U\text{-}R}}|^2}{\sigma_{\mathrm{R}}^2}\right), \quad (6)$$

$$\begin{aligned} E_{\mathrm{a}} &= P_{\mathrm{S}}\,(1-\epsilon)\,\alpha_1 + P_{\mathrm{j}}\,(\alpha_1+\alpha_2)\,, \\ P_{\mathrm{a}} &= \frac{E_{\mathrm{a}}}{\alpha_2}. \end{aligned} \quad (7)$$

While the SE transmits its own information to the receiver in time α_1, the user assists the SE by transmitting the SE's information to the receiver via backscatter communication. $R_a^{(2)}$ is the number of bits that the user transmits to the receiver in α_2 time with the signal transmission power P_{a}, using the harvested energy. While ϵ portion of the signal coming from SE to the user is used for backscatter communication, $(1-\epsilon)$ portion is used for energy harvesting. Therefore, there is a $(1-\epsilon)$ term in the expression for harvested energy E_{a}. The user also harvests energy using the jammer's signal. This energy is then used to transmit information through traditional communication for time α_2. Since the energy required for backscatter communication is very low, it is neglected in the equations [2]. The upper bound of shannon channel capacity formula for wiretap channel is given by the following equation:

$$R_E = \alpha_2 \log_2\left(1 + \frac{P_{\mathrm{a}}\,|g_{\mathrm{U\text{-}E}}|^2}{\sigma_E^2 + P_{\mathrm{j}}\,|g_{\mathrm{j\text{-}E}}|^2}\right) + \alpha_1 \log_2\left(1 + \frac{P_{\mathrm{S}}\,|g_{\mathrm{S\text{-}E}}|^2 + P_{\mathrm{S}}\,\epsilon\,|g_{\mathrm{U\text{-}E}}\,g_{\mathrm{S\text{-}U}}|^2}{\sigma_E^2 + P_{\mathrm{j}}\,|g_{\mathrm{j\text{-}E}}|^2}\right). \quad (8)$$

In (8), there are two signals at time α_1. The reason why the channel capacity is written as given in the equation is that the signal from the SE and the signal from the user can be coherently combined at the ED using Maximal Ratio Combining (MRC) [33]. Secrecy rate is defined as follows:

$$R_{\mathrm{sec}} = (R_a - R_E)^+, \text{ where } (x)^+ = \max(x, 0), \quad (9)$$

$$\max_{\alpha_1,\alpha_2} R_{\mathrm{sec}} \rightarrow \text{s.t.} \begin{cases} R_a^{(1)} \geq R_1^+, \\ R_a^{(2)} \geq R_2^+, \\ \sum_{i=1}^2 \alpha_i \leq 1, \\ \alpha_i \geq 0. \end{cases} \quad (10)$$

In (10), the objective function R_{sec} is maximized over the α_1 and α_2. R_1^+ and R_2^+ are the minimum number of bits that must be transmitted to the receiver per bandwidth at time α_1, α_2 respectively. $R_a^{(1)} \geq R_1^+$ guarantees the number of bits that the SE in the SRNs must transmit to the receiver in a period. $R_a^{(2)} \geq R_2^+$ guarantees the minimum number of bits that the user must send via traditional communication method for Quality of Service (QoS). Constraint $\sum_{i=1}^2 \alpha_i \leq 1$ indicates that in the dynamic time allocation scheme, the sum of the time parameters can be at most $T = 1$ second in the normalized time period. Constraint $\alpha_i \geq 0$ indicates that time parameters cannot be negative. When the $R_a^{(1)} \geq R_1^+$ constraint is examined, the value range of variable α_1 can be found as follows:

$$z_1 = 1 + \frac{P_{\mathrm{S}}\,|g_{\mathrm{S\text{-}R}}|^2}{\sigma_{\mathrm{R}}^2}, \quad z_2 = 1 + \frac{P_{\mathrm{S}}\,\epsilon\,|g_{\mathrm{U\text{-}R}}\,g_{\mathrm{S\text{-}U}}|^2\,a}{\sigma_{\mathrm{R}}^2}, \quad (11)$$

such that z_1 and z_2 are positive constants,

$$\alpha_1 \geq \frac{R_1^+}{\log_2(z_1 z_2)}. \quad (12)$$

Since the value range of α_1 is $0 \leq \alpha_1 \leq 1$, the following inequality is written:

$$\frac{R_1^+}{\log_2(z_1 z_2)} \leq \alpha_1 \leq 1. \quad (13)$$

When the $R_a^{(2)} \geq R_2^+$ constraint is examined, the value range of variable α_2 can be found as follows:

$$z_3 = 1 + \frac{P_{\mathrm{a}}\,|g_{\mathrm{U\text{-}R}}|^2}{\sigma_{\mathrm{R}}^2} \quad (14)$$

where z_3 is positive constant,

$$\frac{R_2^+}{\log_2(z_3)} \leq \alpha_2 \leq 1. \quad (15)$$

3.2 Scenario 2: Under Imperfect SIC and Energy Constraint

The number of bits transmitted per bandwidth of the signal transmitted from the SE and the user to the receiver at time α_1 is given below:

$$R_a = \alpha_1 \log_2\left(1 + \frac{P_{\mathrm{S}}\,|g_{\mathrm{S\text{-}R}}|^2}{\sigma_{\mathrm{R}}^2 + [P_{\mathrm{S}}\,\epsilon\,|g_{\mathrm{U\text{-}R}} g_{\mathrm{S\text{-}U}}|^2\,a k_i]}\right) + \alpha_1 \log_2\left(1 + \frac{P_{\mathrm{S}}\,\epsilon\,|g_{\mathrm{U\text{-}R}}\,g_{\mathrm{S\text{-}U}}|^2\,a}{\sigma_{\mathrm{R}}^2 + P_{\mathrm{S}}\,|g_{\mathrm{S\text{-}R}}|^2\,k_i}\right) + \alpha_2 \log_2\left(1 + \frac{P_{\mathrm{a}}\,|g_{\mathrm{U\text{-}R}}|^2}{\sigma_{\mathrm{R}}^2}\right). \quad (16)$$

In this scenario, $R_a^{(1)}$ and $R_a^{(2)}$ are defined as mentioned before. We denote the coefficient of imperfect SIC at the receiver by $k_i \in [0, 1]$:

$$\begin{cases} k_i = 0, & \text{perfect SIC}, \\ k_i = 1, & \text{no SIC}. \end{cases} \quad (17)$$

Secrecy rate is defined as follows:

$$R_{\text{sec}} = (R_a - R_E)^+, \tag{18}$$

$$\max_{\alpha_1,\alpha_2} R_{\text{sec}} \rightarrow \text{s.t} \begin{cases} R_a^{(1)} \geq R_1^+, \\ R_a^{(2)} \geq R_2^+, \\ E_{\text{a}} \geq E_{\min}, \\ \sum_{i=1}^{2} \alpha_i \leq 1, \\ \alpha_i \geq 0. \end{cases} \tag{19}$$

In (19), the optimization problem of maximizing the secrecy rate under imperfect SIC and energy constraint for scenario 2 is shown. In addition to the constraints in (10), the $E_{\text{a}} \geq E_{\min}$ inequality has been added. This constraint states that the energy that the user harvest must be at least $E_{\min}$. Unlike the first scenario, in the second scenario, SIC coefficient is taken into account. Therefore, the solution of the optimization problem has also changed. Similar to the value ranges of the time parameters in the first scenario, the following inequalities can be expressed for the second scenario:

$$\begin{aligned} z_4 &= 1 + \frac{P_{\text{S}} |g_{\text{S-R}}|^2}{\sigma_{\text{R}}^2 + [P_{\text{S}} \, \epsilon \, |g_{\text{U-R}} g_{\text{S-U}}|^2 \, a k_i]}, \\ z_5 &= 1 + \frac{P_{\text{S}} \, \epsilon \, |g_{\text{U-R}} g_{\text{S-U}}|^2 \, a}{\sigma_{\text{R}}^2 + P_{\text{S}} \, |g_{\text{S-R}}|^2 \, k_i}, \end{aligned} \tag{20}$$

such that z_4 and z_5 are positive constants. When the $R_a^{(1)} \geq R_1^+$ constraint is examined, the value range of variable α_1 can be found as follows:

$$\alpha_1 \geq \frac{R_1^+}{\log_2 (z_4 z_5)}. \tag{21}$$

Since the value range of α_1 is $0 \leq \alpha_1 \leq 1$, the following inequality is written:

$$\frac{R_1^+}{\log_2 (z_4 z_5)} \leq \alpha_1 \leq 1. \tag{22}$$

When the $E_{\text{a}} \geq E_{\min}$ constraint is analyzed, the value range of variable α_1 can be found as follows:

$$P_{\text{S}} (1 - \epsilon) \, \alpha_1 + P_{\text{j}} (\alpha_1 + \alpha_2) \geq E_{\min}. \tag{23}$$

If $\alpha_1 + \alpha_2 = 1$ is accepted for maximum energy harvest and the value range of α_1 is found, the following inequality is defined ($P_{\text{j}} = E_{\text{j}}$):

$$\alpha_1 \geq \frac{E_{\min} - E_{\text{j}}}{P_{\text{S}} (1 - \epsilon)}. \tag{24}$$

The flow diagram used as a reference to find the time parameters is given in Fig. 3. Before the communication network becomes an optimization problem, we assume that the receiver knows the Channel State Information (CSI), all channel gains in the system are found by advanced channel estimation techniques and are known by all terminals [20].

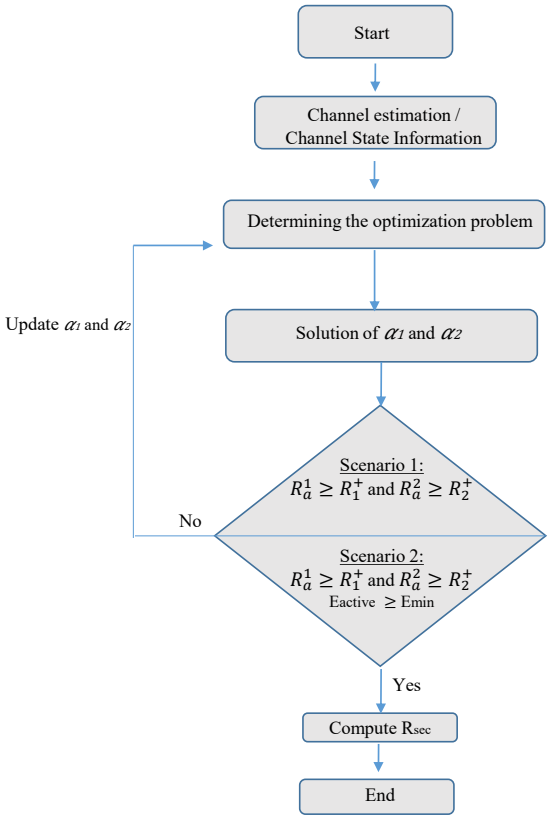

Fig. 3. Flow diagram of time allocation.

4. Simulation Results

The signal transmission power of the SE is $P_{\text{S}} = 17\,\text{kW}$ [34], the signal transmission power of the jammer is $P_{\text{j}} = 100\,\text{W}$, and the power reflection coefficient of the user is $\epsilon = 0.6$, $T = 1\,\text{s}$. In case the user transmits bits via backscatter communication, the performance gap reflecting the real modulation taken into account is $a = 0.8$. The coefficient of imperfect SIC at the receiver considered for scenario 2 is $k_i = 0.5$. The noise power at the receiver and ED is considered equal and $\sigma_{\text{R}}^2 = \sigma_E^2 = 133.59\,\mu\text{W}$ [7]. We set the channel gain between SE and receiver, between SE and user, between SE and ED, between user and ED, between user and receiver, between jammer and ED as $g_{\text{S-R}} = 0.02$, $g_{\text{S-U}} = 0.02$, $g_{\text{S-E}} = 0.01$, $g_{\text{U-E}} = 0.04$, $g_{\text{U-R}} = 0.08$, $g_{\text{j-E}} = 0.1$ respectively. The above parameter values are used in the simulation results unless otherwise stated. In the system model, it is assumed that there is a signal attenuation due to distance, and in the dynamic time allocation scheme, channel gains that remain constant throughout the T-second period but can change in different periods are modeled as quasi-static flat fading.

In the results obtained in Fig. 4, $R_1^+ = 10\,\text{bps/Hz}$ and $R_2^+ = 5\,\text{bps/Hz}$ were set. The minimum energy value considered for symbiotic scenario 2 is $E_{\min} = 1\,\text{kJ}$. Among all scenarios, symbiotic scenario 1 showed the best performance. In symbiotic scenario 1, secrecy rate performance improves

with the increase of P_S. P_S increases the number of bits transmitted to the receiver by both the signal emitter and the user during time α_1. However, this increase is limited by ED due to the wiretap channel. Although the signal constantly sent by the jammer to the ED creates interference on the wiretap channel and reduces the SNR value in the ED, the increase in P_{SE} also increases the number of bits reaching the ED per bandwidth. Therefore, the rate of increase in system performance slows down. The net increase graph according to the $R_{sec} = (R_a - R_E)^+$, where $(x)^+ = \max(x, 0)$. equation is shown in the aforementioned graph. In Fig. 4, symbiotic scenario 1 has a higher secrecy rate than non-symbiotic scenario 1. In non-symbiotic-scenario, the user remains passive for α_1 duration and harvests energy. For this case, $\epsilon = 0$ is accepted. When performance is evaluated for non-symbiotic scenario 1, there is a slower increase than symbiotic scenario 1. In non-symbiotic scenario 1, the user does not assist the SE in transmitting information. It uses time α_1 only to harvest energy. The user adjusts circuit to use this harvested energy for α_2 time. This situation represents a typical wirelessly powered communication networks model. In symbiotic scenario 2, a decrease in R_{sec} is observed due to the increase in P_S. Imperfect SIC reduces the number of total bits that the SE and the user transmit to the receiver. In the system model, due to the $(P_S\ \epsilon\,|g_{U\text{-}R}\,g_{S\text{-}U}|^2\,ak_i)$ and $(P_S\,|g_{S\text{-}R}|^2\,k_i)$ expressions in (16), the increase in R_a is less than the increase in R_E and as a result R_{sec} decreases. In non-symbiotic scenario 2, the $(P_S\ \epsilon\,|g_{U\text{-}R}\ g_{S\text{-}U}|^2\,ak_i)$ term in the denominator in (16) is canceled. This improves secrecy rate performance by increasing the number of bits transmitted by the SE. Considering Scenario 2, non-symbiotic scenario 2 showed better results in terms of R_{sec} compared to symbiotic scenario 2. When looked at carefully, non-symbiotic scenario 2 and symbiotic scenario 2 give the same result at approximately $P_S = 9$ kW.

Figure 5 shows that the change in secrecy rate for different ϵ values according to the signal transmission power of the jammer. The best secrecy rate was found in symbiotic scenario 1 ($\epsilon = 0.8$), while the worst secrecy rate was found in symbiotic scenario 2 ($\epsilon = 0.8$). According to (8), increasing P_j reduces the bit transmission capacity of the wiretap channel. Additionally, since the user harvests energy from P_j, the E_a value increases. As a result, the secrecy rate improves for all scenarios. In symbiotic scenario 1, a better performance emerged as the ϵ value increased. Since the increase of ϵ makes a positive contribution to the number of bits that the SE must transmit to the receiver in the α_1 period, the α_1 period is shortened. As α_1 shortens, α_2 time increases and the user actively works for longer. This takes system performance to higher levels. Increasing ϵ augments the number of bits transmitted by backscatter communication. Therefore, since $(1-\epsilon)$ portion of the signal coming from SE goes to the energy harvesting circuit, the energy harvest decreases according to the $E_a = P_S\,(1-\epsilon)\,\alpha_1 + P_j\,(\alpha_1 + \alpha_2)$ term. This situation causes the rate of performance increase to decrease over time. In symbiotic scenario 2, low ϵ value gave better results in terms of system performance than high ϵ value. Although the second term of R_a has a positive effect on R_{sec} according to the increase of ϵ, the interference caused by the increase of the ϵ variable in the first term of R_a is more dominant and the performance decreases. In this scenario, due to the presence of the imperfect SIC coefficient, the $(P_S\ \epsilon\,|g_{U\text{-}R}\ g_{S\text{-}U}|^2\,ak_i)$ term in the R_a formula significantly reduces the SNR value and it is seen that R_{sec} decreases when the problem is solved under R_1^+, R_1^+ and energy constraint. The two cases with the smallest difference in performance are symbiotic scenario 1 ($\epsilon = 0.4$) and symbiotic scenario 2 ($\epsilon = 0.4$) and the value is $R_{sec} = 7.61$ bps/Hz. When Figure 5 is examined carefully, for all ϵ values, symbiotic scenario 2 has a slightly higher increase rate in R_{sec} than symbiotic scenario 1. For example, in the case of $\epsilon = 0.4$, at $P_j = 100$ W, $R_{sec} = 19.42$ bps/Hz for symbiotic scenario 1, while $R_{sec} = 11.60$ bps/Hz for symbiotic scenario 2. At $P_j = 500$ W, $R_{sec} = 20.74$ bps/Hz for symbiotic scenario 1, while $R_{sec} = 13.13$ bps/Hz for symbiotic scenario 2. If we look at the difference between the first and last value, it is 1.32 for symbiotic scenario 1 and 1.53 for symbiotic scenario 2.

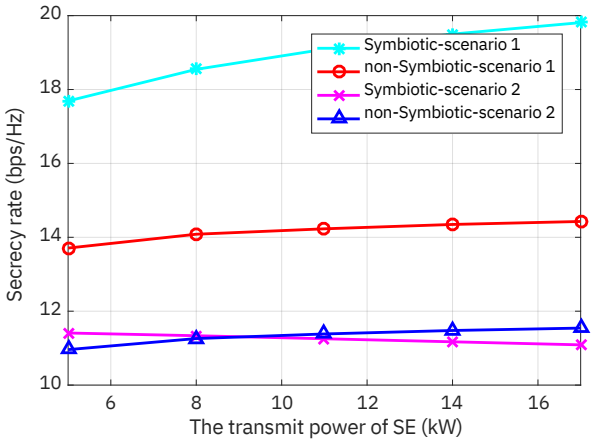

Fig. 4. Secrecy rate change according to signal transmission power of SE.

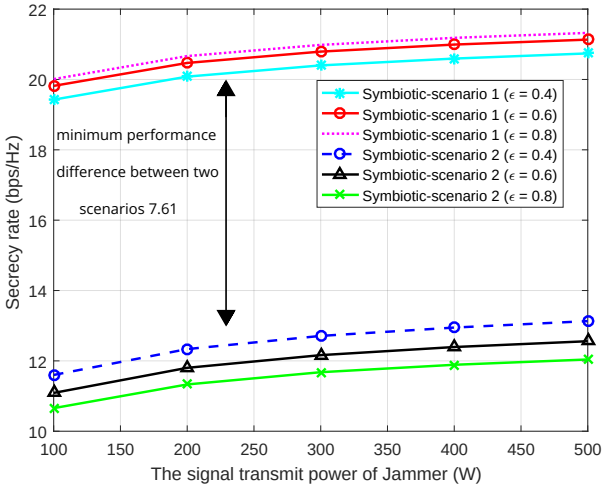

Fig. 5. Secrecy rate change according to signal transmission power of jammer.

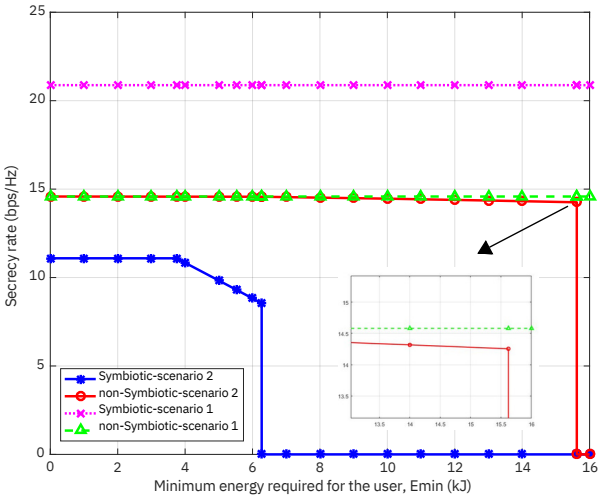

Fig. 6. Secrecy rate according to the change of the minimum energy level required for the user.

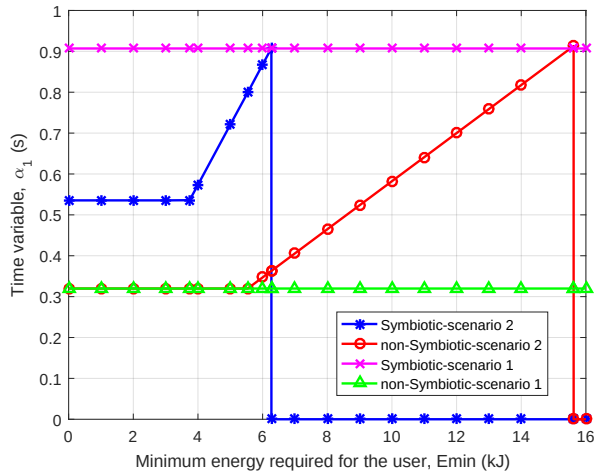

Fig. 7. The variation of the α_1 according to the change of the minimum energy level required for the user.

The change in secrecy rate according to the minimum energy level that the user must harvest in order to operate in active data transmission is shown in Fig. 6. In the simulation, $R_1^+ = 5$ bps/Hz and $R_2^+ = 2$ bps/Hz are set. First, let's give some critical numerical values in the Fig. 6. In symbiotic scenario 2, while $R_{\text{sec}} = 11.1$ bps/Hz at $E_{\min} = 0$, $R = 0$ after $E_{\min} = 6.27$ kJ. After $E_{\min} = 3.742$ kJ, the R_{sec} value begins to decrease. In non-symbiotic scenario 2, while $R_{\text{sec}} = 14.58$ bps/Hz at $E_{\min} = 0$, $R_{\text{sec}} = 0$ after $E_{\min} = 15.62$ kJ. After $E_{\min} = 5.54$ kJ, a very small decrease in the R_{sec} value begins and this decrease continues until $R_{\text{sec}} = 14.25$ bps/Hz. In symbiotic scenario 2, R_{sec} is constant up to $E_{\min} = 3.74$ kJ. Because, in $R_a^{(1)} \geq R_1^+$ inequality, the minimum value of α_1 will have is 0.54. Since the minimum value of α_1 remains below 0.54 in the energy constraint up to $E_{\min} = 3.74$ kJ, the result does not change and R_{sec} remains constant. After the critical value of $E_{\min} = 3.74$ kJ, α_1 changes and its value is determined according to the energy constraint. At $E_{\min} = 3.74$ kJ, $\alpha_1 = 0.54$ s, $\alpha_2 = 0.46$ s are found and $R_{\text{sec}} = 11.08$ bps/Hz is obtained. These values were solved under $R_a^{(1)} \geq R_1^+$, $R_a^{(2)} \geq R_2^+$ constraints. After $E_{\min} = 3.74$ kJ, R_{sec} starts to decrease. As the $E_{\min}$ value increases, the amount of energy the user needs to harvest increases, so α_1 time increases and α_2 time decreases. As α_2 time decreases, the number of bits actively transmitted by the user decreases and the R_{sec} value decreases. After $E_{\min} = 6.27$ kJ, the problem cannot be solved because the $R_a^{(2)} \geq R_2^+$ constraint cannot be met. Therefore, the maximum $E_{\min}$ value that can be set by the system user is 6.27 kJ. In non-symbiotic scenario 2, the user does not serve in transmitting the SE's data and $\epsilon = 0$ is set. The user becomes passive and harvest energy duration α_1. E_{a} becomes higher due to the equation $E_{\text{a}} = P_{\text{S}}(1-\epsilon)\alpha_1 + P_{\text{j}}(\alpha_1 + \alpha_2)$. Therefore, the $E_{\min}$ interval in which the problem is solved in the $E_{\min} \leq E_{\text{a}}$ constraint is at higher levels than in symbiotic scenario 2. For non-symbiotic scenario 2, a very small decrease begins after $E_{\min} = 5.54$ kJ. There is no solution to the problem after $E_{\min} = 15.62$ kJ. The performance decrease in non-symbiotic scenario 2 is much slower than in symbiotic scenario 2. If we evaluate non-symbiotic scenario 1 and symbiotic scenario 1, it can easily be said that the value of R_{sec} remains constant since neither of them have an energy constraint in solving the problem.

In Fig. 7, time α_1 is shown according to the change of $E_{\min}$ value. The results can be evaluated together with the findings in Fig. 6. Since there is no energy constraint in symbiotic scenario 1 and non-symbiotic scenario 1, the α_1 value is constant. As seen in Fig. 6, the R_{sec} value is constant. In symbiotic scenario 2, α_1 is constant up to $E_{\min} = 3.74$ kJ. From this value α_1 increases until $E_{\min} = 6.27$ kJ as α_1 time must be increased in order to obtain the minimum energy level required for the user. As a result, the R_{sec} value decreases. After $E = 6.27$ kJ, $R_{\text{sec}} = 0$ as $R_a^{(1)} \geq R_1^+$ and $R_a^{(2)} \geq R_2^+$ constraints are not met. In non-symbiotic scenario 2, while α_1 was constant until $E_{\min} = 5.54$ kJ, then an increase was observed. As can be seen in Fig. 6, there is a slight decrease in R_{sec} after $E_{\min} = 5.54$ kJ. Since there is no solution to the problem after $E_{\min} = 15.62$ kJ, $\alpha_1 = 0$.

Figure 8 shows secrecy rate according to the change of the coefficient of imperfect SIC. In the simulation, $R_1^+ = 5$ bps/Hz and $R_2^+ = 2$ bps/Hz are set. At $k_i = 0$, symbiotic scenario 2 ($E_{\min} = 0$) shows the same performance as symbiotic scenario 1 and $R_{\text{sec}} = 20.87$ bps/Hz. For symbiotic scenario 2 ($E_{\min} = 5$ kJ) $R_{\text{sec}} = 20.66$ bps/Hz at $k_i = 0$. At $k_i = 0.9$, $R_{\text{sec}} = 10.24$ bps/Hz for symbiotic scenario 2 ($E_{\min} = 0$), while $R_{\text{sec}} = 9.23$ bps/Hz for symbiotic scenario 2 ($E_{\min} = 5$ kJ). Since symbiotic scenario 1 has perfect SIC, $k_i = 0$. Since there is no k_i in the equations considered in this scenario, the system performance does not change and $R = 20.87$ bps/Hz. Symbiotic-scenario 2 ($E_{\min} = 0$) showed better performance than symbiotic scenario 2 ($E_{\min} = 5$ kJ) in all cases. As the increase of $E_{\min}$ increases the value of α_1, the number of bits transmitted by the user via traditional communication decreases. This performance degradation can be better understood with the results in Fig. 6. As seen in (16), k_i is included in the denominator.

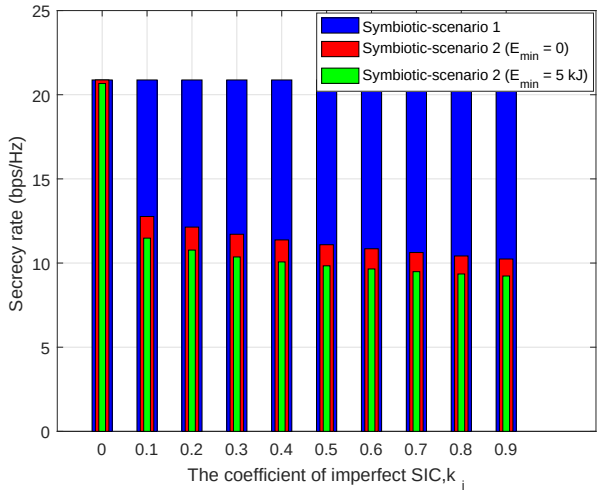

Fig. 8. Secrecy rate according to the change of the coefficient of imperfect SIC.

Therefore, every increase in k_i reduces system performance. The reason for the high performance difference for R_{sec} between $k_i = 0$ and $k_i = 0.1$ is the existence of $\sigma_{\text{R}}^2 + [P_{\text{S}} \epsilon |g_{\text{U-R}}\, g_{\text{S-U}}|^2 a k_i]$ and $\sigma_{\text{R}}^2 + [P_{\text{S}} |g_{\text{S-R}}|^2 k_i]$ equations. Since $\sigma_{\text{R}}^2 = -38.74$ dBW is accepted in these equations, the denominator increases and R_{sec} decreases significantly due to the fact that $[P_{\text{S}} \epsilon |g_{\text{U-R}}\, g_{\text{S-U}}|^2 a k_i]$ and $[P_{\text{S}} |g_{\text{S-R}}|^2 k_i]$ are more dominant than σ_{R}^2 at a value other than 0. However, in the case of $[P_{\text{S}} \epsilon |g_{\text{U-R}}\, g_{\text{S-U}}|^2 a k_i] = [P_{\text{S}} |g_{\text{S-R}}|^2 k_i] = 0$ (if $k_i = 0$), there is a significant increase in R_{sec} since the σ_{R}^2 value remains very small in the denominator. As a matter of fact, the difference in secrecy rate between $k_i = 0$ and $k_i = 0.1$ is approximately 8 bps/Hz.

5. Conclusions and Future Work

In this work, PLS analysis is performed for an SRN containing the SE, user, jammer, receiver and ED. The system model is considered in two different scenarios. In the first scenario, the secrecy rate was maximized by using the perfect SIC technique. In the second scenario, the secrecy rate is maximized by assuming that the imperfect SIC technique is used at the receiver and there is an energy constraint for the user in the system. The secrecy rate according to the system parameters was tested for different situations. Numerical results show that having a symbiotic relationship between the user and the SE increases the secrecy rate of the system compared to the non-symbiotic situation. Adopting the perfect SIC technique at the receiver without energy constraint at the user results in a significant increase in PLS performance compared to imperfect SIC under energy constraint.

References

[1] DANG, S., AMIN, O., SHIHADA, B. What should 6G be? *Nature Electronics*, 2020, vol. 3, p. 20–29. DOI: 10.1038/s41928-019-0355-6

[2] DANGI, R., CHOUDHARY, G., DRAGONI, N., et al. 6G mobile networks: Key technologies, directions, and advances. *Telecom*, 2023, vol. 4, no. 4, p. 836–876. DOI: 10.3390/telecom4040037

[3] ALSABAH, M., NASER, M. A., MAHMMOD, B. M., et al. 6G wireless communications networks: A comprehensive survey. *IEEE Access*, 2021, vol. 9, p. 148191–148243. DOI: 10.1109/ACCESS.2021.3124812

[4] AKYILDIZ, I. F., KAK, A., NIE, S. 6G and beyond: The future of wireless communications systems. *IEEE Access*, 2020, vol. 8, p. 133995–134030. DOI: 10.1109/ACCESS.2020.3010896

[5] IHS MARKIT. *The Internet of Things: A Movement, Not a Market*. 9 pages. [Online] Available at: https://cdn.ihs.com/www/pdf/IoT_ebook.pdf

[6] JANJUA, M. B., ARSLAN, H. A survey of symbiotic radio: Methodologies, applications, and future directions. *Sensors*, 2023, vol. 23, no. 5, p. 1–26. DOI: 10.3390/s23052511

[7] ONAY, M. Y., ERTUG, O. Ambient backscatter communication based cooperative relaying for heterogeneous cognitive radio networks. *Radioengineering*, 2023, vol. 32, no. 2, p. 236–247. DOI: 10.13164/re.2023.0236

[8] ONAY, M. Y., ERTUG, O. Performance analysis under signal jammer in relay aided ambient backscatter cognitive radio networks. In *31st Signal Processing and Communications Applications Conference (SIU)*. Istanbul (Turkey), 2023, p. 1–4. DOI: 10.1109/SIU59756.2023.10223915

[9] AKYILDIZ, I. F., LEE, W.-Y., VURAN, C., et al. A survey on spectrum management in cognitive radio networks. *IEEE Communications Magazine*, 2008, vol. 46, no. 4, p. 40–48. DOI: 10.1109/MCOM.2008.4481339

[10] GOEL, S., NEGI, R. Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications*, 2008, vol. 7, no. 6, p. 2180–2189. DOI: 10.1109/TWC.2008.060848

[11] FURQAN, H. M., SOLAIJA, M. S. J., TURKMEN, H., et al. Wireless communication, sensing, and REM: A security perspective. *IEEE Open Journal of the Communications Society*, 2021, vol. 2, p. 287–321. DOI: 10.1109/OJCOMS.2021.3054066

[12] SOLAIJA, M. S. J., SALMAN, H., ARSLAN, H. Towards a unified framework for physical layer security in 5G and beyond networks. *IEEE Open Journal of Vehicular Technology*, 2022, vol. 3, p. 321–343. DOI: 10.1109/OJVT.2022.3183218

[13] HAMAMREH, J. M., FURQAN, H. M., ARSLAN, H. Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. *IEEE Communications Surveys-Tutorials*, 2019, vol. 21, no. 2, p. 1773–1828. DOI: 10.1109/COMST.2018.2878035

[14] HAN, Y., LIU, Y., ZHANG, T., et al. Artificial noise aided secure NOMA communications in STAR-RIS networks. *IEEE Wireless Communications Letters*, 2022, vol. 11, no. 6, p. 1191–1195. DOI: 10.1109/LWC.2022.3161020

[15] ZHANG, S., SUN, W., LIU, J., et al. Physical layer security in large scale probabilistic caching: Analysis and optimization. *IEEE Communications Letters*, 2019, vol. 23, no. 9, p. 1484–1487. DOI: 10.1109/LCOMM.2019.2926967

[16] LIU, J., LIU, Z., ZENG, Y., et al. Cooperative jammer placement for physical layer security enhancement. *IEEE Network*, 2016, vol. 30, no. 6, p. 56–61. DOI: 10.1109/MNET.2016.1600119NM

[17] WANG, H.-M., ZHENG, T., XIA, X.-G. Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading. *IEEE Transactions on Wireless Communications*, 2015, vol. 14, no. 1, p. 94–106. DOI: 10.1109/TWC.2014.2332164

[18] WANG, H.-M., WANG, C., NG, D. W. K. Artificial noise assisted secure transmission under training and feedback. *IEEE Transactions on Signal Processing*, 2015, vol. 63, no. 23, p. 6285–6298. DOI: 10.1109/TSP.2015.2465301

[19] LIAO, W.-C., CHANG, T.-H., MA, W.-K. QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial noise-aided approach. *IEEE Transactions on Signal Processing*, 2011, vol. 59, no. 3, p. 1202–1216. DOI: 10.1109/TSP.2010.2094610

[20] KAIKAI, C., SUN, J., ZHANG, S., et al. Secrecy rate maximization for multicarrier-based cognitive radio networks with an energy harvesting jammer. *IEEE Sensors Journal*, 2023, vol. 23, no. 3, p. 3220–3232. DOI: 10.1109/JSEN.2022.3226199

[21] LI, X., JIANG, J., WANG, H., et al. Physical layer security for wireless-powered ambient backscatter cooperative communication networks. *IEEE Transactions on Cognitive Communications and Networking*, 2023, vol. 9, no. 4, p. 927–939. DOI: 10.1109/TCCN.2023.3270425

[22] GUO, Y., WANG, G., XU, R., et al. Capacity analysis for wireless symbiotic communication systems with BPSK tags under sensitivity constraint. *IEEE Communications Letters*, 2022, vol. 26, no. 1, p. 44–48. DOI: 10.1109/LCOMM.2021.3125342

[23] WU, N., ZHOU, X., SUN, M. Secure transmission with guaranteed user satisfaction in heterogeneous networks: A two-level Stackelberg game approach. *IEEE Transactions on Communications*, 2018, vol. 66, no. 6, p. 2738–2750. DOI: 10.1109/TCOMM.2018.2801790

[24] WU, H., TAO, X., HAN, Z., et al. Secure transmission in MISOME wiretap channel with multiple assisting jammers: Maximum secrecy rate and optimal power allocation. *IEEE Transactions on Communications*, 2017, vol. 65, no. 2, p. 775–789. DOI: 10.1109/TCOMM.2016.2636288

[25] LIANG, W., WEN, S., NG, S. X., et al. Utility-based cooperative resource sharing in symbiotic-radio-aided internet of things networks. *IEEE Internet of Things Journal*, 2023, vol. 10, no. 22, p. 19368–19384. DOI: 10.1109/JIOT.2022.3229089

[26] AL-NAHARI, A., JANTTI, R., ZHENG, G., et al. Ergodic secrecy rate analysis and optimal power allocation for symbiotic radio networks. *IEEE Access*, 2023, vol. 11, p. 82327–82337. DOI: 10.1109/ACCESS.2023.3301186

[27] YEGANEH, R. S., OMIDI, M. J., GHAVAMI, M. Multi-BD symbiotic radio-aided 6G IoT network: Energy consumption optimization with QoS constraint approach. *IEEE Transactions on Green Communications and Networking*, 2023, vol. 7, no. 4, p. 2067–2080. DOI: 10.1109/TGCN.2023.3281460

[28] DURSUN, Y., WANG, K., DING, Z. Secrecy sum rate maximization for a MIMO-NOMA uplink transmission in 6G networks. *Physical Communication*, 2022, vol. 53, p. 1–7. DOI: 10.1016/j.phycom.2022.101675

[29] HEMA, P. P., BABU, A. V. Full-duplex jamming for physical layer security improvement in NOMA-enabled overlay cognitive radio networks. *Security and Privacy*, 2024, vol. 7, no. 3. DOI: 10.1002/spy2.371

[30] JU, H., ZHANG, R. Throughput maximization in wireless powered communication networks. *IEEE Transactions on Wireless Communications*, 2014, vol. 13, no. 1, p. 418–428. DOI: 10.1109/TWC.2013.112513.130760

[31] KANG, X. P., HO, C. K., SUN, S. Full-duplex wireless-powered communication network with energy causality. *IEEE Transactions on Wireless Communications*, 2015, vol. 14, no. 10, p. 5539–5551. DOI: 10.1109/TWC.2015.2439673

[32] DIAMANTOULAKIS, P. D., PAPPI, K. N., DING, Z., et al. Wireless-powered communications with non-orthogonal multiple access. *IEEE Transactions on Wireless Communications*, 2016, vol. 15, no. 12, p. 8422–8436. DOI: 10.1109/TWC.2016.2614937

[33] LIU, X., LIN, Z., ZHENG, K., et al. Optimal time allocation for backscatter-aided relay cooperative transmission in wireless-powered heterogeneous CRNs. *IEEE Internet of Things Journal*, 2023, vol. 10, no. 18, p. 16209–16224. DOI: 10.1109/JIOT.2023.3267456

[34] HOANG, D. T., NIYATO, D., WANG, P., et al. Ambient backscatter: A new approach to improve network performance for RF-powered cognitive radio networks. *IEEE Transactions on Communications*, 2017, vol. 65, no. 9, p. 3659–3674. DOI: 10.1109/TCOMM.2017.2710338

About the Authors . . .

Muhammed Yusuf ONAY was born in Batman, Turkey in 1992. He received his M.Sc. from Hacettepe University in 2019 and Ph.D. from Gazi University in 2023. His research interests include ambient backscatter communication, symbiotic radio networks, internet of things, 5G and beyond, 6G technology, cognitive radio networks, wireless communication, signal processing. He is currently a Dr. Research Assistant in Electrical and Electronics Engineering at Hitit University, Corum, Turkey.