Secure Communication in TDS-OFDM System Using Constellation Rotation and Noise Insertion

Ruifeng Ma, Linglong Dai, Zhaocheng Wang, *Member*, *IEEE*, and Jun Wang, *Member*, *IEEE*

Abstract — *Time-domain synchronous orthogonal frequency division multiplexing (TDS-OFDM) is the key technology of Chinese digital television terrestrial broadcasting (DTTB) standard. However, the issue of security was not considered, and this limits its application in commercial or military scenarios where secure communication is very important. This paper proposes an encryption scheme based on pseudo random constellation rotation and weak artificial noise insertion, which jointly utilizes the pseudo random key and the irreversible property of wireless channel to guarantee the physical layer security of TDS-OFDM system. Simulation results show that the proposed security scheme can protect the system from eavesdroppers, while the legal receivers only suffer a negligible bit error rate (BER) performance loss compared with the conventional TDS-OFDM system without security*[1].

Index Terms — TDS-OFDM, Security, Constellation Rotation, Artificial Noise.

I. INTRODUCTION

Security is a fundamental problem in wireless communication due to the openness nature of the wireless medium, especially for systems used in military and commercial scenarios. In modern wireless communication network, security is usually realized by cryptographic techniques in link layer and application layer. However, the rapid growth of computational capability and the openness of wireless channel make the communication systems vulnerable to eavesdropping [1].

As the key technology of Chinese digital television terrestrial broadcasting (DTTB) standard [2], time-domain synchronous orthogonal frequency division multiplexing (TDS-OFDM) adopts the known training sequence instead of cyclic prefix (CP) as the guard interval. Compared with traditional CP based OFDM (CP-OFDM) systems, there is no need to insert frequency-domain pilots for TDS-OFDM, which can improve the spectral efficiency [3]. Meanwhile, the known training sequence can be used to achieve fast and reliable synchronization and channel estimation [4-5]. However, TDS-OFDM can not support the secure transmission, which limits its application in military and commercial scenarios.

In this paper, we propose an encryption scheme for TDS-OFDM at the physical layer using pseudo random constellation rotation and artificial noise insertion. The contribution of this scheme lies in three aspects: 1) Inspired by the constellation rotation technique used in the second generation digital video terrestrial broadcasting (DVB-T2) to improve the performance over fading channels, we extend this concept to pseudo random constellation rotation whereby each constellation point is rotated by a specific angle in a pseudo random way, thus secure communication can be guaranteed; 2) Weak artificial noise is added upon the rotated constellation to further enhance the security level; 3) Security can be implemented with the backward compatibility with the infrastructure of Chinese DTTB network.

This rest of this paper is organized as follows. Section II presents the proposed TDS-OFDM security scheme based on pseudo random constellation rotation and artificial noise insertion. The specific implementation of TDS-OFDM physical layer encryption is also described. Section III illustrates the simulation results over AWGN and multi-path channels. Then we conclude this paper in Section IV.

II. CONSTELLATION ROTATION AND ARTIFICIAL NOISE INSERTION BASED SECURITY

In this section, the pseudo random constellation rotation and weak artificial noise insertion based physical layer security is proposed, where the overall block diagram of TDS-OFDM physical layer encryption scheme is presented.

A. Conventional Constellation Rotation

In previous work, it has been confirmed that bit error rate (BER) and diversity performance improvement can be achieved by constellation rotation over fading channels [6].

Fig. 1 (a) shows an example of the rotated constellation for QPSK. Every constellation symbol S_k is rotated by a unique angle α as

$$S'_k = S_k \cdot e^{j\alpha}, \quad 0 \le k \le N-1, \tag{1}$$

where S_k presents the original constellation symbol, S_k' is the rotated symbol of S_k, and N is the number of the transmitted frequency-domain symbol in a signal frame. In conventional constellation rotation, a fixed rotation angle is applied on the complex constellation plane to every transmitted symbol. For example, DVB-T2 adopts the rotation angle α of 29.0

[1] This work was supported in part by Tsinghua University Initiative Scientific Research Program (20091081280) and in part by Standardization Administration of the People's Republic of China (SAC) with AQSIQ Project (200910244).

All the authors are with the Department of Electronic Engineering as well as the Tsinghua National Laboratory of Information Science and Technology (TNList), Tsinghua University, Beijing 100084, P. R. China (e-mail: mrf911@163.com).

Contributed Paper
Manuscript received 07/14/10
Current version published 09/23/10
Electronic version published 09/30/10.

degrees for QPSK modulation, and for 16-QAM modulation α is chosen to be 16.8 degrees [7].

B. *Pseudo Random Constellation Rotation*

Based on the conventional constellation rotation concept, this paper extends the application of constellation rotation to provide security from the physical layer point of view. Unlike the unique rotation angle, the pseudo random symbol-specific rotation angles are suggested for different constellation symbols, whereby the pseudo random angles can be treated as the secret key for physical layer encryption. As illustrated in Fig. 1 (b), a pseudo random rotation angle is assigned to each transmitted symbol as

$$S'_k = S_k \cdot e^{j\theta_k}, \quad 0 \le k \le N-1, \tag{2}$$

where θ_k is the symbol-specific pseudo random rotation angle, which is generated by pseudo random sequence generator. The details of the sequence generator is known to both the transmitter and authentic receivers, but could not be accessed by illegal eavesdroppers. Comparing Fig. 1 (a) and Fig. 1 (b), it is clear that the pseudo randomly rotated symbols are scattered around the unit circle, which can be used to prevent eavesdropping from illegal receivers.

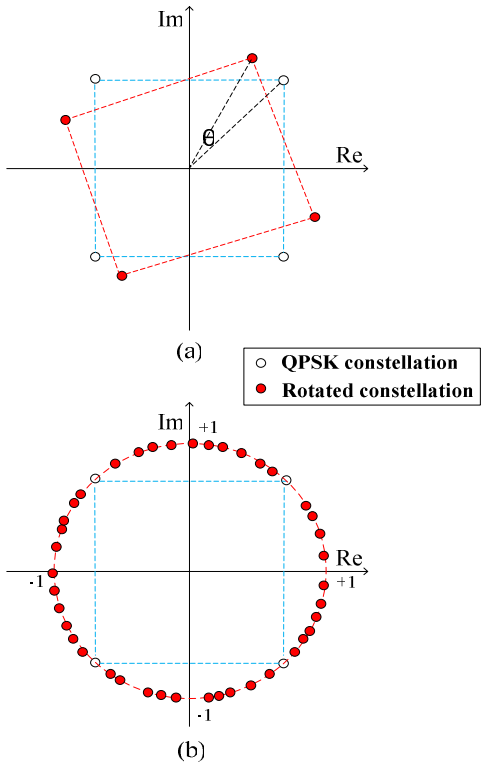


Fig. 1. Comparison of constellation rotation: (a) Conventional scheme in DVB-T2; (b) Proposed scheme in TDS-OFDM.

In TDS-OFDM system, both time-domain PN sequences and multi-carrier PN (PN-MC) sequences can be padded before the inverse discrete Fourier transform (IDFT) block as the guard interval. The PN-MC sequence is the IDFT output of the binary sequence in frequency domain. As shown in Fig. 2, pseudo random constellation rotation can be applied to either PN-MC training sequence or IDFT block, or both of them.

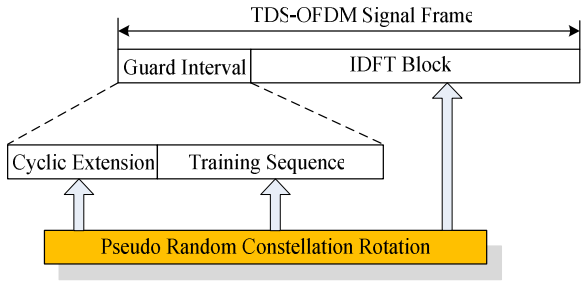


Fig. 2. Implementation of pseudo random constellation rotation in TDS-OFDM systems.

The angle sequence $\{\theta_k\}_{k=0}^{N-1}$ can not be reversible using linear or nonlinear transform of pseudo random sequence generator outputs. Only the legal receiver can get the authentic rotation angle information, while the eavesdroppers without such information can only demodulate the information by enormous enumeration which is almost impossible to be realized in high-speed wireless communications.

Fig. 3 (a) illustrates one example for pseudo random generator to yield random rotation angle sequence $\{\theta_k\}_{k=0}^{N-1}$ by linear transform. First, m bits are selected out of pseudo random sequence generator outputs. Then, the selected m bits are transformed into the corresponding decimal n_k and the rotation angle sequence can be calculated by

$$\theta_k = \frac{n_k}{2^m} \times 2\pi, \quad 0 \le k \le N-1. \tag{3}$$

Fig. 3 (b) demonstrates one selecting method of m bits for θ_k.

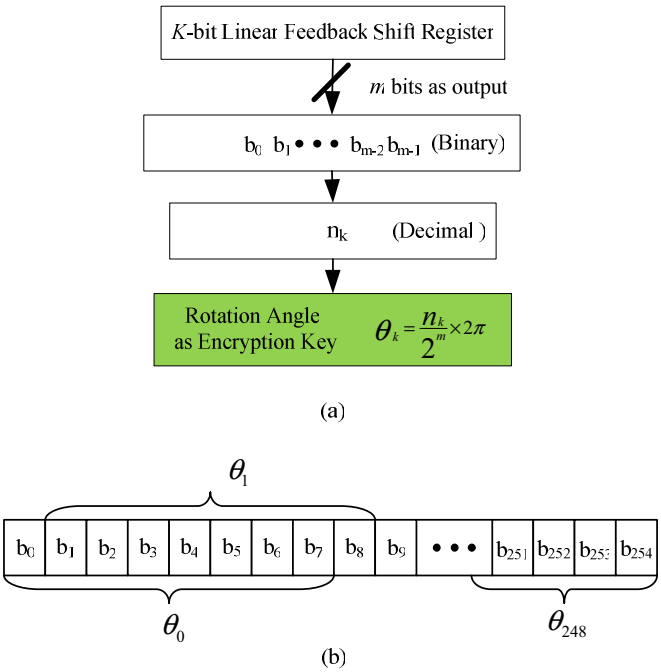


Fig. 3. Generation of the rotation angle sequence: (a) Rotation angle sequence calculation; (b) Bits selection.

Alternatively, we can also apply nonlinear logistic map to sequence generator outputs to further increase the security. A

chaos sequence $\{x_k\}_{k=0}^{N-1}$, $x_k \in (0,1)$ can be generated through classic logistic map

$$x_{i+1} = \gamma x_i (1-x_i), \tag{4}$$

where the coefficient γ is selected between 3.57 and 4.

Based on this idea, we let x_i, x_{i+1} and 1-x_i be q-bit binary numbers in (0,1) and consider equation (5):

$$x_{i+1} = \left\lfloor 2^k x_i (1-x_i) \big|_{\mathrm{mod}\,1} \right\rfloor_q, \tag{5}$$

where $\lfloor \rfloor_q$ means selecting the first q bits in decimal part as output. The coefficient γ is substituted by 2^k and different selections of k result in different non-linear transform methods from x_i to x_{i+1}. Typically, to make the output of logistic map uniformly distributed, k should be half length of x_i, which equals to $q/2$.

In practice of our encryption scheme, the first state number $x_0 \in (0,1)$ (q-bit) can be assigned through random sequence generator in both transmitter and receiver as the encrypted key. A chaos sequence $\{x_k\}_{k=0}^{N-1}$ randomly distributed in (0,1) can be generated by (5). Thus, the pseudo random rotation angle sequence can be obtained by

$$\{\theta_k\}_{k=0}^{N-1} = 2\pi \times \{x_k\}_{k=0}^{N-1}, \quad 0 \le k \le N-1. \tag{6}$$

C. Artificial Noise Insertion

In the pioneering work in [8], Pappu pointed out that when considering encryption algorithm, physical irreversible function was more efficient than reversible function. By using the irreversible property of wireless channel, we deliberately add weak artificial noise [9] to the rotated constellation symbols for more reliable physical layer security.

Compared with the signal power, the power of artificial noise is relatively rather weak. For example, we can configure the noise power as 30 dB lower than the signal power. This physical irreversible weak noise does not influence the legal users quite much, because constellation rotation secret key is known to the legal users. However, regarding to the eavesdroppers, the weak artificial noise can incur great error rate due to the fact that two rotated symbols may be quite near to each other after pseudo random constellation rotation, as shown in Fig. 1 (b).

For illustration, we perform pseudo random constellation rotation on the 16-QAM modulated symbols in Fig. 4 (a), and the output is shown in Fig. 4 (b). After that, weak artificial noise is added with the SNR of 20 dB to generate the results in Fig. 4 (c). Since the rotation angle sequence $\{\theta_k\}_{k=0}^{N-1}$ is known to the legal receiver, Fig. 4 (d) shows the demodulated signal at the receiver, whereby the demodulated signal is only corrupted by weak artificial noise.

In general, both constellation rotation and artificial noise insertion can be used to enhance the security of OFDM physical layer, which is important for consumer electronics as well as military usage where security has to be guaranteed.

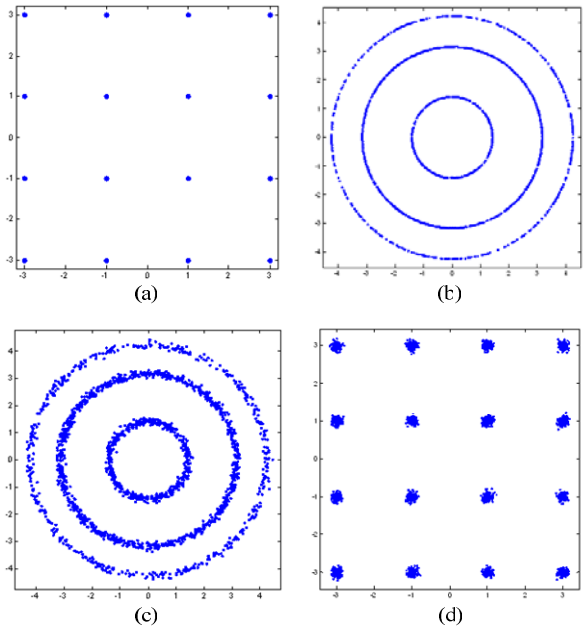


Fig. 4. Pseudo random constellation rotation and artificial noise insertion: (a) 16-QAM modulated symbols; (b) Outputs after pseudo-random constellation rotation; (c) Outputs after artificial noise insertion; (d) Demodulated signal by the legal receiver.

The proposed artificial noise insertion strategy is presented as below:

1) If the transmitter can obtain the instantaneous channel information by channel estimation or receiver feedback, the method of artificial noise insertion can be determined by channel state information (including the amplitude and phase of channel impulse response), which is quite random and irreversible.

Suppose the channel estimation result obtained is

$$H_k = |H_k| e^{j\varphi_k}, \quad 0 \le k \le N-1. \tag{7}$$

The artificial noise insertion can be presented by

$$N_k = S'_k + \frac{A(H_k)}{P}, \quad 0 \le k \le N-1, \tag{8}$$

where S'_k represents the symbols after pseudo random constellation rotation, N_k is the symbol after the insertion of weak artificial noise. Typically, $A(H_k)$ in (8) can be function of channel estimation result $|H_k|$ and φ_k, such as $f(|H_k|, \varphi_k)$. P represents the relative power of noise, e.g., the noise with power 30 dB lower than the signal results in $P=10^3$.

2) If the transmitter can not obtain the instantaneous channel information, such as TDS-OFDM broadcasting system, we could directly add random Gaussian noise to rotated constellation symbols.

One the other hand, based on the recently proposed uplink solution using TDS-OFDM [10] whereby channel state information can be known to the transmitter, the random and irreversible wireless channel can still be used for artificial noise insertion in secure TDS-OFDM systems.

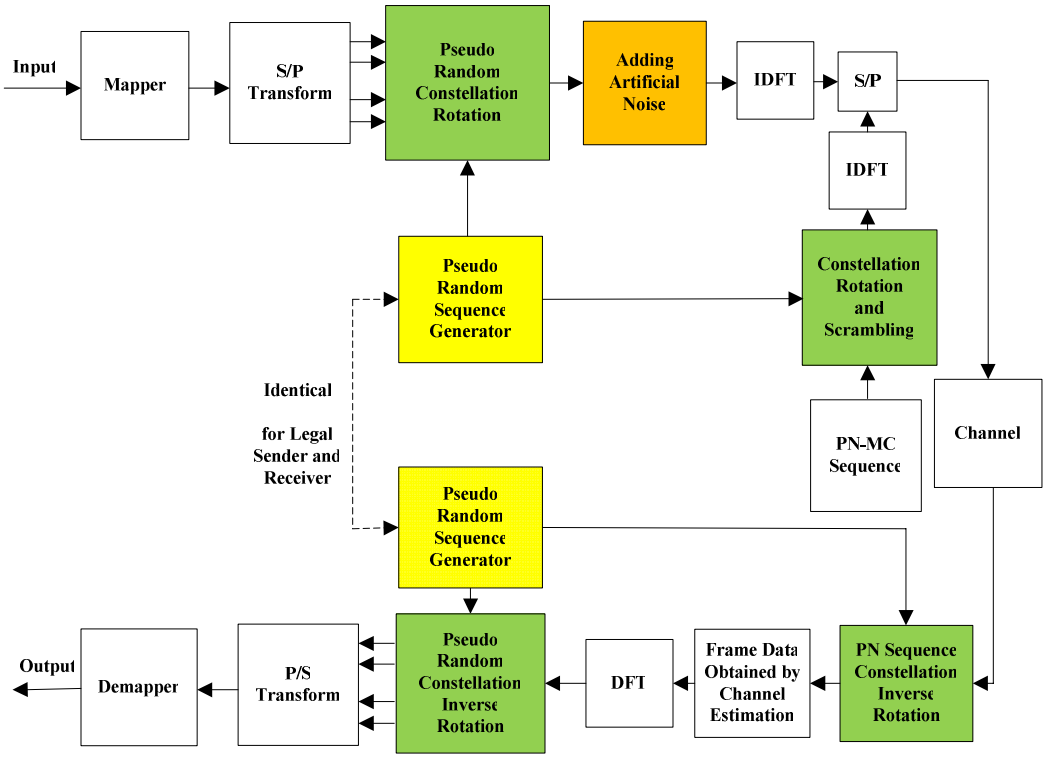


Fig. 5. TDS-OFDM physical layer encryption scheme.

D. Implementation of TDS-OFDM Physical Layer Security

The overall block diagram of proposed TDS-OFDM encryption scheme is shown in Fig. 5. As mentioned above, current Chinese DTTB standard does not have the function of encryption, which limits its application in commercial and military scenarios where security is required. In this paper, we present a physical layer security scheme based on pseudo random constellation rotation and weak artificial noise insertion, which can also be directly applied to TDS-ODFM systems. The performance of the proposed scheme will be presented in the next section.

III. Simulation Results

Computer simulations are provided to verify the feasibility and performance of the proposed method for physical layer security of TDS-OFDM system without channel coding. The main system parameters are listed in Table I. PN-MC training sequence is used as the guard interval. Both AWGN and Brazil A multi-path channels [11] are used.

TABLE I
System Parameters for Simulation

Central Frequency	770 MHz
Signal Bandwidth	8 MHz
IDFT Block Length	3780
Symbol Rate	7.56 MHz
Sub-carrier Spacing	2 kHz
Modulation Scheme	QPSK/16QAM
Guard Interval Length	420

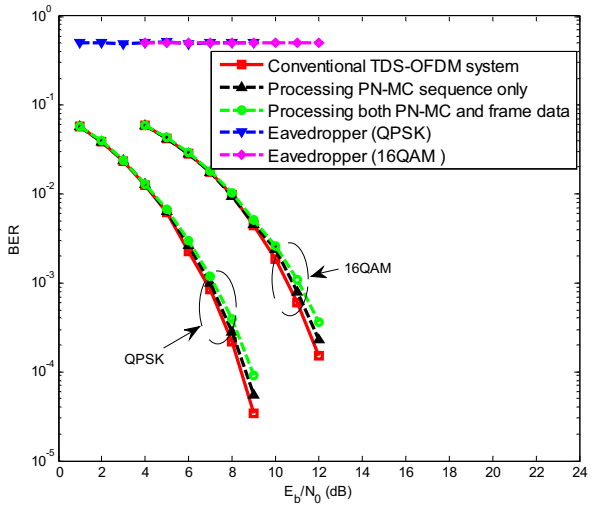


Fig. 6. BER performance of the proposed TDS-OFDM physical layer security scheme over AWGN channel.

Fig. 6 and Fig. 7 illustrate the BER performance of the legal receiver in the proposed secure TDS-OFDM system over AWGN and Brazil A channels, respectively. To compare the performance, BER of the eavesdropper in the proposed encryption system and the conventional TDS-OFDM system without security are included. It is clear that the eavesdropper has the BER of 0.5, which means that it can not demodulate the useful data intended for the legal receivers. Compared with conventional TDS-OFDM system without security, the SNR loss of less than 0.2 dB at the BER of 1×10^{-3} can be observed in the secure TDS-OFDM system when constellation rotation and artificial noise insertion are only applied to the PN-MC

sequence. The SNR loss is less than 0.4 dB if constellation rotation and artificial noise insertion are applied to both the PN-MC sequence and IDFT block. The SNR loss becomes negligible when channel coding is applied.

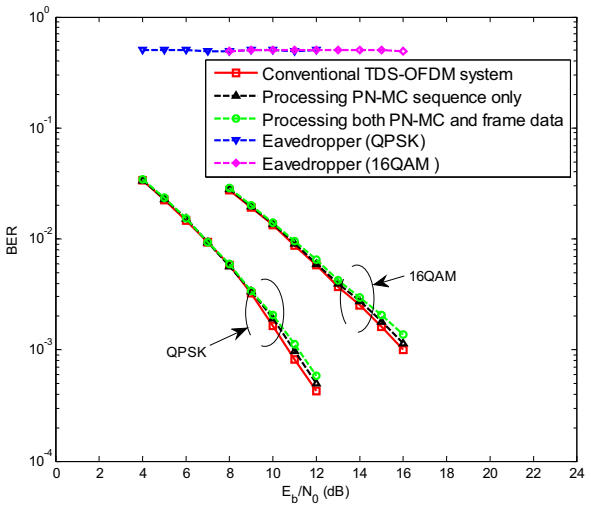


Fig. 7. BER performance of the proposed TDS-OFDM physical layer security scheme over Brazil A channel.

From the simulation results, we can conclude that the proposed physical layer security in TDS-OFDM system using pseudo random constellation rotation and weak artificial noise insertion can support secure communication between the transmitter and legal receiver, while eavesdroppers can not demodulate any useful data. Thus secure communication is guaranteed. On the other hand, the proposed scheme only results in negligible SNR loss compared with the conventional TDS-OFDM system lacking security mechanism.

IV. CONCLUSION

This paper proposes a novel physical layer security scheme for TDS-OFDM system, whereby both pseudo random constellation rotation and weak artificial noise insertion are used to enhance the security level. The secure information can be encoded either in the training sequence, or in the IDFT block, or both of them. The eavesdropper can not demodulate the useful data due to the unknown encryption key encoded in the pseudo random constellation rotation and the irreversibility of the artificial noise, while at the same time the legal receivers only suffer a negligible SNR loss compared with the conventional TDS-OFDM system without security. Further, the proposed scheme can maintain the backward compatibility with current Chinese DTTB network infrastructure, which provides a promising solution to extend the application of TDS-OFDM scheme from broadcasting to commercial or military areas where secure communication is required.

REFERENCES

[1] Y. Liang, H. V. Poor and S. Shamai, "Secure Communication over Fading Channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2470-2492, Jun. 2008.

[2] *Framing Structure, Channel Coding and Modulation for Digital Television Terrestrial Broadcasting System.* Chinese National Standard, GB 20600-2006, Aug. 2006.

[3] Z. Zheng, "Robust Timing Recovery for TDS-OFDM-Based Digital Television Terrestrial Broadcast," *IEEE Trans. Consumer Electron.*, vol. 52, no. 3, pp. 750–756, Nov. 2006.

[4] J. Wang, Z. Yang, C. Pan, M. Han, and L. Yang, "A Combined Code Acquisition and Symbol Timing Recovery Method for TDS-OFDM," *IEEE Trans. Broadcast.*, vol. 49, no. 3, pp. 304–308, Sep. 2003.

[5] F. Yang, J. Wang, J. Wang, J. Song, and Z. Yang, "On Channel Estimation and Equalization in TDS-OFDM Based Terrestrial HDTV Broadcasting System," *IEEE Trans. Consumer Electron.*, vol. 54, no. 4, pp. 1583–1589, Dec. 2008.

[6] C. Han, T. Hashimoto and N. Suehiro, "Constellation-Rotated Vector OFDM and its Performance Analysis over Rayleigh Fading channels", *IEEE Trans. Commun.*, vol. 58, no. 3, pp. 828-838, Mar. 2010.

[7] *Frame Structure, Channel Coding and Modulation for a Second Generation Digital Terrestrial Television Broadcasting System (DVB-T2).* ETSI EN 302 755, V1.1.1, Sep. 2009.

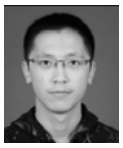
[8] R. Pappu, B. Recht, J. Taylor and N. Gershenfeld, "Physical One-Way Functions," *Science*, vol. 297, no. 5589, pp. 2026-2030, Sep. 2002.

[9] S. Goel and R. Negi, "Guaranteeing Secrecy Using Artificial Noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, Jun. 2008.

[10] L. Dai, J. Fu, J. Wang, J. Song, Z. Yang, "A Multi-user Uplink TDS-OFDM System Based on Dual PN Sequence Padding," *IEEE Trans. Consumer Electron.*, vol.53, no. 3, pp. 1098-1106, Aug. 2009.

[11] *Digital Television Systems-Brazilian Tests-Final Report*. SET/ABERT, ANATEL SP, May 2000.

BIOGRAPHIES



Ruifeng Ma received his bachelor degree from Harbin Institute of Technology, Harbin, China, in 2009. Currently, he is a Ph.D. candidate at the DTV Technology R&D Center, Tsinghua University. His research interests include physical layer security in wireless communication and channel estimation.

Linglong Dai is a Ph.D. candidate at the Department of Electronic Engineering of Tsinghua University, Beijing, China. His research interests lie in the field of synchronization, channel estimation for wireless communication system, space-time coding and diversity techniques, multiple access techniques, as well as wireless positioning.

Zhaocheng Wang received his B.S.E., M.S.E. and Ph.D. degrees in 1991, 1993 and 1996 respectively, from the Department of Electronic Engineering, Tsinghua University. He was a Post Doctoral Fellow with Nanyang Technological University (NTU) in Singapore from 1996 to 1997. He is a Full Professor of the Department of Electronic Engineering at Tsinghua University. His general research interests include wireless communications, digital video broadcasting and signal processing, with emphasis on OFDM, single carrier with frequency domain equalization (SC-FDE) and MIMO techniques. Within these areas, he filed 35 US/EU patent applications, 18 of them have been granted. He has published tens of journal and conference papers.

Jun Wang was born in Henan, P. R. China, on October 5, 1975. He received the B. Eng. and Ph.D degree from the Department of Electronic Engineering in Tsinghua University, Beijing, China, in 1999 and 2003 respectively. He is an assistant professor and member of Digital TV R&D center of Tsinghua University since 2000. His main research interests focus on broadband wireless transmission techniques, especially synchronization and channel estimation. He is actively involved in the Chinese national standard on the Digital Terrestrial Television Broadcasting technical activities, and is selected by the Standardization Administration of China as the Standard committee member for drafting.