Differential LDPC Coded Cooperative Communication Systems for Internet of Things

Yang Yu, Zhi-wen Qian, Lei Zhang, Bo Xue, Zhu-yang Chen

School of Electric Information Engineering, Jiangsu University of Technology, China
{dxyy, dxqzw, zhlei, dxxb, czy}@jsut.edu.cn

Abstract

In this paper, we study an differential LDPC coded cooperative communication systems for improving the communication quality and energy efficiency of the Internet of Things (IoT). In order to avoid the complex channel state information (CSI) estimation, a diffierential LDPC coded cooperative scheme based on multiple-symbol differential detection (MSDD) is first proposed. As the prohibitively high complexity of the decision metric of MSDD soft-input soft-output demodulator (SISOD), a soft-output M-algorithm (SOMA) for reducing the computational complexity of MSDD SISOD is then proposed based on analyzing the conventional M-algorithm that does not work well for MSDD SISOD. To further make the proposed scheme suit for the engineering applications of the IoT, a new method to construct parity check matrix of quasi-cyclic (QC) LDPC codes based on shortening RS codes is proposed for constructing LDPC codes with good minimum distances. The simulation results show that the performance of the systems under consideration can be effectively improved by the proposed scheme with good energy efficiency for the IoT.

Keywords: Low-density parity-check (LDPC) codes, QC-LDPC, Cooperative wireless communication, Multiple-symbol differential detection, Internet of Things

1 Introduction

The basic idea of the cooperative wireless communication is that each node in the system, while transmitting its own information, also helps other nodes to transmit information so that each node utilizes its own spatial channel and utilizes the partner's spatial channel to obtain space diversity gain. In recent years, the cooperative wireless communication technology has been widely concerned and is considered to be one of the key technologies of wireless communication systems such as LTE-Advanced system, WiMAX system, wireless local area network, vehicle communication network and wireless sensor network, etc [1-2].

As well known that most of the cooperative wireless communication systems require the receiver to be able to carry out accurate channel state information (CSI) estimation [3]. Compared with the traditional point-to-point wireless communication, this requirement for the cooperative communication system is a more challenging question. And the performance of the coherent detection receiver will be significantly reduced when there is a large error in channel estimation. Therefore, differential cooperative wireless communication systems using techniques of differential modulation and differential detection have become an attractive alternative scheme because they do not require CSI estimation [4-5].

On the other hand, multipath fading characteristics of wireless channels are the important factor affecting the data transmission rate and the quality of the IoT based on wireless communication systems [6-7]. Especially in the case of users moving at high speed, the fast fading of wireless channels will seriously affect the performance of the IoT based on wireless communication systems [8]. In order to meet this requirement, low-density parity-check (LDPC) codes have been adopted as some important wireless standards like 5G systems, WiMAX and so on, which will also play important role in the IoT. Therefore, it is important to study the LDPC coded systems for the IoT. Based on this background, differential LDPC coded systems with multiple-symbol differential detection (MSDD), which can compensate the performance degradation of differential detection compared to coherent detection, have attracted a wide attention in recent years [9-10]. However, there are few reports on differential LDPC coded cooperative communication systems, and the research on differential LDPC coded communication system is still mainly focused on point-to-point communication environment [11-12].

Against this background, this paper focus on the differential LDPC coded cooperative systems for the IoT. The specific contributions of this paper include the following:

(1) A diffierential LDPC coded cooperative scheme based on MSDD is proposed, and a multi-level tanner

*Corresponding Author: Yang Yu; E-mail: dxyy@jsut.edu.cn
DOI: 10.3966/160792642019032002020

graph of the differential LDPC coded cooperative scheme is analyzed.

(2) The decision metric of MSDD soft-input soft-output demodulator (SISOD) is given, and a soft-output M-algorithm (SOMA) for reducing the computational complexity of MSDD SISOD is proposed.

(3) A new method to construct the parity check matrix of QC-LDPC codes based on shortening RS codes is proposed for easy hardware implementation.

(4) The results of the simulation show that the performance of the system can be effectively improved by the proposed scheme with good energy efficiency for the IoT.

The rest of this paper is organized as follows. The considered system model, the metric of MSDD SISOD and the proposed SOMA are given in Section 2. The construction of check matrix of QC-LDPC Codes is studied in Section 3. In Section 4, the effectiveness of the proposed approaches and how to select the parameters for the proposed system with low complexity and good energy efficiency is analyzed in Section 4 through computer simulation. Finally, the paper is concluded in Section 5.

2 System Description

2.1 System Model

We consider the system model of the differential LDPC coded cooperative communication systems as shown in Figure 1. The corresponding tanner graph is shown in Figure 2. At the source node, a transmitted sequence **b** = $\{b_1, b_2,\ldots,b_K\}$, $b_i\in\{0, 1\}$ is encoded to a LDPC code sequence **c** = $\{c_1, c_2, \ldots, c_{N_1}\}$, $c_i\in\{0, 1\}$ using a rate K/N_1 LDPCs encoder. Then, the sequence **c** is mapped to an MPSK symbols sequence **x** = $\{x_1, x_2, \ldots, x_{N_1/M}\}$, $x_i \in \{e^{j2\pi i/M} \mid i = 0, 1,\ldots, M\text{-}1\}$, where $m = \log 2^M$. Finally, the sequence **x** is differentially encoded to a sequence **s** = $\{s_0, s_1, \ldots, s_{N_1/M}\}$ by the differential encoder, which outputs s_k given by $s_k = x_k s_{k-1}$, where $s_0 = 1$ known by the demodulator. In phase I, the sequence **x** is transmitted to the relay node and the destination node simultaneously.

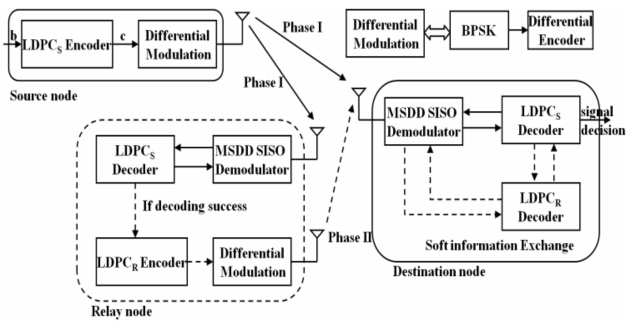

Figure 1. System model

At the relay node, the signals $\mathbf{y}_{sr}$ is received and decoded through the iterative decoding between the LDPC_s decoder and the MSDD_r SISOD demodulator. In every outer iterative decoding, the *a posteriori* information is computed at the MSDD_r SISO demodulator based on the received signals $\mathbf{y}_{sr}$ and the *a priori* information outputed from the LDPC_s decoder. Then the part of extrinsic information is outputed to the LDPC_s decoder as the *a priori* information. Based on this *a priori* information, the LDPC_s decoder performes a number of inner iterative decoding and makes a hard decision. If the decision is a valid LDPC codes, the iteration of the receiver is stopped. If not, similar to the MSDD SISO demodulator, the extrinsic information is outputed to the MSDD SISO demodulator for the following external iterative decoding.

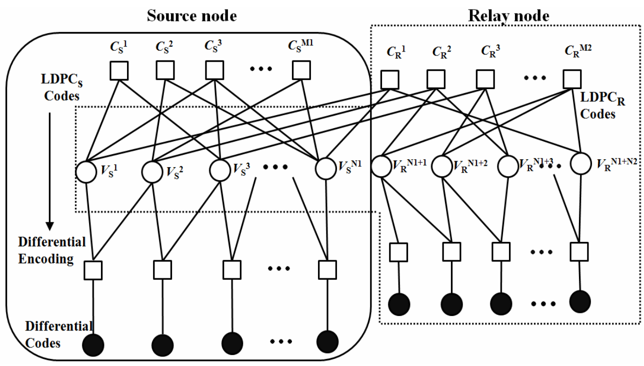

Figure 2. Tanner graph of the system model

This process is executed until the maximum number of the outer iteration is executed or the valid code is obtained. In order to avoid the error propagation and save the energy of the relay node, the decoded sequence is recoded by a rate N_1/N_2 LDPC_r encoder and transmitted to the destination node in phase II only if the success decoding is finally performed.

At the destination node, there are two kinds of decoding cases. The first case is only the transmitted signal of phase I is received. The received signal $\mathbf{y}_{sd}$ is decoded through the iterative decoding between the LDPC_s decoder and the MSDD_d SISO demodulator, and then the hard decesion is finally outputted. The second case is the transmitted signals of phase I and phase II are all received. If the success decoding of the received signal $\mathbf{y}_{sd}$ is performed, the hard decesion is finally output and stop the decoding. Otherwise, the received signals $\mathbf{y}_{rd}$ of phase II is demodulated by the MSDD_d SISO demodulator, and the outer iterative decoding is performed between the LDPC_s decoder and the LDPC_r decoder. Based on this outer iteration, the extrinsic information exchange between them is expected to obtain the higher coding gain.

2.2 MSDD SISO Demodulator

Consider the system communicating over a time-selective Rayleigh fading channel, and use N to represent the observation window size (OWS) of MSDD. In phase I, the received signal of the relay node and destination node can be written into the following vector form respectively:

$$\mathbf{y}_{sr} = \sqrt{E_s}\mathbf{H}_{sr}\mathbf{S}_r + \mathbf{n}_{sr}, \quad (1)$$

$$\mathbf{y}_{sd} = \sqrt{E_s}\mathbf{H}_{sd}\mathbf{S}_d + \mathbf{n}_{sd}. \quad (2)$$

In phase II, the received signal of the destination node can be expressed as

$$\mathbf{y}_{rd} = \sqrt{E_s}\mathbf{H}_{rd}\mathbf{S}_d + \mathbf{n}_{rd}, \quad (3)$$

where h_{sr}, h_{sd} and h_{rd} are independent complex-valued channel gains for the S-R, S-D and R-D links with mean 0 and variance σ_{sr}^2, σ_{sd}^2 and σ_{rd}^2, respectively; n_{sr}, n_{sd} and n_{rd} are independent zero mean complex Gaussian noise with variance N_0 at the relay node and destination node, respectively. In order to express concisely, the vectors omit the subscripts represent as

$$\mathbf{y} = [y_1, y_2, ..., y_N]^T,$$
$$\mathbf{H} = diag\{h_1, h_2, ..., h_N\},$$
$$\mathbf{S} = [s_1, s_2, ..., s_N]^T,$$
$$\mathbf{n} = [n_1, n_2, ..., n_N]^T,$$

and the superscript T denotes the transpose operation.

In the MSDD SISOD, the soft information of each code bit is computed and outputed to the LDPC decoder as the *a priori* probability. Different from the conventional differential detection (CDD) making a decision using only the two adjacent reception signals, MSDD SISOD evaluates the *a posteriori* probability (APP) of each coded bit by extending the length of the OWS to make a joint decision.

MSDD SISOD outputs the APP of each coded bit. The APP of the code bit c_i can be written as

$$L_{M,p}(c_i) = \log\frac{p(c_i = 0 \mid \mathbf{r})}{p(c_i = 1 \mid \mathbf{r})}. \quad (4)$$

The coded bits are asummed independent with each other, (4) can be written to (5) based on the principle of Bayesian theory [13-14].

$$\begin{aligned}
L_{M,p}(c_i) &= \ln\frac{p(c_i = 0 \mid \mathbf{y})}{p(c_i = 1 \mid \mathbf{y})} \\
&= \ln\frac{\sum_{\mathbf{s}:c_i=0} p(\mathbf{y} \mid \mathbf{c})p(\mathbf{c})}{\sum_{\mathbf{s}:c_i=1} p(\mathbf{y} \mid \mathbf{c})p(\mathbf{c})} \\
&= \ln\frac{\sum_{\mathbf{s}:c_i=0} p(\mathbf{y} \mid \mathbf{c})\prod_{j=1}^{N-1} p(c_j)}{\sum_{\mathbf{s}:c_i=1} p(\mathbf{y} \mid \mathbf{c})\prod_{j=1}^{N-1} p(c_j)} \\
&= \ln\frac{\sum_{\mathbf{s}:c_i=0} p(\mathbf{y} \mid \mathbf{s})\prod_{j=1}^{N-1} p(c_j)}{\sum_{\mathbf{s}:c_i=1} p(\mathbf{y} \mid \mathbf{s})\prod_{j=1}^{N-1} p(c_j)},
\end{aligned} \quad (5)$$

where the sums in the numerator and denominator are taken over all sequences $\mathbf{c}$ whose bit in position i is the value 0 or 1, respectively; $p(c_j)$ is the *a priori* probability of each code bit, which can be computed based on the extrinsic information outputted from the LDPC decoder; $p(\mathbf{y} \mid \mathbf{s})$ is the conditional probability density function (PDF) of non-coherently received signals $\mathbf{y}$ given transmitted signals $\mathbf{s}$ as

$$p(\mathbf{r} \mid \mathbf{s}) = \frac{\exp[-\frac{1}{2}\{\mathbf{y}^T\mathbf{R}^{-1}\mathbf{y}^*\}]}{(2\pi)^N \det\mathbf{R}}. \quad (6)$$

Submitting (6) into (5), we can get

$$L_{M,p}(c_i) = \ln\frac{\sum_{\mathbf{s}:c_i=0} \exp[-\frac{1}{2}\{\mathbf{y}^T\mathbf{R}^{-1}\mathbf{y}^*\}]\prod_{j=1}^{N-1} p(c_j)}{\sum_{\mathbf{s}:c_i=1} \exp[-\frac{1}{2}\{\mathbf{y}^T\mathbf{R}^{-1}\mathbf{y}^*\}]\prod_{j=1}^{N-1} p(c_j)}, \quad (7)$$

where $\mathbf{R}$ is the covariance matrix of $\mathbf{r}$, $R_{i,j}$ can be expressed as

$$R_{i,j} = \frac{1}{2}E\{(y_i - \overline{y_i})^*(y_j - \overline{y_j})^T\} = \frac{1}{2}y_i^* y_j E\{h_i^* h_j^T\} + \sigma_n^2\delta_{i,j}, \quad (8)$$

where if $i = j$, $\delta_{i,j} = 1$; otherwise $\delta_{i,j} = 0$; $\rho_{i,j}$ is the correlation coefficient of the fading process, which is given by

$$\rho_{i,j} \approx J_0(2\pi f_D T_s \mid i - j \mid). \quad (9)$$

where $f_D T_s$ is the normalized Doppler frequency, and $J_0(\bullet)$ is the zeroth order Bessel function of the first kind.

2.3 Soft output M-algorithm

It is known that the disadvantage of the MSDD SISOD is the prohibitively high complexity [14], which will result in an unacceptable energy comsuption for IOT so as to makes it difficult to be applied to a actual system. To solve this problem, M-algorithm is usually employed to reduce the complexity of the MSDD [14].

Since the problem of MSDD also can be viewed as a tree decoding problem, the hard output of MSDD actually is the path with the maximum likelyhood (ML) value of the metric. It was proved that it works well for reducing the computational complexity of MSDD in uncoded systems. As shown in Figure 3, the basic principle of the M-algorithm is that starting from the first node of the decoding tree, only M paths which correspond to the best M values of metrics are retained at each tree depth, and the rest paths are discarded. When the M-algorithm reaches the end of the decoding tree, the fist-ranked path in M paths is the most likely candidate. It should be noted that if M is equal to the number of all states of the transmmited signals, the M-algorithm is equivalent to the ML detection algorithm. From Table 1, it is shown that the complexity of MSDD can be greatly by the M-algorithm.

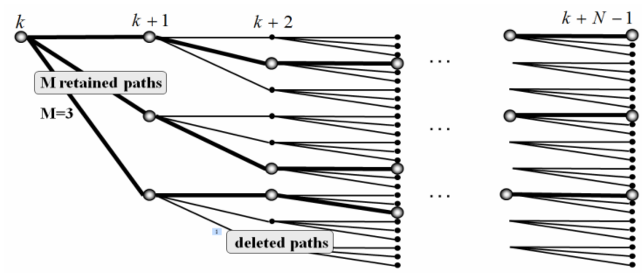

Figure 3. The principle of M-algorithm for MSDD

Table 1. Number of search paths of MSDD for 16PSK

N	4	5	6
Conventional method (Full path search)	4,096	65,536	1,048,576
M-algorithm(M = 16)	528	784	1040

However, if we directly use it for coded systems with MSDD SISOD, we found that finally retained M best paths may have same binary value in the same bit positions as shown in Figure 4. In this case, the value of the numerator or denominator of (5) does not exist. That is, it cannot ensure that the LLR of each code bit can be computed. Therefore, M-algorithm does not work well for reducing the computational complexity of MSDD SISOD.

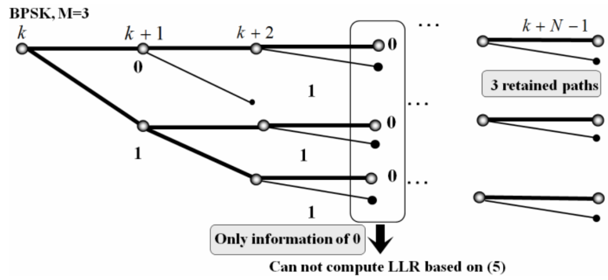

Figure 4. Problem of M-algorithm for MSDD SISOD

To resolve the problems of M-algorithm for MSDD SISOD, a soft-output M-algorithm (SOMA) is proposed. The basic principle of this approach is that the LLRs of code bits at each stage of the decoding tree are recursively computed based on not only the M retained paths but also the discarded paths, the flow chart of which is shown in Figure 5. This scheme can ensure that the LLR of each code bit can be computed, and provide highly reliable LLRs. The difference between M-algorithm and SOMA for MSDD SISOD is also shown in Figure 5.

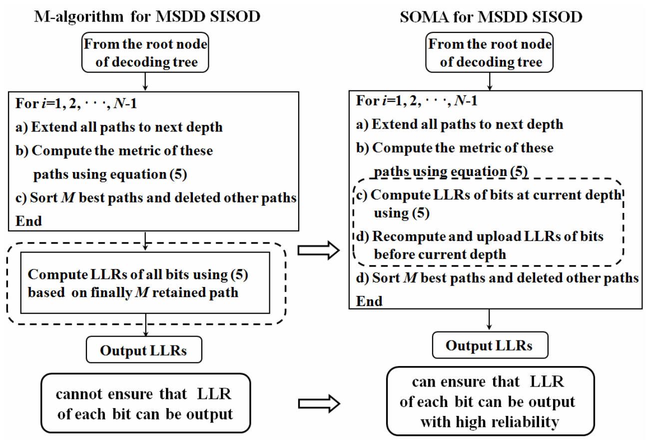

Figure 5. Flow charts of M-algorithm and SOMA for MSDD SISOD

3 Construction of Check Matrix of QC-LDPC Codes

3.1 Structural characteristics of Check Matrix of QC-LDPC Codes

The parity check matrix **H** of QC-LDPC codes consists of cyclic matrices called a cyclic permutation matrix, which can be represented by the formula (10)

$$\mathbf{H}=\begin{bmatrix}\mathbf{I}(P_{11}) & \mathbf{I}(P_{12}) & \dots & \mathbf{I}(P_{1n})\\ \mathbf{I}(P_{21}) & \mathbf{I}(P_{22}) & \dots & \mathbf{I}(P_{2n})\\ \vdots & \vdots & \ddots & \vdots\\ \mathbf{I}(P_{m1}) & \mathbf{I}(P_{m2}) & \dots & \mathbf{I}(P_{mn})\end{bmatrix} \quad (10)$$

where each element $\mathbf{I}(P_{ij})(1 \le i \le m,\ 1 \le j \le n)$ is a cyclic permutation matrix obtained by rightward shifting each row of the unit matrix $\mathbf{I}$ with $b \times b$ dimension, and $P_{ij} \in \{0,1,2,...,\infty\}$, especially, $\mathbf{I}(P_{ij})$ is a unit matrix when $P_{ij} = 0$, while $\mathbf{I}(P_{ij})$ is an all-zero square matrix when $P_{ij} = \infty$.

The cyclic permutation matrix $\mathbf{I}(P_{ij})$ in the check matrix $\mathbf{H}$ is replaced by the number of cyclic shifts P_{ij} to obtain a shift parameter matrix $\mathbf{P}$ with size of $m \times n$ dimension:

$$\mathbf{P} = \begin{bmatrix} P_{11} & P_{12} & \cdots & P_{1n} \\ P_{21} & P_{22} & \cdots & P_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ P_{m1} & P_{m2} & \cdots & P_{mn} \end{bmatrix} \quad \mathbf{(11)}$$

The elements ∞ in the shift parameter matrix $\mathbf{P}$ are replaced by zeros, and the $non-\infty$ elements are replaced by 1s to obtain a base matrix $\mathbf{A}$ of the same size of $m \times n$ dimension:

$$\mathbf{A} = \begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1} & A_{m2} & \cdots & A_{mn} \end{bmatrix}, \quad \mathbf{(12)}$$

where $A_{ij} \in \{0,1\}$, $1 \le i \le m, 1 \le j \le n.$

Thus, when the base matrix **A** and the cyclic shift parameter matrix **P** are determined, the element 1 in the base matrix **A** is substituted for the cyclic permutation matrix $\mathbf{I}(P_{ij})$, and the element 0 in the base matrix **A** is substituted for the all-zeros matrix. Then, the parity check matrix **H** of QC-LDPC codes can be obtained.

The performance of QC-LDPC codes and the complexity of the coding and decoding are related to the structure parameters such as column weight, row weight, girth and minimum code distance of the check matrix. To ensure the low density characteristic of the check matrix, the column weight and row weight of the regular codes are fixed and its values are much smaller than the code length. The girth is the minimum length of the loop connected at the end of the binary graph corresponding to the check matrix. It is requires that the girths with a length of 4 need to be avoided when constructing the check matrix. The minimum code distance is the minimum weight of the codeword that satisfies the constraint relations of the check matrix. The parity check matrix is constructed to ensure that the minimum code distance is large enough. The base matrix **A** and the parity check matrix **H** of the QC-LDPC codes have the following properties:

Property 1 [15]: The parity check matrix $\mathbf{H}$ of QC-LDPC codes has the same degree distribution as the base matrix $\mathbf{A}$.

Property 2 [15]: The minimum code distance of the parity check matrix **H** of QC-LDPC codes is not smaller than the minimum code distance of the base matrix $\mathbf{A}$.

Property 3 [16]: The necessary and sufficient condition of the parity check matrix **H** of QC-LDPC codes owning the loop with the length of at least 2(*l*+1) is

$$\sum_{k=1}^{2l} (-1)^{k+1} p_{ik,jk} \neq 0 \mod b \quad \mathbf{(13)}$$

where $p_{ik,jk}$ is the number of cyclic permutation matrices corresponding to the *k*th vertex in the loop of the base matrix $\mathbf{A}$, and b is the side length of the cyclic permutation matrix.

Property 3 shows that when the base matrix **A** is expanded, the short cycles originally existing in the base matrix **A** can be eliminated in the parity check matrix **H** of QC-LDPC coeds by selecting the shift value P_{ij} of the cyclic permutation matrix. In particular, if the girth of base matrix **A** is 6, the necessary and sufficient condition for parity check matrix **H** of QC-LDPC codes does not contain cycles of length 6 (i.e., their girths are at least 8) is [17]:

$$p_{i_1,j_1} - p_{i_2,j_2} + p_{i_3,j_3} - p_{i_4,j_4} + p_{i_5,j_5} - p_{i_6,j_6} \neq 0 \ mod\, b \quad \mathbf{(14)}$$

3.2 Shortening RS Codes with Two Information Symbols

Let α be a primitive element on Galois field GF(*q*), where *q* be an arbitrary power of a prime number, and $\{0,\alpha^0,\alpha^1,\alpha^2,...,\alpha^{q-2}\}$ be all elements on GF(*q*). If a positive integer ρ satisfies a<b, the code length is *q*-1, the number of information bits is $q+1-\rho$, and the number of parity bits is $\rho-2$. The generator polynomial of the $(q-1,q-\rho+1,\rho-1)$ RS code whose minimum code distance is $\rho-1$ can be written as

$$\begin{aligned} g(x) &= (x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{\rho-2}) \\ &= g_0 + g_1 x + g_2 x + \cdots + g_{\rho-2} x^{\rho-2} \end{aligned} \quad \mathbf{(15)}$$

where $g_i \in GF(q)$, $g_i \neq 0$, $g_{\rho-2} = 1$. The generator matrix of the $(q-1,q-\rho+1,\rho-1)$ RS code obtained from (15) can be represented by (16). The RS code denoted by **C** can be obtained by the information symbols using this generation matrix.

$$\mathbf{G}=\begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{\rho-2} & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & g_{\rho-2} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & g_0 & g_1 & g_2 & \cdots & g_{\rho-2} \end{bmatrix} \quad \textbf{(16)}$$

The shortening RS codes having two information symbols, which is denoted by $\mathbf{C}_b$, is obtained by deleting the first $q-\rho-1$ information symbols of each codeword of the code **C**. Its generator matrix is given by (16) as follows

$$\mathbf{G}_b=\begin{bmatrix} g_0 & g_1 & g_2 & \cdots & 1 & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & 1 \end{bmatrix} \quad \textbf{(17)}$$

If the two information bits are m_0m_1, the shortening RS codes $\mathbf{C}_b=[m_0m_1]$, $\mathbf{G}_b=\left[c_0c_1\cdots c_{\rho-1}\right]$, where m_0、$m_1\in GF(q)$.

3.2 Characteristics of Shortening RS Codes with Two Information Symbols

(1) The code length of $\mathbf{C}_b$ is ρ , the number of information bits is 2, the minimum code distance is $\rho-1$, and the number of codewords in the $\mathbf{C}_b$ set is q^2, and any two codewords have at most one same code symbol.

(2) A codeword **V** with weight ρ is arbitrarily selected from $\mathbf{C}_b$, then the set $\mathbf{C}_b^{(1)}=\{c\boldsymbol{V}:c\in GF(q)\}$ is constructed to obtain a one-dimensional codeword set of $\mathbf{C}_b$ which contains q codewords. Any two codewords in $\mathbf{C}_b^{(1)}$ are different at each location, and the code weight of each non-zero codeword is ρ.

(3) We choose a codeword $\mathbf{C}_1$ with weight $\rho-1$ from $\mathbf{C}_b$, and use the formula (18) to divide the $\mathbf{C}_b$ into cosets to get the q cosets of $\mathbf{C}_b:\mathbf{C}_b{}^{(1)},\mathbf{C}_b{}^{(2)},\mathbf{C}_b{}^{(3)},...,\mathbf{C}_b{}^{(q)}$. The two codewords in any one coset $\mathbf{C}_b^{(i)}$ are different in all ρ positions, and at least $\rho-1$ positions of the two codewords in two different cosets $\mathbf{C}_b^{(i)}$ and $\mathbf{C}_b^{(j)}$ are different.

$$\mathbf{C}_b^{(i)}=\{\alpha^{i-2}\mathbf{C}_1+c\,\big|\,c\in\mathbf{C}_b^{(1)}\},\ \ i=2,...,q \quad \textbf{(18)}$$

3.3 Proposed method for Constructing Base Matrix Based on Shortening RS Codes

The construction rules for constructing the base matrix based on shortening RS codes are as follows:

(1) each line contains ρ ones, that is the row weight is ρ;

(2) each column contains γ ones, that is the column weight is γ;

(3) the number of ones at the same position between any two rows (columns) is not more than 1, to ensure that there is free of cycles of length 4 in the check matrix;

(4) ρ and γ are smaller compared with the code length and the row length of the parity check matrix, so that the constructed parity check matrix exhibits a characteristic of low density.

Usually the above four conditions are called the row and column constraint conditions of LDPC codes. The LDPC codes constructed according to the constraint conditions are regular LDPC codes. The check matrix has fixed row weight ρ and column weight γ . According to the above construction rules, the proposed method of constructing base matrix by using shortening RS codes with two information symbols is as follows:

(1) Determine matrix parameters. If the code length of regular LDPC codes constructed by the base matrix is n and the number of information bits is k, then the number of rows of the base matrix is n-k, and the number of columns is n.

(2) Determine the RS code $\boldsymbol{C}$ on GF(q). For the RS code with length q-1 and $q=2^m$ with an m-th order primitive polynomial $p(x)$, the generation polynomial and the generation matrix of the RS code $\boldsymbol{C}$ are obtained as (15) and (16), respectively. Let the primitive element of the RS code be α , the q-dimensional vector $\mathbf{Z}(\alpha^i)=(0,0,...,0,1,0,0,...,0)$ of GF(2) is defined as the position vector of the element α^i, where the ith component of α^i is 1 and all other components are 0.

(3) Determine the shortening RS codes $(\rho,2,\rho-1)$ $\mathbf{C}_b$ on GF(q). The generation matrix $\mathbf{G}_b$ of $\mathbf{C}_b$ as shown in formula (17). Each symbol of $\mathbf{C}_b$ can be obtained by the generation matrix $\mathbf{G}_b$.

(4) Divide cosets for $\mathbf{C}_b$. Choose a code $\mathbf{C}_1$ with weight $\rho-1$ from $\mathbf{C}_b$, and divide coset for $\mathbf{C}_b$ using formula (9), we can get q cosets of $\mathbf{C}_b:\mathbf{C}_b{}^{(1)},\mathbf{C}_b{}^{(2)},\mathbf{C}_b{}^{(3)},...,\mathbf{C}_b{}^{(q)}$.

(5) Each q codewords in each coset is arranged in a $q\times\rho$ matrix $\mathbf{M}_i(1\le i\le q)$, and all q elements in any column of $\mathbf{M}_i$ are different.

(6) Substituting each element in the matrix $\mathbf{M}_i$ with the corresponding position vector, the $q\times\rho$ matrix $\mathbf{M}_i$ is expanded to a $q\times\rho q$ matrix $\mathbf{H}_i$, which haves a fixed row weight and a column weight of one. No two rows have a common 1 component in the same matrix $\mathbf{H}_i$, and no two rows contain more than a common 1 component between the two different matrices $\mathbf{H}_i$ and $\mathbf{H}_j$.

(7) The following matrix is constructed on GF(2) by choosing $\mathbf{H}_i$ with number of γ, where $1\le\gamma\le q$,

$$H_{GA}(\gamma)=\begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_\gamma \end{bmatrix} \quad \textbf{(19)}$$

$\mathbf{H}_{GA}(\gamma)$ has the following characteristics: it is a $\gamma q\times\rho q$ array on GF(2); it has fixed column weight γ and row weight ρ; no two rows (or two columns) contain more than one common 1 component; density is $1/q$, and when q is large, $\mathbf{H}_{GA}(\gamma)$ is a low-density matrix. It can be seen that the $\mathbf{H}_{GA}(\gamma)$ satisfies the constraint condition of the parity check matrix of LDPC codes. Therefore, it can be used as parity check matrices of regular LDPC codes of Gallager type, where code length is $n=\rho q$, column weight is γ, and row weight is ρ.

3.4 Construction of Parity Check Matrix of QC-LDPC Codes Based on Shortening RS Codes

For constructing parity check matrix of QC-LDPC codes based on shortening RS codes, the base matrix $\mathbf{A}$ free of cycles of length 4 is first constructed by shortening RS codes. Then, the base matrix is optimized and expanded by the cyclic permutation matrix $\mathbf{I}(P_{ij})$ to obtain the parity check matrix $\mathbf{H}$ of QC-LDPC codes. Here, the optimal expansion means that the shift values of the cyclic shift matrix $\mathbf{I}(P_{ij})$ is selected to satisfy the condition of formula (13), so that the resulting of the parity check matrix $\mathbf{H}$ of QC-LDPC codes does not exist cycles of length 6. The specified construction steps are as follows.

(1) Determine the parameters of the parity check matrix of regular LDPC codes. The number of rows and columns of the parity check matrix and the row weight and the column weight are determined according to the code length and the number of information bits stipulated in the design requirement of regular LDPC codes.

(2) Construct the base matrix $\mathbf{A}$ with girth 6 using the algorithm in Section 3.3.

(3) From the position of the element "1" in the base matrix $\mathbf{A}$, the value of the number of cyclic shifts is calculated in accordance with the expression (20).

$$P_{ij}=\begin{cases} i(w-1) \mod b; & A_{ij}=1 \\ \infty ; & A_{ij}=0 \end{cases} \quad \textbf{(20)}$$

where A_{ij} is the element in the base matrix $\mathbf{A}$, and P_{ij} is the number of right shifts; i represents the row number in the base matrix A_{ij}, and w represents the serial number of A_{ij} appearing in each row in the base matrix $\mathbf{A}$.

(4) Determine whether the value of the P_{ij} of the vertex element "1" of the cycles of length 6 in the base matrix $\mathbf{A}$ satisfies formula (14), and if it does not satisfy this condition, amend it until the condition is satisfied.

(5) Expand the base matrix $\mathbf{A}$. The elements "1" of the base matrix $\mathbf{A}$ is replaced by a cyclic permutation matrix $\mathbf{I}(P_{ij})$ with the dimension $b\times b$ obtained by right shifting unit square matrix P_{ij} (correction value) times. Finally, the elements ∞ in the matrix $\mathbf{A}$ are replaced by all zeros unit matrix with dimension $b\times b$.

(6) Repeat step (5) until all "1" elements of the cycles of length 6 are replaced.

Thus, the parity check matrix $\mathbf{H}$ of quasi-cyclic regular LDPC codes is constructed with dimension $mb\times nb$ and code rate $R=(nb-mb)/nb$.

4 Simulation Results and Analysis

In the simulations, the regular LDPC code used in the consisdered systems is (3, 6) LDPC codes with length N_s = 504 and N_r = 1008, respectively. It is assumed that the channels in the cooperative communication system are independent with each other and are flat Rayleigh slow fading channels. The modle of Rayleigh fading channel is Jake's model and $f_D T_s$ is set to 0.001 for slow fading channels. For ease of analysis, we assume that the cooperative is the ideal cooperative, that is the relay node correctly decoding the codeword sent by the source node.

Since the attenuation of the signal is related to the propagation distance, the distance from the relay node to the destination node is shorter than the distance from the source node to the destination node. In the simulations, assuming that the received signal-to-noise ratio (SNR) of the signal sent by the relay node to the destination node is higher 1 dB than the received SNR of the source node transmitting signal to the destination node.

In order to compare the performance of coding cooperative system and non-cooperative coding system under the same conditions, the LDPC codes of the non-cooperative system is (3, 6) LDPC codes with length 1008.

4.1 Effect of the System Parametes on BER Performance for the Considered Systems

Figure 6 shows the BER performance of the considered systems with different inner iteration number of LDPC decoder. The outer iteration number between LDPC decoder and MSDD SISOD is set to 8, and the OWS of MSDD SISOD is set to 4. It is shown that the BER performance can be improved with the increase of the inner iteration. And we note that the improvement of BER performance is not significant when the inner iteration number is bigger than 4.

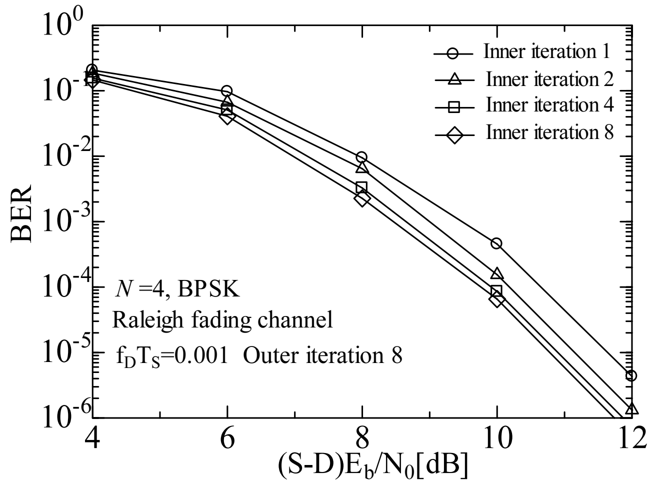

Figure 6. BER performance comparison of different inner iteration number of LDPC decoder with OWS N =4

Then we set the number of the inner iteration as 4 to test the effect of the outer iteration on BER performance. From Figure 7, we can observe that the performance is improved with the increase of the outer iteration number but not significantly when the iteration number is bigger than 2. After testing the impact of the iterative decoding on BER performance, the impact of the OWS of the MSDD SISOD on BER performance is shown in Figure 8. It can be observed that the performance is effectively improved with the increase of the OWS but not significantly when the OWS is bigger than 4.

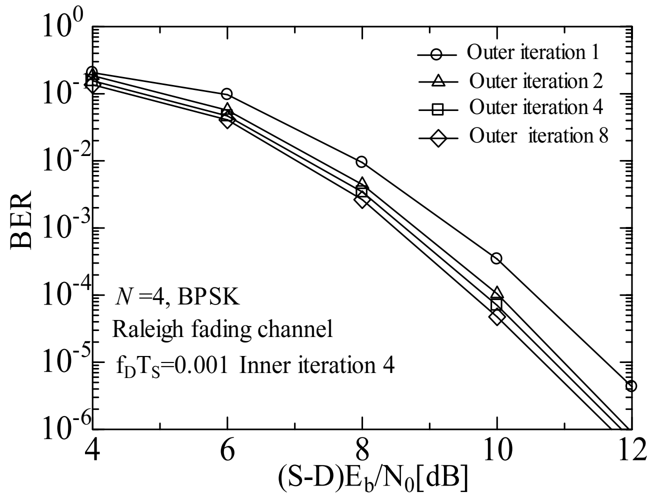

Figure 7. BER performance comparison of different outer iteration number of outer iteration with OWS N = 4

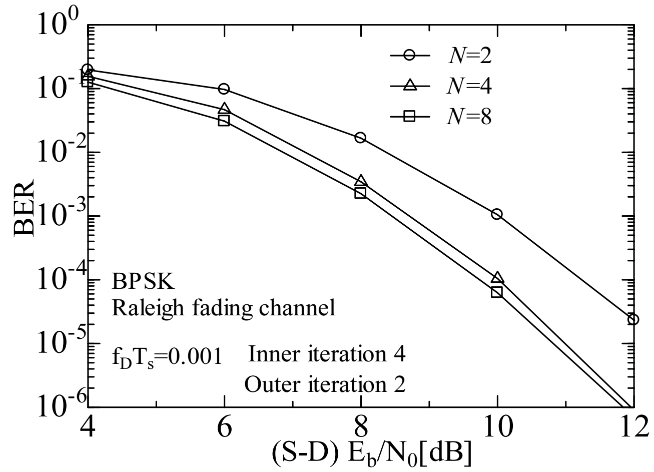

Figure 8. BER performance comparison of MSDD SISOD with different OWS

Figure 9 shows the performance of the systems under consideration using the proposed SOMA for reducing the decoding complexity. We can observe that when $M = 4$, the performance of the SOMA can be very close to the performance achieved by the MAP algorithm.

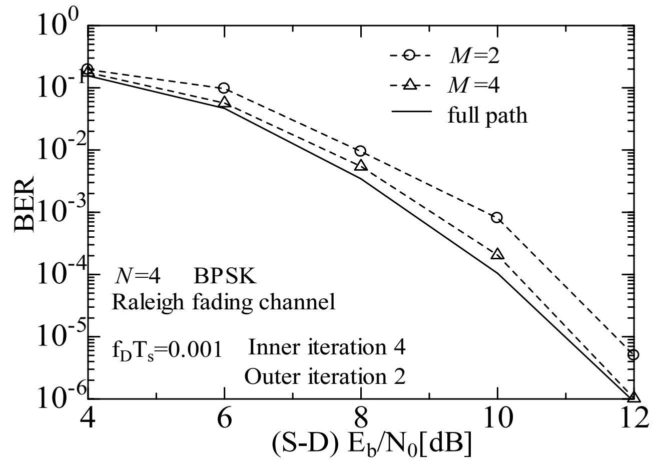

Figure 9. BER performance of the proposed SOMA non-cooperative system

In order to achieve our proposed system for the IOT, it is important to choose the appropriate parameters to reduce system complexity and energy consumption. Based on the above simulations and analysis, we can set the inner iteration mumber, outer iteration number, the OWS of the MSDD SISOD are 4, 2 and 4 for the following simulation, respectively. And SOMA is used in the MSDD SISOD with M =4.

4.2 Evaluation of the Designed QC-LDPC codes for the Considered Systems

In Figure 10, the BER performance of LDPC codes constructed by the proposed algorithm is shown by the curve labeled QC-LDPC. At the same time, the performance of the system using Mackay LDPC with the same parameters and the performance of differential LDPC coded non-cooperative systems are also given in Figure 10, respectively. As can be seen from Figure 10, the regular LDPC code constructed by the proposed algorithm has almost the same error correction performance as the Mackay LDPC codes. Considering the implementation complexity, the performance of the proposed method is better than that of the construction method of the Mackay LDPC codes when long LDPC codes are constructed.

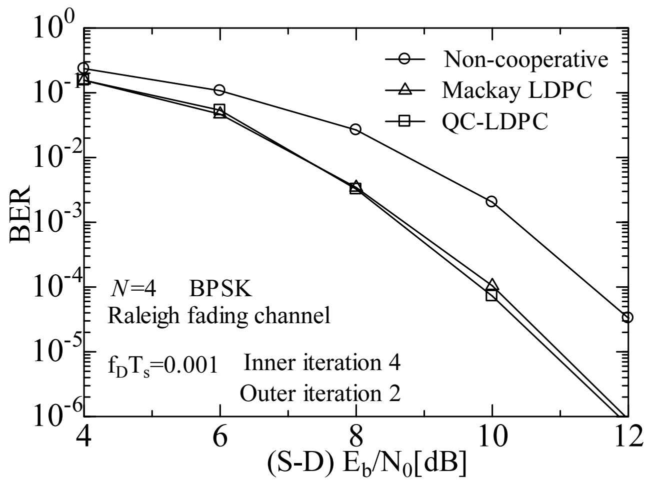

Figure10. BER performance comparison of the systems under consideration with designed QC-LDPC codes and non-cooperative system

In order to verify whether the QC-LDPC codes constructed by the proposed algorithm can effectively improve energy efficiency of the systems under consideration, we test and analyze the energy efficiency following the reference [18]. In order to prove the validity of the QC-LDPC code, the energy efficiencies of the systems without ECC and with BCH codes are also tested, where the parameters of BCH codes with rate 0.43 and length 1023 are same as that of [19]. Figure 11 compares the energy efficiency under the condition of the three cases for different raw bit error rate. As shown in Figure 11, the energy efficiency of the systems using QC-LDPC codes is much better than that of the systems without ECC, and also has higher energy efficiency than that of the systems with BCH codes. It is means that the power consumption can be reduced effectively using the constructed QC-LDPC codes.

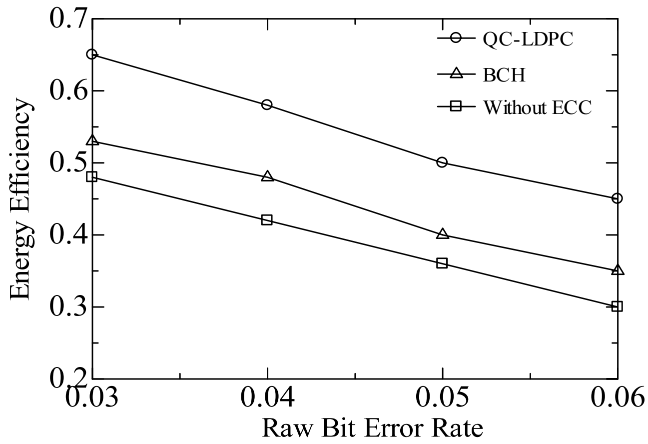

Figure 11. Energy efficiency comparison of QC-LDPC codes, BCH codes and uncoded for the systems under consideration

5 Conclusion

The differential LDPC coded cooperative communication systems scheme for the IoT is studied in this paper. The diffierential LDPC coded cooperative communication scheme based on MSDD is first proposed, and the multi-level tanner graph of the differential cascaded LDPC coded cooperative scheme is then analyzed. The SOMA is proposed for significantly reducing the complexity of the MSDD SISOD based on the analysis of the problem for the M-algorithm used in the systems under consideration. In order to further make the LDPC codes suit for the hareware implemention of the IoT, we propose the new method to construct parity check matrix of QC-LDPC codes based on shortening RS codes. Finally, it is demonstrated that the performance of the system can be effectively improved by the proposed scheme with low complexity and good energy efficiency for the IoT.

Acknowledgements

This work is supported in part by the Natural Science Foundation of Jiangsu Province (Grant No. BK20160294), Changzhou Sci&Tech Program (Grant No. CJ20140058), National Natural Science Foundation of China (Grant No. 61701202) and National Natural Science Foundation of China (Grant No. 61601208).

References

[1] C. Abou-Rjeily, Distributed Space-Time Codes for Full-Duplex IR-UWB Amplify-and-Forward Cooperation, *IEEE Transactions on Wireless Communications*, Vol. 14, No. 4, pp. 2144-2155, April, 2015.

[2] B. Zhang, J. Hu, Y. Huang, M.El-Hajjar, L. Hanzo, Outage Analysis of Superposition Modulation Aided Network Coded

Cooperation in the Presence of Network Coding, *IEEE Transactions on Vehicular Technology*, Vol. 64, No. 2, pp. 493-501, February, 2015.

[3] M. R. Avendi, Ha H. Nguyen, Performance of Differential Amplify-and-Forward Relaying in Multinode Wireless Communications, *IEEE Transactions on Vehicular Technology*, Vol. 62, No. 8, pp. 3603-3613, October, 2013.

[4] Y. Gao, J. Ge, W. Cong, Differential Quadrature Amplitude Modulation and Relay Selection with Detect-and-Forward Cooperative Relaying, *Wireless Personal Communications*, Vol. 72, No. 2, pp. 1399-1414, September, 2013.

[5] M. J. Qian, Y. L. Jin, Z. Wu, Distributed Differential Space-time Coding for Asynchronous Two-Way Relaying Networks with Nakagami-*m* Fading, *Journal of China Universities of Posts Telecommunications*, Vol. 21, No. 6, pp. 17-23, December, 2014.

[6] H. Sun, L. Bi, X. Lu, Y. Guo, N. Xiong, Wi-Fi Network-Based Fingerprinting Algorithm for Localization in Coal Mine Tunnel, *Journal of Internet Technology*, Vol. 18, No. 4, pp. 731-741, July, 2017.

[7] J. Gan, N. Xiong, H. Wen, Q. Zhu, Analysis of SCTP Concurrent Multipath Transfer in Vehicular Network Communication, *Journal of Internet Technology*, Vol. 16, No. 3, pp. 495-504, May, 2015.

[8] B. K. Butler, P. H. Siegel, Error Floor Approximation for LDPC Codes in the AWGN Channel, *IEEE Transactions on Information Theory*, Vol. 60, No. 12, pp. 7416-7441, December, 2014.

[9] Y. Yu, S. Handa, F. Sasamori, O. Takyu, Adaptive Iterative Decoding of Finite-Length Differentially Encoded LDPC Coded Systems with Multiple-Symbol Differential Detection, *IEICE Transactions on Communications*, Vol. 96, No. 3, pp. 847-858, March, 2013.

[10] Y. Yu, Z. Jia, W. Tao, B. Xue, Optimization Design of Differentially Encoded LDPC Coded Systems for Internet of Things, *Journal of Internet Technology*, Vol. 17, No. 7, pp. 1431-1441, December, 2016.

[11] E. Mo, M. A. Armand, Pseudocodeword Weights for LDPC Codes under Differential PSK Transmission over the Noncoherent AWGN Channel, *IEEE Transactions on Communications*, Vol. 59, No. 5, pp. 1218-1223, May, 2011.

[12] M. Gholami, M. Alinia, High-Performance Binary and Non-binary Low-Density Parity-Check Codes Based on Affine Permutation Matrices, *IET Communications*, Vol. 9, No. 17, pp. 2114-2123, November, 2015.

[13] J. Li, Differentially Encoded LDPC Codes-Part II: General Case and Code Optimization, *EURASIP Journal on Wireless Communications and Networking*, Vol. 2008, March, 2008, doi: 10.1155/2008/367287.

[14] S. Handa, Y. Okano, M. Y. Liu, F.Sasamori, S. Oshita, Fast Calculation Algorithm and Error Performance of Multiple-Symbol Differential Detection over Fading Channels, *IEICE Transactions on Communications*, Vol. E86-B, No. 3, pp. 1050-1056, March, 2003.

[15] W. Guan, H. G. Xiang, Construction of QC-LDPC Codes with Large Minimum Distances and Large Girths, *Journal of Circuits & Systems*, Vol. 16, No. 4, pp. 1-5, August, 2011.

[16] M. P. C. Fossorier, Quasicyclic Low-Density Parity-Check Codes from Circulant Permutation Matrices, *IEEE Transactions on Information Theory*, Vol. 50, No. 8, pp. 1788-1793, August, 2004.

[17] H. Matsui, On Generator and Parity-Check Polynomial Matrices of Generalized Quasi-Cyclic Codes, *Finite Fields and Their Applications*, Vol. 34, No. 7, pp. 280-304, July, 2015.

[18] K. Liu, Q. Huang, S. Lin, K. Abdel-Ghaffar, Quasi-cyclic LDPC Codes: Construction and Rank Analysis of Their Parity-check Matrices, *2012 Information Theory and Applications Workshop*, San Diego, CA, 2012, pp. 227-233.

[19] A. Brokalakis, I. Papaefstathiou, Using Hardware-based Forward Error Correction to Reduce the Overall Energy Consumption of WSNs, *2012 IEEE Wireless Communications and Networking Conference*, Shanghai, China, 2012, pp. 2191-2196.

Biographies

Yang Yu received the Dr. Eng degree from Shinshu University, Japan in 2013. Since 2013, he is an assistant professor in the School of Electric Information Engineering, Jiangsu University of Technology, China. His current research interests include sensor networks, coding and modulation for mobile communication systems.

Zhi-wen Qian was born in 1965. She received the B.S. degree from Southeast University in 1987. She is currently an assistant professor in the School of Electric Information Engineering, Jiangsu University of Technology, China. Her research interests include coding and modulation for communication systems.

Lei Zhang was born in 1986. He received the Ph.D. degree from Southeast University in 2016. Now he is a lecturer of School of Electrical and Information Engineering, Jiangsu University of Technology. His research interests include spectrum access and handoff in cognitive radio networks. He is a member of IEEE.

Bo Xue received the B.S. degree in electronic information engineering and the M.S. degree in signal and information processing from Yangzhou University, Yangzhou, China, in 2003 and 2006, respectively.

He is currently a Ph.D. candidate at Nanjing University of Posts and Telecommunications, Nanjing, China. His research interests focus on wireless sensor networks and compressed sensing.

Zhu-yang Chen received the Ph.D. degree from Xidian University, China in 2015. Now he is a lecturer in the School of Electric & Information Engineering, Jiangsu University of Technology, China. His current research interests include computational electromagnetic, light propagation and scattering.