IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 14, 2021, accepted August 23, 2021, date of publication August 30, 2021, date of current version September 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3109001

Security Transmission in MIMO Ubiquitous Power Internet of Things Systems

LINGANG YU[1], QIANG LIU[1], DONGWEN WU[1], QIN YAN[2], GAOPENG YAN[3], AND YONGPENG WU[3], (Senior Member, IEEE)
[1]Jiangxi Power Supply Service Management Center, State Grid, Nanchang 330000, China
[2]Jiangxi Electric Power Company Ltd., State Grid, Nanchang 330000, China
[3]Department of Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

Corresponding author: Yongpeng Wu (yongpeng.wu@sjtu.edu.cn)

The work of Lingang Yu, Qiang Liu, Dongwen Wu, and Qin Yan was supported by State Grid Corporation Headquarters Technology Project under Grant 5700-201941319A-0-0-00.

ABSTRACT Power line communication (PLC) is a promising technique because of its wide distribution and low cost. However, due to the feature of PLC channel, the communication quality is unsatisfactory and there exists security risks. In this paper, we design a frequency division (FD) multiple-input and multiple-output (MIMO) PLC system. Firstly, since power line channels have frequency selectivity problems, it is necessary to select an appropriate frequency band for communication, so we adopt digital front-end (DFE) in the PLC system. The DFE is used to adjust the frequency and bandwidth configuration of the carrier signal. In order to determine the optimal frequency point for upstream and downstream communication, a sweep mechanism under the FD PLC system is designed. The analysis of the sweeping mechanism finds that the sweeping overhead only requires *2N+1* communications, which greatly improves the sweeping efficiency. Secondly, we find this frequency division technology can also be used to enhance the security of MIMO PLC. The real signal can be hidden in the frequency domain and obfuscated in the time domain by using DFEs to adjust the frequency and bandwidth information of the real signal and artificial interference noise. Simulation indicates that the proposed method can guarantee the correct reception and demodulation at the legitimate receiving user end, while the BER at the eavesdropping user end fluctuates around 0.5, thus cannot correctly demodulate the real signal.

INDEX TERMS Digital front end, frequency division, MIMO, power line communication, security.

I. INTRODUCTION

The ubiquitous power Internet of Things (UEIOT) is a smart service system that fully applies modern information technology and advanced communication technology around each link of the power system to realize the interconnection of all things and human-computer interaction in all links of the power system, with comprehensive status awareness, efficient information processing, and convenient and flexible features. With the characteristics of wide distribution and low-cost configuration, power line communication (PLC) has been revitalized [1], [2] and has become an important technology to realize UEIOT [3], [4]. Since multiple-input and multiple-output (MIMO) technique can increase system's data throughput and transmission distance without increasing bandwidth or total transmit power expenditure, it is usually combined with PLC system to increase channel capacity and anti-interference capability. Studies have shown that MIMO PLC can achieve high data rate and increase link reliability [5]–[7].

However, there exist several problems in MIMO PLC. On the one hand, different from wireless and proprietary communication line communication technology, the power line carrier communication channel changes greatly with the power line topology, access to electrical equipment, and communication access location. This includes channel impedance, channel attenuation, and channel noise. Besides, PLC will be subject to interference from narrowband and impulse noise, as well as the existence of frequency selectivity problems [8].

In order to build an effective PLC system that overcomes channel fading and improves communication quality, most of the research has focused on the design of physical layer mode. Common techniques such as channel coding,

The associate editor coordinating the review of this manuscript and approving it for publication was Zheng Yan.

interleaving, and digital modulation are widely studied and applied. Although these technologies can overcome channel fading to a certain extent, power line communication still faces the following problems, namely, most of the existing PLC systems are based on single-carrier and single-channel design. They usually operate at specific frequency points. Further, they do not address the frequency selectivity problem of power line channels. Therefore, it is necessary to design a frequency division (FD) MIMO power line communication system that can selectively transmit signals at arbitrary frequency points depending on the channel conditions.

On the other hand, the fact that eavesdropping users can easily connect to the power line means that it will not only change the topology structure of the power line channel, further affect the communication quality, but also may lead to information leakage and bring hidden dangers to PLC security.

One solution is to enhance physical layer security (PLS) which is a well-studied field. It is usually evaluated by secrecy capacity metric [9], [10]. The PLS of SISO-PLC system was firstly analyzed and compared with wireless communication system [11], [12], and then followed by analyzation of MIMO-PLC system [13]. Many researches have been investigated on the communication link. The best interleaving method was explored in the context of turbo codes in [14], [15]. Another field that has been investigated widely is cooperative relaying system [16]–[21]. The author in [20] considered the application of PLS in cooperative PLC networks in the presence of passive eavesdropping. In [21], the author investigated physical layer security of cooperative relaying PLC systems with artificial noise in the presence of an eavesdropper. Two efficient schemes to improve the PLS in the presence of passive eavesdroppers are cooperative beamforming and jamming [22]. A joint cooperative beamforming and jamming scheme was proposed in [22] to enhance the security of a cooperative relay network. Besides, the property of PLC channel was investigated. In [23], the author found the power line channel is reciprocal rather than symmetric. However, the channel transfer function in the two directions has a wide-sense symmetry that the peaks appears at the same time. This property is then utilized as channel state information to generate a secret key, which is used to encode the transmitted messages.

However, to the authors knowledge, very limited work exists on using frequency division technology to enhance security of MIMO PLC. To achieve this, digital front end (DFE) is adopted. It consists of filters and mixers. By adjusting parameters, the center frequency of the input signal can be changed, and the signal can be moved to other frequencies for transmission. In this context, we propose a method to enhance MIMO PLC security. Before the information message is transmitted, two or more artificial messages are added to it. To maintain the integrity of original information, these artificial messages are shifted to different frequency points so that they are isolated in frequency domain. For security sake, the isolated messages need also to be as close as possible so that they appear to be a continuous signal from frequency domain. The original information is then hided in the frequency domain.

The main contributions of this paper are as follows:

1) In view of the PLC channel situation, we design a frequency division $2*2$ MIMO PLC system.

2) Since the sweeping overhead of conventional PLC systems is too large, the time overhead of a typical N×N sweeping mechanism requires $N^2 + N$ communications. In order to improve the sweeping efficiency, this paper designs a new sweeping mechanism for this frequency division PLC system, where the sweeping overhead only requires $2N+1$ communications, which greatly improves the sweeping efficiency.

3) Unlike traditional physical layer security technique, we propose a DFE based technique to enhance the security of $2*2$ MIMO PLC system.

4) System performance is evaluated and the results show that the security is enhanced evidently.

The rest of the paper is organized as follows. In Section II, we briefly describe the system model used in this paper. In Section III, we present simulation results. Conclusions follow in Section IV.

II. SYSTEM MODEL

In this section, we describe the transceiver structure of frequency division based security enhanced MIMO PLC system. Considering the hardware characteristics and the power line characteristics, we first design a physical layer schema for FD PLC at the transmitter side. To increase the transmission rate, spatial multiplexing is adopted. The system model of $2*2$ MIMO PLC is shown in Fig. 1.

The transmitter is configured as a two-way form. In the first way, the input bit streams Noise1, Noise2 and data1 are first fed into Reed-Solomon (RS) Encoder. After being RS encoded, the bit streams are fed into 1/2 rate Convolutional Code (CC) Encoder. After being CC encoded, the bit streams are fed into scrambler, interleaver, differential binary phase-shift Keying (DBPSK) modulator successively. One of the reasons we design these parts in this order is to reduce the number of serial-parallel conversions, or parallel- serial conversions to facilitate implementation on hardware. The DBPSK modulated symbols are then fed into Orthogonal Frequency Division Multiplexing (OFDM) modulator, which is implemented with IFFT of 1024 length. The OFDM symbols generated from Noise1, Noise2 are then fed into DFE1, DFE3 separately. And the OFDM symbols generated from data1 are fed into DFE2. These three DFEs have been adjusted to different center frequency points. Consequently, the three outputs are shifted to different center frequency. The aim of DFEs is to hide information of data1 in the frequency domain. We then combine the three outputs into one message in the time domain. The combined message1 serves as the first input of $2*2$ MIMO PLC. In the second way, we use the same method to get combined message2 as the second input of $2*2$ MIMO PLC. We choose $2*2$ MIMO for the below considerations: Firstly, considering the fact that in practical

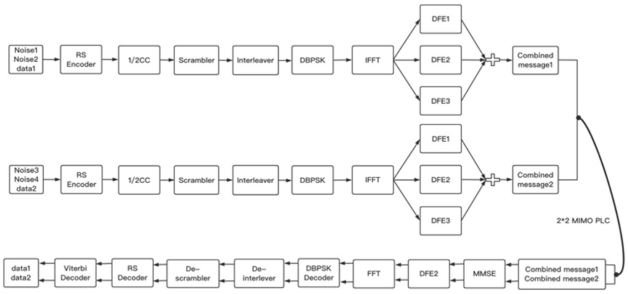


FIGURE 1. Transceiver of 2∗2 MIMO PLC. After a series of data processing in the transmitter, combined messages are transmitted to the receiver through the MIMO PLC channel, and decoded in the receiver to restore the original data.

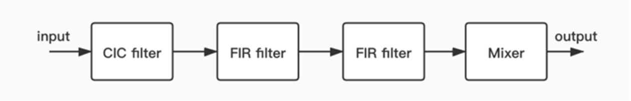


FIGURE 2. The structure of DFE. Input signals pass through CIC filter, FIR filters and mixer in turn.

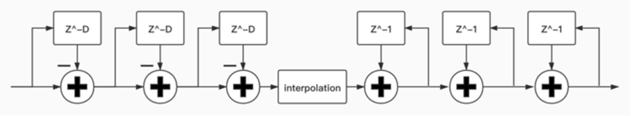


FIGURE 3. Three-stage interpolating CIC filter. On the left of interpolation are three comb filters, on the right of interpolation are three integrators.

design, it is mainly a three-phase, three-wire situation, and that phase-to-phase coupling is more effective than phase-to-ground coupling. Secondly, for the three-phase phase coupling, the matrix rank of A-B and B-C is similar to the matrix rank of A-C, and the effect of 3 × 3 MIMO cannot be fully exploited, so it is more appropriate to implement 2×2 MIMO. Thirdly, compared to 3 × 3 MIMO, 2 × 2 MIMO is more advantageous in terms of implementation complexity and power consumption.

At the receiver side, a reverse process is carried out after receiving messages from 2∗2 MIMO PLC channel. MMSE detection is added to reduce mutual interference between combined message1 and combined message2. DFE2 is used to filter added noises and extract information of data1, data2 from frequency domain. We use the same DFE that processed data1 and data2 from transmitter. However, since the eavesdropper has no information of noises and center frequency point of DFE2, it is difficult to decode data1 and data2 from specially processed messages. A more detailed explanation is as follows.

A. DIGITAL FRONT END

Fig. 2 shows the structure of the DFE in the transmitter. It consists of a cascaded integrator-comb (CIC) filter, two finite impulse response (FIR) filters and a mixer. Among them, the filters act as interpolators to increase the sampling rate of the frames which are generated by OFDM modulator. The mixer is used to adjust the center frequency of the input signal and move it to a specific frequency point for transmission. In fact, CIC filter is an optimized class of FIR filter combined with an interpolator or decimator [24]. But it does not need to do multiplication, and it is more economical and more suitable for application to hardware. Considering the large passband bandwidth of the CIC filter, we add two FIR filters behind the CIC filter to eliminate the image interference caused by the interpolation filtering process. Compared with the CIC filter, the passband bandwidth is smaller, so the filtering effect will be better.

The inner structure of interpolating CIC filter is shown in Fig. 3. It consists of three comb filters, three integrators and up-sampler (interpolation). D is delay factor that used to control the frequency response of the filter and determine the position of the zero point. Usually the value is 1 or 2. Here we take D as 1 in this paper.

B. FREQUECY SWEEP MECHANISM

The frequency selectivity problem of PLC system has been mentioned in the introduction section. In order to solve this problem, in addition to channel coding, we need to design a more flexible PLC system with adjustable center frequency. The structure characteristics of DFE have been described in the previous section. Through digital front-end, the transmitter and receiver can communicate on multiple frequency points, so better communication frequency band can be selected to avoid the problem of frequency selectivity to a certain extent. After the communication frequency can be adjusted, we need to determine the best communication frequency point before formal communication. Therefore, we need to design a corresponding frequency sweep mechanism to deal with the problem of frequency selection.

1) TRADITIONAL N×N FREQUENCY SWEEP MECHANISM

In order to determine the sweep mechanism and analyze the sweep cycle overhead, it is useful to consider the case of communication between the transmitter and receiver at N frequency points. In order to find the best frequency point for upstream and downstream communication among these N frequency points, the upper computer needs to send carrier signals to the lower computer at each of the N frequency points, and the lower computer stores the SNR of the received signal at the corresponding frequency point after receiving it. Similarly, the lower computer also needs to send carrier signals to the upper computer at N frequency points and select the best uplink frequency point by comparing SNRs.

At the same time, it should be noted that the characteristics of this PLC system: first, both center frequency point and bandwidth can be configured; second, because the lower computer works on a specific frequency point for each round of communication, it can only listen to one center frequency and bandwidth configuration, and cannot achieve active event reporting; in addition, power line communication does not provide a specific frequency band for negotiation, so it can only be polled by the upper computer.

Based on the above characteristics of the system, a sweep mechanism is established as shown in Fig. 4. The left side of the figure shows the upper computer and the right side shows the lower computer. Eight communication frequencies were selected in the frequency band from 2 to 12 MHz for communication.

The frequency sweeping process can be described as follows:

- The host computer communicates at 2.625 MHz and waits for a period of time t after sending the signal.
- After receiving the signal, the lower computer determines whether the center frequency point of the signal is consistent with its own center frequency point. If it is consistent, it sends a carrier signal back at 2.625MHz frequency point, records the downlink communication SNR of 2.625MHz frequency point channel, and switches to the next frequency point for signal reception; If it is inconsistent, it will not send the signal back and continue to wait for the next signal at 2.625MHz frequency point. If the waiting time timeout reaches the set $8t$, it will switch to the next frequency point.
- If the upper computer receives the carrier signal in time t, it records the uplink communication SNR of 2.625 MHz frequency point and returns to the initial frequency point to send the carrier signal; On the contrary, it will switch to the next frequency point 3.875 MHz, 5.125 MHz, $\ldots$, 11.375 MHz to send signals, and the lower computer will repeat the previous step.
- Finally, the upper computer and the lower computer select the frequency with the best SNR as the communication frequency according to the SNR of N frequency points.

In typical cases, the upper computer needs to communicate n times per round, and then receives the signal sent by the lower computer once; The lower computer also needs to switch at N frequency points, so the typical sweep time is $(N^2 + N)$ communication times.

2) INCOMPLETE FREQUENCY SWEEP MECHANISM

Through the analysis of the above sweep mechanism, it is concluded that the frequency sweep cycle cost is $(N^2 + N)$ communications. In order to pursue shorter sweep time and reduce the cost of sweep frequency, we can retreat and then consider an incomplete sweep mechanism. In this frequency sweeping mechanism, PLC system does not seek the best uplink and downlink communication frequency points, but only require avoiding the problem of frequency selectivity and selecting the upstream and downstream frequency points that can carry out normal communication.

The incomplete frequency sweeping mechanism is similar to the frequency sweeping mechanism, and the above N = 8 case is still used for analysis. The frequency sweeping process can be described as follows:

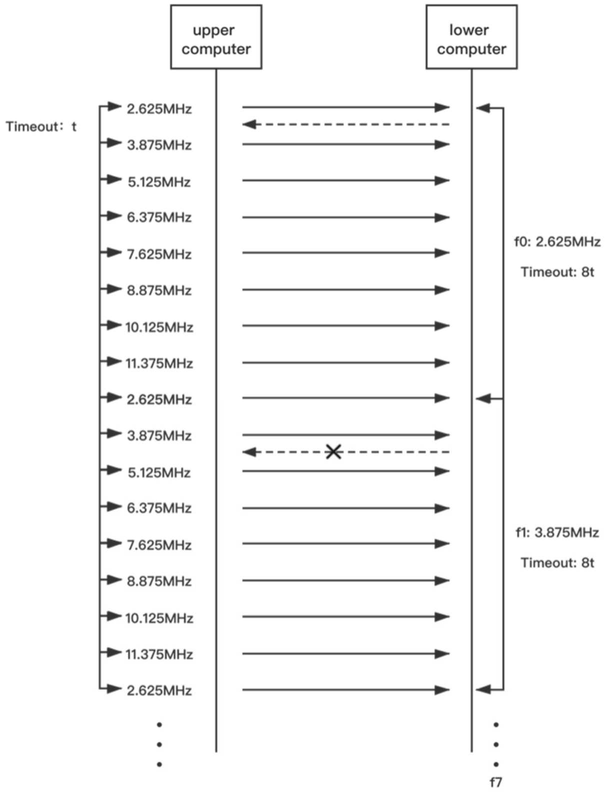


FIGURE 4. **N×N Sweep mechanism.**

- The upper computer sends the carrier signal in turn at eight frequency points for polling, and waits for a certain time t after each frequency point sends the carrier signal. If the carrier signal from the lower computer is received within the time t, the frequency sweeping process ends. Otherwise, after the waiting time t is exhausted, the carrier signal is transmitted to the next frequency point.
- Because there is no fixed communication frequency point between the upper computer and the lower computer, the lower computer can only wait for the polling of the upper computer. Assuming that the carrier signal sent by the upper computer at the third frequency point is received by the lower computer, but the communicable uplink frequency point is the fourth frequency point, then in this case, only after the lower computer waits for three time periods, that is $(3 * 8t)$, and the digital front end of the lower computer switches to work at the fourth frequency point f4, can an incomplete frequency sweep be completed.
- At this time, when the upper computer trains to the third frequency point f3 in turn, it receives the carrier signal sent back by the lower computer, so as to determine the communicable downlink frequency point f3 and uplink frequency point f4, and complete an incomplete frequency sweep.

According to the above frequency sweeping process, considering the equal probability event when N communication frequency points of PLC system can communicate, a typical incomplete frequency sweeping time is $(N/2 \cdot (N + 1) + 2)$ communication times.

3) FREQUENCY SWEEP MECHANISM UNDER FD-PLC SYSTEM

For FD PLC system, because of its two characteristics, one is that the center frequency point and bandwidth can be configured, the other is that the transmitter can send signals at any frequency point, and the receiver can receive signals at any frequency point. We are able to establish a frequency sweep mechanism as shown in Fig. 5.

In Fig. 5, the upper computer on the left represents the sender, and the lower computer on the right represents the receiver. The transmitter and receiver are integrated in the communication equipment when frequency scanning is carried out to determine the optimal uplink and downlink frequency points. Therefore, when the communication equipment receives the carrier signal of a specific center frequency point and bandwidth, it can also send another configured carrier signal, so as to speed up the frequency scanning speed.

The frequency sweeping process in Fig. 5 can be described as follows:

- The host computer sends signals at N frequency points one by one, where $N = 8$ and the frequency band is 2-12MHz.
- After receiving the signal, the receiver determines the frequency point of the signal, records the SNR of the downlink frequency band, and then returns a signal at this frequency point.
- After receiving the signal, the transmitter records the SNR of the uplink band.
- After the upper computer and the lower computer record the SNR of all N frequency points respectively, the optimal frequency points of the uplink and downlink are determined naturally.

Because of the design characteristics of the frequency division system, it only needs the transmitter to send N times of carrier signal in turn, and the receiver also needs to send N times of carrier signal, so as to get the best uplink and downlink communication frequency point. The whole sweep time is $(2N + 1)$ times.

Different from the frequency sweep mechanism supported by traditional power line communication system, this frequency division PLC system needs less time to complete frequency sweep and determine the best communication frequency. In the traditional PLC system, the typical time to complete a frequency sweep is (N^2+N) communication, and the typical time to complete an incomplete frequency sweep mechanism is $(N/2\cdot(N + 1)+2)$ communications. Since only one digital front end is configured in the traditional PLC system, the internal parameters of the digital front end need to be readjusted when the next communication frequency point is sent for testing, which will inevitably bring the time demand beyond the communication times required by the frequency sweep mechanism. For the frequency division PLC system, the receiver is equipped with a multi-channel digital front-end to make it have the ability of blind detection of any frequency point carrier signal. It does not need to wait for the polling of the host computer, and can feed back to the host computer in time after receiving the signal. In a word, the structure design of frequency division system brings great convenience to the frequency sweep mechanism of the system.

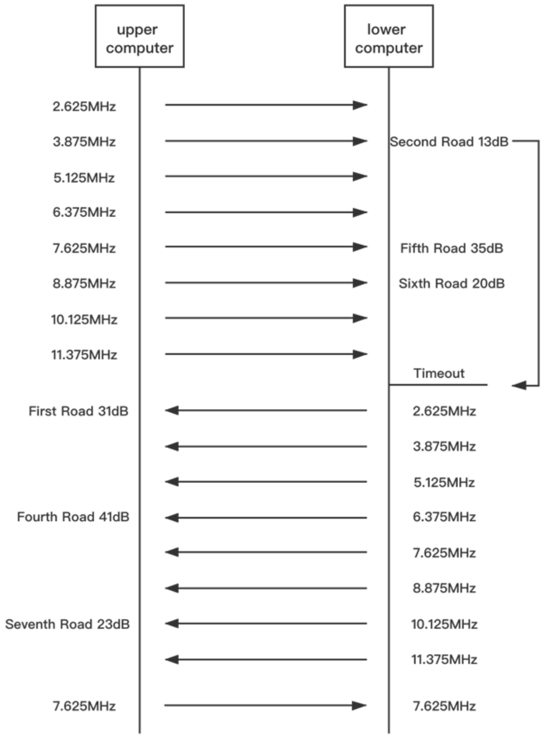


FIGURE 5. **N×N Sweep mechanism under FD PLC system.**

C. FREQUENCY DIVISION TECHNIQUE

The essential idea of this technique is that: Noises are added to message to mask its information in the frequency domain, but does not destroy its integrity. To elaborate, recall the transceiver structure in Fig. 1, after the first way being through a series of signal processing, Noise1, Noise2 and data1 are finally fed into DFE1, DFE3, DFE2 separately. Now, suppose the frequency domain of message sent by transmitter is shown in Fig. 6. It is composed of frequency domains of three messages M_1, M_2, M_3. Let M_1, M_3 represent the corresponding generated noises, M_2 represents the corresponding generated information message. The transmitted message, or the confidential message M can be then expressed as:

$$M = M_1 \cdot sinf_1t + M_2 \cdot sinf_2t + M_3 \cdot sinf_3t \qquad (1)$$

in time domain, where f_1, f_2, f_3 are center frequency of M_1, M_2, M_3 separately. Note the gaps between M_1, M_2, and M_3.

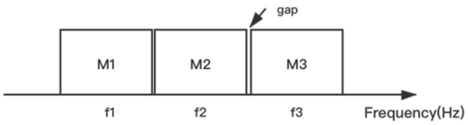
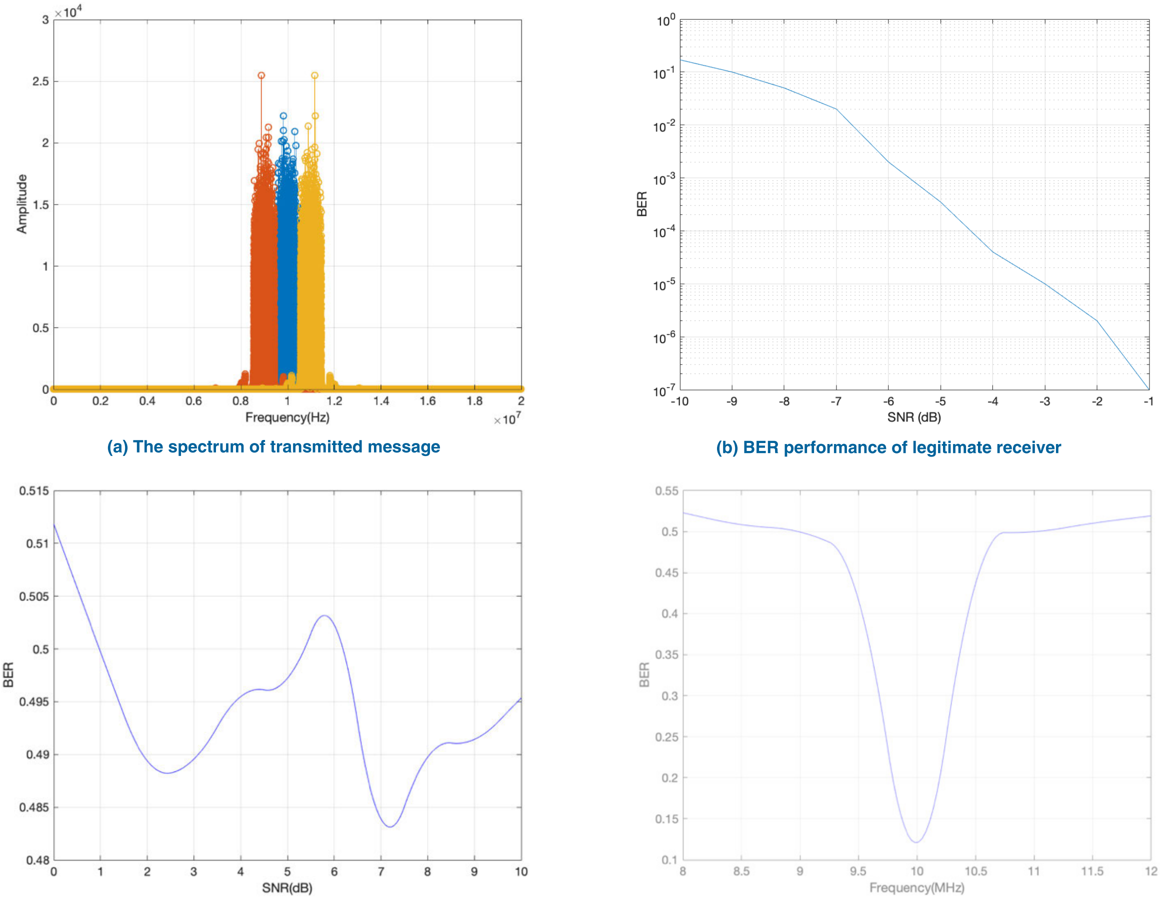


FIGURE 6. **Frequency domain of combined message. It consists of the frequency domain of M1, M2, M3.**



(a) The spectrum of transmitted message

(b) BER performance of legitimate receiver

(c) BER performance of eavesdropper

(d) BER performance of eavesdropper

FIGURE 7. The simulation results of 2∗2 MIMO PLC system (a) The spectrum of transmitted message; (b) BER performance of legitimate receiver; (c) BER performance of eavesdropper; (d) eavesdropper decoding messages at different frequencies.

By altering parameters in DFE, they can be smaller enough so that the frequency domain of M would appear to be a complete message. In this context, the data1 is then hidden in both frequency domain and time domain to enhance the security of MIMO PLC while the information integrity is reserved. Thus, a legitimate user can extract it from the combined message M while it is difficult for a potential eavesdropper to decode received messages correctly.

To elaborate further, we also analyze secrecy capacity under the adoption of FD technique. The secrecy capacity, Cs, is given by the maximum difference between the mutual information of the legitimate user and eavesdropper channels [20], [25], [26]. It is defined by [27]

$$C_s = \max\{C_D - C_E, 0\} \tag{2}$$

where C_D, C_E are the legitimate user and eavesdropper capacities respectively. They are defined by

$$C_D = log_2(1+\gamma_D) \tag{3}$$
$$C_E = log_2(1+\gamma_E) \tag{4}$$

respectively, where γ_D, γ_E represents the instantaneous SINRs at legitimate user and eavesdropper. To investigate and highlight the effect of frequency division technique on enhancing system security, without loss of generality, we suppose the channel state is the same at both legitimate user and eavesdropper. The power spectral density of the AWGN and interferer as N_0, N_1 respectively. In this context, γ_D, γ_E are given by

$$\gamma_D = \frac{P_S\,|h_D|^2}{N_1+N_0} \tag{5}$$
$$\gamma_E = \frac{P_S\,|h_D|^2}{P_1\,|h_{N1}|^2+P_2\,|h_{N2}|^2+N_1+N_0} \tag{6}$$

respectively. h_{N1}, h_{N2}, h_D are the channel coefficient for Noise1, Noise2 and data1. P_1, P_2, P_S are the corresponding powers. Let $W_0 = P_S\,|h_D|^2, N = N_1+N_0, W_1 = P_1\,|h_{N1}|^2 + P_2\,|h_{N2}|^2$. Then C_s is given by

$$C_s = log_2\left(1+\frac{W_0}{N}\right) - log_2\left(1+\frac{W_0}{W_1+N}\right) \tag{7}$$

According to [28], the average secrecy capacity $\overline{C_s}$ is given by

$$\overline{C_s} = \mathbb{E}\left[Cs\right] = \mathbb{E}\left[log_2\left(1+\frac{W_0}{N}\right) - log_2\left(1+\frac{W_0}{W_1+N}\right)\right] \tag{8}$$

where $\mathbb{E}[\cdot]$ is the expectation operator. It is a function of γ_D and γ_E. It can be seen from (8) that $\overline{C_s}$ increases with increasing W_1. Thus, frequency division technique is theoretically applicable to enhance system security.

III. SIMULATION RESULTS

To evaluate the proposed 2∗2 MIMO PLC system in this paper, we simulate BER performance on MATLAB and the results are presented in this section. For the actual simulation, the low-voltage power line channel can be modeled as:

$$H(f) = g \cdot e^{-(a_0+a_1 \cdot f^k)d} \cdot e^{-j2\pi f(\tau_p)} \tag{9}$$

where a_0, a_1, k is the empirical parameter, representing the attenuation factor; f is the frequency of the communication; d is the transmission distance of the path, because there are reflections and refractions in power line transmission, so even though the relative position of the transceiver is constant, the actual transmission distance will still vary; τ_p is the path time delay; g is the weighting factor. The relevant channel parameters k is taken as 1, a_0 as 0, a_1 as $6.6 \times 10 - 11$ s/m, g as 0.041, and d as 267. The convolutional coding code rate is 1/2.

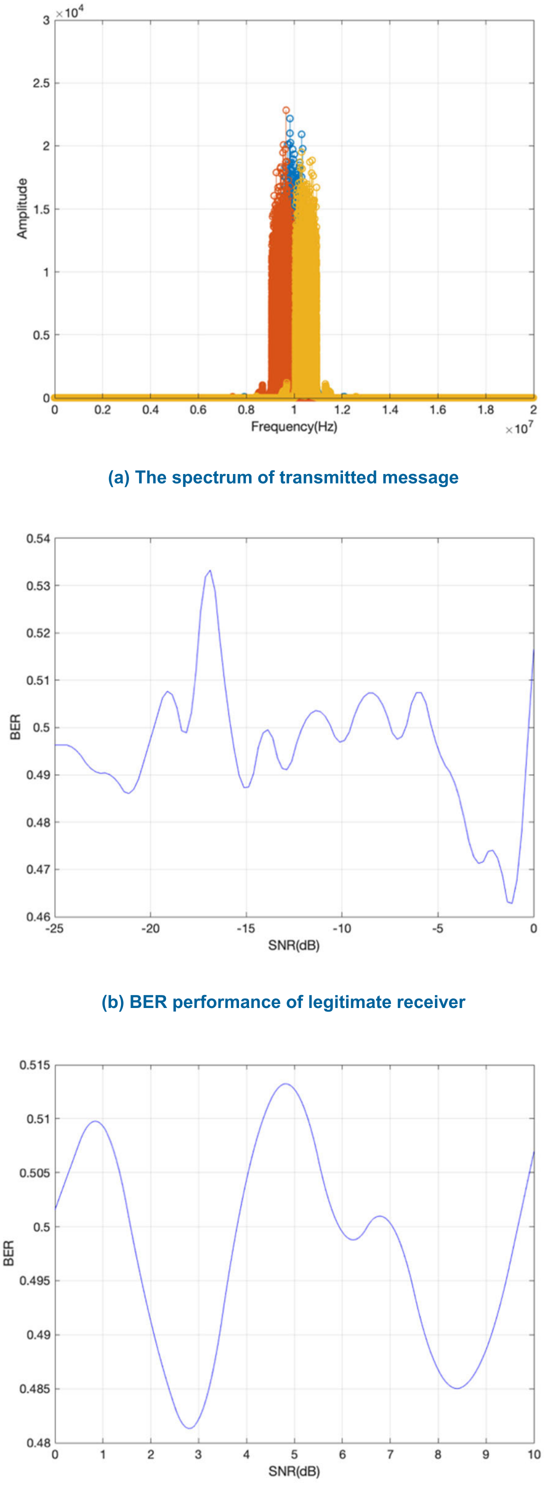
The concept of legitimate user and eavesdropper is introduced to conveniently evaluate security of system that adopt frequency division technique which is implemented with DFE. It is assumed that the legitimate user has the information of transmitter to decode receiving messages in a reverse process. The eavesdropper is assumed that it has ability to de-interleaving, de-scrambling, de-CC, de-RS correctly, while knowing nothing about information of DFE used in transmitter. Thus, system performance of 2∗2 MIMO PLC can be observed from legitimate user side, and security performance can be further observed by comparing it with eavesdropper side. The main reason we consider passive eavesdropping is that there exist exposing risks for eavesdropper to adopt active attack, thus the eavesdropper does not necessarily choose active attack [29], [30].

Fig. 7 is the simulation results of 2∗2 MIMO PLC system. We think it is more straightforward and intuitive to evaluate system security performance by comparing the BER performance of legitimate user and eavesdropper's.

Fig. 7(a) shows the spectrum of transmitted message. The information message represented in blue is shifted onto 10MHz. Artificial messages represented in red and yellow are shifted onto 9MHz and 11MHz respectively. All bandwidth is set to be 1.25MHz and is assumed to be known to the eavesdropper.

Fig. 7(b) shows the BER performance on legitimate side. Fig. 7(c) shows the BER performance on eavesdropper side. We set BER from -10dB to 0dB for legitimate receiver, 0dB to 10dB for eavesdropper.

Since the eavesdropper do not have correct center frequency knowledge, it decodes received message at a random frequency point, here we assume at 11MHz. It can be observed that the legitimate receiver can decode the confidential message correctly, while the eavesdropper can only acquire a messy noise with its BER fluctuating around 0.5. The system security is enhanced greatly.



(a) The spectrum of transmitted message

(b) BER performance of legitimate receiver

(c) BER performance of eavesdropper

FIGURE 8. The simulation results of 2∗2 MIMO PLC system under a smaller gap situation (a) The spectrum of transmitted message; (b) BER performance of legitimate receiver; (c) BER performance of eavesdropper.

Fig. 7(d) shows the BER performance of eavesdropper decoding message at different frequency points. The SNR is set to be 5dB. It is obvious that the closer the frequency is to the central frequency point, the better the BER performance is obtained.

We also investigate the effect of the gap between different spectrum (see Fig. 6).

Fig. 8(a) shows the spectrum of transmitted message. The two artificial messages are shifted onto 9.5MHz and 10.5MHz respectively. Gaps between different spectrums are narrowed.

Fig. 8(b) shows the BER performance on legitimate side. As expected, the performance is not well since the gap is too close that the frequency spectrum of original message has been contained. The performance on eavesdropper side remains poor as shown in Fig. 8(c).

To sum up, large gap may weaken system security since the original message can be easily distinguished on the frequency domain, while small gap destroys the integrity of the information message. Thus, a suitable gap is required.

Fig. 9 shows BER performance comparison of SISO / MIMO PLC system with other parameters remaining the same. It can be observed that the adoption of MIMO technique improves the performance of PLC system.

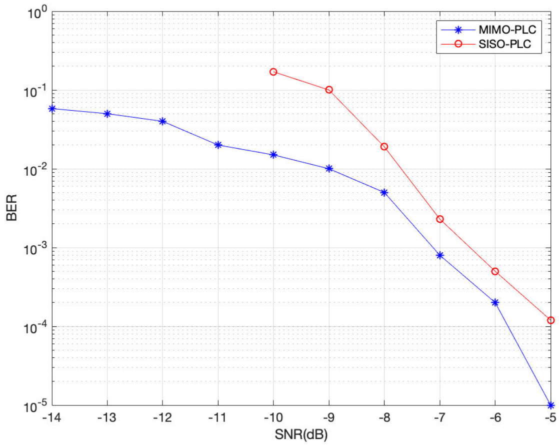


FIGURE 9. BER performance comparison of SISO / MIMO PLC system.

IV. CONCLUSION

In this paper, we presented a security enhanced 2∗2 FD MIMO PLC system. On one side, PLC channel is frequency selective and time-varying. Besides, it is easily disturbed by impulse noise. In this case, we first designed a 2∗2 FD MIMO PLC system. Channel coding include RS encoder, CC encoder are adopted to resist interference and improve BER performance. OFDM technique is adopted to combat multipath fading and inter-symbol interference. Spatial multiplexing is adopted to increase transmission rate. A new sweep mechanism which only needs *2N+1* communications is designed to find the optimal frequency point for upstream and downstream communication. On the other side, since eavesdropper can be easily connected to PLC system through physical access, security became a crucial issue that need to be considered. In this regard, we proposed a frequency division based method to enhance system security. Two artificial noises and data message were firstly shifted onto different frequency points, then combined into one transmitted message. During the processes, frequency domain information of data message was hidden. Finally, we presented simulation results of 2∗2 MIMO PLC system. The results showed that the BER performance of legitimate user side was better than eavesdropper side's. System security was enhanced evidently. Further work might include channel measurement and modeling. With a more precise understanding of channel characteristic, we can optimize the system in a targeted manner.

ACKNOWLEDGMENT

This article was presented at the 2019 IEEE International Conference on Parallel and Distributed Processing with Applications (ISPA) [DOI: 10.1109/ISPA-BDCloud-SustainCom-SocialCom48970.2019.00043].

REFERENCES

[1] T. Oliveira, F. Andrade, A. Picorone, H. Latchman, S. Lima Netto, and M. Ribeiro, "Characterization of hybrid communication channel in indoor scenario," *J. Commun. Inf. Syst.*, vol. 31, no. 1, pp. 224–235, 2016.

[2] T. R. Oliveira, A. A. Picorone, S. L. Netto, and M. V. Ribeiro, "Characterization of Brazilian in-home power line channels for data communication," *Electr. Power Syst. Res.*, vol. 150, pp. 188–197, Sep. 2017.

[3] G. Lopez, J. Matanza, D. De La Vega, M. Castro, A. Arrinda, J. I. Moreno, and A. Sendin, "The role of power line communications in the smart grid revisited: Applications, challenges, and research initiatives," *IEEE Access*, vol. 7, pp. 117346–117368, 2019.

[4] Q. Wang and Y. G. Wang, "Research on power Internet of Things architecture for smart grid demand," in *Proc. 2nd IEEE Conf. Energy Internet Energy Syst. Integr. (EI2)*, Oct. 2018, pp. 1–9.

[5] A. Canova, N. Benvenuto, and P. Bisaglia, "Receivers for MIMO-PLC channels: Throughput comparison," in *Proc. IEEE Int. Symp. Power Line Commun. Its Appl. (ISPLC)*, Mar. 2010, pp. 114–119.

[6] D. Schneider, A. Schwager, J. Speidel, and A. Dilly, "Implementation and results of a MIMO PLC feasibility study," in *Proc. IEEE Int. Symp. Power Line Commun. Appl.*, Apr. 2011, pp. 54–59.

[7] D. Schneider, J. Speidel, L. Stadelmeier, and D. Schill, "Precoded spatial multiplexing MIMO for inhome power line communications," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Nov./Dec. 2008, pp. 1–5.

[8] S. Galli, A. Scaglione, and Z. Wang, "For the grid and through the grid: The role of power line communications in the smart grid," *Proc. IEEE*, vol. 99, no. 6, pp. 998–1027, Jun. 2011.

[9] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[10] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[11] A. Pittolo and A. M. Tonello, "Physical layer security in PLC networks: Achievable secrecy rate and channel effects," in *Proc. IEEE 17th Int. Symp. Power Line Commun. Appl.*, Mar. 2013, pp. 273–278.

[12] A. Pittolo and A. Tonello, "Physical layer security in power line communication networks: An emerging scenario, other than wireless," *IET Commun.*, vol. 8, no. 8, pp. 1239–1247, May 2014.

[13] Y. Zhuang and L. Lampe, "Physical layer security in MIMO power line communication networks," in *Proc. 18th IEEE Int. Symp. Power Line Commun. Appl.*, Mar. 2014, pp. 272–277.

[14] J. Hokfelt, O. Edfors, and T. Maseng, "Turbo codes: Correlated extrinsic information and its impact on iterative decoding performance," in *Proc. IEEE 49th Veh. Technol. Conf.*, vol. 3, May 1999, pp. 1871–1875.

[15] K. V. Koutsouvelis and C. E. Dimakis, "A low complexity algorithm for generating turbo code S-random interleavers," *Wireless Pers. Commun.*, vol. 46, no. 3, pp. 365–370, Aug. 2008.

[16] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[17] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[18] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[19] B. Han, J. Li, J. Su, M. Guo, and B. Zhao, "Secrecy capacity optimization via cooperative relaying and jamming for WANETs," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 1117–1128, Apr. 2015.

[20] A. Salem, K. A. Hamdi, and E. Alsusa, "Physical layer security over correlated log-normal cooperative power line communication channels," *IEEE Access*, vol. 5, pp. 13909–13921, 2017.

[21] A. Salem, K. M. Rabie, K. A. Hamdi, E. Alsusa, and A. M. Tonello, "Physical layer security of cooperative relaying power-line communication systems," in *Proc. Int. Symp. Power Line Commun. Appl. (ISPLC)*, Mar. 2016, pp. 185–189.

[22] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 39–42, Jan. 2013.

[23] F. Passerini and A. M. Tonello, "Physical layer key generation for secure power line communications," 2018, *arXiv:1809.09439*. [Online]. Available: http://arxiv.org/abs/1809.09439

[24] E. Hogenauer, "An economical class of digital filters for decimation and interpolation," *IEEE Trans. Acoust., Speech, Signal Process.*, vol. 29, no. 2, pp. 155–162, Apr. 1981, doi: 10.1109/TASSP.1981.1163535.

[25] Y. W. P. Hong, P.-C. Lan and C.-C. J. Kuo, *Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems*, New York, NY, USA: Springer, 2014.

[26] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[27] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[28] A. U. Makarfi, R. Kharel, K. M. Rabie, O. Kaiwartya, and G. Nauryzbayev, "Physical layer security in vehicular communication networks in the presence of interference," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.

[29] M. Moradikia, H. Bastami, A. Kuhestani, H. Behroozi, and L. Hanzo, "Cooperative secure transmission relying on optimal power allocation in the presence of untrusted relays, a passive eavesdropper and hardware impairments," *IEEE Access*, vol. 7, pp. 116942–116964, 2019.

[30] A. Kuhestani, A. Mohammadi, and M. Mohammadi, "Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 341–355, Feb. 2018.

[31] G. Yan, Z. Wang, Y. Qian, and Y. Wu, "Physical layer security of digital front end based Internet of Things communication in power systems," in *Proc. IEEE Int. Conf. Parallel Distrib. Process. Appl., Big Data Cloud Comput., Sustain. Comput. Commun., Social Comput. Netw. (ISPA/BDCloud/SocialCom/SustainCom)*, Xiamen, China, Dec. 2019, pp. 236–241, doi: 10.1109/ISPA-BDCloud-SustainCom-SocialCom48970.2019.00043.

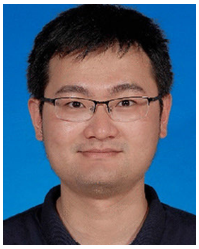
LINGANG YU is currently working with Jiangxi Power Supply Service Management Center, State Grid, China.

QIANG LIU is currently working with Jiangxi Power Supply Service Management Center, State Grid, China. His research interest includes automation of electric power systems.

DONGWEN WU is currently working with Jiangxi Power Supply Service Management Center, State Grid, China. His research interest includes automation of electric power systems.

QIN YAN is currently working with Jiangxi Electric Power Company Ltd., State Grid, Nanchang, China. His research interest includes automation of electric power systems.

GAOPENG YAN is currently pursuing the master's degree with the Department of Electrical Engineering, Shanghai Jiao Tong University, China. His research interest includes power line communication.



YONGPENG WU (Senior Member, IEEE) received the B.S. degree in telecommunication engineering from Wuhan University, Wuhan, China, in 2007, and the Ph.D. degree in communication and signal processing from the National Mobile Communications Research Laboratory, Southeast University, Nanjing, China, in 2013. He is currently a Tenure-Track Associate Professor with the Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai, China. Previously, he was a Senior Research Fellow with the Institute for Communications Engineering, Technical University of Munich, Germany, and Humboldt Research Fellow and a Senior Research Fellow with the Institute for Digital Communications, Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany. During his doctoral studies, he conducted cooperative research with the Department of Electrical Engineering, Missouri University of Science and Technology, USA. His research interests include massive MIMO/MIMO systems, massive machine type communication, physical layer security, and signal processing for wireless communications. He has been a TPC Member of various conferences, including Globecom, ICC, VTC, PIMRC, and so on. He was awarded the IEEE Student Travel Grants for the IEEE International Conference on Communications (ICC), in 2010; Alexander von Humboldt Fellowship, in 2014; the Travel Grants for the IEEE Communication Theory Workshop, in 2016; the Excellent Doctoral Thesis Awards of China Communications Society, in 2016; the Exemplary Editor Award of the IEEE Communications Letters, in 2017; and the Young Elite Scientist Sponsorship Program by CAST, in 2017. He was an Exemplary Reviewer of the IEEE Transactions on Communications, in 2015, 2016, and 2018. He was the Lead Guest Editor of the IEEE Journal on Selected Areas in Communications Special Issue on "Physical layer security for 5G wireless networks" and the IEEE Wireless Communications Special Issue on "Safeguarding 5G-and-beyond networks with physical layer security." He is currently an Editor of IEEE Wireless Communications, IEEE Transactions on Communications, and IEEE Communications Letters.

• • •