Secure Channel Estimation Method in TDD OFDM Systems

Sen-Hung Wang
Institute of Communications Engineering
National Sun Yat-Sen University
Kaohsiung, Taiwan
senhung@staff.nsysu.edu.tw

Frank Po-Chen Lin
Department of Electrical Engineering
National Sun Yat-Sen University
Kaohsiung, Taiwan
frank555076@gmail.com

Chih-Peng Li
Institute of Communications Engineering
Department of Electrical Engineering
National Sun Yat-Sen University
Kaohsiung, Taiwan
cpli@faculty.nsysu.edu.tw

***Abstract*—Physical layer security in wireless communication deals mainly with unauthorized users, eavesdroppers, and/or jammers. It is crucial for wireless network due to its broadcast nature and the channel state information (CSI) is easily acquired by unauthorized receivers. Thus, eavesdroppers can easily obtain information by utilizing the estimated CSI. In this paper, we propose a secure channel estimation method which includes two components, i.e., the designs of pilot signals and estimator for time division duplex orthogonal frequency division multiplexing systems. According to analyses, the CSI can be estimated successfully at the authorized receiver. Eavesdroppers cannot obtain the CSI even if they are close to the transmitter or the authorized receiver.**

I. Introduction

Wireless communications have widely used in our daily life. However, the reliance on wireless networks to communication important or private information is growing in personal, commercial and military applications. Attackers attempt to gather information from wireless channels by employing sophisticated methods. Thus, communication techniques which inherently prevent eavesdropping are taken more attention recently.

Physical layer security in wireless communication deals mainly with unauthorized users, eavesdroppers, and/or jammers. Channel approaches physical layer security methods exploit the channel characteristics to increase security by using methods such as radio frequency (RF) fingerprinting [1], algebraic channel decomposition multiplexing (ACDM) precoding [2], and randomization of MIMO transmission coefficients [3]. The code approaches physical layer security methods includes using error correction coding [4], spread spectrum coding [5], [6], and PHY-layer network coding scheme [7], [8]. The main concept of these methods is encrypting information to prevent eavesdropping. However, it increases the computational complexity at both the transmitter and receiver since it requires to perform encrypting and decrypting continuously during data transmission. The crucial problem for wireless networks is that the channel state information (CSI) is easily estimated by unauthorized receivers due to its broadcast nature. Thus, eavesdroppers might steal information successfully by properly exploiting the CSI. On the contrary, if the unauthorized receivers cannot obtain the CSI, the communication is secure due to the uncertain nature of the wireless channel.

In this paper, we propose a secure channel estimation method to prevent that eavesdroppers obtain CSI. The proposed secure channel estimation method includes two components, i.e., the designs of pilot signals and estimator. A precoding matrix is adopted to encrypt the reference signal which is constructed by using sparse Gaussian integer sequences (SPGISs) [9] with ideal periodic autocorrelation function. The SPGISs were widely applied in various applications, e.g., the peak-to-average power ratio reduction method [10], precoded OFDM system [11], and multiple access technology [12], [13]. A Gaussian integer is a complex number whose real and imaginary parts are both integers. The SPGISs are obtained by linearly combining four base sequences or their cyclic-shift equivalents using nonzero Gaussian integer coefficients of equal magnitudes. The number of nonzero elements of SPGISs is 16 at most. The proposed secure channel estimation method requires four phases, where the precoded reference signals are exchanged between the authorized transmitter and receiver. The precoding matrix is only known at the transmitter of each phase. The receiver does not need to know the precoding matrix.

This paper is organized as follows. Section II describes the system model. Section III presents the proposed secure channel estimation method. Section IV demonstrates the simulation results. Finally, Section V provides the conclusion of this study.

II. System Model

Figure 1 illustrates the environment considered in this paper. Alice is the transmitter, Bob is the authorized receiver and Eve is an eavesdropper. $\mathbf{h}_{AB}$, $\mathbf{h}_{BA}$, $\mathbf{h}_{AE}$ and $\mathbf{h}_{BE}$ denote the channel from Alice to Bob, Bob to Alice, Alice to Eve and Bob to Eve, respectively. A time division duplex (TDD) orthogonal frequency division multiplexing (OFDM) system is considered, where the number of subcarriers is N. Thus, $\mathbf{h}_{AB}$, $\mathbf{h}_{BA}$, $\mathbf{h}_{AE}$ and $\mathbf{h}_{BE}$ are all circulant matrices. In addition, $\mathbf{h}_{AB} = \mathbf{h}_{BA}$ because of the channel reciprocity property.

Assume the frequency-domain reference signal $\mathbf{R}$ is a $N \times 1$

978-1-4673-9044-6/16/$31.00

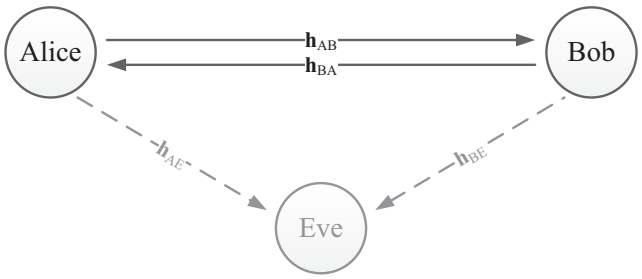

Fig. 1. System Model

matrix. The time-domain transmitted signal is

$$\mathbf{r} = \mathbf{F}^H \mathbf{R}, \tag{1}$$

where $\mathbf{F}^H$ denotes the inverse fast Fourier transform (IFFT) operation. Thus, the received signal in the time domain at Bob is given by

$$\mathbf{y}_b = \mathbf{h}_{AB}\mathbf{F}^H \mathbf{R}. \tag{2}$$

Meanwhile, the received signal in the time domain at Eve is given by

$$\mathbf{y}_e = \mathbf{h}_{AE}\mathbf{F}^H \mathbf{R}. \tag{3}$$

Since the reference signal $\mathbf{R}$ is a predefined signal, $\mathbf{R}$ is known at both Bob and Eve. Bob and Eve can individually estimate $\mathbf{h}_{AB}$ and $\mathbf{h}_{AE}$ by adopting well-known estimators. Consequently, Eve can eavesdrop when Alice transmits information to Bob.

III. Proposed Secure Channel Estimation Method

A secure channel estimation method for TDD OFDM systems is proposed in this paper which includes two components, i.e., the designs of pilot signals and estimator. A precoding matrix is adopted to encrypt the reference signal which is constructed by using sparse perfect Gaussian integer sequences (SPGISs) [9]. A Gaussian integer is a complex number whose real and imaginary parts are both integers. The SPGISs are obtained by linearly combining four base sequences or their cyclic-shift equivalents using nonzero Gaussian integer coefficients of equal magnitudes. The number of nonzero elements of SPGISs is 16 at most.

The four base sequences have length $N = 4p$ and are represented by four $N \times 1$ vectors, $\mathbf{x}_u$, $u = 1, 2, 3, 4$. The nth element of $\mathbf{x}_u$, $n = 0, 1, \ldots, N-1$, can be written as

$$x_u[n] = \exp\left\{\frac{j2\pi(u-1)n}{N}\right\} \cdot \delta\left[n - \left\lfloor\frac{4n}{N}\right\rfloor \cdot \frac{N}{4}\right], \tag{4}$$

where $\lfloor\cdot\rfloor$ returns the largest integer value less than or equal to the arguments. Let an $N \times 1$ vector $\mathbf{z}$ be a SPGIS of length $N = 4p$, where p is a positive integer. The nth element of $\mathbf{z}$ is given by

$$z[n] = \frac{1}{4} \cdot \sum_{u=1}^{4} c_u \cdot x_u\left[(n - s_u)_N\right], \tag{5}$$

where $n = 0, 1, \ldots, N-1$, c_u, $u = 1, 2, 3, 4$, are Gaussian integers of equal magnitude and $s_1, s_2, s_3, s_4 \in \{0, 1, \ldots, N-1\}$.

The proposed secure channel estimation method includes 4 phases. Note that noise is neglected in the following derivations. At the first phase, the time-domain encrypted reference signal transmitted from Alice is written as

$$\mathbf{r}_1 = \mathbf{A}\mathbf{F}^H \mathbf{R}, \tag{6}$$

where

$$\mathbf{A} = [\mathbf{z}^0\ \mathbf{z}^1\ \cdots\ \mathbf{z}^{N-1}] \tag{7}$$

is a $N \times N$ circulant unitary matrix and $\mathbf{z}^m$ denotes the mth cyclic shifts of $\mathbf{z}$.

The received signal at Bob in the frequency domain is given by

$$\mathbf{Y}_{b,1} = \mathbf{F}\mathbf{h}_{AB}\mathbf{A}\mathbf{F}^H \mathbf{R} \equiv \mathbf{\Lambda}_1 \mathbf{R}, \tag{8}$$

where

$$\mathbf{\Lambda}_1 = \mathbf{F}\mathbf{h}_{AB}\mathbf{A}\mathbf{F}^H. \tag{9}$$

Since $\mathbf{R}$ is known, it can easily obtain $\mathbf{\Lambda}_1$ by adopting well-known estimators.

At the second phase, the transmitted signal from Bob is written as

$$\mathbf{r}_2 = \mathbf{B}\mathbf{F}^H \mathbf{\Lambda}_1 \mathbf{R}, \tag{10}$$

where $\mathbf{B}$ is also a circulant matrix constructed by using SPGISs and $\mathbf{B} \neq \mathbf{A}$. The received signal at Alice in the time domain is given by

$$\mathbf{y}_{a,2} = \mathbf{h}_{BA}\mathbf{B}\mathbf{h}_{AB}\mathbf{A}\mathbf{F}^H \mathbf{R}. \tag{11}$$

Since $\mathbf{h}_{BA}$, $\mathbf{B}$, $\mathbf{h}_{AB}$ and $\mathbf{A}$ are circulant matrices, $\mathbf{y}_{a,2}$ can be rewritten as

$$\mathbf{y}_{a,2} = \mathbf{A}\mathbf{B}\mathbf{h}_{BA}\mathbf{h}_{AB}\mathbf{F}^H \mathbf{R}. \tag{12}$$

Multiplying $\mathbf{y}_{a,2}$ by $\mathbf{A}^H$ and performing fast Fourier transform (FFT) to the resulting signal obtains

$$\begin{aligned}\mathbf{Y}_{a,2} &= \mathbf{F}\mathbf{A}^H \mathbf{y}_{a,2} \\ &= \mathbf{F}\mathbf{B}\mathbf{h}_{BA}\mathbf{h}_{AB}\mathbf{F}^H \mathbf{R} \\ &\equiv \mathbf{\Lambda}_2 \mathbf{R},\end{aligned} \tag{13}$$

where

$$\mathbf{\Lambda}_2 = \mathbf{F}\mathbf{B}\mathbf{h}_{BA}\mathbf{h}_{AB}\mathbf{F}^H \tag{14}$$

Similarly, $\mathbf{\Lambda}_2$ can be obtained easily by adopting well-known estimators.

At the third phase, the transmitted signal from Bob is written as

$$\mathbf{r}_3 = \mathbf{B}\mathbf{F}^H \mathbf{\Lambda}_1 \mathbf{\Lambda}_1 \mathbf{R}. \tag{15}$$

The received signal at Alice in the time domain is given by

$$\begin{aligned}\mathbf{y}_{a,3} &= \mathbf{h}_{BA}\mathbf{B}\mathbf{h}_{AB}\mathbf{A}\mathbf{h}_{AB}\mathbf{A}\mathbf{F}^H \mathbf{R} \\ &= \mathbf{A}\mathbf{A}\mathbf{B}\mathbf{h}_{BA}\mathbf{h}_{AB}\mathbf{h}_{AB}\mathbf{F}^H \mathbf{R}.\end{aligned} \tag{16}$$

Multiplying $\mathbf{y}_{a,3}$ by $\mathbf{F}\mathbf{A}^H\mathbf{A}^H$ obtains

$$\begin{aligned}\mathbf{Y}_{a,3} &= \mathbf{F}\mathbf{A}^H\mathbf{A}^H \mathbf{y}_{a,3} \\ &= \mathbf{F}\mathbf{B}\mathbf{h}_{BA}\mathbf{h}_{AB}\mathbf{h}_{AB}\mathbf{F}^H \mathbf{R} \\ &\equiv \mathbf{\Lambda}_2 \mathbf{R},\end{aligned} \tag{17}$$

where

$$\mathbf{\Lambda}_3 = \mathbf{F}\mathbf{B}\mathbf{h}_{BA}\mathbf{h}_{AB}\mathbf{h}_{AB}\mathbf{F}^H. \quad (18)$$

$\mathbf{\Lambda}_3$ can also be obtained easily by adopting well-known estimators.

Note that

$$\mathbf{F}^H\mathbf{\Lambda}_2\mathbf{F} = \mathbf{B}\mathbf{h}_{BA}\mathbf{h}_{AB}. \quad (19)$$

$\mathbf{\Lambda}_3$ can be rewritten as

$$\mathbf{\Lambda}_3 = \mathbf{\Lambda}_2\mathbf{F}\mathbf{h}_{AB}\mathbf{F}^H \equiv \mathbf{\Lambda}_2\mathbf{H}_{AB}, \quad (20)$$

where $\mathbf{H}_{AB}$ is a $N \times N$ diagonal matrix. Since $\mathbf{\Lambda}_2$ and $\mathbf{\Lambda}_3$ are known at Alice, Alice can obtains $\mathbf{H}_{AB}$ by adopting well-known estimators. Moreover, since $\mathbf{h}_{AB} = \mathbf{h}_{BA}$, Alice can also obtain $\mathbf{B}$ from $\mathbf{\Lambda}_2$.

Finally, the transmitted signal from Alice at the fourth phase is given by

$$\mathbf{r}_4 = \mathbf{A}\mathbf{B}\mathbf{h}_{AB}\mathbf{F}^H\mathbf{R}. \quad (21)$$

The received signal at Bob in the time domain is given by

$$\begin{aligned}\mathbf{y}_{b,4} &= \mathbf{h}_{AB}\mathbf{A}\mathbf{B}\mathbf{h}_{AB}\mathbf{F}^H\mathbf{R} \\ &= \mathbf{B}\mathbf{A}\mathbf{h}_{AB}\mathbf{h}_{AB}\mathbf{F}^H\mathbf{R}. \end{aligned} \quad (22)$$

Multiplying $\mathbf{y}_{b,4}$ by $\mathbf{F}\mathbf{B}^H$ obtains

$$\begin{aligned}\mathbf{Y}_{b,4} &= \mathbf{F}\mathbf{B}^H\mathbf{y}_{b,4} \\ &= \mathbf{F}\mathbf{A}\mathbf{h}_{AB}\mathbf{h}_{AB}\mathbf{F}^H\mathbf{R} \\ &\equiv \mathbf{\Lambda}_4\mathbf{R}, \end{aligned} \quad (23)$$

where

$$\mathbf{\Lambda}_4 = \mathbf{F}\mathbf{A}\mathbf{h}_{AB}\mathbf{h}_{AB}\mathbf{F}^H. \quad (24)$$

Since $\mathbf{F}^H\mathbf{\Lambda}_1\mathbf{F} = \mathbf{A}\mathbf{h}_{AB}$, $\mathbf{\Lambda}_4$ can be rewritten as

$$\begin{aligned}\mathbf{\Lambda}_4 &= \mathbf{\Lambda}_1\mathbf{F}\mathbf{h}_{AB}\mathbf{F}^H \\ &\equiv \mathbf{\Lambda}_1\mathbf{H}_{AB}. \end{aligned} \quad (25)$$

Similarly, Bob knows $\mathbf{\Lambda}_1$ and $\mathbf{\Lambda}_4$. Thus, Bob can obtains $\mathbf{H}_{AB}$ by adopting well-known estimators.

For these four phases, the received signals at Eve are respectively written as

$$\mathbf{y}_{e,1} = \mathbf{h}_{AE}\mathbf{A}\mathbf{F}^H\mathbf{R}, \quad (26)$$

$$\mathbf{y}_{e,2} = \mathbf{h}_{BE}\mathbf{B}\mathbf{h}_{AB}\mathbf{A}\mathbf{F}^H\mathbf{R}, \quad (27)$$

$$\mathbf{y}_{e,3} = \mathbf{h}_{BE}\mathbf{B}\mathbf{h}_{AB}\mathbf{A}\mathbf{h}_{AB}\mathbf{A}\mathbf{F}^H\mathbf{R} \quad (28)$$

$$\mathbf{y}_{e,4} = \mathbf{h}_{AE}\mathbf{A}\mathbf{B}\mathbf{h}_{AB}\mathbf{F}^H\mathbf{R}. \quad (29)$$

Eve only knows the reference signal $\mathbf{R}$. Thus, Eve can estimate $\mathbf{h}_{AE}\mathbf{A}$, $\mathbf{h}_{BE}\mathbf{B}\mathbf{h}_{AB}\mathbf{A}$, $\mathbf{h}_{BE}\mathbf{B}\mathbf{h}_{AB}\mathbf{A}\mathbf{h}_{AB}\mathbf{A}$ and $\mathbf{h}_{AE}\mathbf{A}\mathbf{B}\mathbf{h}_{AB}$. Since Eve does not know $\mathbf{A}$ and $\mathbf{B}$, it cannot obtain $\mathbf{h}_{AE}$ and $\mathbf{h}_BE$ accurately.

Consider two specific scenarios that Eve is close to Alice and Eve is close to Bob, i.e., $\mathbf{h}_{BA} \approx \mathbf{h}_{BE}$ and $\mathbf{h}_{AB} \approx \mathbf{h}_{AE}$, respectively. Since $\mathbf{A}$ and $\mathbf{B}$ are not known by Eve, it cannot obtain $\mathbf{h}_{AE}$ and $\mathbf{h}_BE$ even if $\mathbf{h}_{BA} \approx \mathbf{h}_{BE}$ or $\mathbf{h}_{AB} \approx \mathbf{h}_{AE}$.

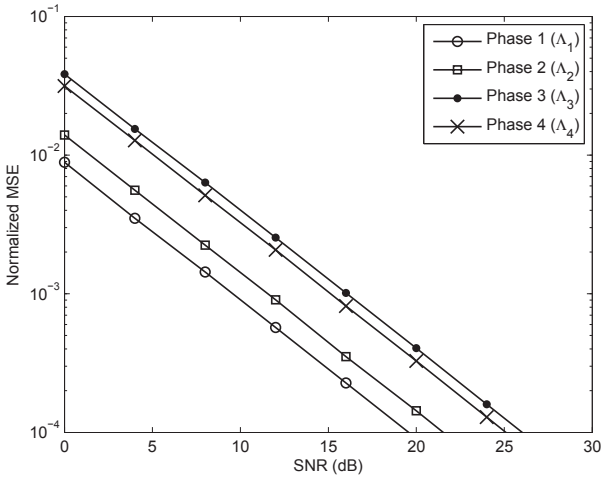

Fig. 2. Normalized MSE comparison of estimating $\mathbf{\Lambda}_1$ to $\mathbf{\Lambda}_4$.

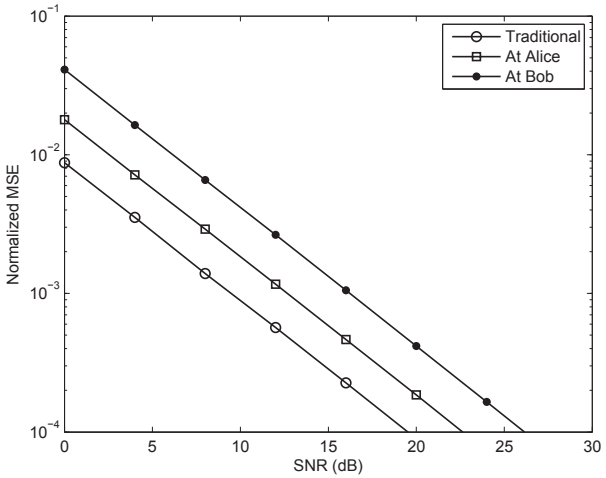

Fig. 3. Normalized MSE comparison of various channel estimation methods.

IV. Simulation Results

A serious of simulations is performed to evaluate the performance of the proposed secure channel estimation method. An OFDM system with 128 subcarriers is considered in simulations. The performance is evaluated under the assumption of a time-invariant frequency selective Rayleigh fading channel with a channel length of $L = 16$ and an exponentially decaying power delay profile. The decay factor is assumed to be $l/5$. The minimum mean square error estimator is employed at each phase to estimate $\mathbf{\Lambda}_1, \mathbf{\Lambda}_2, \mathbf{\Lambda}_3, \mathbf{\Lambda}_4$ and the least square estimator is utilize to estimate $\mathbf{h}_{AB}$ at Alice and Bob.

Figure 2 shows the normalized mean square error (NMSE) of estimating $\mathbf{\Lambda}_1, \mathbf{\Lambda}_2, \mathbf{\Lambda}_3$, and $\mathbf{\Lambda}_4$. From simulation results, the estimation error is increased as the sequence of phases. However, the estimation error of $\mathbf{\Lambda}_3$ is the worst NMSE among four phases. The main reason is that the transmitted signal at the third phase shown in (15) is multiplied by $\mathbf{\Lambda}_1$ twice. The estimation error of the third phase is aggravated.

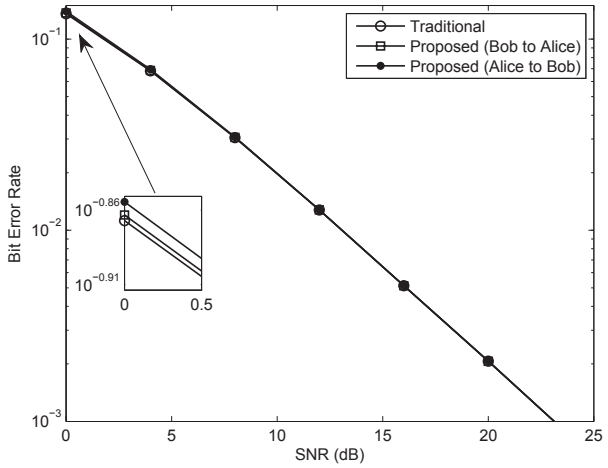

Fig. 4. Bit-error-rate comparison of the TDD OFDM system with various channel estimation methods.

The NMSE of Figure 3 shows the NMSE of the proposed channel estimation method which is measured at Alice and Bob. Note that the CSI is obtained at Alice and Bob at the third and fourth phases, respectively. The NMSEs of the proposed method performed at Alice and Bob are 3 dB and 6.5 dB worse than that of the traditional method when NMSE = 10^{-4}, respectively. Although the proposed method is slightly worse than that of the traditional method, but communication is secure. The CSI can be only estimated successfully at the authorized receiver.

Finally, the bit-error-rate (BER) performance is illustrated in Fig. 4. The BER of the proposed method is almost the same as that of the traditional method which is not secure.

V. Conclusions

In this paper, we propose a secure channel estimation method which includes two components, i.e., the designs of pilot signals and estimator for TDD OFDM systems. Precoding matrices are adopted at both Alice and Bob to encrypt the reference signal which is constructed by using SPGISs. The SPGISs are obtained by linearly combining four base sequences or their cyclic-shift equivalents using nonzero Gaussian integer coefficients of equal magnitudes. The number of nonzero elements of SPGISs is 16 at most. The proposed secure channel estimation method requires four phases, where the precoded reference signals are exchanged between the authorized transmitter and receiver. The precoding matrix is only known at the transmitter of each phase. The receiver does not need to know the precoding matrix. According to analyses, the CSI can be estimated successfully at the authorized receiver. Eavesdroppers cannot obtain the CSI even if they are close to the transmitter or the authorized receiver.

Acknowledgement

This work was supported by Ministry of Science and Technology under Grants MOST 104-3115-E-110-001 and MOST 104-2218-E-110-006.

References

[1] C. Sperandio and P. Flikkema, "Wireless Physical-layer security via transmit precoding over dispersive channels: optimum linear eavesdropping," in *Proc. IEEE Military Commun. Conf. (MILCOM 2002)*, Oct. 2002, pp. 1113–1117.

[2] X. Li and E. Ratazzi, "MIMO transmissions with information-theoretic secrecy for secret-key agreement in wireless networks," in *Proc. IEEE Military Commun. Conf. (IEEE MILCOM 2005)*,Oct. 2005, pp. 1353–1359.

[3] D. Abbasi-Moghadam, V. T. Vakili, and A. Falahati, "Combination of turbo coding and cryptography in non-geo satellite communication systems," in *Proc. Int. Symp. Telecommun.*, Aug. 2008, pp. 666–670

[4] Y. Hwang and H. Papadopoulos, "Physical-layer secrecy in AWGN via a class of chaotic DS/SS systems: analysis and design," *IEEE Trans. Signal Process.*, vol. 52, no. 9, pp. 2637–2649, Sep. 2004.

[5] T. Li, J. Ren, Q. Ling, and A. Jain, "Physical layer built-in security analysis and enhancement of CDMA systems," in *Proc. IEEE Military Commun. Conf. (MILCOM 2005)*, Oct. 2005, pp. 956–962.

[6] G. Noubir, "On connectivity in Ad Hoc network under jamming using directional antennas and mobility," in *Proc. Int. Conf. Wired and Wireless Internet Commun.*, Feb. 2004, pp. 186–200.

[7] J.-P. Cheng, Y.-H. Li, P.-C. Yeh, and C.-M. Cheng, "MIMO-OFDM PHY integrated (MOPI) scheme for confidential wireless transmission," in *Proc. IEEE Wireless Comm. and Networking Conf. (WCNC)*, Apr. 2010, pp. 1–6.

[8] C.-Y. Wu, P.-C. Lan, P.-C. Yeh, C.-H. Lee, and C.-M.Cheng, "Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1687–1700, Sep. 2013.

[9] S.-H. Wang, C.-P. Li, H.-H. Chang, and C.-D. Li, "A systematic method for constructing sparse Gaussian integer sequences with ideal periodic autocorrelation functions," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 365–376, Jan. 2016.

[10] C.-P. Li, S.-H. Wang, and C.-L. Wang, "Novel low-complexity SLM schemes for PAPR reduction in OFDM systems," *IEEE Trans. Signal Process.*, vol. 58, no. 5, pp. 2916–2921, May 2010.

[11] S.-H. Wang, K.-C. Lee, C.-P. Li, and H.-J. Su, "A novel low-complexity precoded OFDM system with reduced PAPR," *IEEE Trans. Signal Process.*, vol. 63, no. 6, pp. 1366–1376, Mar. 2015.

[12] S.-H. Wang and C.-P. Li, "Novel comb spectrum CDMA system using perfect Gaussian integer sequences," in *Proc. 2015 IEEE GLOBECOM*, Dec. 2015.

[13] S.-H. Wang and C.-P. Li, "Novel MC-CDMA system using Fourier duals of sparse perfect Gaussian integer sequences," in *Proc. 2015 IEEE ICC*, May 2016.