Secure Communication for Cognitive Networks Based on MIMO and Spreading LDPC Codes

YANG XIAO, KAIYAO WANG
Institute of Information Science, Beijing Jiaotong University
Beijing 100044, P.R. CHINA
Emails: yxiao@bjtu.edu.cn, 09112089@bjtu.edu.cn

Abstract: The existing cognitive radio (CR) systems lack the ability to deal with the attack of a pretended primary user (PPU), which can palsy cognitive network. To solve the problem, in this paper, a secure cognitive radio (CR) system is proposed. The proposed systems combines MIMO and spread spectrum techniques as well as low density parity check (LDPC) codes to cancel the electronic interference of PPU. The simulation results in Rayleigh flat-fading channel show that, comparing with MIMO cognitive system without the proposed method, the proposed approach can effectively cancel electronic interference from enemy and channel noises interference, and obtain about 9dB gain.

Keywords: secure communication, MIMO cognitive systems, electronic interference cancellation, protograph low density parity check (LDPC) codes, spread spectrum

Received: April 29, 2021. Revised: November 23, 2021. Accepted: December 12, 2021. Published: December 31, 2021.

1. Introduction

Nowadays, radio spectrum has become a very precious resource in wireless communication. There is little radio frequency spectrum left over. The cognitive radio (CR) technology can increase radio frequency spectrum usage efficiency by spectrum sharing. As a promising solution for this problem, the CR technology is being studied extensively [1-8]. Two kinds of users are served in cognitive systems, primary users (PUs) and cognitive users (CUs). However, in the existing schemes [1-8], CUs and PUs share the same frequency spectrum in a time division. If an attacker pretends a primary user, i.e. a PPU, it is difficult to guarantee the multiple CUs communicate over the frequency spectrum using by PPU.

More recently, multi-terminal communication with confidential messages has been studied intensively [9-16]. Most of existing secure communication schemes are focus on the study of secrecy capacity. They interested in protecting the common message against eavesdropping. For the secure transmission of information over an ergodic fading channel in the presence of an attacker, and the attacker can pretend a empowered user. The secrecy capacity of such a system with ergodic fading channel is characterized under the assumption of asymptotically long coherence intervals. [9, 10] investigated the rate-equivocation region and secrecy capacity region for ergodic fading channel. The impact of fading on secure communication also was studied in [11-16], and some of them exploited the feedback and cooperation to improve the secrecy for CR networks. However, the above existing secure communication schemes did not consider that the attacker (PPU) can send electronic interference signal to CR client receiver. Generally, when detecting the channel is occupied by PU, CUs had to withdraw and keep off. Thus, it is difficult to guarantee reliable communications under the condition of strong electronic interference from a PPU by the approaches of [9-16]. To solve the problems, in this paper, a secure MIMO cognitive system is proposed, in which the multiple CUs communicate over Rayleigh flat-fading channels and a PPU sends an electronic interference signal to CUs. We are interested in protecting the secure communication between multiple CUs against electronic interference signal from PPU.

Different from [9-16], the proposed secure MIMO cognitive system introduces spread spectrum technique and LDPC codes for the electronic interference cancellation of PPU. This scheme can ensure multiple CUs secure communication under the condition of strong electronic interference from PPU. Protograph LDPC codes [17-19] and spread spectrum are applied to the proposed secure MIMO cognitive system, the information transmission of CR network can be of the anti-interference ability and error correcting capability through channel coding and spread spectrum mapping, which can cancel electronic interference of PPU and channel noises interference. In our scheme, spread spectrum mapping does only require DSP (Digital Signal Processor) programming to be achieved, but does not require the circuit and spread spectrum synchronization. Protograph LDPC codes have the advantage of high-speed decoding, low error floor and low iterative decoding threshold [20-23]. The protograph LDPC codes used in this method can be of fast encoding. Thus, it can simplify the hardware complexity of communication equipment.

In the proposed secure MIMO cognitive system, the diversity combining is used to increase information transmission reliability. The different antennas of source send the same signals to obtain diversity gain. The electronic interference of PPU and channel noise are looked as a new noise in the receiver. The expected information can be obtained through despreading mapping and channel decoding of the proposed secure MIMO cognitive system. The simulation results in Rayleigh flat-fading channel show that, comparing with MIMO cognitive system without the proposed method, the proposed secure MIMO cognitive system can effectively

This work was supported by the Beijing Natural Science Foundation of China: (No. 4102050).

cancel electronic interference from PU and channel noises interference, and obtain about 9dB gain.

2. Electronic Interference Cancellation of PPU

In this section, we proposed a method that electronic interference cancellation based on spread spectrum LDPC codes in MIMO cognitive system. This method can make multiple CUs secure communication under the condition of strong electronic interference from PU. In this paper, we assume the channel parameters in a transmission cycle of signals frame are constant. In the method, the diversity combining is used to increase information transmission reliability. For the receiver, the received signals were combined by using equal gain combining. The strong electronic interference signals from enemy and channel noise looked as a new noise. It minimizes new noise interference by despreading mapping and decoding.

In this paper, the MIMO cognitive system block diagram showed in Figure 1, including an interference source, a base station and k mobile terminals. In Figure 1, the interference source PPU and the base station both have 2 antennas, and each mobile terminal also has 2 antennas. In this paper, it is assumed that the fading is quasistatic and the channel state information (CSI) of the PPU is not available at the source, while CR mobiles and CR base-station know the CSI of them, which provides the chance to cancel the attack of PPU for the proposed system.

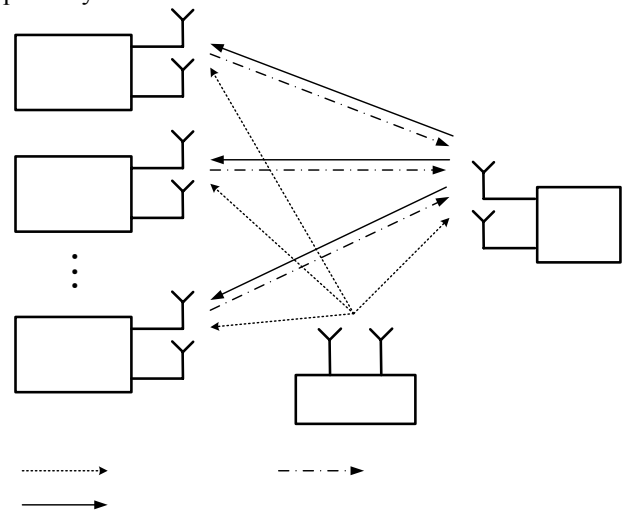


Fig.1 MIMO cognitive system block diagram

From Fig. 1, we know that PPU can attack the communication between CR mobiles and CR base-station in uplink or in downlink by sending an electronic interference signal in the bandwidth of CR network, if PPU occupies the bandwidth of CR network. To solve the problem, we propose a method that electronic interference cancellation based on spread spectrum LDPC codes in MIMO cognitive system under two conditions (uplink communication system and downlink communication system). Refs. [9]-[16] only consider how receivers avoid their information not to be obtained by eavesdropper. Their approaches are not available to our application in Fig.1.

2.1 Uplink Communication System

In the uplink, the mobile terminals transmit data, and the base station receives data. The proposed MIMO cognitive system uplink communication system model is shown in Figure 2.

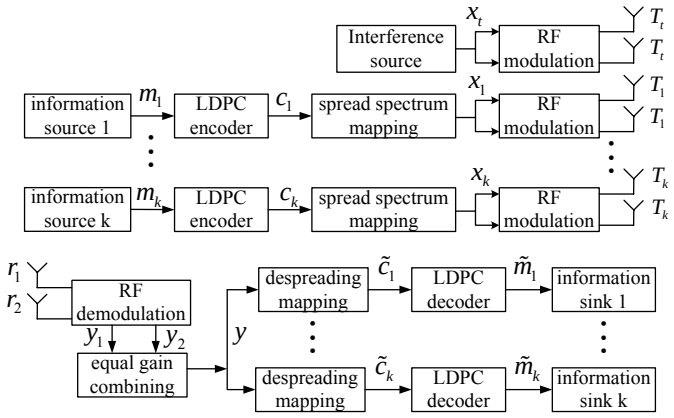


Fig. 2 MIMO cognitive system uplink communication system model

The information bit from mobile terminal is denoted $\boldsymbol{m}_i \in \mathbf{Z}^{1\times M}(1 \le i \le k)$, M is the length of information bit. Protograph LDPC codes encode the information bit $\boldsymbol{m}_i$, and the encoded information is denoted $\boldsymbol{c}_i \in \mathbf{Z}^{1\times N}(1 \le i \le k)$, N is the length of codes. It can be written as $\boldsymbol{c} = \boldsymbol{m} \bullet \boldsymbol{G}$, where $\boldsymbol{G}$ is the generate matrix of protograph LDPC codes.

The spread spectrum signal is denoted $\boldsymbol{x}_i \in \mathbf{Z}^{1\times(N\cdot K)}(1 \le i \le k)$ by spread spectrum mapped encoded information $\boldsymbol{c}_i$. The mapping relation of baseband signals and codes as following: $1 \to \boldsymbol{d}, 0 \to -\boldsymbol{d}$, where $\boldsymbol{d}_i \in \mathbf{Z}^{1\times K}(1 \le i \le k)$ is the spreading codes sequences, and K is the length of spreading codes sequences.

In the proposed scheme, spread spectrum mapping does only require DSP (Digital Signal Processor) programming to achieve, and not require the circuit and spread spectrum synchronization. Thus, it can simplify the hardware complexity of communication equipment.

Spread spectrum signal $\boldsymbol{x}_i = \left[\boldsymbol{x}_i(1) \quad \boldsymbol{x}_i(2) \quad \cdots \quad \boldsymbol{x}_i(N)\right]^{\mathrm{T}}$ is stored in a $N \times K$ two-dimensional matrix. Baseband spread spectrum signal was transmitted successive through the transmitting antenna. The spread spectrum signal block diagram is shown in Figure 3, where $x_i^j(n)$ denotes the j^{th} chip of the n^{th} encoded information bit.

The baseband signal from mobile terminals $i(1 \le i \le k)$ can be written as

$$\boldsymbol{x}_i(n) = c_i(n) \cdot \boldsymbol{d}_i \qquad (1)$$

where, $c_i(n)$ is the n^{th} encoded information bit, $\boldsymbol{x}_i(n) \in \mathbf{Z}^{1\times K}$ is the n^{th} baseband spread spectrum signal sequence.

Baseband signal $\boldsymbol{x}_i$ after the RF modulating obtain send signals $\boldsymbol{T}_i(1 \le i \le k)$. Interference source signals $\boldsymbol{x}_t$ after the RF modulating obtain send signals $\boldsymbol{T}_t$.

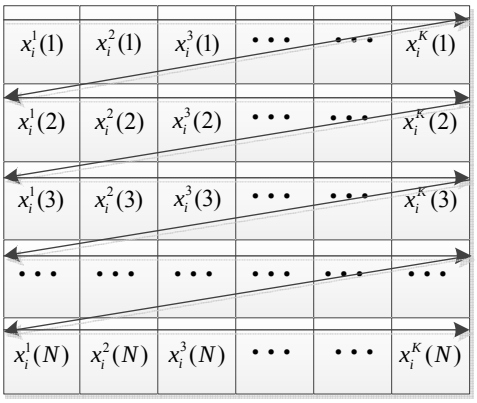


Fig. 3 Spread spectrum signal block diagram

In BPSK (Binary Phase Shift Keying) system, the sending signal from mobile terminal i can be written as

$$T_i(t) = A_i^0 \cdot \cos(2\pi f_c t) \times \sum_n c_i(n) \cdot d_i \cdot p_1(t - nT_c) \qquad (2)$$

where, A_i^0 is the transmission amplitude, f_c is the carrier frequency, p_1 is impulse response of pulse shaping filter.

The receive signal in the receiver can be written as

$$r_j(t) = \sum_i A_{i,j} \cdot \cos(2\pi f_c t + \varphi_{i,j}) \times \sum_n c_i(n) \cdot d_i \cdot p_1(t - nT_c - \tau_{i,j}) + v(t) \quad (j = 1,2) \qquad (3)$$

where, $A_{i,j}$ and $\varphi_{i,j}$ are the carrier amplitude and phase position, $\tau_{i,j}$ is the transmission delay, v is channel white Gaussian noise.

The baseband uplink channel model of MIMO cognitive system is shown in Figure 4.

The channel transfer matrix from mobile terminals $i(1 \le i \le k)$ to base station is denoted $\boldsymbol{H}_i \in \mathbf{Q}^{2\times 2}$, and $\boldsymbol{H}_i = \begin{bmatrix} h_{i,1} & h_{i,2} \\ h_{i,3} & h_{i,4} \end{bmatrix}$, where the entries of $\boldsymbol{H}_i(1 \le i \le k)$ are independent and identically distributed (i.i.d.). The channel transfer matrix from interference source to base station is denoted $\boldsymbol{H}_t \in \mathbf{Q}^{2\times 2}$, and $\boldsymbol{H}_t = \begin{bmatrix} h_{t,1} & h_{t,2} \\ h_{t,3} & h_{t,4} \end{bmatrix}$. $\boldsymbol{x}_i$ is transmission signal from mobile terminals $i(1 \le i \le k)$. $\boldsymbol{x}_t \in \mathbf{Z}^{1\times(N\cdot K)}$ is interference signal from PPU interference source. $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathbf{Q}^{1\times(N\cdot K)}$ are channel white Gaussian noise. $\boldsymbol{y}_1, \boldsymbol{y}_2 \in \mathbf{Q}^{1\times(N\cdot K)}$ are the received signals in base station receiver.

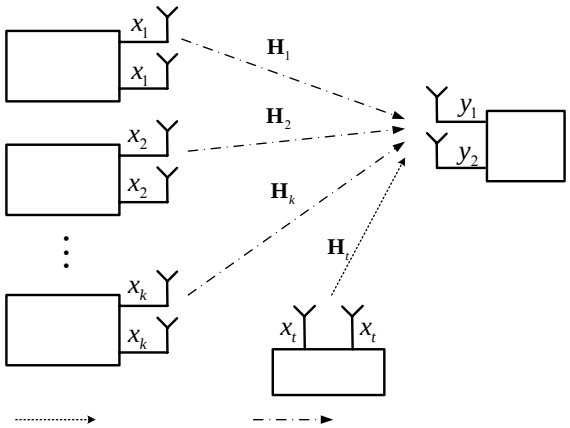


Fig.4 The baseband uplink channel model of MIMO cognitive system

In the base station receiver, the received signals $\boldsymbol{y}_1, \boldsymbol{y}_2$ after equal gain combining, the combining signals $\boldsymbol{y} \in \mathbf{Q}^{1\times(N\cdot K)}$ can be obtained. The electronic interference of PPU and channel noise are looked as a new noise. The expected information can be obtained through dispreading mapping and channel decoding of the proposed system.

In a transmission cycle of signals frame, the baseband signals model in base station receiver is as follows.

$$\begin{bmatrix} \boldsymbol{y}_1(n) \\ \boldsymbol{y}_2(n) \end{bmatrix} = \sum_{i=1}^{k} \boldsymbol{H}_i \cdot \begin{bmatrix} \boldsymbol{x}_i(n) \\ \boldsymbol{x}_i(n) \end{bmatrix} + \boldsymbol{H}_t \cdot \begin{bmatrix} \boldsymbol{x}_t(n) \\ \boldsymbol{x}_t(n) \end{bmatrix} + \begin{bmatrix} \boldsymbol{v}_1(n) \\ \boldsymbol{v}_2(n) \end{bmatrix} \qquad (4)$$

where $\boldsymbol{y}_1(n), \boldsymbol{y}_2(n) \in \mathbf{Q}^{1\times K}$ are the n^{th} received signals sequences. After spread spectrum mapping, $\boldsymbol{x}_t(n) \in \mathbf{Z}^{1\times K}$ is the n^{th} interference signals sequences. $\boldsymbol{v}_1(n), \boldsymbol{v}_2(n) \in \mathbf{Q}^{1\times K}$ are the n^{th} channel white Gaussian noise sequences.

Equation (4) can be written as

$$\begin{aligned} \boldsymbol{y}_1(n) &= \sum_{i=1}^{k} (h_{i,1} + h_{i,2}) \cdot \boldsymbol{x}_i(n) + (h_{t,1} + h_{t,2}) \cdot \boldsymbol{x}_t(n) + \boldsymbol{v}_1(n) \\ \mathbf{y}_2(n) &= \sum_{i=1}^{k} (h_{i,3} + h_{i,4}) \cdot \boldsymbol{x}_i(n) + (h_{t,3} + h_{t,4}) \cdot \boldsymbol{x}_t(n) + \boldsymbol{v}_2(n) \end{aligned} \qquad (5)$$

According to (1), (5) can be written as

$$\begin{aligned} \boldsymbol{y}_1(n) &= \sum_{i=1}^{k} (h_{i,1} + h_{i,2}) \cdot c_i(n) \cdot \boldsymbol{d}_i + (h_{t,1} + h_{t,2}) \cdot \boldsymbol{x}_t(n) \\ &+ \boldsymbol{v}_1(n) \\ \mathbf{y}_2(n) &= \sum_{i=1}^{k} (h_{i,3} + h_{i,4}) \cdot c_i(n) \cdot \boldsymbol{d}_i + (h_{t,3} + h_{t,4}) \cdot \boldsymbol{x}_t(n) \\ &+ \boldsymbol{v}_2(n) \end{aligned} \qquad (6)$$

where $\boldsymbol{d}_i$ is the spreading codes sequences, and $\boldsymbol{d}_i \cdot \boldsymbol{d}_j^T = 0(i \ne j)$, $\boldsymbol{d}_i \cdot \boldsymbol{d}_j^T = \mathrm{A}(i = j)$, A is a positive integer.

In this paper, we define

$\alpha_i = \sum_{j=1}^{4} h_{i,j} (1 \le i \le k)$ and $\alpha_t = \sum_{j=1}^{4} h_{t,j}$.

In the base station receiver, the received signals $\boldsymbol{y}_1$ and $\boldsymbol{y}_2$ after equal gain combining, (6) can be written as

$$\boldsymbol{y}(n) = \boldsymbol{y}_1(n) + \mathbf{y}_2(n) = \sum_{i=1}^{K} \alpha_i \cdot c_i(n) \cdot \boldsymbol{d}_i + \alpha_t \cdot \boldsymbol{x}_t(n) + \sum_{i=1}^{2} \boldsymbol{v}_i(n) \quad (7)$$

The base station receiver extracts mobile terminal 1 signal, the combining signals $\boldsymbol{y}$ after dispreading mapping, (7) can be written as

$$\begin{aligned} \tilde{c}_1(n) &= \boldsymbol{y}(n) \cdot \frac{\boldsymbol{d}_1^T}{\mathrm{A}} = (\sum_{i=1}^{K} \alpha_i \cdot c_i(n) \cdot \boldsymbol{d}_i + \alpha_t \cdot \boldsymbol{x}_t(n) + \sum_{i=1}^{2} \boldsymbol{v}_i(n)) \cdot \frac{\boldsymbol{d}_1^T}{\mathrm{A}} \\ &= \frac{1}{\mathrm{A}} \cdot (\sum_{i=1}^{K} \alpha_i \cdot c_i(n) \cdot \boldsymbol{d}_i \cdot \boldsymbol{d}_1^T + \alpha_t \cdot \boldsymbol{x}_t(n) \cdot \boldsymbol{d}_1^T + \sum_{i=1}^{2} \boldsymbol{v}_i(n) \cdot \boldsymbol{d}_1^T) \\ &= \alpha_1 \cdot c_1(n) + \alpha_t \cdot \frac{\boldsymbol{x}_t(n) \cdot \boldsymbol{d}_1^T}{\mathrm{A}} + \frac{1}{\mathrm{A}} \cdot \sum_{i=1}^{2} \boldsymbol{v}_i(n) \cdot \boldsymbol{d}_1^T \\ &= \alpha_1 \cdot c_1(n) + \alpha_t \cdot x_t'(n) + v'(n) \end{aligned} \quad (8)$$

It can also be written as

$$\tilde{\boldsymbol{c}}_1 = \alpha_1 \cdot \boldsymbol{c}_1 + \alpha_t \cdot \boldsymbol{x}_t' + \boldsymbol{v}' \quad (9)$$

where, $\boldsymbol{x}_t'$ is the interference signal after dispreading mapping, $\boldsymbol{v}'$ is channel white Gaussian noise after dispreading mapping.

From the above equation, after despreading mapping, the interference from other mobile terminals has been eliminated, and the received signals only are of the interference from interference source and channel noise.

According to (9), we can see that signal $\tilde{\boldsymbol{c}}_1$ includes co-channel interference $\alpha_t \cdot \boldsymbol{x}_t'$ from interference source signal $\boldsymbol{x}_t'$. Let interference of PPU be $\boldsymbol{I}_C = \alpha_t \cdot \boldsymbol{x}_t'$. Because interference $\boldsymbol{I}_C$ is not controllable, the despreading mapping in (9) cannot completely cancel the interference $\boldsymbol{I}_C$. In order to solve this problem, we use protograph LDPC codes to cancel the interference $\boldsymbol{I}_C$. The design of protograph LDPC will be provided in next section.

The interference source signal and channel noise interference in equation (9) look as a new noise, it can be written as

$$\boldsymbol{v}_C = \alpha_t \cdot \boldsymbol{x}_t' + \boldsymbol{v}' \quad (10)$$

According to (10), signal $\tilde{\boldsymbol{c}}_1$ can be written as

$$\tilde{\boldsymbol{c}}_1 = \alpha_1 \cdot \boldsymbol{c}_1 + \boldsymbol{v}_C \quad (11)$$

Then, decoding the received signals $\tilde{\boldsymbol{c}}_1$ by protograph LDPC codes, we can obtain the information $\tilde{\boldsymbol{m}}_1$ from transmitter. It can be written as

$$\tilde{\boldsymbol{m}}_1 = \mathrm{dec}(\tilde{\boldsymbol{c}}_1) = \mathrm{dec}(\alpha_1 \cdot \boldsymbol{c}_1 + \boldsymbol{v}_C) \quad (12)$$

where $\mathrm{dec}(\cdot)$ denotes the protograph LDPC decoding.

Now, we analyze the channel coefficient influence the BER performance of cognitive base station receiver.

After normalization processing, (9) can be written as

$$\boldsymbol{y}_1' = \boldsymbol{c}_1 + \frac{\alpha_t}{\alpha_1} \cdot \boldsymbol{x}_t' + \frac{1}{\alpha_1} \cdot \boldsymbol{v}' \quad (13)$$

Generally, the base station receiver extracts signal of mobile terminal i, (13) can be written as

$$\boldsymbol{y}_i' = \boldsymbol{c}_i + \frac{\alpha_t}{\alpha_i} \cdot \boldsymbol{x}_t' + \frac{1}{\alpha_i} \cdot \boldsymbol{v}' \quad (1 \le i \le k) \quad (14)$$

From (14), in this paper we define

$$\mathrm{R}_i = \frac{\alpha_t}{\alpha_i} \quad (15)$$

as channel matrix ratio.

In the uplink communication system receiver, the value of α_i are different, and the value of α_t is fixed. This means that the greater value of α_i, the smaller value of R_i, and the smaller interference of $\frac{\alpha_t}{\alpha_i} \cdot \boldsymbol{x}_t'$ and $\frac{1}{\alpha_i} \cdot \boldsymbol{v}'$ to received signals. The BER performance depends on the value of R_i in the uplink communication system. We will see it in the following simulations.

2.2 Downlink Communication System

In the downlink, the base station transmits data, and the mobile terminals receive data. The downlink communication system model of MIMO cognitive system is shown in Figure 5.

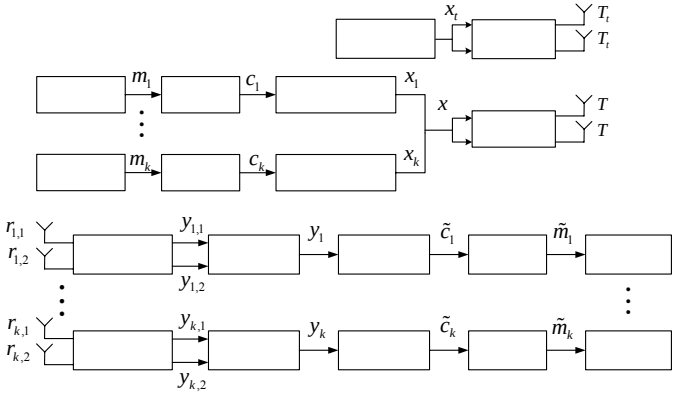


Fig.5 MIMO cognitive system downlink communication system model

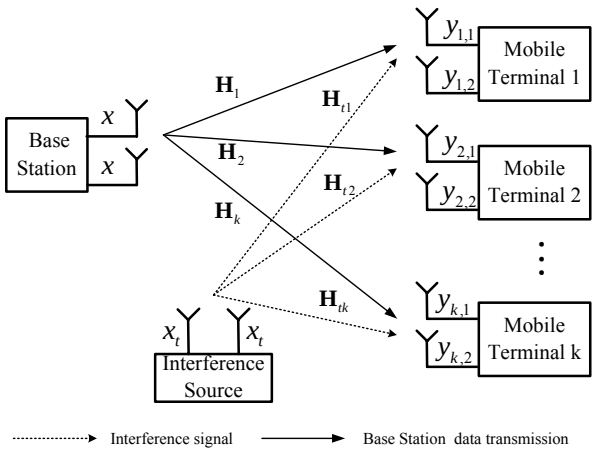
The MIMO cognitive system baseband downlink channel model is shown in Figure 6.

The downlink channel model of MIMO cognitive system baseband

The baseband signals from base station can be written as

$$\boldsymbol{x}(n) = \sum_{i=1}^{K} \boldsymbol{x}_i(n) = \sum_{i=1}^{K} c_i(n) \cdot \boldsymbol{d}_i \quad (16)$$

The channel transfer matrix from interference source to mobile terminal $i(1 \le i \le k)$ is denoted $\boldsymbol{H}_{ti}$, and $\boldsymbol{H}_{ti} = \begin{bmatrix} h_{ti,1} & h_{ti,2} \\ h_{ti,3} & h_{ti,4} \end{bmatrix}$.



In a transmission cycle of signals frame, the baseband signals model in mobile terminal 1 receiver is as follows.

$$\begin{bmatrix} \boldsymbol{y}_{1,1}(n) \\ \boldsymbol{y}_{1,2}(n) \end{bmatrix} = \boldsymbol{H}_1 \cdot \begin{bmatrix} \boldsymbol{x}(n) \\ \boldsymbol{x}(n) \end{bmatrix} + \boldsymbol{H}_{t1} \cdot \begin{bmatrix} \boldsymbol{x}_t(n) \\ \boldsymbol{x}_t(n) \end{bmatrix} + \begin{bmatrix} \boldsymbol{v}_1(n) \\ \boldsymbol{v}_2(n) \end{bmatrix} \tag{17}$$

Equation (17) can be written as

$$\begin{aligned} \boldsymbol{y}_1(n) &= (h_{1,1} + h_{1,2}) \cdot \boldsymbol{x}(n) + (h_{t1,1} + h_{t1,2}) \cdot \boldsymbol{x}_t(n) + \boldsymbol{v}_1(n) \\ \mathbf{y}_2(n) &= (h_{1,3} + h_{1,4}) \cdot \boldsymbol{x}(n) + (h_{t1,3} + h_{t1,4}) \cdot \boldsymbol{x}_t(n) + \boldsymbol{v}_2(n) \end{aligned} \tag{18}$$

According to (16), (18) can be written as

$$\begin{aligned} \boldsymbol{y}_{1,1}(n) &= (h_{1,1} + h_{1,2}) \cdot \sum_{i=1}^{K} c_i(n) \cdot \boldsymbol{d}_i + (h_{t1,1} + h_{t1,2}) \cdot \boldsymbol{x}_t(n) \\ &+ \boldsymbol{v}_1(n) \\ \boldsymbol{y}_{1,2}(n) &= (h_{1,3} + h_{1,4}) \cdot \sum_{i=1}^{K} c_i(n) \cdot \boldsymbol{d}_i + (h_{t1,3} + h_{t1,4}) \cdot \boldsymbol{x}_t(n) \\ &+ \boldsymbol{v}_2(n) \end{aligned} \tag{19}$$

In this paper, we define $\alpha_{ti} = \sum_{j=1}^{4} h_{ti,j}$.

In the mobile terminal 1 receiver, the received signals $\boldsymbol{y}_{1,1}$ and $\boldsymbol{y}_{1,2}$ after equal gain combining, (19) can be written as

$$\begin{aligned} \boldsymbol{y}_1(n) &= \boldsymbol{y}_{1,1}(n) + \mathbf{y}_{1,2}(n) \\ &= \alpha_1 \cdot \sum_{i=1}^{K} c_i(n) \cdot \boldsymbol{d}_i + \alpha_{t1} \cdot \boldsymbol{x}_t(n) + \sum_{i=1}^{2} \boldsymbol{v}_i(n) \end{aligned} \tag{20}$$

The mobile terminal 1 receiver extracts the signal from base station, the combining signals $\boldsymbol{y}_1$ after dispreading mapping, (20) can be written as

$$\begin{aligned} \tilde{c}_1(n) &= \boldsymbol{y}_1(n) \cdot \frac{\boldsymbol{d}_1^T}{\mathrm{A}} = (\alpha_1 \cdot \sum_{i=1}^{K} c_i(n) \cdot \boldsymbol{d}_i + \alpha_{t1} \cdot \boldsymbol{x}_t(n) + \sum_{i=1}^{2} \boldsymbol{v}_i(n)) \cdot \frac{\boldsymbol{d}_1^T}{\mathrm{A}} \\ &= \frac{1}{\mathrm{A}} \cdot (\alpha_1 \cdot \sum_{i=1}^{K} c_i(n) \cdot \boldsymbol{d}_i \cdot \boldsymbol{d}_1^T + \alpha_{t1} \cdot \boldsymbol{x}_t(n) \cdot \boldsymbol{d}_1^T + \sum_{i=1}^{2} \boldsymbol{v}_i(n) \cdot \boldsymbol{d}_1^T) \\ &= \alpha_1 \cdot c_1(n) + \alpha_{t1} \cdot \frac{\boldsymbol{x}_t(n) \cdot \boldsymbol{d}_1^T}{\mathrm{A}} + \frac{1}{\mathrm{A}} \cdot \sum_{i=1}^{2} \boldsymbol{v}_i(n) \cdot \boldsymbol{d}_1^T \\ &= \alpha_1 \cdot c_1(n) + \alpha_{t1} \cdot x_t'(n) + v'(n) \end{aligned} \tag{21}$$

It can also be written as

$$\tilde{\boldsymbol{c}}_1 = \alpha_1 \cdot \boldsymbol{c}_1 + \alpha_{t1} \cdot \boldsymbol{x}_t' + \boldsymbol{v}' \tag{22}$$

where, $\boldsymbol{x}_t'$ is the interference signal after dispreading mapping, $\boldsymbol{v}'$ is channel white Gaussian noise after dispreading mapping.

From the above equation, after despreading mapping, the interference from other mobile terminals has been eliminated, and the received signals only are of the interference from interference source and channel noise.

The PPU interference source signal and channel noise interference in equation (22) look as a new noise, it can be written as

$$\boldsymbol{v}_C = \alpha_{t1} \cdot \boldsymbol{x}_t' + \boldsymbol{v}' \tag{23}$$

According to (23), signal $\tilde{\boldsymbol{c}}_1$ can be written as

$$\tilde{\boldsymbol{c}}_1 = \alpha_1 \cdot \boldsymbol{c}_1 + \boldsymbol{v}_C \tag{24}$$

Then, decoding the received signals $\tilde{\boldsymbol{c}}_1$ by protograph LDPC codes, we can obtain the information $\tilde{\boldsymbol{m}}_1$ from transmitter. It can be written as

$$\tilde{\boldsymbol{m}}_1 = \mathrm{dec}(\tilde{\boldsymbol{c}}_1) = \mathrm{dec}(\alpha_1 \cdot \boldsymbol{c}_1 + \boldsymbol{v}_C) \tag{25}$$

where $\mathrm{dec}(\cdot)$ denotes the protograph LDPC decoding.

3. Protograph LDPC Codes

In this section, we give the construction of protograph LDPC codes with fast encoding, which is used to cancel the electronic interference and channel noises interference.

The proposed rate 1/2 protograph LPDC (N, M) codes are short codes with good BER performance, simple structure and low encoding complexity. The size of parity check matrix $\boldsymbol{H} = \begin{bmatrix} \boldsymbol{H}_a & \boldsymbol{H}_b \end{bmatrix}$ of protograph LDPC codes is $M \times N$, where matrix $\boldsymbol{H}_a$ and $\boldsymbol{H}_b$ consists of 8×8 sub matrices.

The matrix $\boldsymbol{H}_b$ is shown as below,

$$\boldsymbol{H}_b = \begin{bmatrix} \boldsymbol{I} & & & \boldsymbol{0} \\ \boldsymbol{I} & \boldsymbol{I} & & \\ & \ddots & \ddots & \\ \boldsymbol{0} & & \boldsymbol{I} & \boldsymbol{I} \end{bmatrix}_{8 \times 8} \tag{26}$$

where $\boldsymbol{I}$ and $\boldsymbol{0}$ are $N/16 \times N/16$ identity and zero matrices, respectively.

We give the matrix $\boldsymbol{H}_a$. It can be written as

$$\boldsymbol{H}_a=\begin{bmatrix}\boldsymbol{L}_1\oplus\boldsymbol{L}_2 & \boldsymbol{L}_6\oplus\boldsymbol{L}_7\\ \boldsymbol{L}_3\oplus\boldsymbol{L}_4\oplus\boldsymbol{L}_5 & \boldsymbol{L}_8\oplus\boldsymbol{L}_9\end{bmatrix} \tag{27}$$

where matrix $\boldsymbol{L}_1\sim\boldsymbol{L}_8$ are $N/4\times N/4$ permutation matrices.

The permutation matrices we used in this paper are similar to [26].

Permutation matrix $\boldsymbol{L}_k$ has non-zero entries in row i and column $\pi_k(i)$ for $i\in\{0,\cdots,N/4-1\}$ and

$$\pi_k(i)=\frac{N}{16}\left(\left(\theta_k+\lfloor i\cdot 16/N\rfloor\right)\bmod 4\right)+\left(\phi_k\left(\lfloor i\cdot 16/N\rfloor\right)+i\right)\bmod\frac{N}{16} \tag{28}$$

The permutation matrix can be divided into 4×4 unit circulate sub-matrices, the matrix $\boldsymbol{H}_a$ consist of 8×8 sub matrices. The matrix $\boldsymbol{H}_a$ also can be written as

$$\boldsymbol{H}_a=\begin{bmatrix}\boldsymbol{I}^{a_{1,1}} & \boldsymbol{I}^{a_{1,2}} & \cdots & \boldsymbol{I}^{a_{1,8}}\\ \boldsymbol{I}^{a_{2,1}} & \boldsymbol{I}^{a_{2,2}} & \cdots & \boldsymbol{I}^{a_{2,8}}\\ \vdots & \vdots & \ddots & \vdots\\ \boldsymbol{I}^{a_{8,1}} & \boldsymbol{I}^{a_{8,2}} & \cdots & \boldsymbol{I}^{a_{8,8}}\end{bmatrix} \tag{29}$$

where the matrix $\boldsymbol{I}^{a_{i,j}}$ is identity matrix right shift $a_{i,j}$ bit.

Now, we give the fast encoding algorithm of protograph LDPC codes.

Suppose, codes vector is denoted $\boldsymbol{c}=[\boldsymbol{S}\quad\boldsymbol{P}]$, where $\boldsymbol{S}=[\boldsymbol{S}_1\quad\boldsymbol{S}_2\quad\cdots\quad\boldsymbol{S}_8]$ is the information vector, and $\boldsymbol{P}=[\boldsymbol{P}_1\quad\boldsymbol{P}_2\quad\cdots\quad\boldsymbol{P}_8]$ is the check vector.

According to the channel coding theory, we know that $\boldsymbol{H}\times\boldsymbol{c}^T=\boldsymbol{0}$, it can be written as

$$[\boldsymbol{H}_a\quad\boldsymbol{H}_b]\cdot[\boldsymbol{S}\quad\boldsymbol{P}]^T=\boldsymbol{0} \tag{30}$$

$$\begin{aligned}&\boldsymbol{I}^{a_{1,1}}\times\boldsymbol{S}_1^T\oplus\boldsymbol{I}^{a_{1,2}}\times\boldsymbol{S}_2^T\oplus\cdots\boldsymbol{I}^{a_{1,8}}\times\boldsymbol{S}_8^T\oplus\boldsymbol{P}_1^T=\boldsymbol{0}\\ &\boldsymbol{I}^{a_{2,1}}\times\boldsymbol{S}_1^T\oplus\boldsymbol{I}^{a_{2,2}}\times\boldsymbol{S}_2^T\oplus\cdots\boldsymbol{I}^{a_{2,8}}\times\boldsymbol{S}_8^T\oplus\boldsymbol{P}_1^T\oplus\boldsymbol{P}_2^T=\boldsymbol{0}\\ &\qquad\vdots\\ &\boldsymbol{I}^{a_{8,1}}\times\boldsymbol{S}_1^T\oplus\boldsymbol{I}^{a_{8,2}}\times\boldsymbol{S}_2^T\oplus\cdots\boldsymbol{I}^{a_{8,8}}\times\boldsymbol{S}_8^T\oplus\boldsymbol{P}_7^T\oplus\boldsymbol{P}_8^T=\boldsymbol{0}\end{aligned} \tag{31}$$

Then we can obtain $\boldsymbol{P}_1^T,\boldsymbol{P}_2^T,\cdots,\boldsymbol{P}_8^T$.

$$\begin{cases}\boldsymbol{P}_1^T=\sum_{j=1}^{8}\boldsymbol{I}^{a_{1,j}}\times\boldsymbol{S}_j^T\\ \boldsymbol{P}_2^T=\boldsymbol{P}_1^T\oplus\sum_{j=1}^{8}\boldsymbol{I}^{a_{2,j}}\times\boldsymbol{S}_j^T\\ \qquad\vdots\\ \boldsymbol{P}_8^T=\boldsymbol{P}_7^T\oplus\sum_{j=1}^{8}\boldsymbol{I}^{a_{8,j}}\times\boldsymbol{S}_j^T\end{cases} \tag{32}$$

Equation (32) is the proposed fast encoding algorithm.

If the information codes vector $\boldsymbol{S}$ and check matrix $\boldsymbol{H}$ are known, applying (32), we can obtain the code vector $\boldsymbol{c}=[\boldsymbol{S}\quad\boldsymbol{P}]$.

The sub-matrices of the parity check matrix $\boldsymbol{H}$ are unit circulate matrices, if the first row of matrix is known, the other rows can be obtained by first row of right shift. Thus we only need to store the first row of each sub-matrix in the encoding process. This can reduce the computation and storage space. The proposed fast encoding algorithm (32) simplifies the hardware complexity of LDPC encoder.

4. Evaluations and Simulation Results

In this section, we evaluate performances of the proposed method that electronic interference cancellation based on spread spectrum LDPC codes in MIMO system. According to the design approach of protograph LDPC codes in Section III, let $N=1024$, we can obtain the parity check matrix $\boldsymbol{H}$ of rate 1/2 protograph LDPC $(N=1024,M=512)$ codes by (27) and (28), where the functions θ_k and $\phi_k(j)$ are defined in Table 1.

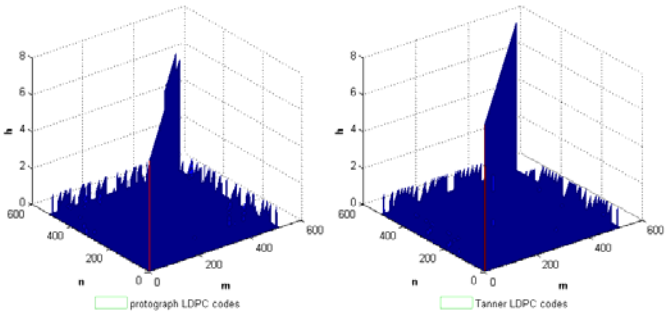
Table 1 Description of θ_k and $\phi_k(j)$

k	θ_k	$\phi_k(0)$	$\phi_k(1)$	$\phi_k(2)$	$\phi_k(3)$
1	0	39	40	31	9
2	2	20	18	53	11
3	0	12	30	1	38
4	2	29	59	8	43
5	3	24	23	7	2
6	0	41	17	18	47
7	2	10	15	14	3
8	1	45	6	39	41
9	3	51	5	49	26

According to [27], we can obtain the check matrix $\boldsymbol{H}$ of rate 1/2 Tanner LDPC codes $(n=1024,k=512)$, where $a=5,b=2,m=128$.

Theorem 1[28]: If and only if the elements of $\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}}$ are 0 or 1 except in diagonal line, the LDPC codes has no girth-4, where $\boldsymbol{H}$ is the parity check matrix.

Now, we test girth_4 of protograph LDPC codes and Tanner LDPC codes by applying theorem 1, as shown in Fig.6.



The girth_4 test of protograph LDPC codes and Tanner LDPC codes

According to Fig.6, we observe that the elements of $\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}}$ are 0 or 1 except in diagonal line, and we found that there is no girth-4 in both protograph LDPC codes and Tanner LDPC codes.

In the simulation results, method 1: electronic interference cancellation based on spread spectrum protograph LDPC codes; method 2: electronic interference cancellation based on spread

spectrum Tanner LDPC codes; method 3: electronic interference cancellation based on spread spectrum codes.

Conditions of simulation experiment: Rayleigh fading channel, the decoders of two codes (protograph LDPC codes and Tanner LDPC codes) use the same BP algorithm [28], the same code rate 1/2, 4000 data frames per SNR point, the spreading codes sequences of method 1 and 2 use 128-order hadamard matrix, the spreading codes sequences of method 3 use 256-order hadamard matrix. The code rates of three methods are 1/256.

Take a MIMO system with 16 mobile terminals, a base station and an interference source for example. We evaluate the BER performances of the proposed interference cancellation based on spread spectrum protograph LDPC codes under two conditions (uplink communication system and downlink communication system).

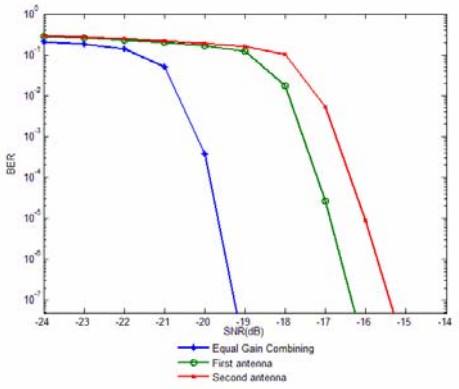
Uplink communication system

The channel transfer matrix from mobile terminal 1 to base station is $\boldsymbol{H}_1 = \begin{bmatrix} 0.4503 & 0.3714 \\ 0.3359 & 0.4208 \end{bmatrix}$; The channel transfer matrix from mobile terminal 2 to base station is $\boldsymbol{H}_2 = \begin{bmatrix} 0.3106 & 0.2874 \\ 0.2417 & 0.3462 \end{bmatrix}$; The channel transfer matrix from interference source to base station is $\boldsymbol{H}_t = \begin{bmatrix} 0.9201 & 0.3746 \\ 0.3314 & 0.8947 \end{bmatrix}$. $\alpha_1 = 1.5784$, $\alpha_2 = 1.1859$ and $\alpha_t = 2.5208$.

$$R_1 = \frac{\alpha_t}{\alpha_1} = \frac{2.5208}{1.5784} = 1.5971 \text{ , } R_2 = \frac{\alpha_t}{\alpha_2} = \frac{2.5208}{1.1859} = 2.1256 \text{ ,}$$

$R_1 < R_2$.

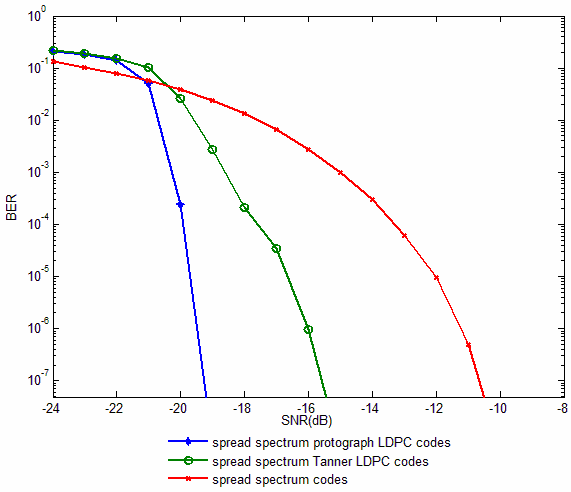
In the base station receiver, we use spread spectrum protograph LDPC codes to extract mobile terminal 1 signal under three conditions (equal gain combining signals, the first antenna signals, the second antenna signals). The BER performance comparison of three conditions in uplink communication system is show in Fig.8.



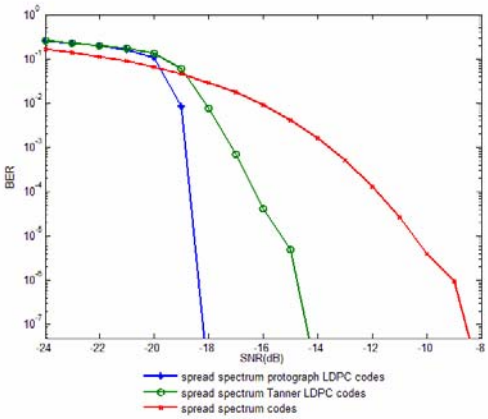
compare BER performance under three conditions (equal gain combining signals, the first antenna signals, the second antenna signals) in uplink communication system

According to BER performance in Fig.8, we observe that equal gain combining signals obtained about 3dB and 4 dB gains comparing with the first antenna signals and the second antenna signals in Rayleigh flat-fading channel, respectively. It verifies that the equal gain combining can increase information transmission reliability.

The BER performance comparison of the method 1, 2and 3 in uplink communication system is show in Fig.9.



(a) Base station extracts mobile terminal 1 signal



(b) Base station extracts mobile terminal 2 signal

compare BER performance of method 1, 2and 3 in uplink communication system

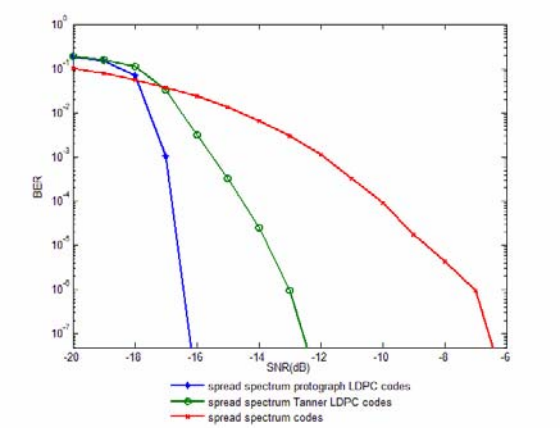
According to BER performance in Fig.9 (a), we observe that method 1 obtained about 4dB and 9dB gain comparing with method 2 and 3 in Rayleigh flat-fading channel, respectively. According to BER performance in Fig.9 (b), we observe that method 1 obtained about 4dB and 10dB coding gain comparing with method 2 and 3 in Rayleigh flat-fading channel, respectively. It verifies the validity of the proposed approach; it can effectively cancel electronic interference from enemy and channel noises interference.

Compare Fig.9 (a) and (b), we observe that method 1,2 and 3 in Fig.9 (a) obtained about 1dB, 1dB and 2dB gain comparing with method 1,2 and 3 in Fig.9 (b) , respectively. And the value of R_1 in Fig.9 (a) is smaller than R_2 in Fig.9 (b) .We can see that, the smaller value of R, the better BER performance in uplink communication system.

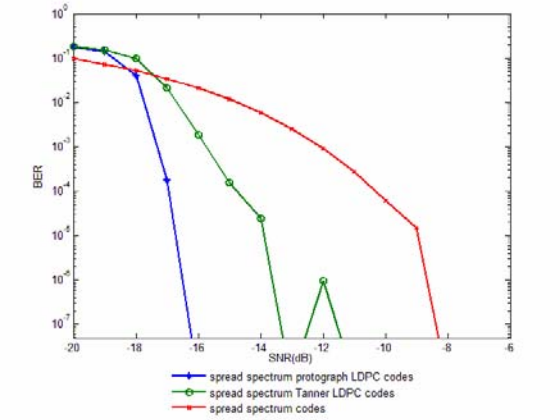
downlink communication system

The channel transfer matrix from base station to mobile terminal 1 is $\boldsymbol{H}_1 = \begin{bmatrix} 0.3503 & 0.2114 \\ 0.2459 & 0.3208 \end{bmatrix}$; The channel transfer matrix from base station to mobile terminal 2 is $\boldsymbol{H}_2 = \begin{bmatrix} 0.3306 & 0.2274 \\ 0.2523 & 0.3463 \end{bmatrix}$; The channel transfer matrix from interference source to mobile terminal 1 is $\boldsymbol{H}_{t1} = \begin{bmatrix} 0.9201 & 0.3746 \\ 0.3314 & 0.8947 \end{bmatrix}$; The channel transfer matrix from interference source to mobile terminal 2 is $\boldsymbol{H}_{t1} = \begin{bmatrix} 0.9501 & 0.4046 \\ 0.3714 & 0.9347 \end{bmatrix}$.

The BER performance comparison of the method 1, 2and 3 in downlink communication system is show in Fig.10.



(a) Mobile terminal 1 extracts cognitive base station signal



(b) Mobile terminal 2 extracts cognitive base station signal

compare BER performance of method 1, 2and 3 in downlink communication system

According to BER performance in Fig.10 (a), we observe that method 1 obtained about 4dB and 10dB coding gain comparing with method 2 and 3 in Rayleigh flat-fading channel, respectively. According to BER performance in Fig.10 (b), we observe that method 1 obtained about 3dB and 8dB coding gain comparing with method 2 and 3 in Rayleigh flat-fading channel, respectively. And the method 2 have error floor between -13dB and -11dB. It verifies the validity of the proposed approach; it can effectively cancel electronic interference from enemy and channel noises interference.

5. Conclusions

In this paper, we propose a method that electronic interference cancellation based on spread spectrum LDPC codes in MIMO cognitive system. Protograph LDPC codes and spread spectrum are applied to MIMO cognitive system in the proposed scheme, the information transmission can be of the anti-interference ability and error correcting capability through channel coding and spread spectrum mapping, which can cancel electronic interference and channel noises interference. This method can make multiple CUs secure communication under the condition of strong electronic interference from PU. The simulation results in Rayleigh flat-fading channel show that, comparing with MIMO cognitive system without the proposed method, the proposed approach can effectively cancel electronic interference from enemy and channel noises interference and obtain about 9dB gain.

References

[1] S. Haykin. Cognitive radio: brain-empowered wireless communications [J]. IEEE J. Sel. Areas Commun, 2005, 23(2):201-220.

[2] Hou Y. Thomas, Shi Yi, Sherali Hanif D. Spectrum sharing for multi-hop networking with cognitive radios [J]. IEEE J. Sel. Areas Commun, 2008, 26(1):146-155.

[3] H. Islam, Y. Liang, A. Hoang. Joint power control and beamforming for cognitive radio networks [J]. IEEE Trans. on Wireless Communications, 2008, 7(7):2415-2419.

[4] Ma Jun Li, Geoffrey Ye, Juang Biing Hwang. Signals processing in cognitive radio[J]. Proceedings of the IEEE, 2009, 97(5):805-823.

[5] Mitola, Joseph. Cognitive Radio Architecture Evolution[J]. Proceedings of the IEEE, 2009, 97(4):626-641.

[6] Yang Xiao, Kiseon Kim, Guangzhi Qu. A Cognitive Spatial Multiplexing Scheme for MIMO-CDMA Networks[C]. Proc. of Conference on Wireless, Mobile and Multimedia Networks, Beijing, China, 2010: 147-150.

[7] Yang Xiao,Yingkang Zhang, Guangzhi Qu, et al. Spatial Multiplexing Algorithms of Cognitive Base-Stations[C]. Proc. of Conference on Wireless, Mobile and Multimedia Networks, Beijing, China, 2010: 221-224.

[8] Gao, Cunhao, Shi, Yi, Hou, Y. Thomas, et al. On the Throughput of MIMO-Empowered Multihop Cognitive Radio Networks [J]. IEEE Trans. on mobile computing, 2011, 10(11):1505-1519.

[9] Y. Liang, H. V. Poor. Multiple access channels with confidential messages[J]. IEEE Trans. Inf. Theory, 2008,54(3): 976–1002.

[10] R. Liu, I. Maric, R. Yates, et al. The discrete memoryless multiple access channel with confidential messages [C]. Proc. of

IEEE Int. Symp. Information Theory, Seattle, USA, 2006: 957–961.

[11] E. Tekin, A. Yener. The Gaussian multiple access wire-tap channel [J]. IEEE Trans. Inf. Theory, 2008, 54(12): 5747–5755.

[12] E. Ekrem, S. Ulukus. Effects of cooperation on the secrecy of multiple access channels with generalized feedback [C]. Proc. of Conference on Information Sciences and Systems, Princeton, USA, 2008:791–796.

[13] R. Bassily, S. Ulukus. A new achievable ergodic secrecy rate region for the fading multiple access wiretap channel [C]. Proc. of Conference on Communications, Control and Computing, Monticello, USA, 2009: 819–826.

[14] O. Simeone, A. Yener. The cognitive multiple access wire-tap channel [C]. Proc. of Conference on Information Sciences and Systems, Baltimore, USA, 2009:158–16.

[15] Y. Liang, H. V. Poor, S. Shamai. Secure communication over fading channels [J]. IEEE Trans. Inf. Theory, 2008, 54(6): 2470–2492.

[16] P. Gopala, L. Lai, H. El Gamal. On the secrecy capacity of fading channels [J]. IEEE Trans. Inf. Theory, 2008, 54(10): 4687–4698.

[17] X. Tang, R. Liu, P. Spasojevic, H. V. Poor. On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels [J]. IEEE Trans. Inf. Theory, 2009, 55(4): 1575–1591.

[18] Ruoheng Liu, Yingbin Liang, H.V. Poor. Fading Cognitive Multiple-Access Channels With Confidential Messages [J]. IEEE Trans. Inf. Theory, 2011, 57(8): 4992–5005.

[19] X. He, A. Yener. Cooperation with an untrusted relay: A secrecy perspective [J]. IEEE Trans. Inf. Theory, 2010, 56(8): 3807–3827.

[20] E. Ekrem, S. Ulukus. Secrecy in cooperative relay broadcast channels [J]. IEEE Trans. Inf. Theory, 2011, 57(1): 137–155.

[21] J. Thorpe. Low density parity check (LDPC) codes constructed from protographs [C]. JPL Workshop on Interplanetary Network, USA, 2003:42-154.

[22] A. Abbasfar, D. Divsalar, K. Yao. Accumulate-repeat-accumulate codes [J]. IEEE Trans. on Communications, 2007, 55(4): 692-702.

[23] Y. Xiao, K. Kim. Good encodable irregular quasi-cyclic LDPC codes [C]. Proc. of Conference on Communication Systems, Singapore, 2008, pp.1291-1296.

[24] Kaiyao Wang, Shaohai Hu, Yang Xiao, et al. Construction of protograph LDPC codes based on Jacket matrices [C]. Proc. of Conference on Signals Processing, Beijing, China, 2010:1604-1607.

[25] Kaiyao Wang, Yang Xiao, Kiseon Kim. Construction of protograph LDPC codes with circular generator matrices [J]. Journal of Systems Engineering and Electronics, 2011, 22(5): 840-847.

[26] CCSDS131.1-O-2. Low density parity check codes for use in near-Earth and deep space applications [S].USA: CCSDS, 2007.

[27] R. M. Tanner, D. Sridhara, A. Sridharan, et al. LDPC block and convolutional codes based on circulant matrices [J]. IEEE Trans. on Inforation Theory, 2004,50(12):2966-2984.

[28] Y. Xiao, M. H. Lee. Low complexity MIMO-LDPC CDMA systems over multipath channels [J]. IEICE Trans. on Communications, 2006, E89-B(5) :1713- 1717.