IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 2, 2017, accepted May 24, 2017, date of publication June 1, 2017, date of current version July 17, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2710081

Physical Layer Secure Transmission Based on Fast Dual Polarization Hopping in Fixed Satellite Communication

XIAOKAI ZHANG, BANGNING ZHANG, (Member, IEEE), AND DAOXING GUO, (Member, IEEE)
College of Communications and Engineering, PLA University of Science and Technology, Nanjing 210007, China

Corresponding author: Bangning Zhang (bangning_zhang@sina.com)

This work was supported by the Jiangsu Provincial Natural Science Foundation of China under Grant BK20141069.

ABSTRACT A fast dual polarization hopping (FDPH) system is designed to enhance the physical layer secure transmission in fixed down-link satellite communications. In order to prevent the eavesdropper from detecting transmitted signals, a pair of dual polarization states is chosen to carry the modulated signal by the designed FDPH pattern. The polarized signal is transmitted through orthogonal dual polarized parabolic antennas by the virtual polarization technique. Due to the assumption that the designed FDPH pattern is synchronous among the legitimate users, the legitimate receivers apply oblique projection polarization filter to suppress one of dual polarization states, and then have a polarization match to recover the scalar modulated signal and demodulate the scalar signal, whereas the eavesdropper cannot match the right polarization state. Therefore, the eavesdropper receives random amplitudes signal owing to the fast polarization hopping. If the modulation scheme is ASK and quadrature amplitude modulation, the demodulation performance of the eavesdropper would be very poor, resulting in a high bit error rate. Moreover, there is severe distinction in orthogonal dual polarized channel. The legitimate users would have a pre-linear compensation with perfect channel state information, which further worsen eavesdropping. Thus, the eavesdropper cannot even demodulate the phase-shift keying signal because of the time varying orthogonal dual polarized channel and auxiliary polarized angle. Simulation results demonstrate the secure performance of our design.

INDEX TERMS Physical layer secure transmission, satellite communications, fast dual polarization hopping, oblique projection polarization filter, orthogonal dual polarized channel.

I. INTRODUCTION

Satellite communications (SATCOM) systems, due to the inherent broadcasting nature and vast coverage area, are especially prone to security threats [1]. However, higher-layer cryptographic mechanisms are faced to be cracked with the development of computing power. In wireless communications, the key assumption to guarantee positive secrecy rate is that the legitimate users have better signal-to-noise ratios (SNR) than the eavesdroppers according to information theory, which is not always the case [2], [3]. To improve the secrecy rate under unfavorable conditions where legitimate users have worst SNR, one possible way to ensure positive secrecy rate is adopted multiple-input multiple-output (MIMO) antennas at the transmitter and/or receivers. When channel state information (CSI) is available, the secrecy capacity and optimization of the systems have been studied in [4]–[6]. Another promising approach is embed artificial noise (AN) [7] in the transmission of the information bearing signal for the purpose of degrading the channels to eavesdroppers, and AN is chosen to lie in the null space of the legitimate channel. Another typical secure model [8]–[10] applies multi-relays, which is designed to perform one of three different operation modes: amplify-and-forward (AF), decode-and-forward (DF), and cooperative jamming (CJ). Both MIMO and multi-relays are aimed to enhance the legitimate user's channel quality and deteriorate the malicious eavesdropper's.

However, there is severely distinction between the terrestrial communications and fixed SATCOM. The channel is almost addictive white Gaussian noise (AWGN) channel, whilst it is impossible to achieve multi-relays in fixed SATCOM. In order to ensure secure transmission in SATCOM, the feasible way is to prevent the eavesdropper from detecting the target communication signal, such as direct sequence spread spectrum (DSSS) techniques [11], frequency hopping spread spectrum (FHSS) techniques [12], beam-forming techniques [13], [14] and meteor burst communication (MBC) techniques [15], etc. DSSS and FHSS become less attractive choices owing to high cost involved in the spectrum occupation. Beam forming requires the location of eavesdroppers as a priori information. Actually, it is very hard to find the specific location of the eavesdroppers in practical case. Moreover, the satellite ought to be equipped phased array antennas, which costs a lot. Nonetheless, MBC has advantages in security and reliability. However, the long intermission for data transmission and the low average throughput of meteor channels limit its wide applications.

Fortunately, the polarization of the electromagnetic (EM) wave, an inherent attribute like frequency, amplitude and phase, provides an additional independent resource domain [16], [17]. It has been studied over several decades and also has many applications in optical fiber, radar, and satellite communications. One major advantage of polarization utilization is its potential to enhance channel capacity, since polarization provides independent degrees of freedom (DoFs) for information transmission. Theoretically, six co-located orthogonally polarized electrical and magnetic dipoles can offer up to six DoFs in a multipath scattering environment, that is, the ultimate sixfold improvement in channel capacity can be achieved [18]. Recently, co-located orthogonally dual-polarized antennas (ODPAs) have become a promising cost- and space-effective configuration and have been widely used in practical deployed wireless communication systems [19], [20]. The use of dual-polarized antennas enables receivers to obtain polarization information derived from the amplitude ratio and relative phase between two orthogonally polarized branch signals [21]. Since polarization is an independent parameter of waves, it can be used to design several technologies, such as polarization-based modulation [22], polarization-based signal sensing [23], polarization-based orthogonal transmission [24] and polarization-based filtering [25].

The fast polarization hopping has been used to mitigate prolonged deep fades in wireless communications [26]. Whereas, in this paper, the focus turns to employ a physical layer secure transmission scheme at polarization domain in the fixed down-link SATCOM system. To be specific, a high spectral efficiency fast dual polarization hopping (FDPH) system is designed to combine anti-detection and modulation information protection. We choose a pair of dual polarization states by the designed FDPH pattern to carry the modulated signal. The legitimate users apply oblique projection polarization filter (OPPF) to suppress one of dual polarization states, and then have a polarization match to recover the scalar modulated signal. On the contrary, the eavesdroppers are not aware of the FDPH pattern and can't recognize the accurate polarization state either to have polarization match. Therefore, the eavesdropper would receive random amplitude signals. In addition, due to the significant difference between the legitimate user and the eavesdropper in orthogonal dual polarized channel, the eavesdropper would receive time varying auxiliary polarized angle. More specifically, the main contributions are summarized as follows.

- In order to prevent the eavesdropper from detecting the polarized signal, a FDPH system is designed. The transmitted signals are carried by a pair of quickly hopping dual polarization states. The hopping rule is based on the designed FDPH pattern by two pseudo random sequences. The FDPH pattern is synchronous among the legitimate users. The secure performance is shown by the distinct bit error rate (BER) between the legitimate user and the eavesdropper.
- To further improve the FDPH secure performance, the difference of the orthogonal dual polarization channel between the eavesdroppers and the legitimate user is analyzed. The pre-linear compensation is conducted at the transmitter by CSI to eliminate the polarization coupling at the legitimate user and have further polarization scramble at the eavesdroppers.
- Amplitude and phase modulation schemes are adopted in the FDPH system. Simulation results show the secure performance of FDPH system under the ASK, phase-shift keying (PSK) and quadrature amplitude modulation (QAM) modulation schemes when the eavesdroppers employ unipolar antennas or orthogonal dual-polarized parabolic antennas (ODPPAs). Moreover, the performance of pre-linear transformation is also taken into account.

The rest of this paper is organized as follows. In Section II, the secure communication system model is introduced, then the characteristics of polarization channel and the polarization-based techniques are described. The FDPH system is set up for anti-detection, and the pre-linear transformation is proposed in Section III. Simulation results are presented in Section IV. Finally, Section V concludes this paper.

Notations: The superscript † and ^{H} are used to denote the pseudo-inverse and Hermitian transpose of a vector or matrix, respectively. Vectors and matrices are represented by bold lowercase and uppercase letters. $\arg[x]$ indicates the argument of x. $[\mathbf{A}]^T$ denotes the transpose of matrix $\mathbf{A}$.

II. SYSTEM MODEL AND POLARIZATION FUNDAMENTALS

A. THE SECURE COMMUNICATION SYSTEM MODEL

There are mainly three users in the proposed secure fixed down-link SATCOM system model, say Alice, Bob and Eve as shown in Fig. 1. Alice and Bob are legitimate users, and Eve is the eavesdropper. In order to recognize arbitrary polarization state, both of the legitimate users are equipped with ODPPAs. Whereas, the eavesdropper may apply unipolar parabolic antennas or ODPPAs. In this paper, a FDPH system is designed to prevent the eavesdropper from detecting the polarized signal. In addition, the confidential messages between Alice and Bob are transmitted through the polarized channel matrix $\mathbf{H}_{AB}$, and the polarized channel between Alice and Eve is $\mathbf{H}_{AE}$. $\mathbf{H}_{AB}$ and $\mathbf{H}_{AE}$ are distinct in orthogonal dual polarized channel because of different depolarized situations, which will be discussed below.

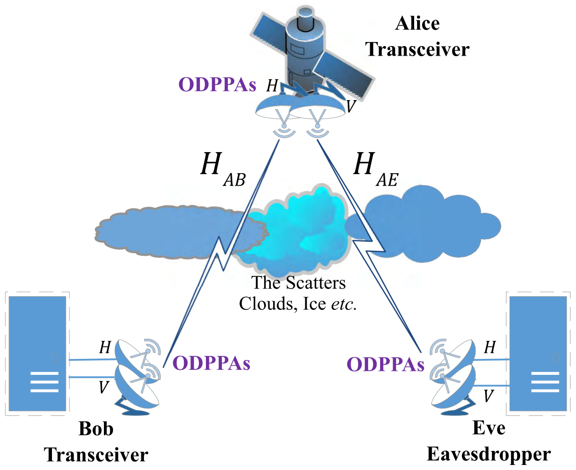


FIGURE 1. The secure communication system model.

B. FUNDAMENTALS OF POLARIZATION

The mathematical representation of a completely polarized EM wave in a right-handed *Cartesian* coordinate system uses Jones vector $\mathbf{E}$. $\mathbf{E}$ decomposes the electrical field signal into horizontal and vertical feeds ($\mathbf{H}$, $\mathbf{V}$), which is shown as [10]

$$\mathbf{E}_P(t) = \begin{bmatrix} E_h(t) \\ E_v(t) \end{bmatrix} = \begin{bmatrix} E_n \cos\gamma\, e^{j(\omega t+\phi_n)} \\ E_n \sin\gamma\, e^{j(\omega t+\delta+\phi_n)} \end{bmatrix}, \tag{1}$$

where $\gamma = \arctan(|E_v(t)|/|E_h(t)|)$ is called polarized angle in range of $[0, \pi/2]$, $\delta = \arg[E_h(t)] - \arg[E_v(t)]$ is auxiliary polarized angle in range of $[0, 2\pi]$, ω is the carrier frequencies of the signal, and $E_n e^{j(\omega t+\phi_n)}$ denotes the amplitude-phase modulation signal. $\mathbf{E}_P$ represents that the modulated signal is carried by the generated polarization state.

With the development of the digital signal processing (DSP) algorithms and high-performance polarization-agile antennas, virtual polarization utilizes power division units (PDU) and phase shift units (PSU) to generate arbitrary polarization state. virtual polarization have been widely employed polarization-based techniques [16]. The PDU is adjusted to divide modulated signal into two same components and then modify the amplitude ratio between these two components. The PSU is adjusted to modify the phase difference between the above two components. The polarization state is determined by the amplitude ratios and relative phase between two orthogonally polarized branch signals. Finally, the two signal components are radiated transverse electric and magnetic (TEM) wave by ODPAs, such as the horizontal and vertical polarized antennas, respectively.

C. SATELLITE DEPOLARIZATION CHANNEL MODEL

In fixed SATCOM polarization domain, there are two kinds of depolarization mechanisms in practical application during the propagation [16].

- Antenna depolarization: a linearly polarized antenna has a non-zero pattern for the cross-polar field. In other words, a vertically polarized antenna receiving a horizontally polarized wave will not be zero.
- Scatterer-based depolarization: the existing various clouds, rain and the small ice crystal in the air inducing reflection, diffraction and diffuse scattering usually modify the polarization state of the incident wave.

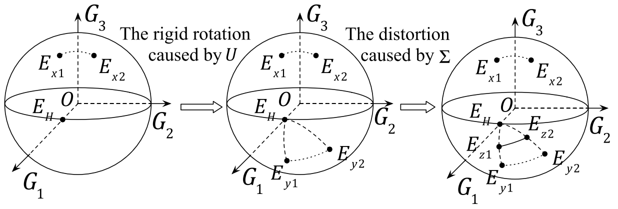


FIGURE 2. The impairment of polarization states by $\mathbf{H}$.

Therefore, the depolarization channel need be taken into consideration even in line-of-sight (LOS) condition. ODPPAs are adopted in both the transmitter and the receiver. The dual-orthogonal depolarized channel can be seen as 2x2 MIMO, which is defined as [22]

$$\mathbf{H} = \begin{bmatrix} h_{HH} & h_{HV} \\ h_{VH} & h_{VV} \end{bmatrix} = \mathbf{U}\Sigma\mathbf{V} = \mathbf{U}\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}\mathbf{V}, \tag{2}$$

where h_{XY} is the complex gain between the input *X-polarized* component and the output *Y-polarized* component. By singular value decomposition (SVD), $\mathbf{U}$ and $\mathbf{V}$ are unitary matrixes, and λ_i $(i = 1, 2)$ is the eigenvalue of $\mathbf{H}$, respectively. The unitary matrixes produce a rigid rotation effect on the surface of Poincare sphere [22]. It means that the power remain unchanged, while the polarized angles and the auxiliary polarized angles are changed, such as $\mathbf{E}_{xi}(i = 1, 2)$ rotates to $\mathbf{E}_{yi}(i = 1, 2)$ in Fig. 2. Σ creates asymmetries [22]: the polarization-sensitive power coupling behavior and the anisotropy of channels lead to structural distortion, which is the main reason of polarization dependent loss (PDL). For instance, $\mathbf{E}_{yi}(i = 1, 2)$ distorts to $\mathbf{E}_{zi}(i = 1, 2)$ in Fig. 2.

D. THE BLIND POLARIZATION STATE RECOGNITION SCHEME

If the modulated signal is carried by only one polarization state, the eavesdropper can recognized the polarization by received amplitudes and relative phases from sample values of ODPPAs, which is called the blind polarization state recognition scheme.

Fig. 3 shows the block digram of the receiver by blind polarization state recognition scheme. Two orthogonally polarized branch signals are received by ODPPAs, and down-converted (DC), sampled and filtered. The E_{hR} and E_{vR} are used to calculate ratios of amplitudes and their relative phase by Jones vector of the received polarized signal $\mathbf{E}_R$. We obtain

$$\begin{cases} \gamma_R = \arctan\left(|E_{vR}(t)| \,/\, |E_{hR}(t)|\right) \\ \delta_R = \arg[E_{hR}(t)] - \arg[E_{vR}(t)]. \end{cases} \tag{3}$$

After the polarization recognition, we employ this polarization to match the polarized vector signal to obtain the scalar

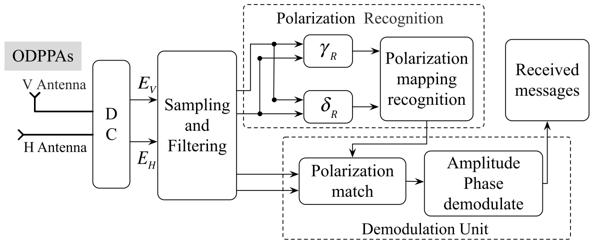


FIGURE 3. The block digram of the receiver by blind polarization state recognition scheme.

amplitude and phase signal. We obtain

$$E_R(t) = \begin{bmatrix} E_n \cos\gamma\, e^{j(\omega t+\phi_n)} \\ E_n \sin\gamma\, e^{j(\omega t+\delta+\phi_n)} \end{bmatrix} \begin{bmatrix} \cos\gamma_R \\ \sin\gamma_R e^{j\delta_R} \end{bmatrix}^T$$
$$= E_n e^{j(\omega t+\phi_n)} \left(\cos\gamma\cos\gamma_R + \sin\gamma\sin\gamma_R e^{j(\delta_R-\delta)}\right). \quad (4)$$

When $\gamma = \gamma_R$ and $\delta = \delta_R$, the received scalar signal is $E_R(t) = E_n e^{j(\omega t+\phi_n)}$, which can be demodulated by amplitude-phase demodulator.

E. DUAL POLARIZATION STATES SEPARATION BY OPPF

The oblique projection operator is a mature polarization signal separation method [27]. If matrixes $\mathbf{S}, \mathbf{I}$ and $[\mathbf{S}, \mathbf{I}]$ are column full rank, the oblique projection operator along subspace $\langle\mathbf{I}\rangle$ onto subspace $\langle\mathbf{S}\rangle$ is defined as [25]

$$\mathbf{P}_{SI} = \begin{bmatrix} \mathbf{S} & \mathbf{I} \end{bmatrix} \begin{bmatrix} \mathbf{S}^H\mathbf{S} & \mathbf{S}^H\mathbf{I} \\ \mathbf{I}^H\mathbf{S} & \mathbf{I}^H\mathbf{I} \end{bmatrix}^{\dagger} \begin{bmatrix} \mathbf{S}^H \\ \mathbf{I}^H \end{bmatrix}. \quad (5)$$

Furthermore, according to the property of the oblique projection operator, we have $\mathbf{P}_{SI}\mathbf{S} = \mathbf{S}$ and $\mathbf{P}_{SI}\mathbf{I} = \mathbf{0}$.

There are two polarization states $\mathbf{S}$ and $\mathbf{I}$, which are represented as $\left[\cos\gamma_S, \sin\gamma_S e^{j\delta_S}\right]^T$, $\left[\cos\gamma_I, \sin\gamma_I e^{j\delta_I}\right]^T$, respectively. Both of them are column full rank vectors.

According to (5), the oblique projection operator for polarization filter is given by

$$\tilde{\mathbf{H}}_{PF} = \mathbf{S}\left(\mathbf{S}^H\mathbf{P}_I^{\perp}\mathbf{S}\right)^{-1}\mathbf{S}^H\mathbf{P}_I^{\perp}, \quad (6)$$

where $\mathbf{P}_I^{\perp} = \mathbf{E} - \mathbf{I}\left(\mathbf{I}^H\mathbf{I}\right)^{-1}\mathbf{I}^H$ is the orthogonal projection operator onto the subspace $\mathbf{S}$, and $\mathbf{E}$ is an identity matrix.

Consider the received signal

$$\mathbf{R}_{input}(t) = \mathbf{S}E_n e^{j\omega t} + \mathbf{I}E_n e^{j\omega t} + \mathbf{n}(t), \quad (7)$$

where $\mathbf{n}(t)$ is the two dimensional additive white Gaussian noise (AWGN), which has independent and identically distributed (i.i.d), entries with normal distribution $\mathcal{CN}\left(0, \sigma^2\right)$. The theoretical OPPF can be given as (6), then the output signal can be written as

$$\begin{aligned} \mathbf{R}_{output}(t) &= \tilde{\mathbf{H}}_{PF}\left(\mathbf{S}E_n e^{j\omega t} + \mathbf{I}E_n e^{j\omega t} + \mathbf{n}(t)\right) \\ &= \tilde{\mathbf{H}}_{PF}\mathbf{S}E_n e^{j\omega t} + \tilde{\mathbf{H}}_{PF}\mathbf{I}E_n e^{j\omega t} + \tilde{\mathbf{H}}_{PF}\mathbf{n}(t) \\ &= \tilde{\mathbf{H}}_{PF}\mathbf{S}E_n e^{j\omega t} + \tilde{\mathbf{H}}_{PF}\mathbf{n}(t) = \mathbf{S}E_n e^{j\omega t} + \tilde{\mathbf{H}}_{PF}\mathbf{n}(t). \end{aligned} \quad (8)$$

If two polarization states carry the same modulated signal at the same time, only one polarization state can be left without loss, and another will be suppressed perfectly by OPPF. In (8), the noise power after processing by $\tilde{\mathbf{H}}_{PF}$ is denoted as [27]

$$\hat{\sigma}^2 = trace\left(\sigma^2\tilde{\mathbf{H}}_{PF}\tilde{\mathbf{H}}_{PF}^H\right) = \frac{\sigma^2}{\sin^2(\zeta)}, \quad (9)$$

where ζ is the principal angle between subspace $\mathbf{S}$ and $\mathbf{I}$ on poincare sphere. It is obvious that the noise is amplified by the OPPF. Therefore, the relationship between the output SNR and input SNR can be described for the degree of deterioration. We have

$$\Delta SNR = SNR_{output} - SNR_{input} = 20\log\sin(\zeta). \quad (10)$$

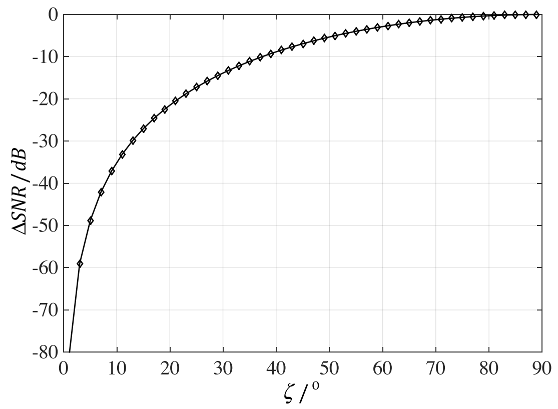


FIGURE 4. The relationship between ΔSNR and the principal angle ζ of OPPF.

Fig. 4 shows that the principal angle between subspace $\mathbf{S}$ and $\mathbf{I}$ determines the performance of OPPF. In designed dual polarization hopping system, the principal angle must be taken into account.

III. SIGNAL DESIGN FOR FDPH SYSTEM

A. THE DUAL POLARIZATION STATES SIGNAL DESIGN FOR ANTI-DETECTION

If only one polarization state even fast hopping is applied to carry modulated signal, it is easy to be eavesdropped by the blind polarization state recognition scheme by Section II-D.

In order to prevent the eavesdropper from using the blind polarization recognition scheme to intercept signals, we propose to utilize a pair of dual polarization states

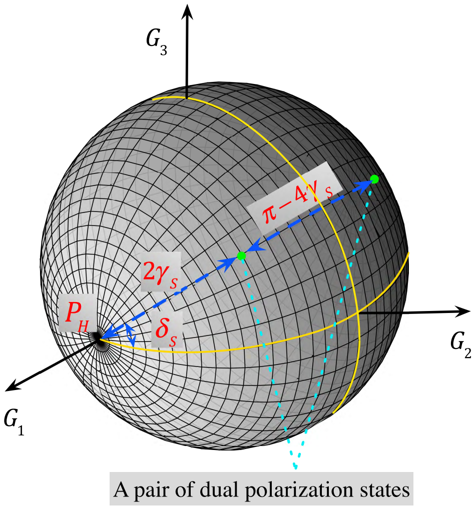


FIGURE 5. A pair of dual polarization states on Poincare Sphere. $2\gamma_S$ and $\pi-2\gamma_S$ are the double polarized angle of dual polarization states and ϕ_S is the auxiliary polarized angle. The principal angle of dual polarization states is $\pi-4\gamma_S$.

to carry modulated signal at the same time. One polarization state $\mathbf{E}_1$ is $\left[\cos\gamma_S, \sin\gamma_S e^{j\delta_S}\right]^T$, which is seen as target polarization states. Another polarization state $\mathbf{E}_2$ is $\left[\cos(\pi/2-\gamma_S), \sin(\pi/2-\gamma_S)\, e^{j\delta_S}\right]^T$, which is seen as the self-interference in polarization domain. $\mathbf{E}_1$ and $\mathbf{E}_2$ are on *G2-O-G3* plane symmetry in Fig. 5. Thus, the transmitted signal is

$$\mathbf{E}_T(t) = \begin{bmatrix} E_{hT}(t) \\ E_{vT}(t) \end{bmatrix} = \begin{bmatrix} E_{1h}(t) \\ E_{1v}(t) \end{bmatrix} + \begin{bmatrix} E_{2h}(t) \\ E_{2v}(t) \end{bmatrix} = \begin{bmatrix} E_n\left[\cos\gamma_S + \cos\left(\frac{\pi}{2}-\gamma_S\right)\right] e^{j(\omega t+\phi_n)} \\ E_n\left[\sin\gamma_S + \sin\left(\frac{\pi}{2}-\gamma_S\right)\right] e^{j(\omega t+\delta_S+\phi_n)} \end{bmatrix}. \quad (11)$$

The applied dual polarization states are known as a priori information among the legitimate users. Thus, the OPPF is utilized to suppress one of dual polarization states. It is obvious that the legitimate user won't be affected by applying dual polarization states to transmit at the same time.

Nevertheless, for eavesdroppers, if they utilize the unipolar antenna to receive the signal, the amplitude and phase of received signal are random because of fast polarization hopping. Another option is using blind polarization state recognition scheme by ODPPAs. According to Section II-D, the eavesdroppers obtain amplitude ratios and relative phases, which are

$$\begin{cases} \gamma_E = \arctan\left(\dfrac{\cos\gamma_S + \cos\left(\frac{\pi}{2}-\gamma_S\right)}{sin\gamma_S + \sin\left(\frac{\pi}{2}-\gamma_S\right)}\right) = \dfrac{\pi}{4} \\ \delta_E = \arg\left[E_{hT}(t)\right] - \arg\left[E_{vT}(t)\right] = \delta_S. \end{cases} \quad (12)$$

The recognized polarization angle is $\pi/4$, while the transmitted polarization angles are random by polarization hopping. The blind polarization recognition scheme is failed and the eavesdropper can't match the polarization to get lossless modulated signals.

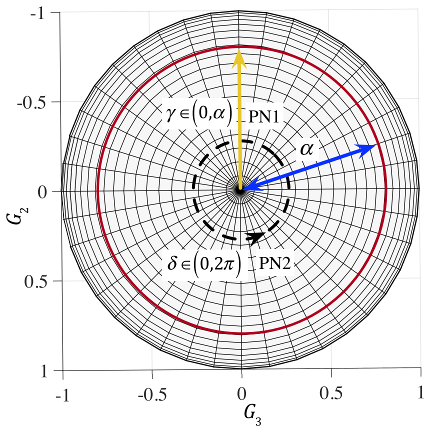


FIGURE 6. One of dual polarization hopping pattern on Poincare Sphere, which projects to G_2-O-G_3 plane. Another polarization state is on G_2-O-G_3 plane symmetry.

B. FAST POLARIZATION HOPPING PATTERN DESIGN

As mentioned above, fast polarization hopping rule is key to prevent the eavesdropper from detecting the dual polarized signals.

In order to generate a FDPH pattern, pseudo random sequences, like *M* sequence or *Gold* sequence, are used to map different polarization states. To obtain polarization scramble as much as possible, two independent PN sequences are employed to control the pattern mapping, i.e. PN1 and PN2. Due to the polarization are on *G2-O-G3* plane symmetry, one of the dual polarization states is determined, and the other is fixed. The fast polarization hopping pattern is generated as follow steps.

- Generate two independent binary pseudo-random sequences, say PN1 and PN2, and detect the homogeneity and randomness of PN sequence.
- According to the requirement of the system, determine the pairs number of variable polarization.
- In order to obtain polarization scramble as much as possible, the number of polarized angle and auxiliary polarized angles should be split as consistent as possible. The half of polarization angle, ranged of $[0,\alpha]$, and auxiliary polarized angle, ranged of $[0,2\pi]$, are equally divided, which is shown in Fig. 6. α is ranged of $(0,\pi/4)$. Two dimension sets are built.
- PN1 is chosen to determine the set of different polarization angles and PN2 is chosen to determine the set of different auxiliary polarized angles.

Through the polarization hopping design, the γ_S entries with uniform distribution $\mathrm{U}(0,\alpha)$, where α is ranged of $(0,\pi/4)$, and the ϕ_S entries with uniform distribution $\mathrm{U}(0,2\pi)$. The principal angle of dual polarization is ranged of $[\pi/2-2\alpha, \pi/2]$. The selection of α would influence the performance of OPPF on the basis of Fig. 4. α is getting closer to $\pi/4$, the worse the BER performance of legitimate users, nevertheless, the degree of polarization scramble is deep.

The legitimate users are aware of the fast dual polarization pattern, which is strictly synchronized. However, the eavesdropper doesn't know the pattern and it is impossible to intercept and capture from the received signal.

C. THE PRE-LINEAR COMPENSATION FOR THE LEGITIMATE ORTHOGONAL DUAL POLARIZED CHANNEL

Although SATCOM own long latency characteristics, the variation of polarized channel is relatively slow in the fixed SATCOM system. Applying pre-linear compensation would decouple two orthogonally polarized branch signals.

Bob obtains the CSI through the pilot sent by Alice, and Alice receives the CSI by feedback channel. Thus, the orthogonal dual polarized channel matrix $\mathbf{H}_{AB}$, which is $\mathbf{H}_{AB} = \mathbf{U}_{AB}\Sigma_{AB}\mathbf{V}_{AB}$ by SVD, is both known to Alice and Bob. The scaling of transmitter by the singular may be compensated at the transmitter by using the linear compensation $\mathbf{V}_{AB}^{H}\Sigma_{AB}^{-1}$ or at the receiver by the linear compensation $\Sigma_{AB}^{-1}\mathbf{U}_{AB}^{H}$. We adopt the linear compensation $\mathbf{V}_{AB}^{H}\Sigma_{AB}^{-1}$ at the transmitter, then have

$$\mathbf{E}_R = \mathbf{H}_{AB}\mathbf{V}_{AB}^{H}\Sigma_{AB}^{-1}\mathbf{E}_T + \mathbf{n} = \mathbf{U}_{AB}\mathbf{E}_T + \mathbf{n}. \qquad (13)$$

If we process polarization states by $\mathbf{U}_{\text{AB}}$ before matching the received signal at the receiver, the signal received by Bob would be decoupled and may be detected individually.

The orthogonal dual polarized channel matrix $\mathbf{H}_{AE}$ between Alice and Eve are unknown for both of them. $\mathbf{H}_{AB}$ and $\mathbf{H}_{AE}$ are hardly identical owing to the uneven distribution of water vapor, small ice crystals and the troposphere during the propagation, as well as the polarization characteristics between the different ODPPAs. Thus, the eavesdropper receives

$$\begin{aligned}\mathbf{E}_{RE} &= \mathbf{H}_{AE}\mathbf{V}_{AB}^{H}\Sigma_{AB}^{-1}\mathbf{E}_T + \mathbf{n}\\ &= \mathbf{U}_{AE}\Sigma_{AE}\mathbf{V}_{AE}\mathbf{V}_{AB}^{H}\Sigma_{AB}^{-1}\mathbf{E}_T + \mathbf{n}.\end{aligned} \qquad (14)$$

The Σ_{AE} and Σ_{AB}^{-1} would lead to serious damage to the amplitude of signal received at the eavesdropper. $\mathbf{U}_{AE}$, $\mathbf{V}_{AE}$ and $\mathbf{V}_{AB}^{H}$ would produce a rigid rotation effect on the surface of Poincare sphere of transmitted polarization states.

IV. NUMERICAL SIMULATION RESULTS

In the designed FDPH system, we assume the fast dual polarization hopping pattern have been perfectly synchronized and the CSI is known for legitimate users. The structure of transceiver is designed as shown in Figs. 7/8.

Fig. 7 is the block digram of the legitimate transmitter. The input data is modulated at first, i.e. ASK, PSK, QAM *etl.* Then, a pair of dual polarization states is generated to carry the modulated signal at the same time by the designed FDPH pattern. To reduce the couple between parallel branches, the pre-linear compensation $\mathbf{V}_{AB}^{H}\Sigma_{AB}^{-1}$ is adopted.

Fig. 8 is the block digram of the legitimate receiver. The OPPF, which is generated by designed FDPH pattern by (6), separates dual polarization states after DC, sampling and filtering. Then, polarization match is applied to recover the scalar signal for demodulating the original input information.

Due to the OPPF amplify the noise and the uniform distribution of the principal angle ζ, the BER performance of the legitimate receiver can be reformulated as

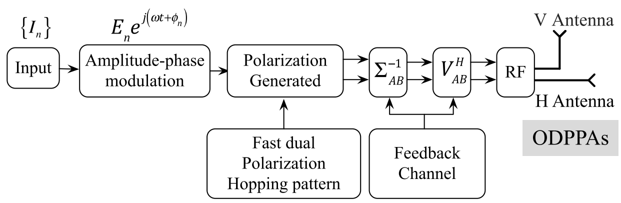


FIGURE 7. The block digram of the transmitter, which is design for Alice.

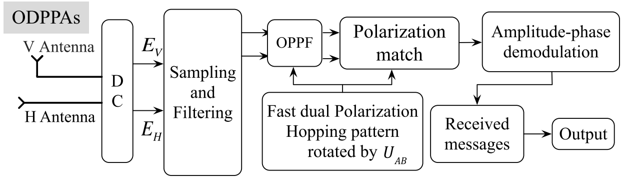


FIGURE 8. The block digram of the receiver, which is design for Bob.

$$Pe_{legi} = \int_{\frac{\pi}{2}-2\alpha}^{\frac{\pi}{2}} \frac{1}{2\alpha} Pe_{\,\text{mod}}\left(SNR * \sin^2(\zeta)\right) d\zeta, \qquad (15)$$

where $Pe_{\,\text{mod}}$ denotes the BER formula of employed modulation scheme in AWGN channel, SNR is the bit or symbol SNR at the certain modulation scheme. Owing to the range of α is $[0, \pi/4]$ and a better BER performance, we choose $\alpha = \pi/8$ in our simulations.

To enhance the fast hopping performance, we assume one hop per symbol. Therefore, the security performance is related to the different types of antennas at the eavesdropper and the distinction of the dual polarized channels between the legitimate user and the eavesdropper.

A. THE SECURE PERFORMANCE BY EMPLOYING DIFFERENT TYPES OF ANTENNAS AT THE EAVESDROPPER

In this subsection, we assume the orthogonal dual polarized channel is almost the same between the eavesdropper and the legitimate user. There are two situations according to the different types of antennas at the eavesdropper.

There is unipolar for most conventional parabolic antenna. If the eavesdropper applies unipolar parabolic antenna, the received signal would be

$$E_{Eve} = (A_i + jB_i)\, E_n e^{j(\omega t+\phi_n)}, \qquad (16)$$

where $A_i + jB_i$ is a random plural because of the fast polarization hopping. If the modulation employs amplitude or phase modulation, the eavesdropper can hardly detect the information. Simulation results are shown in Fig. 9, which indicate that eavesdroppers can't demodulate the received FDPH signal. If they employ unipolar parabolic antenna, BER performance of the eavesdropper is very poor at arbitrary SNR.

Another situation is that the eavesdropper is equipped with the ODPPAs. The eavesdropper would recognize the

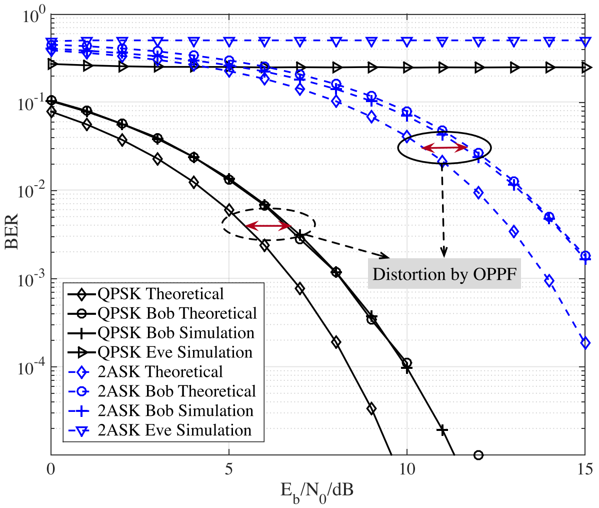


FIGURE 9. BER versus E_b/N_0 performance of 2ASK and QPSK when the legitimate user applies ODPPAs and the eavesdropper employs the unipolar antenna.

polarization state first, just like Fig. 3. Due to applying a pair of dual polarization states to load the signal at the transmitter, the eavesdropper identifies polarization state as $\left[\cos(\pi/4), \sin(\pi/4)\, e^{j\phi_s}\right]^T$ in (8). The scalar output after polarization match is

$$E_{Eve} = \sqrt{2}\sin\left(\gamma_S + \frac{\pi}{4}\right) E_n e^{j(\omega t+\phi_n)}. \tag{17}$$

Due to the random amplitudes of the received scalar signal, ASK and QAM would be severely affected by fast hopping of γ_S, while the PSK wouldn't be affected due to the unchanged of auxiliary polarized angle. Simulation results are shown in Figs. 10/11/12.

Figs. 10/11 show extraordinary secure performance by applying ASK and QAM as modulation scheme. Due to employing a pair of dual polarization to load the modulated signal at the same time, the eavesdropper can't identify the polarization angle, which leads to severe amplitude scramble. For ASK and QAM, the demodulation is related to amplitude. Hence, the eavesdropper exhibit a high BER at arbitrary SNR, whilst the legitimate user would suffer a little distortion owing to separate dual polarization by OPPF.

Fig. 12 shows the secure transmission scheme is entirely noneffective when PSK is employed as modulation scheme. The reason is that the auxiliary polarized angle δ_S can be recognized by the eavesdropper in (12). The variation of amplitudes have little impact in PSK. When ignoring the distinction of dual polarized channel, PSK is unsuitable for secure transmission.

B. THE SECURE PERFORMANCE AT DIFFERENT ORTHOGONAL DUAL POLARIZED CHANNEL

In last subsection, both ASK and QAM play a predominant secure performance in proposed FDPH scheme even without considering the difference of orthogonal dual polarized channel. However, the performance of PSK is not entirely

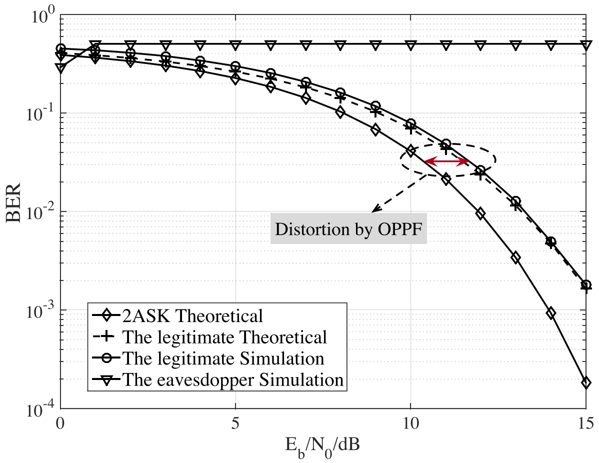


FIGURE 10. BRE versus E_b/N_0 performance of 2ASK when both the legitimate user and the eavesdropper apply ODPPAs.

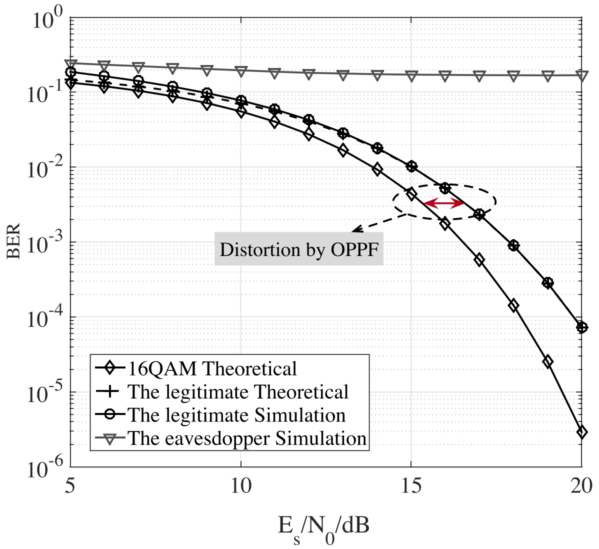


FIGURE 11. BER versus E_S/N_0 performance of 16QAM when both the legitimate user and the eavesdropper apply ODPPAs.

satisfactory. Another situation is that the eavesdropper are aware of FDPH pattern by spies or other non-direct physical mans.

In this subsection, we take the time varying orthogonal dual polarized channel into account to further enhanced secure performance of FDPH system. Due to distinct co-polar antenna direction pattern and uneven distribution of the water vapor, the small ice crystal and the troposphere flashing, the orthogonal dual polarized channel between $\mathbf{H}_{AB}$ and $\mathbf{H}_{AE}$ is quite different. The orthogonal dual polarized channel can be reduced to $\mathbf{H} = \mathbf{U}\Sigma\mathbf{V}$ by SVD in (2). The diagonal matrix Σ lead to structural distortion, which means that only the amplitude of signal would be changed. The unitary matrixes $\mathbf{U}$ and $\mathbf{V}$ produce a rigid rotation effect on the surface of Poincare sphere, which means that the polarized angle and auxiliary polarized angle would be severely distinct from the

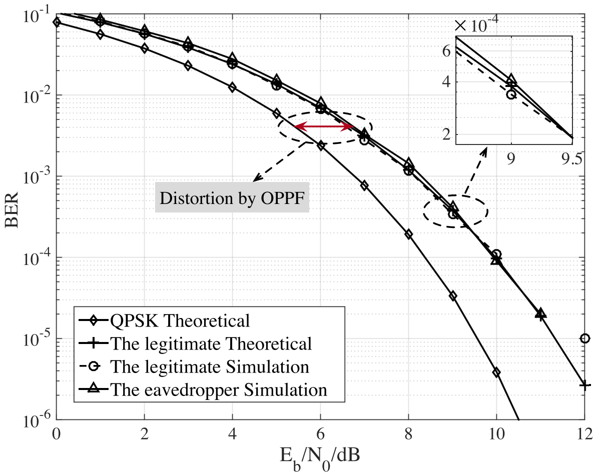
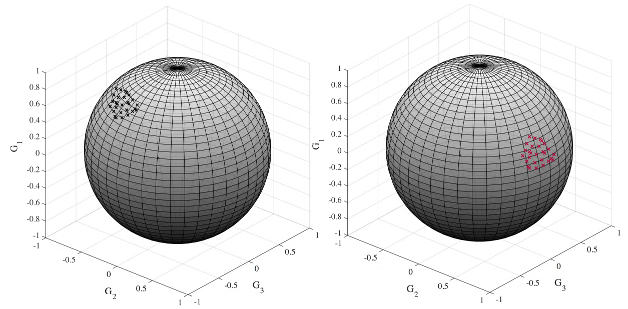


FIGURE 12. BER versus E_b/N_0 performance of QPSK when both the legitimate user and the eavesdropper apply ODPPAs.



(a) (b)

FIGURE 13. The unitary matrixes produce a rigid rotation effect on the surface of Poincare sphere. (a) is before rotation; (b) is after rotation.

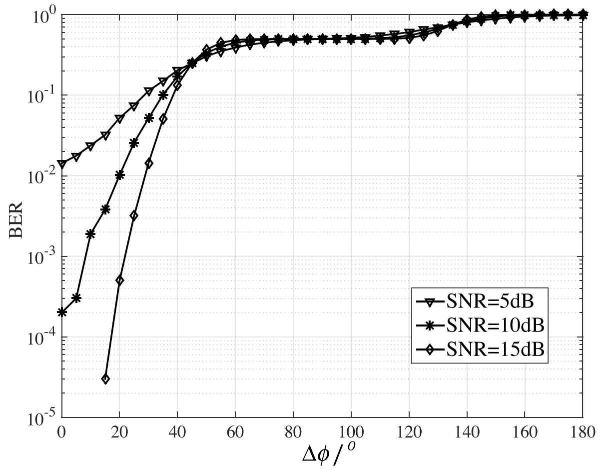


FIGURE 14. The BER performance of QPSK versus $\Delta\phi$, when SNR=5dB, 10dB and 15dB.

transmitted signal and is shown as Fig. 13. According to (4), the varying polarized angle is related to the amplitude and the varying auxiliary polarized angle is related to the phase of received signal.

The legitimate users employ the pre-linear compensation for the time varying orthogonal dual polarized channel by CSI. The eavesdroppers would suffer the influence of $\mathbf{U}_{AE}\Sigma_{AE}\mathbf{V}_{AE}\mathbf{V}_{AB}^{H}\Sigma_{AB}^{-1}$ by (14).

The secure performance of ASK and QAM would be the same to last subsection because of varying Σ_{AB}^{-1} and Σ_{AE}. However, the secure performance of PSK is far different owing to the random varying phase. For PSK, Σ_{AB}^{-1} and Σ_{AE} have little influence on the secure performance, while $\mathbf{U}_{AE}$, $\mathbf{V}_{AE}$ and $\mathbf{V}_{AB}^{H}$ would result in random changes in phase. We define the vary phase as

$$\Delta\phi = (\delta_R - \delta)\ \mathrm{MOD}\ \pi, \tag{18}$$

where MOD denotes the modulo operation. The eavesdropper would received a random phase owing to unitary matrixes. Therefore, $\Delta\phi$ entries approximately with uniform distribution $U(0, \pi)$.

Fig. 14 shows the BER performance versus $\Delta\phi$. When the $\Delta\phi \geq 40^\circ$, the BER is more than 10^{-1} at the any symbol SNR. Since $\Delta\phi$ can be approximately seen as uniform distribution, the eavesdropper would get a highly BER from a long time in PSK. Thus, the legitimate users can apply PSK as modulation scheme for secure transmission when the discrimination of the different time-varying orthogonal dual polarized channel is taken into account.

V. CONCLUSION

In this paper, we introduce a FDPH system, which is designed to enhance the physical layer secure transmission in fixed down-link SATCOM. We choose a pair of dual polarization states by FDPH pattern to carry the modulated signal. The legitimate users apply OPPF to eliminate one of dual polarization states, and then have a polarization match to recover the modulated signal and demodulate the transmitted information. Whereas, the eavesdropper can't recognize the accurate polarization state to have polarization match and receives random amplitude signals, say ASK and QAM as modulation scheme. Thus, the demodulation performance of the eavesdropper is poor, resulting in a high bit error rate. Moreover, due to the quite difference between the legitimate user and the eavesdropper in polarized channel, the eavesdropper can't even demodulate the PSK signal because of the time varying auxiliary polarized angle. Simulation results demonstrated the effectiveness of the FDPH system. In a practical system, there are eavesdroppers and jammers at the same time. Therefore, a secure and anti-jamming scheme would be designed at polarization domain in our future work.

REFERENCES

[1] K. An, M. Lin, J. Ouyang, and W.-P. Zhu, "Secure transmission in cognitive satellite terrestrial networks," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 11, pp. 3025–3037, Nov. 2016.

[2] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[3] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015.

[4] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[6] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[7] W. Wang, K. C. Teh, and K. H. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1470–1482, Jun. 2017.

[8] J. H. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 525–528, Apr. 2015.

[9] H.-M. Wang and X.-G. Xia, "Enhancing wireless secrecy via cooperation: Signal design and optimization," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 47–53, Dec. 2015.

[10] C. Xing, S. Ma, Z. Fei, Y. C. Wu, and H. V. Poor, "A general robust linear transceiver design for multi-hop amplify-and-forward MIMO relaying systems," *IEEE Trans. Signal Process.*, vol. 61, no. 5, pp. 1196–1209, Mar. 2013.

[11] Q. Z. Ahmed, K.-H. Park, and M.-S. Alouini, "Ultrawide bandwidth receiver based on a multivariate generalized Gaussian distribution," *IEEE Trans. Wireless Commun.*, vol. 14, no. 4, pp. 1800–1810, Apr. 2014.

[12] L. Zhao, L. Wang, G. Bi, L. Zhang, and H. Zhang, "Robust frequency-hopping spectrum estimation based on sparse Bayesian method," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 781–793, Feb. 2015.

[13] G. Zheng, P.-D. Arapoglou, and B. Ottersten, "Physical layer security in multibeam satellite systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 852–863, Feb. 2012.

[14] X. Wang, K. Wang, and X.-D. Zhang, "Secure relay beamforming with imperfect channel side information," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2140–2155, Jun. 2013.

[15] Z. Li, F. Zhou, X. Chen, Y. Li, and F. Gao, "An adaptive state assignment mechanism based on joint data detection and channel estimation on fading meteor channel," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 4627–4635, Jun. 2017, doi: 10.1109/TVT.2016.2618938.

[16] C. Guo, F. Liu, S. Chen, C. Feng, and Z. Zeng, "Advances on exploiting polarization in wireless communications: Channels, technologies, and applications," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 125–166, 1st Quart., 2016.

[17] M. R. Andrews, P. P. Mitra, and R. deCarvalho, "Tripling the capacity of wireless communications using electromagnetic polarization," *Nature*, vol. 409, no. 6818, pp. 316–318, 2001.

[18] T. Svantesson, M. A. Jensen, and J. W. Wallace, "Analysis of electromagnetic field polarizations in multiantenna systems," *IEEE Trans. Wireless Commun.*, vol. 3, no. 2, pp. 641–646, Mar. 2004.

[19] X.-W. Dai, Z.-Y. Wang, C.-H. Liang, X. Chen, and L.-T. Wang, "Multiband and dual-polarized omnidirectional antenna for 2G/3G/LTE application," *IEEE Antennas Wireless Propag. Lett.*, vol. 12, pp. 1492–1495, Nov. 2013.

[20] B. Cao, H. Liang, J. W. Mark, and Q. Zhang, "Exploiting orthogonally dual-polarized antennas in cooperative cognitive radio networking," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 11, pp. 2362–2373, Nov. 2013.

[21] T. Pratt, B. Walkenhorst, and S. Nguyen, "Adaptive polarization transmission of OFDM signals in channels with polarization mode dispersion and polarization-dependent loss," *IEEE Trans. Wireless Commun.*, vol. 8, no. 7, pp. 3354–3359, Jul. 2009.

[22] D. Wei, C. Feng, C. Guo, and L. Fangfang, "A power amplifier energy efficient polarization modulation scheme based on the optimal pre-compensation," *IEEE Commun. Lett.*, vol. 17, no. 3, pp. 513–516, Mar. 2013.

[23] C. Guo, X. Wu, C. Feng, and Z. Zeng, "Spectrum sensing for cognitive radios based on directional statistics of polarization vectors," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 3, pp. 379–393, Mar. 2013.

[24] M. Yofune, J. Webber, K. Yano, H. Ban, and K. Kobayashi, "Optimization of signal design for poly-polarization multiplexing in satellite communications," *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2017–2020, Nov. 2013.

[25] B. Cao, J. Yu, Y. Wang, and Q. Zhang, "Enabling polarisation filtering in wireless communications: Models, algorithms and characteristics," *IET Commun.*, vol. 7, no. 3, pp. 247–254, Feb. 2013.

[26] K. T. Wong, S. L. A. Chan, and R. P. Torres, "Fast-polarization-hopping transmission diversity to mitigate prolonged deep fades in indoor wireless communications," *IEEE Antennas Propag. Mag.*, vol. 48, no. 3, pp. 20–27, Jun. 2006.

[27] W. Zhao, C. Feng, F. Liu, and C. Guo, "Polarization oblique projection based self-interference cancellation against PA nonlinear distortion in MIMO full duplex system," *China Commun.*, vol. 13, no. 11, pp. 49–59, Nov. 2016.

XIAOKAI ZHANG received the B.S. degree from the Harbin Institute of Technology, Harbin, China, in 2015. He is currently pursuing the M.S. degree with the PLA University of Science and Technology, Nanjing, China. His research interests include satellite communications, polarization shift keying, anti-jamming system, and physical layer security.

BANGNING ZHANG received the B.S. and M.S. degrees from the Institute of Communications Engineering, Nanjing, China, in 1984 and 1987, respectively. He is currently a Full Professor and the Head of the College of Communications Engineering, PLA University of Science and Technology. He has authored or co-authored over 80 conference and journal papers and has been granted more than 20 patents in his research areas. His current research interests include communication anti-jamming technologies, microwave technologies, polarization technologies, satellite communications systems, cooperative communications, and physical layer security. Prof. Zhang has served as a Reviewer for several journals in the communication field.

DAOXING GUO received the B.S., M.S., and Ph.D. degrees from the Institute of Communications Engineering, Nanjing, China, in 1995, 1999, and 2002, respectively. He is currently a Full Professor and also a Ph.D. Supervisor with the PLA University of Science and Technology. He has authored or co-authored over 40 conference and journal papers and has been granted more than 20 patents in his research areas. His current research interests include satellite communications systems and transmission technologies, communication anti-jamming technologies, polarization technologies, and communication anti-interception technologies, including physical layer security. Prof. Guo has served as a Reviewer for several journals in the communication field.

• • •