Space-time block code based cooperative physical layer security schemes for LEO Satellite Systems

Heyin Lee and Sooyoung Kim
IT Convergence Research Center, Div. of Elec. Eng.
Jeonbuk National University
Jeonju, Republic of Korea
{leehyein96, sookim}@jbnu.ac.kr

***Abstract*—LEO satellite communication systems can be powerful and effective means to provide 6G services as a component of non-terrestrial networks. In this paper, we propose efficient cooperative and secure diversity schemes which can provide performance enhancement as well as high security protection. In the proposed scheme, multiple LEO satellites with terrestrial repeaters cooperatively transmit signals using various space-time block codes with physical layer security capability.**

***Index Terms*—LEO satellite, physical layer security, MIMO, artificial noise**

I. Introduction

Satellite networks as a part of non-terrestrial networks (NTNs) will be a key component to provide cost-effective and high-capacity connectivity in future 6th generation (6G) wireless networks [1]. Especially, low earth orbit (LEO) satellite communications will play an important role in realizing anywhere anytime connectivity capability [2]. Despite their advantages, an emerging concern for LEO satellite communications is their vulnerability to security threats due to their broadcasting nature and extensive coverage area [3].

Given that traditional encryption techniques entail additional complexity and energy for computations, the concept of physical layer security (PLS) has garnered attention as an effective means to achieve high confidentiality in 6G systems without a significant increase in complexity. Notably, several studies have reported results on PLS-aided multi-antenna schemes that provide authorized receivers access to information with diversity gains and security protection [4–9]. However, previous research has primarily focused on terrestrial network scenarios, assuming the lack of line of sight (LoS), a key feature of satellite communication, and correlation between the main channel and the wiretap channel.

In this paper, we propose efficient cooperative PLS schemes for LEO satellite systems, taking into consideration LoS and correlation effects. In the proposed method, LEO satellites and terrestrial repeaters collaboratively transmit signals encoded using space-time block coding (STBC) schemes with security protection capability. The simulation results demonstrate that the proposed method can achieve high security protection without significant performance degradation or additional power consumption.

This research was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (NRF-2021R1A2C1003121).

II. Related Works

PLS leverages the distinction in channel conditions experienced by authorized receivers and potential eavesdroppers due to their varying locations. In most of the researches on PLS, it was assumed that the legitimate communication parties, Alice and Bob share the channel characteristics, enabling Bob to differentiate between genuine information and the purposeful distortion introduced by Alice. These assumptions can be employed to guarantee that Bob obtains signals of superior quality relative to Eve.

A. Artificial noise-aided PLS

One of the representative techniques among PLS schemes is artificial noise (AN) which causes serious interference to the illegal eavesdropper [4–8]. One strategy to generate artificial noise (AN) involves utilizing the null space of the main channel condition. In this scenario, transmitter embeds AN into the information, which then becomes nullified as it traverses the signal path to legitimate receiver. Consequently, intended receiver extracts only the AN-free signal, as if no PLS scheme had been employed. However, for eavesdropper, AN cannot be eliminated due to the differing channel conditions. As a result, AN functions as interference, disrupting signal detection for eavesdropper. In the AN method, the power ratio assigned to information and AN plays a crucial role in determining the level of secrecy achieved. While allocating a significant portion of power to AN can effectively thwart information leakage to eavesdropper, it simultaneously results in an energy inefficiency in terms of communication capacity. This inefficiency arises from the fact that AN is a component that ultimately gets nullified at the end of Bob. Another inefficiency of AN lies in its contribution to a high peak-to-average power ratio (PAPR), attributed to its reliance on the random distribution of channel conditions.

B. Phase distorting PLS

In order to solve the problems of the AN-aided method, phase distorting (PD) PLS method is introduced. The PD technique exclusively operates in the phase domain by capitalizing on the phase of the channel condition. Transmitter

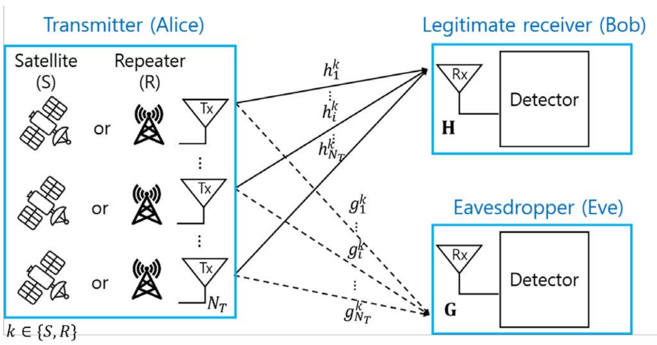

Fig. 1. System configuration for the LEO satellite communication.

combines signal and a phase distortion factor that represents the inverse of the channel phase information, allowing it to be nullified during transmission to intended recipient. However, illegal receiver is unable to separate the phase distortion factor from the signal, causing the entire received signal to be treated as noise. Moreover, thanks to the unit power of the phase distortion factor applied through multiplication to the information, there is no need for additional power consumption and PAPR problem as well. Therefore, the PD method takes the advantages of enhanced secrecy and power efficiency, mitigating the trade-off present in the AN approach [9].

III. Cooperative and Secure Diversity Scheme for LEO Systems

This paper proposes the above introduced PLS schemes, and introduces methods to apply to LEO systems. Figure 1 depicts the system configuration for the LEO satellite communications with the proposed scheme. In the system, we consider a main channel between a transmitter (Alice) and a legitimate receiver (Bob), and a wiretap channel including Alice and a passive eavesdropper (Eve). In addition, Alice in our system model forms N_T transmitters consisting of either LEO satellites (S) and/or repeaters (R). Here, we assume that Alice and Bob share the channel state information. In the proposed scheme, N_T transmitters cooperatively encode the $N_\mathrm{T} \times 1$ information vector $\mathbf{s}$ for p time periods, followed by linear operations for PLS. Upon the $p \times N_\mathrm{T}$ STBC encoded signal matrix, $\mathbf{S}$, a linear operator transforms it to $\mathbf{S}'$ for PLS.

A. Application example of AN-aided PLS scheme

As a simple example, we use a simple 2×2 O-STBC system, commonly known as the Alamouti code, and present how AN is designed for security protection. For the scenario where $N_\mathrm{T} = 2$, the information vector is $\mathbf{s} = [s_1, s_2]^T$ is encoded using Alamouti code, as follows [10]:

$$\mathbf{S} = \begin{bmatrix} s_1 & s_2 \\ -s_2^* & s_1^* \end{bmatrix}, \tag{1}$$

where x^* denotes the complex conjugate of the signal x. The AN matrix $\mathbf{W}$ is formulated in the null space of the legitimate channel vector $\mathbf{h} = [h_1^k, \ldots, h_{N_\mathrm{T}}^k]^T$ where h_i^k represents the channel gain from i-th transmit antenna to Bob when $k \in \{\mathrm{S}, \mathrm{R}\}$. An example of a possible $\mathbf{W}$ can be expressed as follows [6]:

$$\mathbf{W} = \begin{bmatrix} h_2^k \mu & -h_1^k \mu \\ -h_2^k \mu^* & h_1^k \mu^* \end{bmatrix}, \tag{2}$$

where μ denotes the complex Gaussian AN with zero-mean. Consequently, the transmission matrix that incorporates both the information signal and AN can be designed as follows:

$$\mathbf{S}' = \frac{1}{\sqrt{P_\mathrm{s} + P_\mathrm{w}}} \left(\mathbf{S} + \mathbf{W} \right), \tag{3}$$

where P_s and P_w represent the average power of information signal and AN, respectively.

The AN design ensures its nullification as it traverses the main channel, allowing Bob to receive a decipherable signal $\mathbf{y}_\mathrm{B}$ as follows:

$$\begin{aligned} \mathbf{y}_\mathrm{B} &= \mathbf{S}'\mathbf{h} + \mathbf{n}_\mathrm{B} \\ &= \frac{1}{\sqrt{P_\mathrm{s} + P_\mathrm{w}}} \mathbf{S}\mathbf{h} + \mathbf{n}_\mathrm{B} = \frac{1}{\sqrt{P_\mathrm{s} + P_\mathrm{w}}} \mathbf{H}\mathbf{s} + \mathbf{n}_\mathrm{B}, \end{aligned} \tag{4}$$

where $\mathbf{H}$ is the channel matrix between Alica and Bob. In contrast, Eve suffers from the effect of uncanceled AN, as follows:

$$\begin{aligned} \mathbf{y}_\mathrm{E} &= \mathbf{S}'\mathbf{g} + \mathbf{n}_\mathrm{E} \\ &= \frac{1}{\sqrt{P_\mathrm{s} + P_\mathrm{w}}} (\mathbf{G}\mathbf{s} + \mathbf{W}\mathbf{g}) + \mathbf{n}_\mathrm{E}, \end{aligned} \tag{5}$$

where $\mathbf{g}$ and $\mathbf{G}$ are the chennel vector and the channel matrix between Alice and Eve, respectively.

After receiving $\mathbf{y}_\mathrm{B}$ and $\mathbf{y}_\mathrm{E}$ at Bob and Eve, respectively, they perform a linear decoding process to retrieve the information $\hat{\mathbf{s}}_\mathrm{B}$ and $\hat{\mathbf{s}}_\mathrm{E}$ as follows:

$$\begin{aligned} \hat{\mathbf{s}}_\mathrm{B} &= \frac{1}{\sum_i^{N_\mathrm{T}} |h_i^k|^2} \mathbf{H}^H \mathbf{y}_\mathrm{B} = \frac{1}{\sqrt{P_\mathrm{s} + P_\mathrm{w}}} \mathbf{s} + \frac{1}{\sum_i^{N_\mathrm{T}} |h_i^k|^2} \mathbf{H}^H \mathbf{n}_\mathrm{B}, \\ \hat{\mathbf{s}}_\mathrm{E} &= \frac{1}{\sum_i^{N_\mathrm{T}} |g_i^k|^2} \mathbf{G}^H \mathbf{y}_\mathrm{E} \\ &= \frac{1}{\sqrt{P_\mathrm{s} + P_\mathrm{w}}} \mathbf{s} + \frac{1}{\sum_i^{N_\mathrm{T}} |g_i^k|^2} \mathbf{G}^H \left(\frac{1}{\sqrt{P_\mathrm{s} + P_\mathrm{w}}} \mathbf{W}\mathbf{g} + \mathbf{n}_\mathrm{E} \right), \end{aligned} \tag{6}$$

where $(\mathbf{X})^H$ is the Hermitian operator of matrix $\mathbf{X}$. Note that the AN matrix $\mathbf{W}$ acts as a severe interference to Eve. Due to this added interference to the existing AWGN, Eve faces much stronger noise impact compared to Bob. We note that this principle of adding An can be applied to any kind of existing STBC schemes with $N_T > 2$.

B. Application example of PD-aided PLS scheme

While we discuss an example using an O-STBC system with $N_\mathrm{T} = 4$, it is important to note that the PD scheme is not confined to specific transmit antenna sizes as like AN-aided scheme. A key distinction between the PD and the AN methods is that the PD scheme employs real-numbered O-STBC matrices, even when the transmit signals are complex

[9]. For example, 4×4 real-numbered O-STBC matrix $\mathbf{S}$ can be expressed as follows [11]:

$$\mathbf{S} = \begin{bmatrix} s_1 & s_2 & s_3 & s_4 \\ -s_2 & s_1 & -s_4 & s_3 \\ -s_3 & s_4 & s_1 & -s_2 \\ -s_4 & -s_3 & s_2 & s_1 \end{bmatrix}. \quad (7)$$

In the PD scheme, $\mathbf{S}'$ is constructed by using phase of channel information in a way that the phase distortion factor $\theta_i = e^{-j\angle h_i^k}$ can be nullified as it traverses the main channel path. as it traverses the main channel path. Therefore, $\mathbf{S}'$ for PD can be designed as follows [9]:

$$\mathbf{S}' = \begin{bmatrix} \theta_1 s_1 & \theta_2 s_2 & \theta_3 s_3 & \theta_4 s_4 \\ -\theta_1 s_2 & \theta_2 s_1 & -\theta_3 s_4 & \theta_4 s_3 \\ -\theta_1 s_3 & \theta_2 s_4 & \theta_3 s_1 & -\theta_4 s_2 \\ -\theta_1 s_4 & -\theta_2 s_3 & \theta_3 s_2 & \theta_4 s_1 \end{bmatrix} \quad (8)$$

The received signals at Bob and Eve can then be represented as follows:

$$\begin{aligned} \mathbf{y}_{\mathrm{B}} &= \mathbf{S}'\mathbf{h} + \mathbf{n}_{\mathrm{B}} = \mathbf{H}_{\mathrm{PD}}\mathbf{s} + \mathbf{n}_{\mathrm{B}}, \\ \mathbf{y}_{\mathrm{E}} &= \mathbf{S}'\mathbf{g} + \mathbf{n}_{\mathrm{E}} = \mathbf{G}_{\mathrm{PD}}\mathbf{s} + \mathbf{n}_{\mathrm{E}}, \end{aligned} \quad (9)$$

where $\mathbf{H}_{\mathrm{PD}}$ is a channel matrix comprised solely of the amplitudes of the legitimate channel information, and $\mathbf{G}_{\mathrm{PD}}$ is a phase distorted channel matrix at Eve. The phase distortion factor θ_i, which is the inverse phase of the legitimate channel, i.e., $\theta_i h_i^k = e^{-j\angle h_i^k} e^{j\angle h_i^k} |h_i^k| = |h_i^k|$. For instance, when $N_{\mathrm{T}} = 4$, $\mathbf{H}_{\mathrm{PD}}$ and $\mathbf{G}_{\mathrm{PD}}$ are given by:

$$\begin{aligned} \mathbf{H}_{\mathrm{PD}} &= \begin{bmatrix} |h_1^k| & |h_2^k| & |h_3^k| & |h_4^k| \\ |h_2^k| & -|h_1^k| & |h_4^k| & -|h_3^k| \\ |h_3^k| & -|h_4^k| & -|h_1^k| & |h_2^k| \\ |h_4^k| & |h_3^k| & -|h_2^k| & -|h_1^k| \end{bmatrix}, \\ \mathbf{G}_{\mathrm{PD}} &= \begin{bmatrix} \theta_1 g_1^k & \theta_2 g_2^k & \theta_3 g_3^k & \theta_4 g_4^k \\ \theta_2 g_2^k & -\theta_1 g_1^k & \theta_4 g_4^k & -\theta_3 g_3^k \\ \theta_3 g_3^k & -\theta_4 g_4^k & -\theta_1 g_1^k & \theta_2 g_2^k \\ \theta_4 g_4^k & \theta_3 g_3^k & -\theta_2 g_2^k & -\theta_1 g_1^k \end{bmatrix}, \end{aligned} \quad (10)$$

where $|x|$ indicates the absolute value of complex x.

After receiving $\mathbf{y}_{\mathrm{B}}$ and $\mathbf{y}_{\mathrm{E}}$ at Bob and Eve, respectively, they perform a linear decoding process to retrieve information $\hat{\mathbf{s}}_{\mathrm{B}}$ and $\hat{\mathbf{s}}_{\mathrm{E}}$, as follows:

$$\begin{aligned} \hat{\mathbf{s}}_{\mathrm{B}} &= \frac{1}{\sum_i^{N_{\mathrm{T}}} |h_i^k|^2} \mathbf{H}_{\mathrm{PD}}^H \mathbf{y}_{\mathrm{B}} = \mathbf{s} + \frac{1}{\sum_i^{N_{\mathrm{T}}} |h_i^k|^2} \mathbf{H}_{\mathrm{PD}}^H \mathbf{n}_{\mathrm{B}}, \\ \hat{\mathbf{s}}_{\mathrm{E}} &= \frac{1}{\sum_i^{N_{\mathrm{T}}} |g_i^k|^2} \mathbf{G}^H \mathbf{y}_{\mathrm{E}} = \frac{1}{\sum_i^{N_{\mathrm{T}}} |g_i^k|^2} \mathbf{G}^H (\mathbf{G}_{\mathrm{PD}}\mathbf{s} + \mathbf{n}_{\mathrm{E}}). \end{aligned} \quad (11)$$

Since $\mathbf{G}_{\mathrm{PD}}$ incorporates the phase distortion factor unknown to Eve, signal decoding becomes challenging when the PD method is applied.

IV. Simulation results

We estimate the performance of the proposed scheme under two different environments. In the first case, we assume rural environments where the user terminal has comparatively good line of sight (LOS) conditions with multiple satellites. On the other hand, the second case assumes (sub)urban environments where the user terminal is able to receive multiple signals in combination of satellites and repeaters with 50% of probability respectively. In the simulations, we assumed that the channel gains from repeaters, h_i^{R} and g_i^{R}, are modeled by a frequency flat Rayleigh fading. On the other hand, the channel gains from LEO satellites, h_i^{S} and g_i^{S}, are modeled by a Rician fading with a random Rician factor, $K \in [0, 20]$.

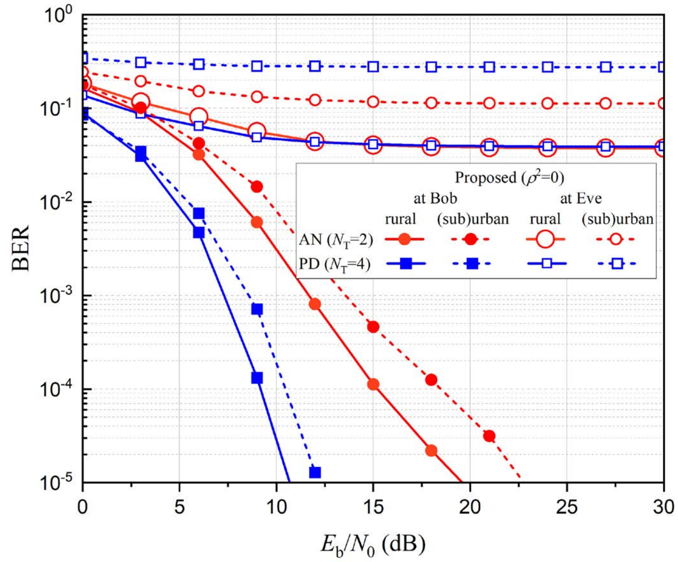

Fig. 2. BER performance comparison for the proposed methods.

First, we compare the BER performance of the proposed PLS schemes applied to LEO systems in Figure 2. In the figure legend, AN and PD indicate AN and PD-aided PLS schemes introduced in Section III, respectively. The results clearly shows that the proposed methods invoke significant performance degradation to Eve, and ensuring security protection. In rural area, Bob has a better performance than the one in (sub)urban area due to prevailed LOS conditions. However, this LOS condition also enables Eve to have a better performance. Among two PLS schemes, PD-aided scheme shows much better security protection providing better performance to Bob as well as inducing worse performance to Eve. This is because the PD method in this investigation employed a larger number of antenna than the AN method, and it did not require further power allocation.

In addition, we should consider the correlation coefficient ρ between Bob and Eve when the satellite signal was received because of wide satellite beam coverage. Therefore, h_i^{S} and g_i^{S} can be modeled as follows [12]:

$$\begin{aligned} h_i^{\mathrm{S}} &= \sqrt{\frac{K}{K+1}} + \sqrt{\frac{1}{K+1}} z_{1,i} \\ g_i^{\mathrm{S}} &= \sqrt{\frac{K}{K+1}} + \sqrt{\frac{1}{K+1}} \left(\sqrt{\rho^2} z_{1,i} + \sqrt{1-\rho^2} z_{2,i} \right) \end{aligned} \quad (12)$$

where $z_{1,i}$ and $z_{2,i}$ are two complex normal random variables with zero mean and unit variance from the i-th LEO satellite. Note that for $K = 0$, the scenario reduces to the case of Rayleigh fading.

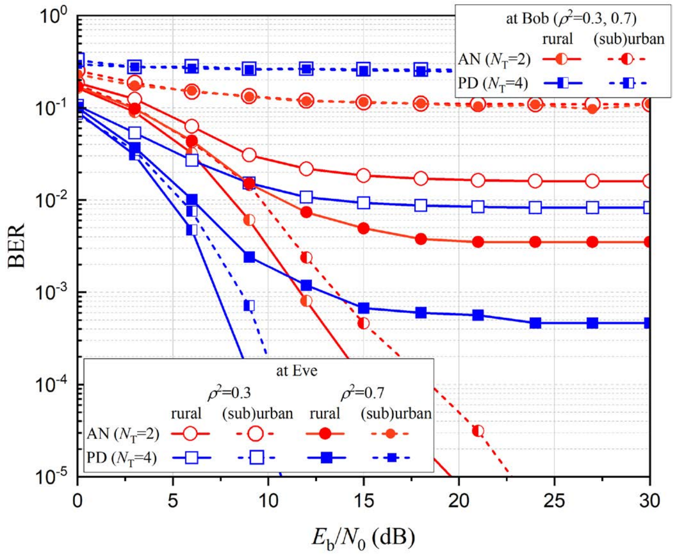

Fig. 3. BER performance comparison according to the correlation effect.

Figure 3 shows that the BER performance comparison when $\rho^2 = 0.3$ and 0.7. As far as the security protection is concerned, rural environment is difficult to utilize the PLS schemes. Even though Eve may have similar performance to Bob at low signal to noise ratio (SNR) range, due to comparatively close correlation in rural areas, her performance certainly shows error floors. Therefore, she cannot retrieve proper information even with very high SNR . Among two PLS schemes, the PD-aided method is particularly vulnerable to the correlation effect.

On the other hand, the proposed method efficiently works in (sub)urban environments by taking advantages of the diversities gained from the terrestrial repeaters. Although, the performance at Bob deteriorates in (sub)urban areas, Bob can certainly have better security protection as BER performance degradation at Eve is so serious regardless of ρ^2 values. In the main paper, we will provide extensive simulation results under various conditions, analyze the results in various aspects, and discuss the practical application to the satellite systems.

V. Conclusions

In this paper, we proposed efficient cooperative and secure diversity schemes for LEO satellite communication systems. The simulation results showed that the proposed method can achieve a high level of secrecy performance without decreasing power efficiency. Even though prevailed LOS condition with high level of channel correlation between the main and wiretap channels degraded the security performance, the proposed scheme succeeded to invoke error floor at the eavesdropper channel, thereby preventing from information leakage.

References

[1] M. Giordani and M. Zorzi, "Non-terrestrial networks in the 6g era: Challenges and opportunities," *IEEE Network*, vol. 35, no. 2, pp. 244–251, 2020.

[2] E. Yaacoub and M.-S. Alouini, "A key 6g challenge and opportunity—connecting the base of the pyramid: A survey on rural connectivity," *Proceedings of the IEEE*, vol. 108, no. 4, pp. 533–582, 2020.

[3] A. K. Yerrapragada, T. Eisman, and B. Kelley, "Physical layer security for beyond 5g: Ultra secure low latency communications," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 2232–2242, 2021.

[4] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE vehicular technology conference*, vol. 62, no. 3. Citeseer, 2005, p. 1906.

[5] P. Shang, W. Yu, K. Zhang, X.-Q. Jiang, and S. Kim, "Secrecy enhancing scheme for spatial modulation using antenna selection and artificial noise," *Entropy*, vol. 21, no. 7, p. 626, 2019.

[6] P. Shang, S. Kim, and X.-Q. Jiang, "Efficient alamouti-coded spatial modulation for secrecy enhancing," in *2019 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2019, pp. 860–864.

[7] T. Allen, A. Tajer, and N. Al-Dhahir, "Secure alamouti multiple access channel transmissions: Multiuser transmission and multi-antenna eavesdroppers," *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1510–1513, 2019.

[8] P. Yang, X. Qiu, and F. Mu, "Artificial noise-aided secure generalized spatial modulation for multiuser transmission," *IEEE Communications Letters*, vol. 24, no. 11, pp. 2416–2420, 2020.

[9] H. Lee, S. Chan, and S. Kim, "Efficient mimo signal predistortion for secrecy-enhancing," *Electronics*, vol. 11, no. 9, p. 1425, 2022.

[10] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE Journal on selected areas in communications*, vol. 16, no. 8, pp. 1451–1458, 1998.

[11] V. Tarokh, H. Jafarkhani, and A. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1456–1467, 1999.

[12] A. Tarrías-Muñoz, J. L. Matez-Bandera, P. Ramírez-Espinosa, and F. J. López-Martínez, "Effect of correlation between information and energy links in secure wireless powered communications," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3780–3789, 2021.