Physical Layer Security in MIMO PLC Systems under the Presence of a Passive Eavesdropper

Pedro Henrique Sartorello, Evelio M. G. Fernandez, and Ândrei Camponogara

Abstract— **This paper investigates the physical layer security (PLS) of in-home and broadband multiple-input multiple-output (MIMO) power line communication (PLC) systems in the presence of a passive PLC eavesdropper. To this end, a MIMO-multiple eavesdroppers (MIMO-ME) PLC wiretap channel model is adopted, and the secrecy outage probability (SOP) is analyzed through numerical simulations. The results show that the multiple-input multiple-output (MIMO) approach significantly enhances the PLS compared to the single-input single-output (SISO) configuration. In particular, the MIMO-single eavesdropper (MIMO-SE) scenario consistently achieves the lowest SOP across different target secrecy rates and transmission power levels. The findings highlight the potential of MIMO to improve PLS in PLC systems.**

Keywords— **Power line communication, physical layer security, MIMO**

I. Introduction

Power line communication (PLC) is a mature and widespread technology with most applications related to medium- and low-voltage electric power grids (outdoor and indoor). The main advantage of PLC is the use of existing electrical power cables, which makes this technology particularly advantageous in environments where wireless channels are congested or physical accessibility is limited, which can be useful for emerging applications such as internet of things (IoT), industry 4.0, and smart grids [1].

Moreover, because of Kirchoff's laws, multiple-input multiple-output (MIMO) approach can also be adopted in PLC systems, taking advantage of the fact that typical indoor and outdoor electric power grids include three conductors (phase, neutral, and protective earth). Using more than two conductors effectively creates multiple independent propagation channels, allowing spatial multiplexing and diversity gains [2]. For instance, in [3], it is shown that the capacity of MIMO PLC system considering a transmitter equipped with two ports and a receiver with four ports is, on average, twice that of single-input single-output (SISO) in frequencies up to 100 MHz. In [4], the authors demonstrated a capacity increase up to 90% using a 2×2 MIMO configuration on typical three-wire indoor power lines. In addition, in [5], it was further demonstrated that the use of multiple conductors can produce substantial performance improvements over conventional SISO schemes when using precoding schemes. Therefore, it is evident that the MIMO approach can significantly boost data rates in PLC systems, improve link reliability through diversity, and extend coverage, making it a highly promising approach for next-generation broadband communication over existing electric power grid infrastructure.

However, due to the broadcast nature of PLC and the use of unshielded cables, this data communication technology is vulnerable to eavesdropping and unauthorized access. Additionally, any device connected to the electric power grid in which the PLC system operates could access private information. As an alternative to cryptography, which is computationally demanding and complex, physical layer security (PLS) can provide security within an information-theoretic context, exploring the random nature of the transmission channel. In this regard, in 1975, Wyner proved that secure communication at the physical layer level is possible whenever the signal-to-noise ratio (SNR) of the legitimate receiver outperforms the eavesdropper's SNR [6].

Several studies that investigated the PLS in PLC systems can be found in the literature. For instance, in [7], Camponogara *et al.* showed that an SISO broadband in-home PLC system can provide high values of secrecy outage probability when a malicious PLC device tries to eavesdrop private messages. Next, in [8], the authors evaluated the effective secrecy throughput and provided the respective wiretap code rates when an in-home and broadband PLC systems is threatened by three type of passive malicious device: PLC device, wireless device, and hybrid PLC/wireless device. In [9], Pitollo *et al.* assessed the achievable secrecy rate for in-home and broadband PLC systems under the presence of a malicious PLC device. In [10], the authors investigated the PLS for MIMO PLC systems threatened by a malicious MIMO PLC device in terms of secrecy achievable rate, assuming that the transmitter has available the instantaneous channel state information (CSI) of both the legitimate and malicious PLC devices. They concluded that multiple conductors allowed for simultaneously boosting data rates and enhancing confidentiality.

To the best of the Authors knowledge, there is no study in the literature that investigates the PLS for MIMO PLC system in the presence of a passive malicious MIMO PLC device, i.e., the legitimate transmitter does not have access to instantaneous CSI of the malicious device. Therefore, this paper investigates the secrecy outage probability (SOP) of an in-home and broadband MIMO PLC system under the presence of a passive MIMO PLC malicious device.

The remainder of the paper is organized as follows. Section II presents the system model. Section III reviews the secrecy outage probability. Section IV details the analysis of

This study was supported in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES)—Finance Code 001.

Pedro Henrique Sartorello, Ândrei Camponogara, and Evelio M. G. Fernandez are with the Department of Electrical Engineering, Federal University of Paraná, Curitiba, PR, Brasil (e-mail: pedro.sartorello@ufpr.br; andrei.camponogara@ufpr.br; evelio@ufpr.br).

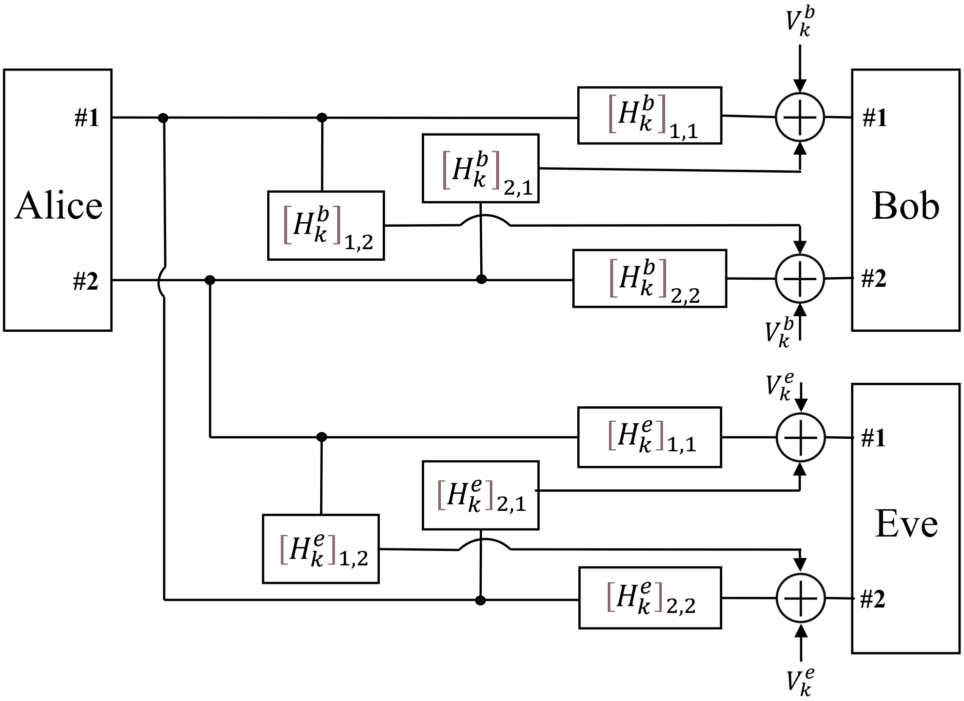

Fig. 1. Block diagram that represents the MIMO-ME PLC wiretap channel model.

the numerical results. Finally, Section V offers the concluding remarks.

II. System Model

Let the block diagram in Fig.1 represent the MIMO-multiple eavesdroppers (MIMO-ME) PLC wiretap channel model. In this scenario, the transmitter (Alice) communicates private information to a legitimate receiver (Bob) while a passive eavesdropper (Eve) attempts to intercept the transmission. All devices operate over the same electric power grid, which consists of three conductors: phase (P), neutral (N), and protective earth (E). The PLC transmitter is equipped with two ports for signal transmission, referred to as port $\#1$ and port $\#2$. Port $\#1$ drives the phase–neutral pair (PN), and port $\#2$ drives the phase–earth pair (PE). Each PLC receiver also has two ports for signal reception: port $\#1$ is connected between the phase conductor (P) and the reference, and port $\#2$ is connected between the neutral conductor (N) and the reference.

The PLC channels are assumed to be linear and time-invariant during a block symbol interval. Also, the transmission of a block symbol in the discrete-time domain considers the presence of the cyclic-prefix to ensure negligible intersymbol interference. It ensures that the channel convolution matrix is circulant, and, consequently, it can be treated similar to the n-block circular Gaussian broadcast channel detailed in [11] for channel capacity computation. Finally, it assumes perfect synchronization.

SISO Capacity

Let $\mathbf{X} = [X_1\, X_2 \cdots X_N]^{\mathrm{T}}$ represent the transmitted symbol block of length N in discrete-frequency domain, where $\mathbb{E}\{\mathbf{X}\} = \mathbf{0}_N$, $\mathbb{E}\{\mathbf{X}\mathbf{X}^{\dagger}\} = \sigma_X^2 \mathbf{I}_N$, X_k is the k^{th} complex symbol from an M-ary constellation, $\mathbf{I}_N$ denotes the identity matrix of dimension $N \times N$, and $\mathbb{E}\{\cdot\}$, $(\cdot)^{\mathrm{T}}$ and $(\cdot)^{\dagger}$ represents the expectation, transpose, and Hermitian operators, respectively. As the uniform power allocation is adopted, the total power transmission is $P_{\mathrm{t}} = \sigma_X^2$. Furthermore, $\mathbf{V}^{(l)} = [V_1^{(l)}\, V_2^{(l)} \cdots V_N^{(l)}]^{\mathrm{T}}$ is the vector representation of the additive noise in the discrete-frequency domain, with $l \in \{b, e\}$ denoting Bob and Eve, respectively. Also, one assumes $\mathbb{E}\{\mathbf{V}^{(l)}\} = \mathbf{0}_N$ and $\mathbb{E}\{\mathbf{V}^{(l)}\mathbf{V}^{(l)\dagger}\} = \mathbf{\Lambda}_{\sigma_V^2}^{(l)}$, where $\mathbf{\Lambda}_{\sigma_V^2}^{(l)} = \mathrm{diag}\{\sigma_{V,1}^{2(l)}, \sigma_{V,2}^{2(l)}, \cdots, \sigma_{V,N}^{2(l)}\}$ is a diagonal matrix of dimension $N \times N$ and $\sigma_{V,k}^{2(l)}$ is the noise variance at the k^{th} subchannel and at the l^{th} receiver.

The received block symbol at the l^{th} receiver in the discrete-frequency domain can be expressed as

$$\mathbf{Y}^{(l)} = \mathbf{\Lambda}_H^{(l)} \mathbf{X} + \mathbf{V}^{(l)}, \tag{1}$$

in which $\mathbf{\Lambda}_H^{(l)} = \mathrm{diag}\{H_1^{(l)}, H_2^{(l)}, \cdots, H_N^{(l)}\}$, with $H_k^{(l)}$ being the channel frequency response (CFR) associated with the k^{th} subchannel and the l^{th} receiver.

Considering that $\mathbf{X}$ and $\mathbf{V}^{(l)}$ are independent random vectors, the SNR related to the k^{th} subchannel at the l^{th} receiver is given by

$$\Gamma_k^{(l)} = \frac{\sigma_X^2 \left|H_k^{(l)}\right|^2}{\sigma_{V,k}^{2,(l)}}. \tag{2}$$

Consequently, the channel capacity between Alice and the l^{th}

receiver assuming a SISO configuration can be expressed as

$$C_l = \frac{1}{N}\sum_{k=1}^{N}\log_2\left(1+\Gamma_k^{(l)}\right) \quad \text{[bit/s/Hz]}. \tag{3}$$

MIMO Capacity

Consider a MIMO system with N_t transmit and N_r receive ports. For each subchannel $k \in \{1, 2, \ldots, N\}$, one defines the transmitted symbol vector as $\mathbf{X}_k = [X_{k,1}, X_{k,2}, \cdots, X_{k,N_\mathrm{t}}]^\mathrm{T}$, where each $X_{k,i}$ is obtained from an M-ary constellation with average energy σ_X^2/N_t. Also, it is assumed that $\mathbb{E}\{\mathbf{X}_k\} = \mathbf{0}$ and $\mathbb{E}\{\mathbf{X}_k\mathbf{X}_k^\dagger\} = \frac{\sigma_X^2}{N_\mathrm{t}}\mathbf{I}_{N_\mathrm{t}}$, so that the total transmit power per subchannel is $P_\mathrm{t} = \sigma_X^2$.

Similarly, let the additive noise vector at the l^th receiver for the k^th subchannel be $\mathbf{V}_k^{(l)} = [V_{k,1}^{(l)}, V_{k,2}^{(l)}, \cdots, V_{k,N_r}^{(l)}]^\mathrm{T}$, with $\mathbb{E}\{\mathbf{V}_k^{(l)}\} = \mathbf{0}$ and $\mathbb{E}\{\mathbf{V}_k^{(l)}\mathbf{V}_k^{(l)\dagger}\} = \mathbf{\Lambda}_{\sigma_{V,k}^2}^{(l)}$, where $\mathbf{\Lambda}_{\sigma_{V,k}^2}^{(l)} = \mathrm{diag}\{\sigma_{V_{k,1}}^{2(l)}, \sigma_{V_{k,2}}^{2(l)}, \cdots, \sigma_{V_{k,N_\mathrm{r}}}^{2(l)}\}$.

The vector representation of the received signal in the discrete-frequency domain at the k^th subchannel and the l^th receiver is

$$\mathbf{Y}_k^{(l)} = \mathbf{H}_k^{(l)}\,\mathbf{X}_k + \mathbf{V}_k^{(l)}, \tag{4}$$

with $\mathbf{H}_k^{(l)} \in \mathbb{C}^{N_r \times N_t}$ denoting the channel matrix corresponding to the k^th subchannel. The element in the i^th row and j^th column of this matrix, $[H_k^{(l)}]_{i,j}$, represents the CFR from the j^th transmit port of Alice to the i^th receive port of the l^th receiver at the k^th subchannel.

Applying singular value decomposition (SVD), $\mathbf{H}_k^{(l)}$ can be expressed as

$$\mathbf{H}_k^{(l)} = \mathbf{U}_k^{(l)}\,\mathbf{\Sigma}_k^{(l)}\,\mathbf{V}_k^\dagger, \tag{5}$$

where $\mathbf{U}_k^{(l)} \in \mathbb{C}^{N_r \times N_r}$ and $\mathbf{V}_k \in \mathbb{C}^{N_t \times N_t}$ are unitary matrices, and $\mathbf{\Sigma}_k^{(l)} = \mathrm{diag}\left\{\sqrt{\lambda_{k,1}^{(l)}}, \sqrt{\lambda_{k,2}^{(l)}}, \ldots, \sqrt{\lambda_{k,R}^{(l)}}\right\}$ contains the singular values, with $R = \min(N_\mathrm{t}, N_\mathrm{r})$.

Assuming uniform power allocation, the SNR of the p^th parallel stream in subchannel k is given by

$$\Gamma_{k,p}^{(l)} = \frac{(\sigma_X^2/N_t)\,\lambda_{k,p}^{(l)}}{\sigma^{2}{}_{V,k,p}^{(l)}}. \tag{6}$$

Consequently, the MIMO channel capacity for at the l^th receiver is given by

$$C_l = \frac{1}{N}\sum_{k=1}^{N}\sum_{p=1}^{R}\log_2\left(1+\Gamma_{k,p}^{(l)}\right) \quad \text{[bit/s/Hz]}. \tag{7}$$

III. Secrecy Outage Probability

In the PLS context, the secrecy capacity provides the largest amount of information that can be confidentially sent from Alice to Bob in the presence of Eve. It is given by

$$C_s = [C_b - C_e]^+, \tag{8}$$

where C_b represents the capacity between Alice and Bob, and C_e is the capacity between Alice and Eve. Also, the operator $[x]^+ = \max(x, 0)$ ensures that the secrecy capacity is non-negative.

In the context where Alice does not have access to the instantaneous CSI of Eve, the SOP is an interesting metric to assess security at the physical layer level. The SOP provides the probability of occurring a secrecy outage event when a target secrecy rate R_s is adopted by Alice. Then, the SOP can be expressed as

$$P_\mathrm{out}(R_s) = \mathbb{P}\{C_s < R_s\}. \tag{9}$$

IV. Numerical Results

This section assesses the SOP of the MIMO-ME PLC wiretap channel model. To do so, 10^4 sets of independent random MIMO PLC channels for representing Alice-Bob and Alice-Eve links are generated using the synthetic statistical channel emulator addressed in [12]. This emulator generates Delta-style transmitting and the Star-style receiving modes CFRs in the frequency band $1.8 - 100$ MHz. Also, the noise power is obtained from the power spectral density (computed using the Welch's method) of additive noise measures obtained from a measurement campaign carried out in several Brazilian houses and detailed in [1]. It is assumed $N = 1727$. Moreover, the MIMO PLC channel model is evaluated by comparing five different configurations, as listed in Table I.

TABLE I
MIMO PLC configurations

	Alice	**Bob**	**Eve**
SISO-SE	Port #1	Port #1	Port #1
MISO-SE	Ports #1, #2	Port #1	Port #1
MISO-ME	Ports #1, #2	Port #1	Ports #1, #2
MIMO-SE	Ports #1, #2	Ports #1, #2	Port #1
MIMO-ME	Ports #1, #2	Ports #1, #2	Ports #1, #2

Fig. 2 shows the SOP in terms of the target secrecy rate R_s for the total transmission power $P_t = 20$ dBm. Examining the curves reveals that, as R_s increases, the SISO-SE configuration exhibits a behavior similar to that of MISO-ME, despite Eve having access to one additional reception signal compared to Bob. Moreover, the MISO-SE scenario introduces extra transmit signals from Alice to Bob, leading to a noticeable reduction of the SOP compared to the previous SISO-SE and MISO-ME. Such an improvement highlights the benefits of adding more transmit signals, even if Bob only has a single port available. Another interesting observation is that, as R_s increases, the MIMO-ME scenario proves more effective in keeping the SOP lower than that of MISO-SE. Finally, the MIMO-SE configuration consistently shows the lowest SOP for all tested values of R_s. These findings show the potential of MIMO PLC systems in enhancing data communication security under the presence of a passive Eve.

Fig. 3 depicts the SOP versus P_t considering a target secrecy rate $R_s = 1$ bps/Hz. It can be observed that the SOP decreases as P_t increases. This behavior reflects the fact that higher P_t improves the capacity of the Alice-Bob link relative to that of the Alice-Eve link. Among the analyzed MIMO configurations, the MISO-ME consistently exhibits the highest SOP for P_t greater than around 13 dBm. And

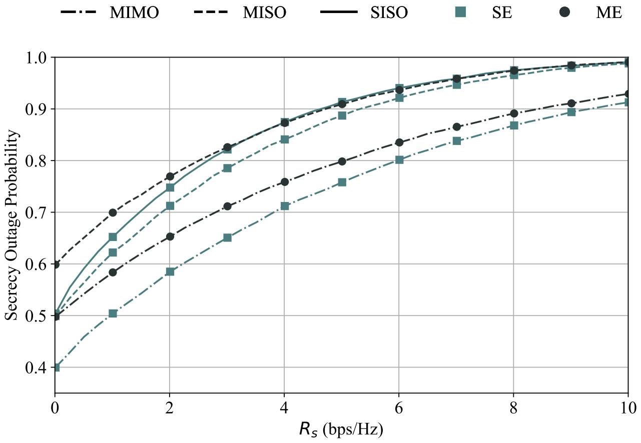

Fig. 2. Secrecy outage probability in terms of target secrecy rate R_s for the total power transmission $P_\mathrm{t} = 20$ dBm and different configurations of the MIMO PLC wiretap channel model.

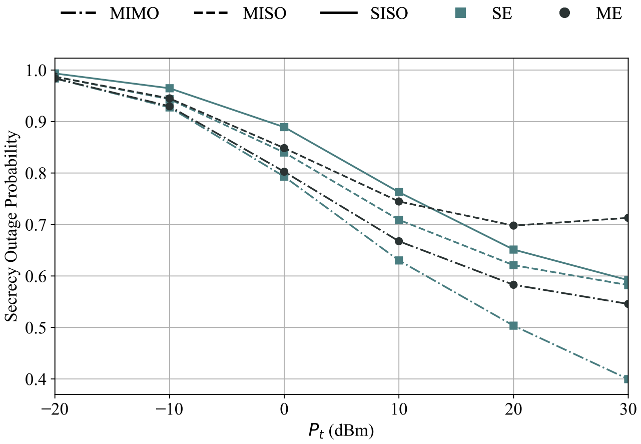

Fig. 3. Secrecy outage probability in terms of total power transmission P_t for a target secrecy rate $R_s = 1$ bps/Hz, considering different configurations of the MIMO PLC wiretap channel.

below this value, only SISO-SE provides a higher SOP. In the MISO-SE case, the SOP drops significantly compared to SISO-SE, indicating that even when only Alice has two ports available, data communication security is improved. The MIMO-ME closely follows the MISO-SE performance until around $P_\mathrm{t} = 10$ dBm, where MISO-SE slightly outperforms it. The strongest security performance appears when both Alice and Bob employ multiple ports while Eve has only a single port available, i.e., MIMO-SE, with SOP approaching 0.4 for $P_\mathrm{t} = 30$ dBm. These results highlight the potential of the MIMO technology to provide secrecy at the physical layer level even when Eve can also exploit multiple ports for eavesdropping on private messages exchanged between Alice and Bob.

V. Conclusion

This paper investigates the physical layer security (PLS) of an in-home and broadband multiple-input multiple-output (MIMO) power line communication (PLC) system. To do so, a MIMO-multiple eavesdroppers (MIMO-ME) PLC wiretap channel has been adopted, where a legitimate transmitter (Alice) sends private messages to a legitimate receiver (Bob) under the presence of a passive eavesdropper (Eve). The PLS has been evaluated in terms of secrecy outage probability (SOP) considering several configurations of the MIMO-ME PLC wiretap channel model.

The numerical results have demonstrated that, by exploiting the MIMO approach, secrecy at the physical layer level can be significantly increased when compared to the single-input single-output (SISO) approach. In particular, it has been shown that the MIMO-SE configuration, where Alice and Bob have two ports available and Eve has a single port available, shows the lowest SOP across all adopted target secrecy rates and total transmission power values. This finding highlights the strong potential of the MIMO approach to improve PLS in PLC systems.

References

[1] T. R. Oliveira, F. J. A. Andrade, A. M. Picorone, H. A. Latchman, S. L. Netto, and M. V. Ribeiro, “Characterization of hybrid communication channel in indoor scenario,” *Journal of Communication and Information Systems*, vol. 31, no. 1, pp. 224–235, Sep. 2016.

[2] M. Rathinasabapathy, “Investigations on mimo broadband power line communication system with joint precoding under impulsive noise scenario,” Ph.D. thesis, Department of Electronics and Communication Engineering, Pondicherry Engineering College (Pondicherry University), Puducherry, India, 2017.

[3] R. Hashmat, P. Pagani, A. Zeddam, and T. Chonavel, “Mimo communications for inhome plc networks: Measurements and results up to 100 mhz,” in *ISPLC2010*, 2010, pp. 120–124.

[4] M. C. de Sousa, Cantarino *et al.*, “Characterizing mimo channels in low-voltage electric power line communication through impedance and scattering parameters analysis,” *Journal of Microwaves, Optoelectronics and Electromagnetic Applications*, vol. 23, no. 2, p. e2024279943, May 2024.

[5] M. Biagi, “Mimo self-interference mitigation effects on plc relay networks,” in *2011 IEEE International Symposium on Power Line Communications and Its Applications*, 2011, pp. 182–186.

[6] A. D. Wyner, “The wire-tap channel,” *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[7] A. Camponogara, H. V. Poor, and M. V. Ribeiro, “Physical layer security of in-home plc systems: Analysis based on a measurement campaign,” *IEEE Systems Journal*, vol. 15, no. 1, pp. 617–628, Mar. 2021.

[8] A. Camponogara and M. V. Ribeiro, “The effective secrecy throughput for the hybrid wiretap channel,” *Journal of Communication and Information Systems*, vol. 36, no. 1, pp. 44–51, Feb. 2021.

[9] A. Pittolo and A. M. Tonello, “Physical layer security in power line communication networks: An emerging scenario, other than wireless,” *IET Communications*, vol. 8, no. 8, pp. 1239–1247, 2014.

[10] Y. Zhuang and L. Lampe, “Physical layer security in mimo power line communication networks,” in *18th IEEE International Symposium on Power Line Communications and Its Applications*, 2014, pp. 272–277.

[11] A. Goldsmith and M. Effros, “The capacity region of broadcast channels with intersymbol interference and colored gaussian noise,” *IEEE Trans. Inf. Theory*, vol. 47, no. 1, pp. 219–240, 2001.

[12] A. Pittolo and A. M. Tonello, “A synthetic statistical mimo plc channel model applied to an in-home scenario,” *IEEE Transactions on Communications*, vol. 65, no. 6, pp. 2543–2553, 2017.