Jointly Optimized Design of Distributed Goppa Codes and Decoding

FangAn FENG, FengFan YANG, Chen CHEN, ChunLi ZHAO

College of Electronics and Information Engg., Nanjing Univ. of Aeronautics and Astronautics, Nanjing, 210016 China

820363384@qq.com, yang_fengfan@vip.sina.com, chen_chen0518@163.com, 1562178154@qq.com

Submitted August 11, 2022 / Accepted November 1, 2022 / Online first December 16, 2022

Abstract. *In order to improve the adverse influence of fading channel in communication system, a distributed Goppa coding scheme is proposed in this paper. Two Goppa codes are set at the source node and the relay node in this scheme respectively. An optimal design criterion at the relay is proposed to obtain the optimal joint resultant code at the destination. Furthermore, two novel joint decoding algorithms are proposed to enhance the overall BER performance of the proposed scheme. Monte Carlo simulations show that the proposed distributed Goppa coding scheme outperforms the non-cooperative scheme. Moreover, the proper information selection approach at the relay performs better than random selection in the proposed distributed Goppa coding scheme.*

Keywords

Goppa codes, distributed coding schemes, joint decoding algorithms

1. Introduction

In the wireless communication system, signal fading occurs that is a significant element influence the performance of the communications system. When transmitting a signal through a fading channel, the strength of the received signal will also change due to the change of fading. When the channel is in deep fading, the signal received by the receiver is very weak, which will lead to reception error. In order to achieve the identical transmission performance as non-fading channel, greater signal transmission power is required in fading channel. Diversity technology is an effective means to improve the system performance in fading channel [1]. Its core idea is that the receiver can get the signal carrying the same information and transmitted through multiple independent channels. Common technologies include polarization diversity, frequency diversity, spatial diversity and time diversity.

Spatial diversity is an effective means of combating wireless channel fading. Multiple-input multiple-output (MIMO) system can obtain high-order diversity gain and effectively reduce the transmission bit error rate; or reduce the transmission power while keeping the bit error rate unchanged, or improve the system capacity [2]. However, in wireless communication systems such as cellular mobile communication and wireless sensor networks, it is difficult to implement multi-antenna technology due to the limitations of volume, weight, power consumption and cost. Even if multiple antennas are implemented on the terminal equipment, significant diversity gain cannot be obtained because the distance between antennas is not far enough. In this way, the physical multi antenna can only be realized on the base station. The core idea of cooperative diversity is to achieve virtual multiple antennas by cooperating among end users with only a single antenna and sharing their antennas with each other in some way, so as to obtain diversity gain and improve system performance.

The idea of cooperative diversity can be traced back to the relay channel studied by Cover and Gamal [3]. A relay channel is formed by a source node, destination node and a relay node. The source node transmits signals, which are subsequently processed and transmitted by the relay. Ultimately, the destination node receives signals from both the source node and the relay node, so it can receive multiple copies of the signal from the source node, enabling transmission diversity. In the relay channel, the relay node only forwards the signal from the transmitting node and does not transmit the signal itself. Cover and Gamal analyzed the capacity of the relay channel and concluded that the capacity of the whole relay channel is better than that between the source node and the destination node in most cases. Different cooperative relay information forwarding protocols have been presented, such as amplify-and-forward [4], compress-and-forward [5] and decode-and-forward [6]. Combining these protocols with channel coding builds a more effective mode of cooperation, which is known as coded-cooperative. Low density parity check (LDPC) codes [7], turbo codes [8], polar codes [9] and Reed-Muller (RM) codes [10] are applied to coded-cooperative schemes in the existing literature [11–15].

Recently, with the rapid development of Internet of Things technology, communication between devices and between machines has been widely used. For those types of wireless communication, most of them use short or medi-

DOI: 10.13164/re.2023.0023

um length information sequences for transmission. Umar et al. [10] used RM codes in the coded-cooperative scheme. Mughal et al. [16] applied polar codes in the code-cooperative scheme. However, in the existing literature, the coding cooperation scheme of Goppa code has not been studied so far. Goppa code construction is more powerful, as it is sure that there exist some Goppa code which meet the Gilbert-Varshamov bound [17]. Goppa code is a simple manifestation of the highly developed theory of algebraic-geometric duality between rational functions and differentials on an algebraic curves over finite fields. Goppa code [18], as a subcode of Generalized Reed-Solomon (GRS) code, is similar to Bose-Chaudhuri-Hocquenghem (BCH) code as a subcode of Reed-Solomon (RS) code. It is very similar to BCH code in encoding and decoding [19], [20]. However, the difference is that Goppa code is very flexible in construction, and the code length is not limited like BCH and RS code. We propose a distributed Goppa coding scheme where Goppa codes are adopted at source and relay nodes, which together construct a new code at the destination. The relay decodes and forwards the information received from the source node. Different information selection at relay results in the code structure of joint code. Hence, two different information selection approaches are proposed to optimize the resultant code at the destination.

The rest of this paper is organized structurally as follows. Section 2 details the sing relay cooperative communication system model and design of distributed Goppa coding scheme after a brief preliminary on Goppa codes. Two information selection methods at relay are described in Sec. 3. Section 4 describes two joint decoding algorithms. Section 5 presents simulation results of the distributed Goppa coding scheme. Finally, Section 6 concludes the paper.

2. Design of Distributed Goppa Code

2.1 Single Relay Cooperative Communication System Model

A model of single relay cooperative communication system model is shown in Fig. 1. Single relay communication system generally consists of three nodes: source node S, relay node R and destination node D. Relay transmission mode adopts half-duplex transmission mode. All nodes use a single antenna to transmit and receive signals.

In the first time slot, the source node S sends the signal $\mathbf{x}_S$ to the relay node R and the destination node D. This stage can be regarded as the broadcast stage. The relay node receives the signal $\mathbf{y}_{SR}$ and the destination node receives the signal $\mathbf{y}_{SD}$:

$$\begin{aligned} \mathbf{y}_{SR} &= \mathbf{h}^1_{SR}\mathbf{x}_S + \mathbf{n}^1_{SR}, \\ \mathbf{y}_{SD} &= \mathbf{h}^1_{SD}\mathbf{x}_S + \mathbf{n}^1_{SD} \end{aligned} \tag{1}$$

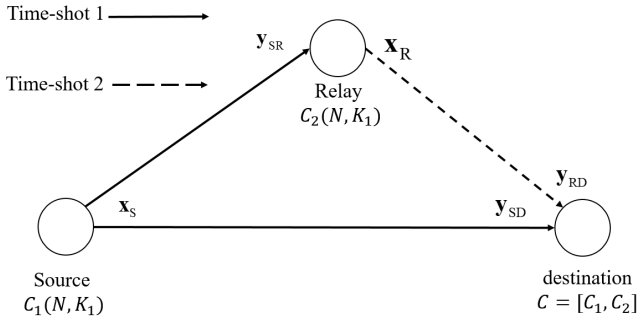

Fig. 1. Single relay cooperative communication system model.

where $\mathbf{n}^1_{SR}$ is the additive white Gaussian noise in the channel, a complex Gaussian variable with zero-mean and $\sigma^2/2$ variance per dimension in the channel from the source node to the relay node, where σ^2 is the power spectral density (PSD) of noise. The $\mathbf{h}^1_{SR}$ is channel fading coefficient from the source node to the relay node, a complex Gaussian variable with zero-mean and 0.5-variance per dimension [1], [21]. The $\mathbf{n}^1_{SD}$ and $\mathbf{h}^1_{SD}$ are defined similar to $\mathbf{n}^1_{SR}$ and $\mathbf{h}^1_{SR}$, and the subscript means the channel of transmission.

In the second time slot, the relay node R sends the signal $\mathbf{x}_R$ which is recoded signals from the correct decoding of the signal $\mathbf{y}_{SR}$ received from the source node. The signal $\mathbf{y}_{SD}$ is received in the destination node:

$$\mathbf{y}_{RD} = \mathbf{h}^2_{RD}\mathbf{x}_R + \mathbf{n}^2_{RD} \tag{2}$$

where $\mathbf{h}^2_{RD}$ and $\mathbf{n}^2_{RD}$ are defined similar to $\mathbf{h}^1_{SR}$ and $\mathbf{n}^1_{SR}$ in (1). The destination node concatenates the received information sent from the source node and the relay node into a joint code. Assume $\mathbf{y}_{SR} = [y^1_0, y^1_1, \ldots, y^1_{n-1}]$ and $\mathbf{y}_{RD} = [y^2_0, y^2_1, \ldots, y^2_{n-1}]$, then the joint code $\boldsymbol{y}$.

$$\mathbf{y} = \left[\mathbf{y}_{SR}, \mathbf{y}_{RD}\right] = \left[y^1_0, y^1_1, ..., y^1_{n-1}, y^2_0, y^2_1, ..., y^2_{n-1}\right]. \tag{3}$$

Then demodulate the joint signal $\mathbf{y}$ and perform joint decoding. In this manuscript, the Goppa code is applied to this communication system model.

2.2 Goppa Code

Let $L = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ be a subset of n distinct elements in $\Omega = GF(q^m)$ (q is prime or prime power, m is a positive integer) and $g(z) \in \Omega[z]$ ($\deg g(z) = r$, $0 \le r \le n$) be a monic polynomial of degree such that $g(\alpha_i) \neq 0$ for all $\alpha_i \in L$. Then the Goppa code $\Gamma(L, g(z))$ is a set of all codewords $\mathbf{c} = \{c_0, c_1, \ldots, c_{n-1}\} \in F^n$ ($F = GF(q)$) such that:

$$\sum\nolimits_{i=0}^{n-1} \frac{c_i}{z - \alpha_i} \equiv 0 \mod g(z) . \tag{4}$$

The polynomial $g(z)$ is called Goppa polynomial. If the Goppa polynomial is irreducible, then $\Gamma(L, g(z))$ is said to be an irreducible Goppa code. The parity check matrix of the Goppa code $\Gamma(L, g(z))$ is given by:

$$\mathbf{H}=\begin{bmatrix} G(\alpha_0)^{-1} & G(\alpha_1)^{-1} & \dots & G(\alpha_{n-1})^{-1} \\ \alpha_0 G(\alpha_0)^{-1} & \alpha_1 G(\alpha_1)^{-1} & \dots & \alpha_{n-1} G(\alpha_{n-1})^{-1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{r-1} G(\alpha_0)^{-1} & \alpha_1^{r-1} G(\alpha_1)^{-1} & \dots & \alpha_{n-1}^{r-1} G(\alpha_{n-1})^{-1} \end{bmatrix}. \quad (5)$$

A Goppa code has length n equal to the number of elements in set L, dimension $k \geq n - mr$ and the minimal distance d satisfying $d \geq r + 1$.

Example 1: Take $g(z) = z^2 + z + 1$ and $L = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^5, \alpha^4, \alpha^6\} \subseteq GF(2^3)$ where α a primitive element of $GF(2^3)$. None of the elements in set L is the root of polynomial $g(z)$. We obtain a Goppa code $\Gamma(L, g(z))$ with parameter $n = 8$, $k = 2$, $d = 5$. Its parity check matrix is as follows:

$$\mathbf{H}=\begin{bmatrix} \frac{1}{G(0)} & \frac{1}{G(1)} & \frac{1}{G(\alpha)} & \frac{1}{G(\alpha^2)} & \frac{1}{G(\alpha^3)} & \frac{1}{G(\alpha^5)} & \frac{1}{G(\alpha^4)} & \frac{1}{G(\alpha^6)} \\ \frac{0}{G(0)} & \frac{1}{G(1)} & \frac{\alpha}{G(\alpha)} & \frac{\alpha^2}{G(\alpha^2)} & \frac{\alpha^3}{G(\alpha^3)} & \frac{\alpha^5}{G(\alpha^5)} & \frac{\alpha^4}{G(\alpha^4)} & \frac{\alpha^6}{G(\alpha^6)} \end{bmatrix} = \begin{bmatrix} 1 & 1 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha & \alpha & \alpha^4 \\ 0 & 1 & \alpha^3 & \alpha^6 & \alpha^5 & \alpha^6 & \alpha^5 & \alpha^3 \end{bmatrix}. \quad (6)$$

Each element in matrix **H** is converted into its corresponding 3-dimensional vector, and we obtain the binary check matrix of the Goppa code.

$$\mathbf{H}_1=\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}. \quad (7)$$

Perform elementary row transformation on $\mathbf{H}_1$ to obtain the system check matrix $\mathbf{H}_2$.

$$\mathbf{H}_2=\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}, \quad (8)$$

$$\mathbf{G}=\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}. \quad (9)$$

So far, we get the generating matrix **G** then obtain the (8,2,5) Goppa code, whose codeword set is {(0 0 0 0 0 0 0 0), (1 1 1 1 0 0 1 0), (1 1 0 0 1 1 0 1), (0 0 1 1 1 1 1 1)}. End of example.

2.3 Optimized Design for Distributed Goppa Codes

Figure 2 illustrates the system model of distributed Goppa coding scheme. The information sequence m generated by the source node requires two time slots and two different sets of Goppa encoders for transmission over Rayleigh fading channel. Goppa code $\mathbf{C}_1(N,K_1,d_1)$ is applied by the source and $\mathbf{C}_2(N,K_2,d_2)$, $(K_2 \leq K_1)$ is employed by the relay.

During the first time-slot, the message sequence m is encoded by systematic Goppa code $\mathbf{C}_1(N,K_1,d_1)$ to obtain codeword sequence $\mathbf{c}_1$. After 16-QAM modulation, the source node sends the modulation signals $\mathbf{x}_S$ to both the relay and destination nodes. The relay receives signals $\mathbf{y}_{SR}$ and the destination receives signals $\mathbf{y}_{SD}$.

During the second time-slot, the signals $\mathbf{y}_{SR}$ is demodulated to obtain the sequence $\mathbf{r}_1$. Then sequence $\mathbf{r}_1$ is sent to the Goppa decoder and decoded by Euclidean algorithm [22] to obtain the estimated information sequence $\mathbf{m}_1$. The relay selects K_2 symbols from the information sequence $\mathbf{m}_1$ as the information sequence $\mathbf{m}_2$ of the second group Goppa code. The method of selecting information for the relay station is discussed in Sec. 4. The information sequence $\mathbf{m}_2$ is encoded by systematic Goppa code $\mathbf{C}_2(N, K_2, d_2)$ to obtain codeword sequence $\mathbf{c}_2$. After 16-QAM modulation, the relay node broadcasts the modulation signals $\mathbf{x}_R$ to the destination. The destination receives signal $\mathbf{y}_{RD}$ and then combines the two received signals to obtain the joint signal $\mathbf{y} = [\mathbf{y}_{SR}, \mathbf{y}_{RD}]$. Demodulate joint signal $\mathbf{y}$ to get joint estimated codeword sequence $[\mathbf{r}_1,\mathbf{r}_2]$. Finally jointly decode the joint estimated sequence $[\mathbf{r}_1,\mathbf{r}_2]$. to get message $\mathbf{m}$.

The Goppa codes applied to proposed distributed Goppa code scheme in this paper are shown in Tab. 1. Set L contains all elements except 0 in the corresponding field, and α is the primitive element in the corresponding field.

Goppa code	Field	g(*x*)
(15,11,3)	GF(2^4)	x
(15,7,5)	GF(2^4)	x^2+x+a^3
(31,21,5)	GF(2^5)	x^2+x+1
(21,16,7)	GF(2^5)	x^3+x+1
(63,51,5)	GF(2^6)	x^2+x+1
(63,21,15)	GF(2^6)	x^7+x+1

Tab. 1. Goppa codes applied for scheme.

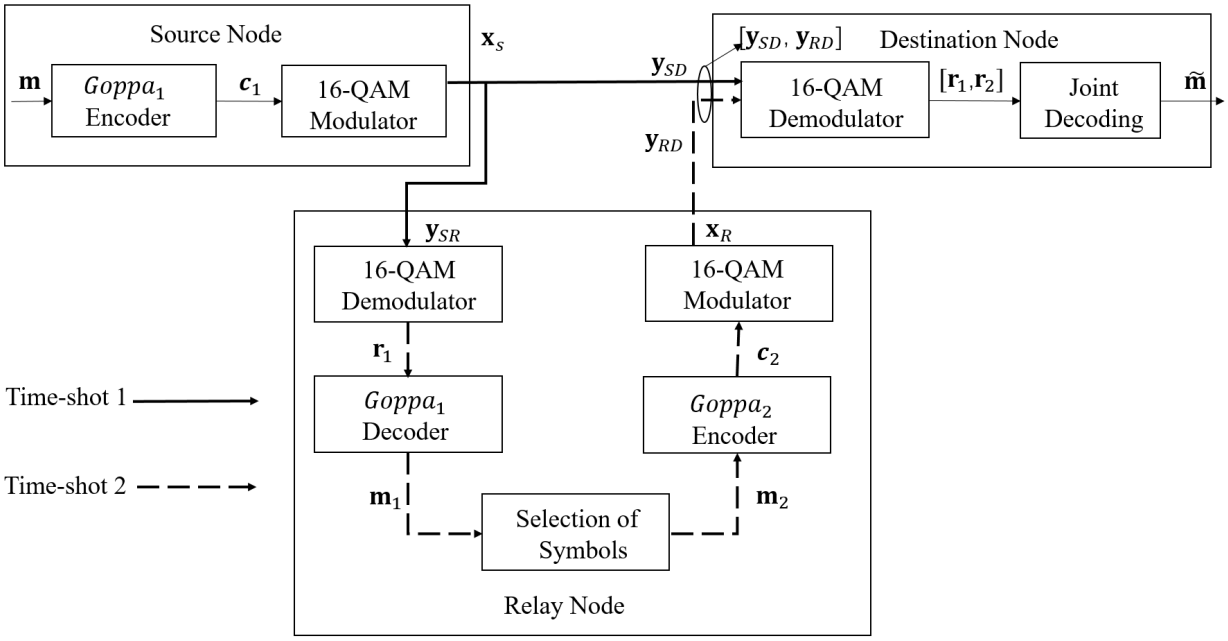

Fig. 2. Distributed Goppa coding scheme.

3. Information Selection at the Relay

The selection of information at the relay is crucial in the construction of code for the destination. Different relay selections of information can affect the overall performance of the coding cooperation scheme. Assume that the minimum Hamming distance of joint code **C** is d_3. The minimum distance d_3 is considered as large as possible, however, random selection methods may make d_3 smaller. Hence, the optimized selection approaches need to be adopted. In this situation, we will adopt this selection method so that the amount of codewords **C** with a minimum weight d_3 is as small as possible. The joint codes selected by this approach have better weight distribution than other joint codes with the same minimum distance. This section presents two efficient methods for proper selection at the relay.

3.1 Method 1: Exhaustive Search (Global Optimal)

Step 1: Determine the set $B = \{\eta_q\}$ of all selection patterns $\eta_q = [j_1, j_2, \ldots, j_{K_2}]$, where $j_i \in \{1, 2, \ldots, K_1\}$ ($i = 1,2,\ldots,K_2$), $q = 1,2,\ldots,Q$ and Q is defined as:

$$Q = \binom{K_1}{K_2} = \frac{K_1!}{K_1!(K_1 - K_2)!}. \tag{10}$$

Step 2: Encode all information sequences separately using each selection pattern in set B_i. Determine the number ν_1 of joint codewords with weight d (initial state $i = 0$, $B_0 = B$, $d = d_1 + i$).

Step 3: Find the minimum value $\min(\nu_i)$ of ν_i and save the corresponding selection patterns η_q in set B_{i+1}. If $|B_{i+1}| = 1$, move to next step otherwise $i = i + 1$ then return step 2.

Step 4: The final remaining selection pattern η_q is optimized selection pattern $\eta^{(1)}$. End of method 1.

Method 1 is effective in selecting K_2 information symbols at the relay. However, we need to encode all information sequences before searching. As the information bits K_1 become larger, the encoded information increases exponentially. Meanwhile, the number of selection methods is also very huge. Therefore, the complexity of determining the selection pattern $\eta^{(1)}$ is greatly increased. We propose a low complexity search method.

3.2 Method 2: Partial Search (Local Optimal)

This approach selects message sequences that can be encoded as codewords with a weight of d_1. Therefore, for each selection pattern, only a subset of message sequences is chosen. Additionally, the number of selection patterns is minimized. The specific steps are as follows:

Step 1: We consider that only 1 bit of message sequence is non-zero, and the other bits are all 0. We encode this, find the corresponding codeword with minimum weight d_1, and save the non-zero position in set τ. The relay selects K_2 message bits from K_1 recovered message bits. In order to increase the minimum distance of the joint code, the corresponding positions of the elements in τ must be selected. If those positions are not selected, the second part of the joint code will not provide any weight, and the minimum distance will not be increased. Therefore, we specifically select the corresponding positions of elements in τ if $\tau \le K_2$. Then select other $K_2 - |\tau|$ positions from the rest. Set $B' = \{\eta_p\}$ of partial message selection patterns

$\eta_p = [j_1, j_2, \ldots, j_{K_2}]$ is determined, where $p = 1,2,\ldots,|\mathrm{B}'|$ and $|\mathrm{B}'| = \binom{K_1 - |\tau|}{K_2 - |\tau|}$. If $\tau > K_2$, we select K_2 positions out of the corresponding positions of elements in τ. Then set $\mathrm{B}' = \{\eta_p\}$ of partial message selection patterns $\eta_p = [j_1, j_2, \ldots, j_{K_2}]$ is determined, where $p = 1,2,\ldots,|\mathrm{B}'|$ and $|\mathrm{B}'| = \binom{K_2}{|\tau|}$.

Step 2: Determine the set $\mathrm{A} = \{\mathbf{m}_a\}$ of all message sequences that generate a codeword with weight d_1.

Step 3: Encode all information sequences in set A separately using each selection pattern in set B′. Determine the number u_0 of joint codewords with weight $d = d_1$.

Step 4: Find the minimum value $\min(u_0)$ of u_0 and save the corresponding selection patterns η_p in set B'_0. If $|\mathrm{B}'_0| = 1$, skip to step 9 otherwise skip to the next step.

Step 5: Encode all information sequences in set A separately using the remaining selection pattern in set B'_0. Determine the number u_1 of joint codewords with weight $d = d_1 + d_2$.

Step 6: Find the minimum value $\min(u_1)$ and save the corresponding selection patterns η_p in set B'_1. If $|\mathrm{B}'_1| = 1$, skip to step 9 otherwise move to the next step.

Step 7: Encode all information sequences in set A separately using the remaining selection pattern in set B'_1. Increase d and then determine the number u_2 of joint codewords with weight d.

Step 8: Find the minimum value $\min(u_2)$ and save the corresponding selection patterns η_p in set B'_2. If $|\mathrm{B}'_2| = 1$, skip to step 9 otherwise return to step 7.

Step 9: The final remaining selection pattern η_p is optimized selection pattern $\eta^{(1)}$. End of method 2.

3.3 Examples of Two Methods

Consider a distributed Goppa coding scheme, Goppa code $\mathbf{C}_1(15,11,3)$ and $\mathbf{C}_1(15,7,5)$ are applied at source and relay, respectively. Both set L_1 and L_2 contain all non-zero elements of $GF(2^4)$ using the polynomial $X^4 + X + 1$. Their Goppa polynomials are $g_1(x) = x$ and $g_2(x) = x^2 + x + a^3$. The polynomial coefficients are taken $GF(2^4)$, and α is the primitive in $GF(2^4)$. The selection process of $K_2 = 7$ out of $K_1 = 11$ using proposed methods are as follow.

Firstly, method 1 is adopted to the selection process:

Step 1: Determine selection patterns $\eta_q = [j_1, j_2, \ldots, j_7]$ and save them in B. Selection method quantity is $Q = 330$.

Step 2: Encode all information sequences separately using each selection pattern in set B. Determine the number v_0 of joint codewords with weight 3.

Step 3: Find the minimum value $\min(v_0) = 0$ and save the corresponding selection patterns η_q in set B_1. Since $|\mathrm{B}_1| = 1$, skip to next step.

Step 4: The optimized selection pattern is $\eta^{(1)} = \eta_q = [1,3,6,7,9,10,11]$. Searching is terminated. The process of obtaining the selection method is shown in Tab. 2.

Method 2 is applied to the selection process:

Step 1: Encode the message sequence with only one non-zero bit, and find the corresponding codeword with minimum weight 3. Six codewords are qualified and save the non-zero position in set τ. $\tau = [1,6,7,9,10,11]$, so 6 of the 11 positions have been determined, and $7 - |\tau|$ positions are drawn from remaining 5 positions. Selection method quantity is $|\mathrm{B}| = 5$.

Step 2: Determine the set $\mathrm{A} = \{\mathbf{m}_a\}$ of all message sequences that generate a codeword with weight $d_1 = 3$. Number of codewords that meet the requirements is $|\mathrm{A}| = 48$.

Step 3: Encode all information sequences in set A separately using each selection pattern in set B′. Determine the number u_0 of joint codewords with minimum weight 3.

Step 4: Find the minimum value $\min(u_0) = 0$ and save the corresponding selection patterns η_p in set B'_1. Since $|\mathrm{B}'_1| = 1$, skip to step 9.

Step 9: $\eta^{(2)} = \eta_q = [1,3,6,7,9,10,11]$ is the optimal selection pattern. Searching is terminated. The process of obtaining the selection pattern by using method 2 is shown in Tab. 3.

From the example given, we can see that the selection pattern we get from partial search method 2 is the same as that from exhaustive search method 1. This demonstrates the validity of the proposed partial search method 2. The complexity of exhaustive search method 1 increases sharply as the information bits K_1 and codeword length N. Therefore, we adopt method 2 in two other schemes.

Serial number	Selection pattern	v_0
1	[1,3,6,7,9,10,11]	0
2	[1,2,3,4,5,6,11]	3
3	[2,3,4,7,8,10,11]	3

Tab. 2. The criterion value $\min(v_0)$ about determining the selection pattern under method 1 with $\mathrm{Goppa}_1(15,11,3)$ and $\mathrm{Goppa}_2(15,7,5)$.

Serial number	Selection pattern	u_0
1	[1,2,3,4,5,6,11]	3
2	[1,3,6,7,9,10,11]	0
3	[1,4,6,7,9,10,11]	3
4	[1,5,6,7,9,10,11]	3
5	[1,6,7,8,9,10,11]	3

Tab. 3. The criterion value $\min(u_0)$ about determining the selection pattern under method 2 with $\mathrm{Goppa}_1(15,11,3)$ and $\mathrm{Goppa}_2(15,7,5)$.

Goppa code $\mathbf{C}_1(31,21,5)$ and $\mathbf{C}_2(31,16,7)$ are adopted at source and relay in the second scheme, respectively. In the third scheme, Goppa code $\mathbf{C}_1(63,51,5)$ and $\mathbf{C}_2(63,21,15)$ are adopted at source and relay in the third scheme, respectively. Table 4 and 5 show the processes of obtaining the selection pattern for these two schemes by using method 2. All three schemes and selection patterns for distributed Goppa codes are listed in Tab. 6.

3.4 Complexity Analysis for the Two Searching Methods

Encoding a sequence of message of length K requires $\zeta^{\times} = K(N-K)$ multiplication operations and $\zeta^{+} = K(N-K)$ addition operations and totals $\zeta = 2K(N-K)$ operations. For method 1, all information sequences need to be encoded at the source, the amount of operations is $\zeta_S^{(1)} = 2^{K_1} 2K_1 (N-K_1)$. The same quantity information is encoded at relay, and the number of selection patterns is $|\mathrm{B}|$, so the amount of operations at relay is $\zeta_R^{(1)} = |\mathrm{B}|\, 2^{K_1} 2K_2 (N-K_2)$. The amount of total operations of method 1 is

$$\zeta^{(1)} = 2^{K_1+1}[NK_1 - (K_1)^2 + |\mathrm{B}|\, NK_2 - |\mathrm{B}|(K_2)^2] \quad (11)$$

if method 1 converges at step v_0. For method 2, $|\mathrm{A}|$ information sequences need to be encoded at the source, the amount of operations is $\zeta_S^{(2)} = 2|\mathrm{A}|\, K_1 (N-K_1)$. The same quantity information is encoded at relay, and the number of selection patterns is $|\mathrm{B}'|$, so the amount of operations at relay is $\zeta_R^{(2)} = 2|\mathrm{A}|\,|\mathrm{B}'|\, K_2 (N-K_2)$. The amount of total operations of method 2 is

$$\zeta^{(2)} = 2|\mathrm{A}|[NK_1 - (K_1)^2 + |\mathrm{B}'|\, NK_2 - |\mathrm{B}'|(K_2)^2] \quad (12)$$

if method 2 converges at step u_0.

4. Joint Decoding

Joint decoding is the key of distributed coding cooperative system. Based on the coding cooperative system proposed above, two joint decoding methods are proposed. The details of those methods are as follows:

4.1 Naive Decoding Algorithm

Step 1: The demodulated sequences $\mathbf{r}_1$ and $\mathbf{r}_2$ are decoded by Goppa1 decoder and Goppa2 decoder respectively to obtain information sequences $\hat{\mathbf{m}}_1$ and $\hat{\mathbf{m}}_2$.

Step 2: In channel coding, in the case of low SRN, the BER performance of Goppa2 with stronger error correction ability is worse than Goppa1 with weak error correction ability. While in the case of high SNR, Goppa2 is better than Goppa1. Therefore, set the threshold ρ which is the SNR value of the intersection of the BER performance curves of two sets of Goppa codes over the fast Rayleigh fading channel.

Step 3: If $SNR < \rho$, jointly decoded information sequence $\tilde{\mathbf{m}} = \hat{\mathbf{m}}_1$; $SNR \geq \rho$, the K_2 elements in the sequence $\hat{\mathbf{m}}_1$ are replaced with $\hat{\mathbf{m}}_2$ in the manner previously selected. Then jointly decoded information sequence $\tilde{\mathbf{m}} = \hat{\mathbf{m}}_1$.

4.2 Smart Decoding Algorithm

Step 1: Decode the demodulated sequence $\mathbf{r}_2$ by Goppa2 decoder to obtain information sequence $\hat{\mathbf{m}}_2$.

Step 2: Since the system code is used, the demodulation sequence $\mathbf{r}_1$ is composed of a parity check sequence $\mathbf{p}_1$ and an information sequence $\mathbf{m}_1$. Therefore, K_2 elements in the sequence $\mathbf{m}_1$ are replaced with $\hat{\mathbf{m}}_2$ in the manner previously selected and obtain joint sequence $\tilde{\mathbf{r}}_1$.

Step 3: The sequence $\tilde{\mathbf{r}}_1$ is decoded by Goppa1 decoder to obtain the estimated sequence $\hat{\mathbf{m}}_1$, the estimated sequence $\hat{\mathbf{m}}_1$ is the information sequence $\tilde{\mathbf{m}}$ ($\tilde{\mathbf{m}} = \hat{\mathbf{m}}_1$) of the final joint decoding.

5. Simulation Results

Based on the system constructed in Sec. 2, three different distributed Goppa codes schemes are simulated. The Goppa codes and selection patterns used are presented in Tab. 2 and Tab. 6. In the first scheme, the code rates are $R_1 = 11/15$ and $R_2 = 7/15$, the joint code rate is $R_3 = 11/30$. In the second scheme, the code rates are $R_1 = 21/31$ and $R_2 = 16/31$, the joint code rate is $R_3 = 21/62$. In the last scheme, the code rates are $R_1 = 51/63$ and $R_2 = 21/63$, the joint code rate is $R_3 = 51/126$. All schemes adopt 16-QAM modulation and are tested through fast Rayleigh fading channel. $\gamma_{S,D}$, $\gamma_{S,R}$, $\gamma_{R,D}$ denote the SNR of the source-destination link, the source-relay link and relay-destination link, respectively. Because the relay node is closer to the destination, the relay node has the advantage of SNR. Suppose $\gamma_{R,D} = \gamma_{S,D} + 2$ dB.

5.1 Performance Comparison under Different Information Selection Methods for Distributed Goppa Coding Scheme

Figures 3, 4 and 5 show the performance of three different distributed Goppa code schemes for different selection methods, respectively. It is assumed that source-relay link is ideal, i.e., ($\gamma_{S,R} = \infty$) and the smart decoding algorithm is applied. In first scheme, we searched the same selection pattern by adopt method 1 exhaustive search and method 2 partial search. In second and third schemes, due to high complexity, we only adopt method 2 partial search to obtain suboptimal selection pattern and then compare the performance with the random selection pattern. The simulation results show that the distributed Goppa coding scheme under method 2 has better performance than the scheme with random selection applied. The simulation results illustrate the effect of appropriate information selection and validate the correctness of method 2.

Serial number	Selection pattern	u_0	u_1
1	[2,4,5,7,9,10,11,12,13,14,15,16,18,19,20,21]	0	13
2	[2,3,4,5,7,8,9,10,11,12,13,14,16,17,18,19]	0	14
3	[2,3,4,5,7,9,10,11,12,13,14,16,18,19,20,21]	0	14

Tab. 4. The criterion value min(u_0) and min(u_1) about determining the selection pattern under method 2 with Goppa$_1$(31,21,5) and Goppa$_2$(31,16,7).

Serial number	Selection pattern	u_0	u_1
1	[1,6,7,9,11,14,18,23,25,26,28,32,33,35,37,39,41,42,43,46,51]	0	689
2	[2,4,7,9,14,16,17,23,25,36,38,32,33,35,37,39,41,42,43,46,51]	0	714
3	[2,3,7,9,11,14,18,23,25,26,32,33,35,37,39,41,42,43,46,51]	0	852

Tab. 5. The criterion value min(u_0) and min(u_1) about determining the selection pattern under method 2 with Goppa$_1$(63,51,5) and Goppa$_2$(63,21,15).

Serial number	C_1(N,K_1,d_1)	C_2(N,K_2,d_2)	$\eta^{(1)}$	$\eta^{(2)}$
1	(15,11,3)	(15,7,5)	[1,3,6,7,9,10,11]	[1,3,6,7,9,10,11]
2	(31,21,5)	(31,21,7)	-	[2,4,5,7,9,10,11,12,13,14,15,16,18,19,20,21]
3	(63,51,5)	(63,21,15)	-	[1,6,7,9,11,14,18,23,25,26,28,32,33,35,37,39,41,42,43,46,51]

Tab. 6. Optimized selection patterns of corresponding distributed Goppa codes.

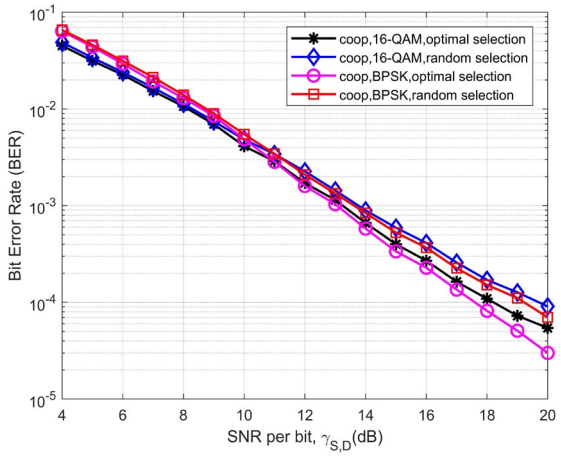

Fig. 3. BER performance comparison under different information selection methods for distributed Goppa coding scheme with Goppa$_1$(15,11,3) and Goppa$_2$(15,7,5).

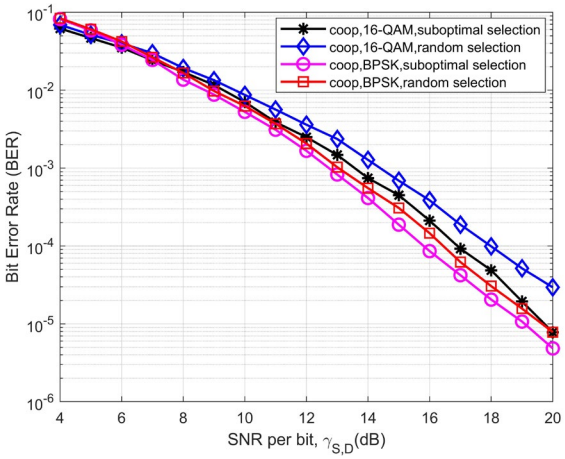

Fig. 5. BER performance comparison under different information selection methods for distributed Goppa coding scheme with Goppa$_1$(63,51,5) and Goppa$_2$(63,21,15).

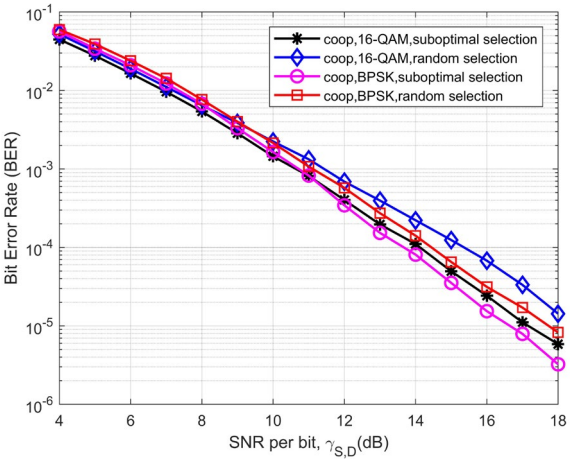

Fig. 4. BER performance comparison under different information selection methods for distributed Goppa coding scheme with Goppa$_1$(31,21,5) and Goppa$_2$(31,16,7).

5.2 Performance Comparison between Naive and Smart Decoding Algorithms for Distributed Goppa Coding Scheme

Figures 6, 7 and 8 demonstrate the performance of three different distributed Goppa coding schemes between naive and smart decoding algorithms, respectively. It is assumed that source-relay link is ideal, i.e., ($\gamma_{S,R} = \infty$) and the method 2 is applied in the three schemes. In Fig. 6, the distributed Goppa coding scheme applying smart algorithm has a SNR advantage of about 2 dB over the scheme with naive algorithm ($\rho = 4$ dB) at BER $\approx 1.03 \times 10^{-4}$. Figure 7 demonstrates the distributed Goppa coding scheme adopting smart algorithm that achieves a performance gain of 1.7 dB over the naive algorithm at BER $\approx 2 \times 10^{-5}$. Figure 8 shows the distributed Goppa coding scheme using smart decoding algorithm that achieves a 1.8 dB gain over scheme using naive algorithm at BER $\approx 4 \times 10^{-5}$.

5.3 Performance Comparison on Non-ideal and Ideal Source-to-Relay Channels for Distributed Goppa Coding Scheme

Figures 9, 10 and 11 show the performance of three different distributed Goppa coding schemes and their corresponding non-cooperative scheme, respectively. It is assumed smart decoding algorithm and the method 2 is applied in the three schemes. The proposed distributed Goppa coding scheme and its non-cooperative scheme should have the same code rate during transmission for a fair comparison. As can be seen from Fig. 9, under the ideal source-to-relay channel ($\gamma_{S,R}=\infty$), the distributed Goppa coding scheme performs better than the corresponding non-cooperative scheme at BER $\approx 4.2\times10^{-4}$ with a gain of about 4 dB. This demonstrates the effectiveness of relay node for path diversity. Furthermore, simulation results indicate the distributed Goppa coding scheme with $\gamma_{S,R}=$ 12 dB performs similarly to the scheme with $\gamma_{S,R}=\infty$ at low SNR. As the SNR increases, the role of the relay node gradually fails. The overall BER performance degrades significantly as the repeater transmits incorrect information.

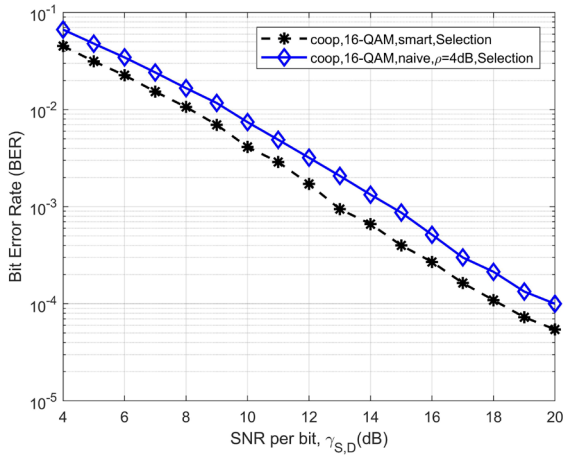

Fig. 6. BER performance comparison using different joint decoding algorithms for distributed Goppa coding scheme with $\text{Goppa}_1(63,51,5)$ and $\text{Goppa}_2(63,21,15)$.

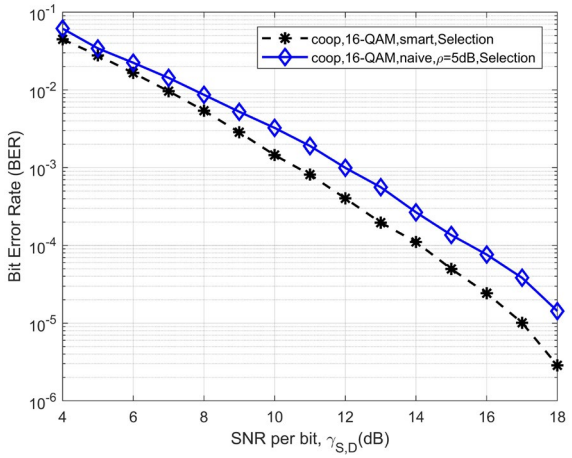

Fig. 7. BER performance comparison using different joint decoding algorithms for distributed Goppa coding scheme with $\text{Goppa}_1(31,21,5)$ and $\text{Goppa}_2(31,16,7)$.

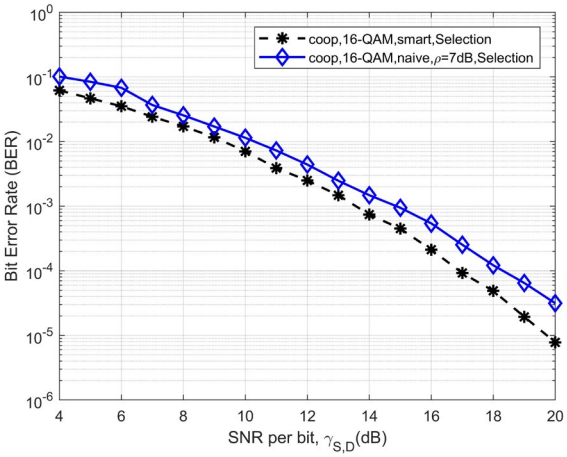

Fig. 8. BER performance comparison using different joint decoding algorithms for distributed Goppa coding scheme with $\text{Goppa}_1(63,51,5)$ and $\text{Goppa}_2(63,21,15)$.

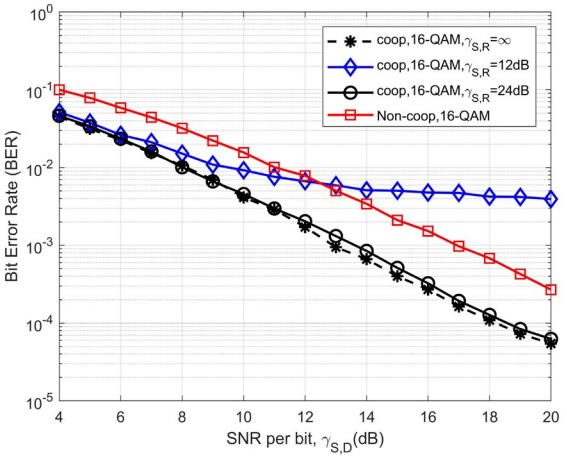

Fig. 9. BER performance comparison of distributed Goppa coding scheme at different $\gamma_{S,R}$ and non-cooperative scheme with $\text{Goppa}_1(15,11,3)$ and $\text{Goppa}_2(15,7,5)$.

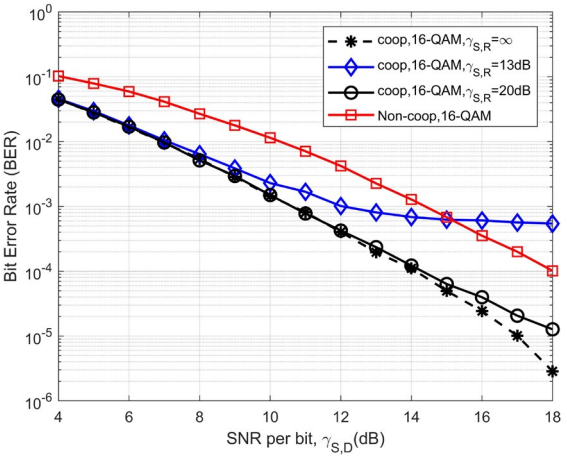

Fig. 10. BER performance comparison of distributed Goppa coding scheme at different $\gamma_{S,R}$ and non-cooperative scheme with $\text{Goppa}_1(31,21,5)$ and $\text{Goppa}_2(31,16,7)$.

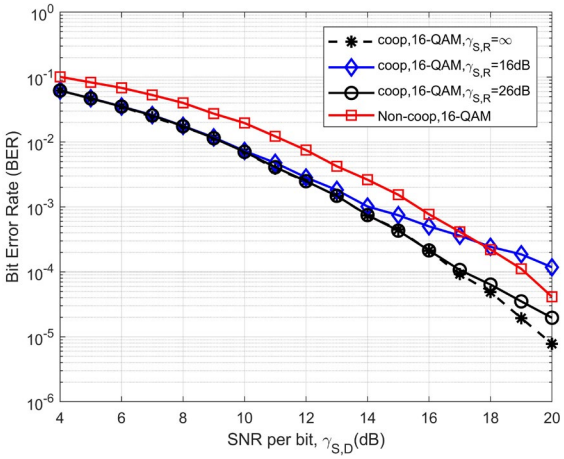

Fig. 11. BER performance comparison of distributed Goppa coding scheme at different $\gamma_{S,R}$ and non-cooperative scheme with $\text{Goppa}_1(63,51,5)$ and $\text{Goppa}_2(63,21,15)$.

In addition, the performance of distributed Goppa coding scheme at $\gamma_{S,R} = \infty$ is very close that of the scheme at $\gamma_{S,R} = 24$ dB. We can also observe the similar situation in Figs. 10 and 11. Under the ideal source-to-relay channel ($\gamma_{S,R} = \infty$), the distributed Goppa coding scheme outperforms the corresponding non-cooperative scheme. When the source to relay channel $\gamma_{S,R}$ is large, the performance approaches that of the ideal case while when $\gamma_{S,R}$ is small, the performance curve becomes flat, because no error controlled propagation is adopted at the relay.

6. Conclusion

This paper proposed two information selection methods at relay for a distributed Goppa coding cooperative system. Through Monte-Carlo simulations, we can see the advantages of two selection methods. Two joint decoding algorithms are proposed to decode joint code at the destination. By simulation and comparison, the smart algorithm outperforms the naive algorithm under the same conditions. Furthermore, comparisons with non-cooperative scheme show that our proposed distributed Goppa coding scheme is effective. In our future work, we aim to find Goppa codes with better performance and reduce the complexity of information selection.

Acknowledgments

This work was supported by National Natural Science Foundation of China under the Contract No. 61771241.

References

[1] SHANKAR, P. M. *Fading and Shadowing in Wireless Systems*. 2nd ed., rev. USA: Springer Nature, 2017. ISBN: 978-3-319-53198-4

[2] PAULRAJ, A. J., GORE, D. A., NABAR, R. U., et al. An overview of MIMO communications - A key to gigabit wireless. *Proceedings of the IEEE,* 2004, vol. 92, no. 2, p. 198 to 218. DOI: 10.1109/JPROC.2003.821915

[3] COVER, T. M. GAMEL, A. Capacity theorems for the relay channel. *IEEE Transactions on Information Theory,* 1979, vol. 25, no. 5, p. 572–584. DOI: 10.1109/TIT.1979.1056084

[4] OU, Q., HOU, X., LIU, F., et al. Joint partial relay and antenna selection for full-duplex amplify-and-forward relay networks. In *Proceedings of the 9th International Conference Wireless Internet (WICON2016)*. Haikou (China), 2016, p. 149–154. DOI: 10.1007/978-3-319-72998-5_16

[5] DAI, L., YU, L., MA, Z. Compress-and-forward strategy for the relay broadcast channel with confidential messages. In *Proceedings of 2016 IEEE International Conference on Communications Workshops (ICC)*. Kuala Lumpur (Malaysia), 2016, p. 254–259. DOI: 10.1109/ICCW.2016.7503796

[6] HAN, L. Ergodic capacity upper bound for multi-hop full-duplex decode-and-forward relaying. In *Proceedings of International Conference in Communications, Signal Processing, and Systems*. 2018, p. 157–164. DOI: 10.1007/978-981-10-3229-5_17

[7] WANG, H., CHEN, Q. LDPC based network coded cooperation design for multi-way relay networks. *IEEE Access,* 2019, vol. 7, p. 62300–62311. DOI: 10.1109/ACCESS.2019.2915293

[8] EJAZ, S., YANG, F. Turbo codes with modified code matched interleaver for coded-cooperation in half-duplex wireless relay networks. *Frequenz,* 2015, vol. 69, no. 3-4, p. 171–184. DOI: 10.1515/freq-2014-0072

[9] BLASCO-SERRANO, R., THOBABEN, R., ANDERSSON, M., et al. Polar codes for cooperative relaying. *IEEE Transactions on Communications,* 2012, vol. 60, no. 11, p. 3263–3273. DOI: 10.1109/TCOMM.2012.081412.110266

[10] UMAR, R., YANG, F., MUGHAL, S. Distributed Reed Muller code with multiple relays for cooperative broadband wireless networks. *Radioelectronics and Communications Systems*, 2019, vol. 62, no. 9, p. 449–461. DOI: 10.3103/S0735272719090024

[11] CHEN, B., FLANAGAN, M. F. Network-turbo-coding-based cooperation with distributed space-time block codes. *Transactions on Telecommunications*, 2015, vol. 26, no. 6, p. 992–1002. DOI: 10.1002/ett.2780

[12] LIU, Y., PANG, B., ZHANG, Y., et al. Diversity of distributed linear convolutive space-time codes on fast fading Rayleigh channels. In *Proceedings of 2016 International Conference on Computing, Networking and Communications (ICNC)*. Kauai (HI, USA), 2016, p. 1–5. DOI: 10.1109/ICCNC.2016.7440676

[13] QIU, J., CHEN, L., LIU, S. A novel concatenated coding scheme: RS-SC-LDPC codes. *IEEE Communications Letters,* 2020, vol. 24, no. 10, p. 2092–2095. DOI: 10.1109/LCOMM.2020.3004917

[14] DONG, Y., NIU, K., DAI, S., et al. Joint source and channel coding using double polar codes. *IEEE Communications Letters,* 2021, vol. 25, no. 9, p. 2810–2814. DOI: 10.1109/LCOMM.2021.3088941

[15] GUO, P., YANG, F., ZHAO, C., et al. Jointly optimized design of distributed Reed-Solomon codes by proper selection in relay. *Telecommunication Systems,* 2021, vol. 78, no. 3, p. 391–403. DOI: 10.1007/s11235-021-00822-w

[16] MUGHAL, S., YANG, F., XU, H., et al. Coded cooperative spatial modulation based on multi-level construction of polar code. *Telecommunication Systems,* 2019, vol. 70, no. 3, p. 435–446. DOI: 10.1007/s11235-018-0485-6

[17] TSFASMAN, M. A., VLADUT, G., ZINK, T. Modular curves, Shimura curves, and Goppa codes better than the Varshamov-Gilbert bound. *Mathematische Nachrichten,* 1982, vol. 109, p. 21–28.

[18] MACWILLIAMS, F. J., SLOANE, N. J. A. *The Theory of Error-Correcting Codes*. North-Holland Publishing Company, 1977. ISBN: 978-0444851932

[19] SUGIYAMA, Y., KASAHARA, M., HIRASAWA, S., et al. A method for solving key equation for decoding Goppa codes. *Information and Control,* 1975, vol. 27, no. 1, p. 87–99. DOI: 10.1016/S0019-9958(75)90090-X

[20] SUGIYAMA, Y., KASAHARA, M., HIRASAWA, S., et al. An erasures-and-errors decoding algorithm for Goppa codes. *IEEE Transactions on Information Theory,* 1976, vol. 22, no. 2, p. 238–241. DOI: 10.1109/TIT.1976.1055517

[21] GOLDSMITH, A. *Wireless Communications.* 1st ed. London (UK): Cambridge University Press, 2005. ISBN: 9780521837163

[22] LIN, S. *Error Control Coding*. 2nd ed., rev. Englewood Cliffs (USA): Prentice-Hall, 2004. ISBN: 978-1-4613-6787-1

About the Authors ...

FangAn FENG (corresponding author) was born in Guangxi, China. He received his B.Sc. from Nanjing University of Aeronautic and Astronautics, Nanjing, China in 2020. His research interests include circuits and systems, signal processing and channel coding. Now he is a graduate student at Nanjing University of Aeronautic and Astronautics, Nanjing, China.

FengFan YANG received the M.Sc. and Ph.D. degrees from the Northwestern Polytechnical University and South-east University, China in 1993, and 1997, respectively, all in Electronic Engineering. He has been with the College of Information Science and Technology, Nanjing University of Aeronautics and Astronautics since May 1997. From October 1999 to May 2003, he was a research associate at the Centre for Communication Systems Research, University of Surrey, UK, and Dept. of Electrical and Computer Engineering, McGill University, Canada. His major research interests are information theory, channel coding and their applications for mobile and satellite communications.

Chen CHEN received her B.S degree in Electronic and Information Engineering from Yangzhou University, China, in 2020. She is currently doing Ph.D. from the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, China. Her research interests are circuits and systems, signal processing and channel coding.

ChunLi ZHAO received her B.S. degree in Electronic and Information Engineering from Henan Normal University, Xinlian College, China, in 2014. She obtained her M.Sc. degree in Circuits and Systems at Henan Normal University, China, in 2017. She is currently doing Ph.D. from the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, China. Her research interests are circuits and systems, signal processing and channel coding.