Performance of Low Rank Parity Check Codes for Multi-source Wireless Sensor Networks

Oussama Habachi, Vahid Meghdadi, Jean-Pierre Cances, Imad El Quachchach

Performance of Low Rank Parity Check Codes for Multi-source Wireless Sensor Networks

Imad EL QACHCHACH, Jean-Pierre CANCES, Oussama HABACHI and Vahid MEGHDADI

Xlim Institute of Technology, University of Limoges, France

Email: {el-qachchach, jean-pierre.cances, oussama.habachi, vahid.meghdadi}@xlim.fr

Abstract

Random linear network coding (RLNC) is one of the most promising high-performance techniques for wireless sensor networks (WSNs). One of its most relevant characteristics is that it allows intermediate nodes to combine incoming packets and send only the combined packets. Nevertheless, few works have focused on the use of multi-source networks using error correcting codes. In fact, when an intermediate node fails, errors may occur and since RLNC combines packets from different sources, several packets may be affected. Furthermore, we consider a realistic model for the wireless links in the network taking into account the ambient thermal noise. In this paper, we consider the problem of multi-source networks and we propose a novel error correction mechanism using modified low rank parity check (M-LRPC) decoding algorithm based on LRPC code, as an outer code and a convolutional code as an inner code to correct sparse errors. Moreover, we investigate the performance of the proposed coding technique in terms of success decoding rate. Then, we derive a theoretical expression for the decoding probability of the proposed M-LRPC. Simulation results show the accuracy of the proposed bound. These results prove that the proposed scheme significantly improves the decoding probability compared to Gabidulin codes.

Index Terms

Wireless sensor networks; random network coding; multi-source networks; LRPC codes; decoding probability.

I. Introduction

Wireless sensor networks consist of a large number of sensors where the information is usually transmitted from sensors to the sink via intermediate sensors, called relays. WSNs are designed to support a large variety of applications such as tracking, exploration, monitoring and sensing tasks [1]. In recent years, they have attracted a lot of research activities both in the academic and industrial worlds. In fact, they are developed to provide fast, cheap, reliable and scalable solutions for a large number of applications. Forwarding the sensed data from a source node to a destination node is one of those applications. By considering various performance parameters, such as power limitation, routing, reliability and security, the scientific community is proposing novel techniques to improve the behavior of wireless networks.

One of the most promising solutions transport in WSNs is network coding (NC). Network coding has been originally proposed by R. Ahlswede et al. in [2] as a way to improve the communication throughput over a wired multi-hop network. In broadcast channels, where all users request the same set of packets, the basic idea is to make use of the available packets at different receivers. Note that using network coding, information can be transmitted to multiple receivers simultaneously even when each receiver expects different packets. Several forms of NC can be found in the literature, each one with its own benefits and drawbacks.

One of the most promising techniques is Random Linear Network Coding (RLNC) [3], which is a simple form of network coding that can approach system capacity with negligible feedback overhead. In fact, using RLNC, intermediate nodes combine randomly multiple incoming packets and typically relay one combined packet towards the next intermediate nodes or destination nodes. After the successful reception of coded packets, the receivers can successfully decode them using a Gaussian elimination. Some initial works, by Koetter and Li [3], have shown that the use of random combinations may lead to the optimum broadcast capacity. Afterwards, different studies have analyzed the benefits of RLNC solutions, demonstrating that NC can bring a more efficient usage of network resources. Nevertheless, if packet error occurs, the erroneous packets are combined with unharmed ones causing the whole combination to be affected. This kind of errors can be illustrated in three use-cases. The first use-case is when a malicious user injects erroneous packets into the network to disrupt the overall system, such as the scenarios studied in [4], [5] and [6]. The second use-case is depicted by the presence of a node failure within the network, see [3] for example. The third case is when we take into consideration the impact

of background noise that is caused by propagation channel and electronic impairment (additive white Gaussian noise (AWGN) for example). In order to solve the problem of background noise, we propose to use convolutional codes. Each node uses a linear combination of the received packets and decodes them using convolutional decoder. The first and the second cases can be solved by using rank metric codes. It has been proven that rank codes are efficient against criss-cross errors and rank error [7]. In particular, Gabidulin has figured out this kind of errors and proposed a class of correcting codes named *Gabidulin codes*. A new class of rank metric codes has been proposed in [8], called Low Rank Parity Check (LRPC), that has approximately the same performance of Gabidulin codes. Koetter and Kschischang tested the performance of rank codes combined with RLNC schemes for intentional attacks [9]. This work is concerned with the transmission of coded packets from a single source to a single destination through multiple relays using rank codes. Note that, using Gabidulin codes in multi-source networks is not beneficial, since relay nodes cannot combine packets of different sources [10]. In fact, source nodes have to wait until the active source node transmits all its packets before another source can start the transmission. Indeed, when receiving packets simultaneously from different source node, relay can only transmit packets of one source and store the packets of other nodes using *store-and-forward* method (see [11]). However, this solution increases the latency and is greedy in terms of storage and battery.

Similar contexts of the present work can be found in [12] and [13], where two source nodes transmit streams of coded packets to both a relay and a destination nodes. They studied the performance of RLNC using a simple system model (two-source single-relay network) and derived a theoretical framework for the performance characterization of the considered network. In contrast to [14] and [15], where only one source network has been considered for transmitting data to the destination, we consider the problem of multi-source multi-relay network. Other notable differences with [15], relays do not only perform decode-and-forward, but also combine linearly the coded packets. In other words, relays employ RLNC and forward the combined packets. Following the approach proposed in [16], the authors have considered a framework with a direct transmission link called network coded cooperation (NCC) and they have derived the theoretical successful decoding probability of NCC for generalized multi-source multi-relay networks. However, there is no direct reliable link between the source and the sink for many applications in WSNs. It is due to geographical location and power limitation.

These observations have motivated us to design a coding scheme that extend the LRPC codes

to multi-source network. In this paper, we investigate existing solutions in the literature for multi-source networks using error correcting codes and we propose a generalized solution. We derive also the theoretical failure decoding probability of LRPC codes in multi-source networks.

Our main contributions are depicted as follows:

- We propose a new decoding technique, Modified-Low Rank Parity Check M-LRPC, based on LRPC code in the case of multi-source networks as a way to improve the communication reliability. Also, we use convolutional code in order to limit the background noise.
- We propose some modifications in the decoding algorithm of LRPC codes such as using q-polynomials in order to recover the error basis and using a simple construction of the parity check matrix in order to reduce the decoding complexity.
- We derive theoretical expression of failure decoding probability at the destination for M-LRPC in multi-source networks.
- We validate the theoretical results with simulations and we show that our proposition achieves good performance compared to existing ones. The simulations illustrate the advantages of using M-LRPC decoding algorithm.

The rest of this paper is organized as follows. In section II, notations and fundamental preliminaries of finite field and vector spaces are detailed. A detailed description of rank codes and q-polynomials is provided in Section III. Section IV describes the system model and formulates the problem statement. The framework of the calculation of the failure decoding probability and the M-LRPC decoding algorithm are expressed in Section V. The numerical results are presented in Section VI and the conclusions are drawn in Section VII.

II. Preliminaries

Let q be a power of prime number p and $\mathbf{u}$ be an element of $\mathbb{F}_{q^m} \setminus \mathbb{F}_q$. In this paper, all coefficients of a vector are in the finite field $\mathbb{F}_{q^m}$. Let $\mathbb{F}_q^{m\times N}$ denote the set of all $m \times N$ matrices over $\mathbb{F}_q$ such that $m \geq N$ and let $\mathbf{b} = \{b_1, b_2, \ldots, b_m\}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. If E and F are two subspaces of $\mathbb{F}_{q^m}^N$, then $< EF >$ denotes the subspace generated by the product of elements of E and F. If X is a matrix in $\mathbb{F}_q^{m\times N}$, the row space of a matrix X is denoted by $\langle X \rangle$.

As it has been shown in [17], the number of t-dimensional subspace of an m-dimensional vector space over $\mathbb{F}_q$ is the Gaussian coefficient calculated by

$$\begin{bmatrix} m \\ t \end{bmatrix} \triangleq \prod_{i=0}^{t-1} \frac{q^m - q^i}{q^t - q^i}. \tag{1}$$

Hence, we can deduce from (1) the number of matrices of rank t in the space $\mathbb{F}_q^{m\times N}$, which is

$$S(m,N,q,t)=\prod_{i=0}^{t-1}\frac{(q^m-q^i)(q^N-q^i)}{q^t-q^i}. \tag{2}$$

Therefore, the number of matrices of rank less than or equal to t in the space $\mathbb{F}_q^{m\times N}$ is

$$B(m,N,q,t)=\sum_{i=0}^{t}S(m,N,q,i). \tag{3}$$

Let Y_1 and Y_2 be two $m\times N$ matrices over $\mathbb{F}_q$. The row space of a matrix Y_1 is denoted by $\langle Y_1\rangle$. It means that the the space $\langle Y_1\rangle$ is generated by the rows of the matrix Y_1. Then, we have

$$\left\langle \begin{bmatrix} Y_1 \\ Y_2 \end{bmatrix} \right\rangle = \langle Y_1\rangle + \langle Y_2\rangle. \tag{4}$$

Therefore

$$\begin{aligned} rank \begin{bmatrix} Y_1 \\ Y_2 \end{bmatrix} &= dim\left(\langle Y_1\rangle + \langle Y_2\rangle\right) \\ &= rank(Y_1) + rank(Y_2) - dim(\langle Y_1\rangle \cap \langle Y_2\rangle). \end{aligned} \tag{5}$$

Definition 1. *We consider a matrix $M=(M_{ij})$ in $\mathbb{F}_q^{m\times N}$, where $m\geq N$. M is a lower triangular matrix if it verifies the following properties:*

- $M_{ii}=1$, *for* $i=1,\ldots,N$.
- $M_{ij}=0$, *for* $i,j=1,\ldots,N$ *and* $i<j$.

Let M be a lower triangular matrix in $\mathbb{F}_q^{m\times N}$. M^* denotes a matrix in $\mathbb{F}_q^{N\times N}$, where $M^*_{ij}=M_{ij}$, for $i=1,\ldots,N$ and $j=1,\ldots,N$.

The matrix M^* is invertible and we have

$$M^*=M^{*-1}_{N-1}\times M^{*-1}_{N-2}\times\cdots\times M^{*-1}_1, \tag{6}$$

where,

$$M_i^{*-1}=\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & (q-1)M^*_{i+1,i} & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & (q-1)M^*_{N,i} & 0 & 0 & \cdots & 1 \end{pmatrix}$$

Let E be a subspace of $\mathbb{F}_{q^m}$ of dimension r over $\mathbb{F}_q$. We suppose that $2r \ll m$ and we investigate the typical dimension of the subspace $E + \mathbf{u}E$. We rely on the following observation:

Proposition 1. *The probability that $E + \boldsymbol{u}E$ is of dimension $2r$ is given by*

$$\mathbb{P}(dim(E + \boldsymbol{u}E) = 2r) \approx 1 - \frac{q^{2r} - q^{r+1}}{q^m - q}.$$

Proof. Let us take a fixed r-dimensional subspace E in $\mathbb{F}_{q^m}$. Suppose that the dimension of $E + \mathbf{u}E$ is less than $2r$ for $\mathbf{u}$ randomly chosen in $\mathbb{F}_{q^m} \setminus \mathbb{F}_q$. It means that: $\exists (e_1, e_2) \in E^2$, that verifies $\mathbf{u}e_2 = e_1$. Now, we compute the number of possibilities of choosing $\mathbf{u}$ that verifies $\mathbf{u} = e_1 e_2^{-1}$, for $(e_1, e_2) \in E^2$. The number of possible values of (e_1, e_2) is q^{2r} and since $\mathbf{u}$ is not in $\mathbb{F}_q$ the case $(\alpha e, e)$ for $\alpha \in \mathbb{F}_q$ and $e \in E$ is not a possible case. Then, the number of possibilities to choose $\mathbf{u}$ that verifies $\mathbf{u} = e_1 e_2^{-1}$, for $(e_1, e_2) \in E^2$ is $q^{2r} - q^{r+1}$. The number of possible values of $\mathbf{u}$ is $q^m - q$.
In this proof we did not take into account the case when a set $\{e_1, e_2, e_1^{-1}, e_2^{-1}\}$ is in E for $e_1, e_2 \in \mathbb{F}_{q^m}$. □

Let A be a matrix in $\mathbb{F}_q^{2r \times N-k}$ and suppose that $2r \leq N - k$. By using (2), the probability that A is a full rank matrix is given by

$$\mathbb{P}(rank(A) = 2r) = \prod_{i=0}^{2r-1} (1 - q^{i-(N-k)}). \tag{7}$$

Let E be a subspace of dimension r over $\mathbb{F}_q$. Let s be a vector in $E + \mathbf{u}E$ of length $N - k$. We have the following proposition:

Proposition 2. *The probability that the subspace $\langle s \rangle$ is of dimension $2r$ over $\mathbb{F}_q$ is given by*

$$\mathbb{P}(dim(\langle s \rangle) = 2r) \approx \left(1 - \frac{q^{2r} - q^{r+1}}{q^m - q}\right) \prod_{i=0}^{2r-1} (1 - q^{i-(N-k)}).$$

Proof. Suppose that dimension of $E + \mathbf{u}E$ is $2r$ and let $\{E_1, E_2, ..., E_r, \mathbf{u}E_1, \mathbf{u}E_2, ..., \mathbf{u}E_r\}$ be a basis of $E + \mathbf{u}E$. All coefficients of the vector s are in $E + \mathbf{u}E$ by definition of s. The vector s can be written as follows:

$$s = (E_1, ..., E_r, \mathbf{u}E_1, ..., \mathbf{u}E_r) \times A,$$

where, A is a matrix in $\mathbb{F}_q^{2r \times N-k}$. Since the coefficients of s are random elements of $E + \mathbf{u}E$, the matrix A is also random. The probability that the set of all coefficients of s generates the whole

space is the probability that A is a full rank matrix. From (7), the probability that a random matrix A is full rank is $\prod_{i=0}^{2r-1}(1-q^{i-(N-k)})$. Now, the probability that $dim(E+\mathbf{u}E)=2r$ is given in the Proposition 1. □

It is interesting to remark that in practice the probability $\mathbb{P}(dim(E+\mathbf{u}E)=2r)$ decreases much more faster to 0 when $2r \ll m$. Thus, the probability that $dim(\langle s\rangle)=2r$ given in the previous proposition can be replaced by:

$$\mathbb{P}(dim(\langle s\rangle)=2r) \approx \prod_{i=0}^{2r-1}(1-q^{i-(N-k)}). \tag{8}$$

III. Rank metric

In this section, we present some concepts from rank metric coding theory. The reader is referred to [8] and [17] and references therein for further details. A brief overview of concepts relevant to this work can be found in [18]. Afterwards, we introduce Gabidulin codes and LRPC codes, and then we propose the M-LRPC decoding algorithm.

Let $\mathbf{v}$ be a vector of length N. For $i \in \{1,2,\ldots,N\}$, we have $v_i = \sum_{j=1}^{m} v_{ij}b_j$ and $\mathbf{v}$ can be interpreted as a matrix $V=(v_{ij})$ over $\mathbb{F}_q$. We define the rank weight of $\mathbf{v}$ over $\mathbb{F}_q$ as the rank of the associated matrix V denoted $rank(\mathbf{v})$. If $\mathbf{v}$ and $\mathbf{w}$ are two vectors of length N, we define $d_r(\mathbf{v},\mathbf{w})=rank(\mathbf{v}-\mathbf{w})$.The function d_r is a distance over $\mathbb{F}_{q^m}^N$ and we call it the rank distance.

Definition 2. *A rank code C of length N and dimension k over $\mathbb{F}_{q^m}$ is a subspace of dimension k of $\mathbb{F}_{q^m}^N$ equiped with the rank metric.*

Similar to the minimum Hamming distance for linear codes we define the minimum rank distance of a code C.

Definition 3. *The minimum rank distance of a code C is given by:*

$$d_r^m = min\{rank(\boldsymbol{v}) \mid \boldsymbol{v} \in C, \boldsymbol{v} \neq 0\}.$$

Definition 4. *A code C is called maximum rank distance (MRD) code, if $d_r^m = N-k+1$.*

A. The q-polynomials

The q-polynomials have been originally studied by Öre in [19]. This kind of polynomials is useful in coding theory since the determination of the q-polynomial is equivalent to finding a basis of all it roots.

Definition 5. *A q-polynomial of q-degree n in $\mathbb{F}_{q^m}$ is a polynomial of the form*

$$P(X) = p_0X + p_1X^q + \cdots + p_nX^{q^n}, \tag{9}$$

where the coefficients $p_0, p_1, \ldots, p_n$ are in $\mathbb{F}_{q^m}$ and $p_n \neq 0$.

An important property of q-polynomials is $P(\alpha X_1 + \beta X_2) = \alpha P(X_1) + \beta P(X_2)$ for all $\alpha, \beta \in \mathbb{F}_q$ and $X_1, X_2 \in \mathbb{F}_{q^m}$. Hence, any linear combination of roots of a q-polynomials is also a root.

The set of q-polynomials of coefficients in $\mathbb{F}_{q^m}$ provided with two internal laws, the addition and the composition, is a non-commutative ring with the identity element $x^{q^0} = x$. The symbolic product of two q-polynomials $P(X)$ and $Q(X)$ is defined as a composition:

$$P(X) \otimes Q(X) = P(Q(X)).$$

The main property of q-polynomial is given in the following proposition, which shows the link between a vector space and q-polynomials [19].

Proposition 3. *Let E be a subspace of $\mathbb{F}_{q^m}$ of dimension r over $\mathbb{F}_q$. The polynomial*

$$P(X) = \prod_{e \in E} (X - e)$$

is a q-polynomial. Moreover, $P(X)$ is the unique monic q-polynomial of q-degree r whose roots are all in E.

The previous proposition is the key solution for decoding rank codes. Finding the q-polynomial that has as roots errors basis is equivalent to find the error space.

We say that $P(X)$ is a right symbolic divisor of $S(X)$ if there exists a q-polynomial $Q(X)$ such that $S(X) = Q(X) \otimes P(X)$. If $P(X)$ is not a right symbolic divisor of $S(X)$ and $deg_q(P(X)) \leq deg_q(S(X))$, there exists two q-polynomials $Q(X)$ and $R(X)$ such that $S(X) = Q(X) \otimes P(X) + R(X)$ and $deg_q(R(X)) < deg_q(P(X))$.

Lemma 1. *Let $S(X)$ and $P(X)$ be two q-polynomials of coefficients in $\mathbb{F}_{q^m}$. If $P(X)$ is a classic divisor of $S(X)$, then $P(X)$ is a right symbolic divisor of $S(X)$.*

Proof. Suppose That $P(X)$ is a classic divisor of $S(X)$. Then, there exists a polynomial $\widetilde{Q}_1(X)$ such that $S(X) = \widetilde{Q}_1(X) \times P(X)$, where $\times$ is the classical product operation of two polynomials. Now, there exists two q-polynomials $Q(X)$ and $R(X)$ such that $S(X) = Q(X) \otimes P(X) + R(X)$ and

$deg_q(R(X)) < deg_q(P(X))$. One can write $Q(X) \otimes P(X) = \widetilde{Q}_2(X) \times P(X)$, where $\widetilde{Q}_2(X)$ is not necessarily a q-polynomial. Thus,

$$\widetilde{Q}_1(X) \times P(X) - \widetilde{Q}_2(X) \times P(X) = R(X).$$

Which means that $R(X)$ is a classic divisor of $P(X)$ and since $deg_q(R(X)) < deg_q(P(X))$ then $deg(R(X)) < deg(P(X))$. Therefore, $R(X) = 0$ and this completes the proof. □

Algorithm 1 The remainder of a right division [20]

Input:

$S(X), P(X)$, ▷ Two q-polynomials

Output:

$R(X)$, ▷ The remainder of the right division of $S(X)$ and $P(X)$

1: $d_S \leftarrow deg_q(S(X))$
2: $d_P \leftarrow deg_q(P(X))$
3: **while** $d_S \geq d_P$ **do**
4: $\quad S(X) \leftarrow S(X) - \frac{s_{d_S}}{p^{q^{d_S - d_P}}_{d_P}} . X^{q^{d_S - d_P}} \otimes P(X)$
5: $\quad d_S \leftarrow deg_q(S(X))$
6: **end while**
7: $R(X) \leftarrow S(X)$

One can use algorithm 1 in order to calculate the remainder of right division of two q-polynomials. The maximum number of iterations performed in the previous algorithm is $d_S - d_P + 1$.

In this work, we aim to compute the *right greatest common divisor* (RGCD) of two q-polynomials in order to recover the error basis. The following proposition shows the link between the intersection of two vector spaces and q-polynomials.

Proposition 4. *Let E and F be two subspaces in $\mathbb{F}_{q^m}$ and let $P_E(X)$ and $P_F(X)$ their associate q-polynomials. The associate q-polynomial of the intersection of E and F is $P_{E \cap F}(X) = RGCD(P_E(X), P_F(X))$.*

Proof. Using the Lemma 1 we can easily prove that $P_{E \cap F}(X)$ is a right symbolic divisor $RGCD(P_E(X), P_F(X))$. Now, if $X - a$ divides $RGCD(P_E(X), P_F(X))$, then $X - a$ divides $P_E(X)$

and $P_F(X)$. Thus, a is in E and F. Hence, the q-polynomial $X - a$ divides $P_{E\cap F}(X)$. Therefore, $RGCD(P_E(X), P_F(X))$ is a divisor of $P_{E\cap F}(X)$. This completes the proof of the proposition. □

The $RGCD(P_E(X), P_F(X))$ can be calculated using *extended euclidean algorithm* given in [21]. Suppose that one knows the q-degree of $P_{E\cap F}(X)$. The last non-zero remainder is $P_{E\cap F}(X)$ and it has q-degree equals to r.

Algorithm 2 Extended euclidean algorithm

Input:

$P_E(X), P_F(X)$, ▷ Two q-polynomials of q-degree N

r, ▷ The q-degree of $RGCD(P_E(X), P_F(X))$

Output:

$R(X)$, ▷ The $RGCD$ of $P_E(X)$ and $P_F(X)$

1: $R_0(X) \leftarrow P_E(X)$
2: $R_1(X) \leftarrow P_F(X)$
3: **while** q-degree$(R_1(X)) \neq r$ **do**
4: $\quad R_2(X) \leftarrow RDiv(R_0(X), R_1(X))$ ▷ Using algorithm 1
5: $\quad R_0(X) \leftarrow R_1(X)$
6: $\quad R_1(X) \leftarrow R_2(X)$
7: **end while**
8: $R(X) \leftarrow R_1(X)$

B. Gabidulin codes

Gabidulin codes are introduced in [17], the well-known class of MRD codes. They have been already used successfully in many applications such as cryptography [22], power-line communications [18], [23] and network coding [9].

The Gabidulin code of length N, dimension k and support $g = (g_1, g_2, \ldots, g_N)$ is the set of words obtained by evaluating q-polynomials of q-degree at most $k - 1$ at g_1, g_2 and g_N.

$$Gab(g, k, N) = \big\{(P(g_1), \ldots, P(g_N)) \mid deg_q(P) \leq k - 1\big\}.$$

The generator matrix of Gabidulin code is defined as follows

$$\mathbf{G} = \begin{bmatrix} g_1 & g_2 & \cdots & g_N \\ g_1^q & g_2^q & \cdots & g_N^q \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{q^{k-1}} & g_2^{q^{k-1}} & \cdots & g_N^{q^{k-1}} \end{bmatrix},$$

where elements $g_1, g_1, ..., g_N \in \mathbb{F}_{q^m}$ are linearly independent over $\mathbb{F}_q$.

The decoding of Gabidulin codes can be done based on q-polynomials by using modified Berlekamp-Massey algorithm [24] or extended euclidean algorithm in the non-commutative ring of q-polynomial.

C. Low Rank Parity Check codes

The LRPC code and its parity check matrix are described in the following definition.

Definition 6. *A Low Rank Parity Check code of low rank d, length N and dimension k and with a parity check matrix* $\boldsymbol{H} = (h_{ij})$ *over* $\mathbb{F}_{q^m}$ *such that the sub-vector space of* $\mathbb{F}_{q^m}$*, generated by the coefficients* h_{ij} *of the matrix* $\boldsymbol{H}$*, has dimension equals to d.*

Without loss of generality, in this article we are interested in the case $d = 2$. Let $M = (m_{ij})$ be a lower triangular matrix in $\mathbb{F}_q^{2(N-k)\times N}$ and let F be a subspace of $\mathbb{F}_{q^m}$ of dimension 2 generated by the basis $\{1, \mathbf{u}\}$. The matrix $\mathbf{H} = (h_{ij})$ is constructed such that $h_{ij} \in F$. Then, for $1 \leq i \leq N-k, 1 \leq j \leq N$, $h_{ij} = h_{ij1} + \mathbf{u}h_{ij2}$, where h_{ij1} and h_{ij2} are elements of $\mathbb{F}_q$. In order to reduce the complexity of decoding the LRPC codes, we set $h_{ij1} = m_{(2i-1),j}$ and $h_{ij2} = m_{2i,j}$, for $1 \leq i \leq N-k$ and $1 \leq j \leq N$.

Suppose that the error $(e_1, ..., e_N)$ is of weight r and e_i are elements of the error space E of dimension r generated by a basis $\{E_1, E_2, \cdots, E_r\}$. Then, all $e_i (1 \leq i \leq N)$ can be written as $e_i = \sum_{j=1}^{r} e_{ij}E_j$. Suppose that the dimension of the space $E + \mathbf{u}E$ is exactly $2r$ (see Proposition 1). It is then possible to express the system of equations $\mathbf{H}.e^T = s$ over $\mathbb{F}_{q^m}$ into system of equations over $\mathbb{F}_q$, by expressing the syndrome coordinates in the product basis $\{E_1, .., E_r, \mathbf{u}E_1, ..., \mathbf{u}E_r\}$, for $1 \leq i \leq N-k$, as follows:

$$s_i = \sum_{k=1}^{r} s_{i1k}E_k + \mathbf{u}\sum_{k=1}^{r} s_{i2k}E_k.$$

We have $\mathbf{A}_H^r.e'^T = s'$, where $e' = (e_{11}, ..., e_{1r}, e_{21}, ..., e_{nr})$ and $s' = (s_{111}, ..., s_{11r}, ..., s_{(n-k)2r})$. We have detailed the matrix A_H^r in a previous work (see [18]) and it can be calculated using the following definition:

Definition 7. *We consider a* $2(N-k)r \times nr$ *matrix* $A_H^r = (a_{ij})$*, where* $a_{u+(v-1)r+(i-1)rd,u+(j-1)r} = h_{ijv}$ *for* $1 \leq u \leq r$*,* $1 \leq i \leq N-k$*,* $1 \leq j \leq N$ *and* $1 \leq v \leq 2$*.*

The matrix A_H^r can be also defined as a function of M:

$$A_H^r = \begin{pmatrix} M_{11} & M_{12} & \cdots & M_{1N} \\ M_{21} & M_{22} & \cdots & M_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ M_{2(N-k),1} & M_{2(N-k),2} & \cdots & M_{2(N-k),N} \end{pmatrix},$$

where $M_{ij} = m_{ij} \times I_r$, for $1 \leq i \leq 2(N-k)$ and $1 \leq j \leq N$. In this case, the complexity of the inversion of the matrix A_H^r is equal to the complexity of the inversion of M, which is $O(N^2)$ in $\mathbb{F}_q$.

IV. System Model and Problem Formulation

We consider a network comprising a base station BS, s source nodes $\mathcal{S}_1, \mathcal{S}_2, ..., \mathcal{S}_s$ and a number of relay nodes. Each source node is attempting to transmit m packets to the BS through relay nodes, as illustrated in Fig. 1. To this end, the source S_i segments data into m packets

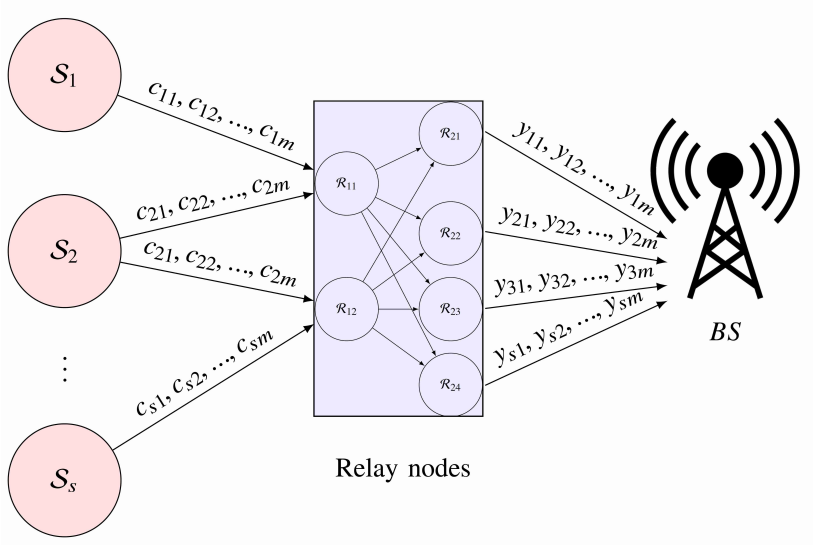


Fig. 1: System model of s sources, 6 relay nodes and BS.

$u_{i1}, u_{i2}, ..., u_{im}$ of length k , then encodes them using a rank code and transmits the coded packets to the relay nodes. Let $c_{i1}, c_{i2}, ..., c_{im}$ denote the coded packets of node $\mathcal{S}_i$. Hence, $\mathcal{S}_1, \mathcal{S}_2, ..., \mathcal{S}_s$

transmit $m \times s$ coded packets of length N to the relay nodes. Each relay node that receives the source packets employs RLNC to combine them and generates coded packets. Note that the coefficients are randomly chosen from $\mathbb{F}_q$, where q is the field size. Afterwards, relays send the generated packets to other relays until the coded packets are received by the destination BS. Let $y_{11}, y_{12}, ..., y_{sm}$ denote the received packets which can be expressed in s block matrices of size $(m \times N)$ as follows

$$Y = \begin{bmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_s \end{bmatrix}.$$

We assume that the BS has a prior knowledge of seeds used to generate the received packets such that the coding vector of each packet can be regenerated. Note that the considered network is different from the one proposed in [12], [13] and [16], since there is no direct link connecting the sources to the BS. The BS has $m \times s$ encoded packets of length N to decode. Indeed, the source packets are coded twice using rank code and RLNC. We can use LRPC code or Gabidulin code as a rank code.

We consider the application of physical layer network coding (PNC) between the relay nodes as shown in Fig. 2. Each stage of the network behaves as independent network and differently of other stages. In this model, relays $\mathcal{N}_1, \mathcal{N}_2, ..., \mathcal{N}_l$ send information to a node $\mathcal{N}$ in the next stage. We assume that all nodes are half-duplex. The first time slot corresponds to an uplink phase, in which nodes $\mathcal{N}_1, \mathcal{N}_2, ..., \mathcal{N}_l$ transmit their coded packets simultaneously to the node $\mathcal{N}$. The node $\mathcal{N}$ then constructs a network coded packet based on the simultaneously received signals from $\mathcal{N}_1, \mathcal{N}_2, ..., \mathcal{N}_l$. The second time slot corresponds to a downlink phase, in which $\mathcal{N}$ attempts to recover the original packet transmitted by $\mathcal{N}_1, \mathcal{N}_2, ..., \mathcal{N}_l$ and sends it to next stage nodes.

In the following, we focus on improving the error decoding performance of convolutional code. As shown in Fig.2, nodes $\mathcal{N}_1, \mathcal{N}_2, ..., \mathcal{N}_l$ adopt the same convolutional code with length N and k. In this paper, nodes use the same pseudo-random bit-interleaver instead of the conventional bit-interleaver to allocate the coded bits to different modulation levels. Without loss of generality, we focus on BPSK modulation. Our framework can be easily extended to higher order constellations. We assume that the power control and the synchronization at all nodes are perfect.

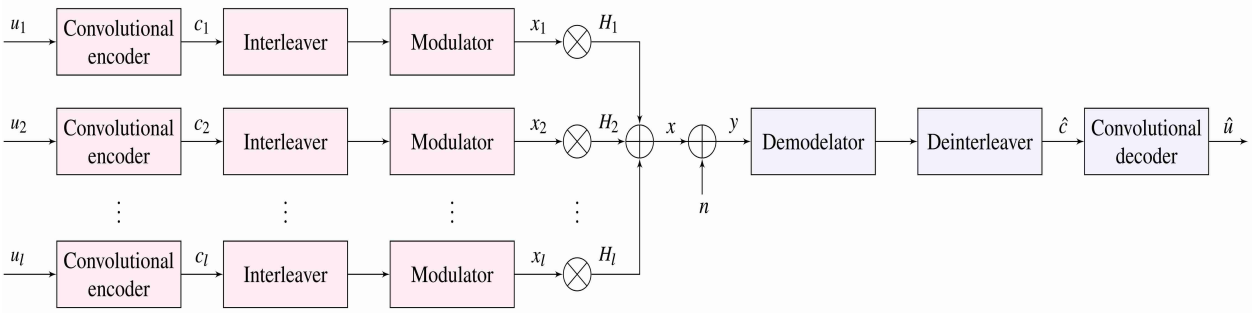


Fig. 2: System model for the inner code.

Consider transmission of l packets to the node $\mathcal{N}$. The received packet is:

$$y = (x_1H_1 + n_1) + (x_2H_2 + n_2) + \cdots + (x_lH_l + n_l), \tag{10}$$

where H_i is the channel coefficients of the channels between the node $\mathcal{N}_i$ and the node $\mathcal{N}$. It can be considered as an $N \times N$ diagonal matrix where diagonal coefficients have a Rayleigh distribution with parameter $\sigma = \sqrt{\frac{1}{2}}$. The parameter $n = n_1 + n_2 + \cdots + n_l$ represents the channel additive Gaussian noise (AWGN), where $n_1, n_2, ..., n_l$ are independent Gaussian variables with zero mean and variance $\sigma_1^2 = \sigma_2^2 = \cdots = \frac{N_0}{2}$; i.e. $n \sim \mathcal{N}(0, \frac{mN_0}{2})$.

In order to limit the impact of background noises that are caused by the nature of the wireless channel, we use a convolutional code. Each relay node verifies the integrity of the received packets. If the received packets is erroneous, the node uses convolutional decoder in order to recover the transmitted packet. However, if we combine a big number of packets the total variance of the noise increases significantly and then the convolutional decoder cannot recover the correct codeword. Also, packets generated by malicious nodes cannot be detected by the convolutional since the latter can use convolutional code too. In this case, relay node that receives the wrong packets combine them with the correct ones generating a wrong packet too. Let N_E denote the number of erroneous packets caused by the combination of a big number of received packets.

Suppose that N_E erroneous packets are injected into the network during the transmission of the $m \times s$ source packets. Since packets are randomly combined, errors may affect all the packets. Particularly, errors may affect all the packets of one source. At the BS, the packets of each source are put together in order to apply the rank decoder. By using a classical rank code, the decoding algorithm uses the information of m received packets so as to recover the source packets. For

a particular source, if N_E is bigger than m, the rank error may be bigger than the decoding capability of the rank code. Thus, the BS cannot recover the source packets.

The main idea of this paper is to use the error information of all received packets in order to recover the error basis. Then, we use the error basis in the decoding algorithm to recover packets of each source.

V. System Presentation and Analysis

A. System presentation

We now turn our attention towards the multi-source network described in Section IV. Our goal is to use a rank code at source nodes in order to maximize the decoding probability. We propose to use LRPC code to perform decoding at the BS with a high decoding probability.

Let Z denote the rank error matrix of dimension $ms \times N$ over $\mathbb{F}_q$. Z is composed of s sub-matrix Z_i, where $1 \leq i \leq s$. Equation 5 gives

$$rank(Z) = rank(Z_1) + rank \begin{bmatrix} Z_2 \\ \vdots \\ Z_s \end{bmatrix} - dim(\langle Z_1 \rangle \cap \left\langle \begin{bmatrix} Z_2 \\ \vdots \\ Z_s \end{bmatrix} \right\rangle).$$

We can deduce that if $rank(Z) = N_E$ and Z_1 verifies

$$\langle Z_1 \rangle \cap \left\langle \begin{bmatrix} Z_2 \\ \vdots \\ Z_s \end{bmatrix} \right\rangle = \{0\}, \tag{11}$$

then, the average rank of Z_1 is $\frac{N_E}{s}$. However, this case happens with a low probability. In general, because of the random combinations, the intersection (11) is not $\{0\}$. Therefore, the average rank of Z_1 is bigger than $\frac{N_E}{s}$, which means that the decoding performance of the code deteriorates.

The key idea to guarantee optimal packet decoding is to use error information that are provided by syndromes of all coded packets. For that reason, we propose modified-low rank parity check (M-LRPC) decoding algorithm (described in Algorithm 3). The principle of this algorithm is to pre-compute the error basis by using the syndromes of all coded packets, then apply the LRPC decoder.

Fig. 3 illustrates an example of decoding at the BS using the M-LRPC algorithm. $\{Y_i\}_{i=1,2,3}$ represents a set of m packets of length N, each packet is a combination of the coded packets. We start by applying the inverse of $RLNC$ matrix A_i^{-1}, used in each transmission, in order to

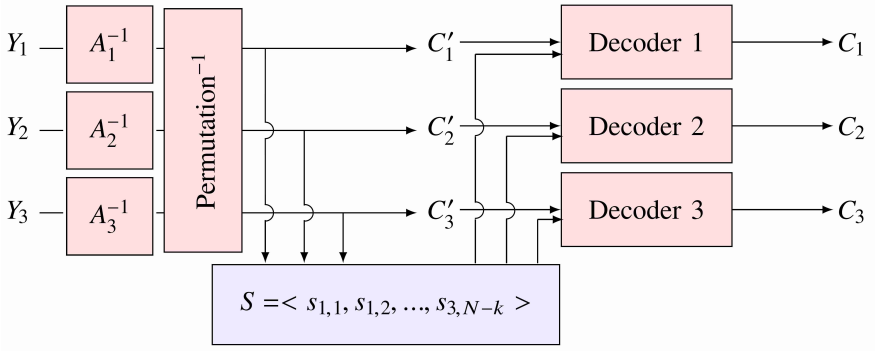


Fig. 3: Example of decoding structure at the BS using M-LRPC.

recover the coded packets. In each transmission we can use the same matrix A_i^{-1}. Afterwards, we compute the subspace S generated by syndrome coefficients of all sources and we suppose that $dim(S) = 2r$. The error basis E is given by: $E = S \cap \mathbf{u}^{-1}S$. We denote by $P(X)$ the associated q-polynomial of S. Then, the associated q-polynomial of $\mathbf{u}^{-1}.S$ is $P(u.X)$. Now, in order to recover the error basis E we can use the extended euclidean algorithm depicted in Algorithm 2.

The inverse permutation is then applied in such a way that packets of each source are put together. The final step consists of using M-LRPC algorithm in order to recover the transmitted packets of each source.

In the following, we propose M-LRPC algorithm to decode the source packets. Afterwards, we present the failure decoding probability of this algorithm.

Algorithm 3 M-LRPC decoding algorithm

Input:

$\mathbf{H}$, ▷ Parity check matrix

C', ▷ Received codeword

E, ▷ Error basis

Output:

x, ▷ Message

1: $s \leftarrow \mathbf{H}.C'^T$

2: $\{E_1, E_2, \ldots, E_r\} \leftarrow \mathbf{basis}(E)$

3: $s' \leftarrow (s_{111}, \ldots, s_{11r}, \ldots, s_{(N-k)2r})$

4: $e' \leftarrow$ **Resolve**$(A^r_{\mathbf{H}}, s')$ ▷ $A^r_H.e' = s'$

5: $(e_{11}, e_{12}, ..., e_{Nr}) \leftarrow e'$

6: **for** $i := 1$ **to** N **do**

7: $\quad e_i \leftarrow \sum_{j=1}^{r} e_{ij} E_j$

8: **end for**

9: $x \leftarrow$ **Resolve**$(G, y - e)$ ▷ $x.G = C' - e$

Note that Algorithm 3 decodes the received packets since we have assumed that $dim(S)$=$2r$. The following proposition presents the failure decoding probability of the M-LRPC decoding algorithm.

Proposition 5. *The probability that M-LRPC does not successfully recover the initial transmitted code C verifies*

$$\mathbb{P}(C' \neq C) \approx 1 - \prod_{i=0}^{2r-1} (1 - q^{i - min(m,(N-k)s)}). \tag{12}$$

Proof. We follow exactly the same reasoning as in the proof of Proposition 8.

Suppose that $m > (N-k)s$, the probability that the set s_i does not generate the whole space $E + \mathbf{u}E$ is roughly $1 - \prod_{i=0}^{2r-1} (1 - q^{i-(N-k)s})$.

Now, suppose that $m \leq (N-k)s$, the subspace S generated by s_i is at most of dimension m. The probability that S does not generate the whole space $E + \mathbf{u}E$ is roughly $1 - \prod_{i=0}^{2r-1} (1 - q^{i-m})$. □

Remark 1. *The decoding capability of the M-LRPC is* $min(m, s(N-k))/2$ *at most.*

Remark 2. *The LRPC code has random parity check matrix. Therefore, if two parity check matrices are generated by the same basis F, then they can be superposed.*

B. Theoretical Decoding Probability for M-LRPC

In this subsection, we aim at approximating the probability P_R that M-LRPC cannot recover the transmitted packets in the presence of N_E injected error packets into the network.

Let us consider the $m.s \times N$ matrix C', composed of s matrices $C'_1, C'_2, ..., C'_s$, expressed as follows

$$C'_i = A_i^{-1} \times Y_i \ ,$$

where $A_1, A_2, ..., A_s$ are $m \times m$ full-rank matrices.

Lemma 2. *We have* $rank(C') = rank(Y)$

Proof. The matrix C' can be expressed as the product of a matrix A and Y, where

$$A = \begin{pmatrix} A_1^{-1} & & & \\ & A_2^{-1} & & \\ & & \ddots & \\ & & & A_s^{-1} \end{pmatrix}.$$

A is full-rank, hence $rank(C') = rank(A \times Y) = rank(Y)$. □

The proposed model can be seen as a one-source network, with LRPC code, where the parity check matrix of the source is the superposition of matrices of s sources and the channel matrix is A (*coding-independently decoding-jointly*). This method gives us the same performance in term of decoding capability but is more complex than the M-LRPC (*coding-independently decoding-independently*).

Theorem 1. *The probability that the matrix C' is of rank r is given by*

$$\mathbb{P}(rank(C') = r) = \frac{S(m,N_E,q,r)}{q^{mN_E}}.$$

Proof. This theorem is based on equation (2) and Lemma 2. Let Y' be a matrix composed of N_E non-zero lines of Y. The probability that the matrix Y' is of rank equal to r is $\frac{S(m,N_E,q,r)}{q^{mN_E}}$. On the other hand, $rank(C') = rank(Y) = rank(Y')$. Hence, $\mathbb{P}(rank(C') = r) = \mathbb{P}(rank(Y') = r)$. □

This theorem will be used to derive the failure decoding probability P_R. Let us now consider our system model, we establish the following theorem.

Theorem 2. *The failure decoding probability for a multi-source RLNC network using M-LRPC decoding algorithm, defined by parameters q, m, N, s, r and N_E, is given by*

$$P_R(N_E) = \sum_{r=0}^{N_E} \frac{S(m,N_E,q,r)}{q^{mN_E}} \left(1 - \prod_{i=0}^{2r-1} (1 - q^{i-min(m,(N-k)s)})\right).$$

Proof. Suppose that BS receives C' and let $E = C' - C$. Denote the failure decoding of C', if E has rank r, by $C' \neq C \mid rank(E) = r$.

Using *total probability formula*, we obtain the following failure decoding probability

$$P_R(N_E) = \sum_{r=0}^{N_E} \mathbb{P}(rank(E) = r)\mathbb{P}(C' \neq C \mid rank(E) = r).$$

From Theorem 1 and Proposition 5, we deduce the result. □

VI. Numerical Results

In this section, we investigate the performance of the proposed model via simulation and compare the results of the proposed M-LRPC with the well-known Gabidulin code. First, we test the behavior of the two codes in the absence of AWGN noise and then, we evaluate the impact of background noise on both codes.

A. The comparison between Gabidulin code and the proposed M-LRPC in the absence of AWGN

We set the number of source packets to 40 and the number of source nodes to 1, 5 and 10 respectively. The source coded packets have the same length N. The relevant dimensions of the parity-check matrix are $N = 30$, $k = 15$ and $d = 2$. We use a binary phase shift keying (BPSK).

We start by illustrating the importance of the exact formulation of the decoding probability. To this end, we consider the performance of the multi-source network described in Section IV. The aforementioned theoretical characterization plays an important role in the analysis of the relay network. For the sake of simplicity, we suppose that N_E erroneous packets are injected into the network.

We use the exact expressions for the failure decoding probability given in Theorem 2 and compare the resulting values with the simulation results. Fig. 4 depicts simulated and theoretical values of the failure decoding probability P_R of the M-LRPC decoding algorithm for $m = 30$ and $m = 40$ as a function of the number of erroneous packets injected into the network for $s = 10$ sources. It can be observed that the system performance is very close to the exact formula given in Theorem 2.

Fig. 5a illustrates the failure decoding probability P_R as a function of the number of erroneous packets injected into the network for different numbers of sources and a fixed $m = 40$. It can be observed that M-LRPC has a good behavior compared to the Gabidulin code for $s = 5$ and $s = 10$. This result is somehow predictable since the M-LRPC uses error information of other sources to decode packets. Error correction capability of Gabidulin code is $\frac{N-k}{2}$. If the number of errors N_E is bigger than the error correction capability of Gabidulin code, the BS cannot recover initial messages. On the other hand, the error correction capability of M-LRPC is equal

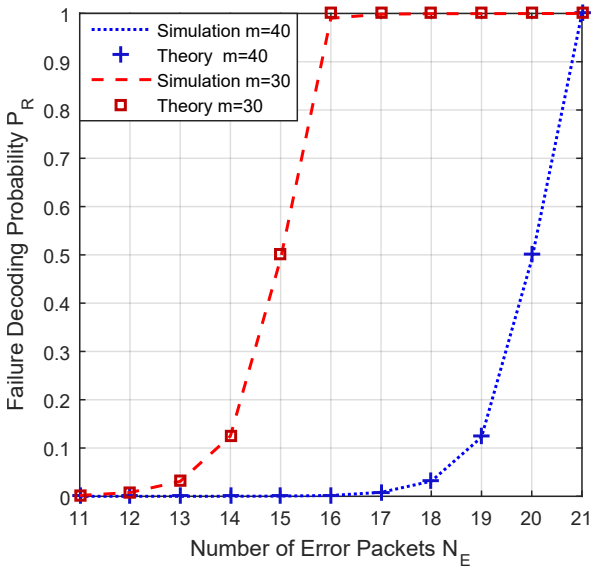
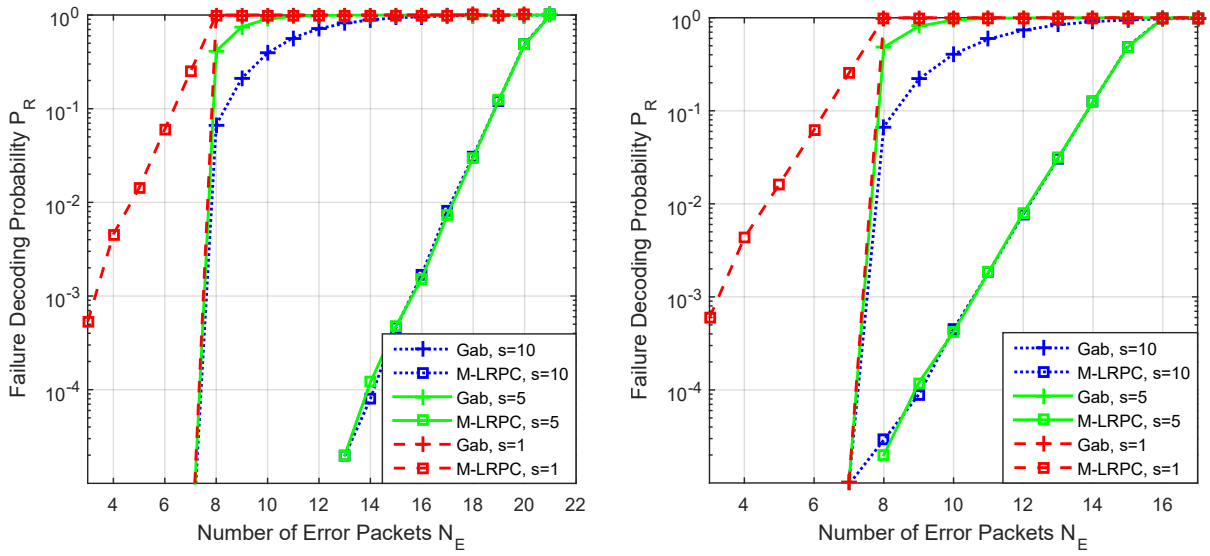


Fig. 4: Performance of M-LRPC in a multi-source network as a function N_E, for $s = 10$ and different values of m.

to $min(m, s(N-k))/2$ at most, which is 40 when $s = 5$ or $s = 10$, and 7 when $s = 1$. Note that, in the case of $s = 5$ or $s = 10$, the decoding probability increases. The performance of separate decoding of the received packets for Gabidulin code might be severely affected, which could damage the overall system performance. Finally, it can be seen that Gabidulin code is more efficient than M-LRPC in the case of one source network that because M-LRPC has the same performance as LRPC in the case of one source network. The decoding capability in that case is 7 for Gabidulin code and 7 at the most for M-LRPC.

Finally, to exploit the advantage of using a large $\mathbb{F}_q^m$ field, we assume that $m = 30$, where the decoding capability remains unchanged for Gabidulin code. The performance of M-LRPC in RLNC network is investigated for $m = 30$ in Fig. 5b. In this scenario, we compare the Gabidulin code and the M-LRPC for the same values of $s = 1$, $s = 5$ and $s = 10$. It can be observed that the decoding capability for M-LRPC deteriorates for $s = 5$ and $s = 10$, while it is not changed for $s = 1$. This can be explained by the fact that P_R depends on m for $s = 5$ and $s = 10$. For the same reason, we expect that there will be no deterioration for P_R when changing m for Gabidulin code. As it is obvious from Fig. 5b, the performance of the proposed scheme is still higher compared to Gabidulin code.



(a) $m = 40$ (b) $m = 30$

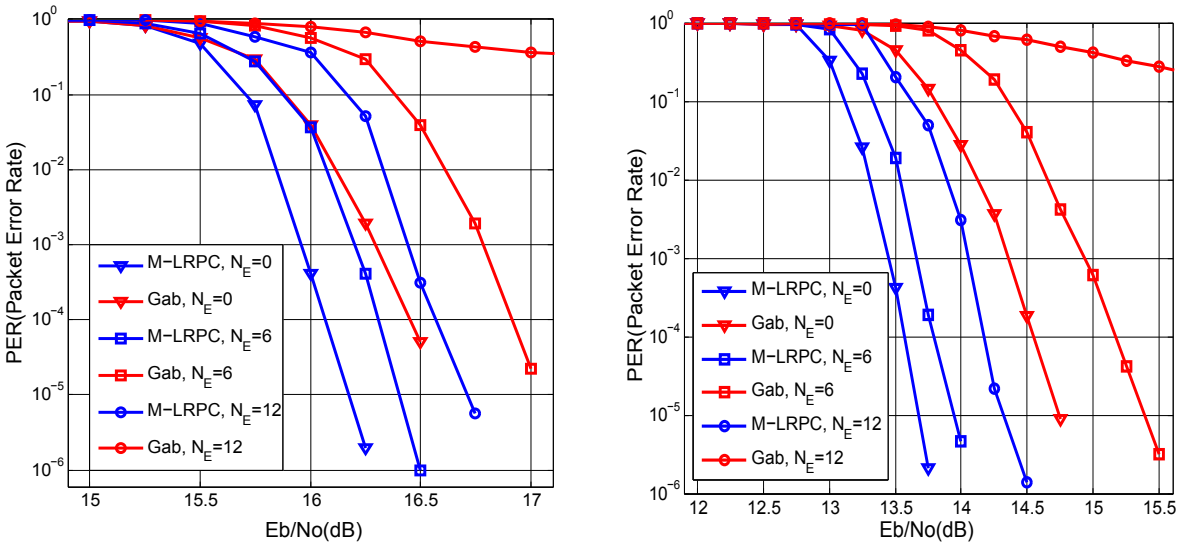
Fig. 5: Performance of M-LRPC compared to Gabidulin code in a multi-source network as a function N_E, for different values of s, $N = 30$, $k = 15$ and for $m = 40$ and $m = 30$.

B. The comparison between Gabidulin code and the proposed M-LRPC in the presence of AWGN

In the second experiment we compare the performance of the M-LRPC and Gabidulin code in the presence of additive white Gaussian noise.

We use M-LRPC and Gabidulin code as *outer code*. We fix $m = 40, k = 15, N = 30, s = 10$ and number of stages is fixed at 10. Then, the coded packets are coded again using convolutional code at the source nodes, and transmitted to the next relays. At the intermediate levels, we use the classical RLNC. At the destination node, naturally, the received packets are multiplied by A^{-1}. Then, they are decoded using M-LRPC and Gabidulin code. For convolutional encoder, with a standard $rate = \frac{1}{2}$ and $K = 7$, we use an interleaver to improve the error correction.

First, we compare M-LRPC concatenated with convolutional code with Gabidulin codes concatenated with convolutional code in the absence of rank errors $N_E = 0$. The only disturbance is the channel errors (AWGN). We add to this condition the fact that each node that receives packets x-ored them and decodes them using convolutional decoder. We can observe, in Fig. 6a, that the M-LRPC is about $0.5dB$ better than the Gabidulin. Moreover, it is about 3 dB better than the Gabidulin code at 10^{-4}. The use of a rank code does not have a beneficial contribution regards to the channel errors. This is because of the property of the white noise, each symbol has



(a) Random combination of received packets.

(b) maximum number of combinations equals to 3.

Fig. 6: Performance of M-LRPC compared to Gabidulin code in a multi-source network as a function SNR

a big probability to generate a rank error and therefore reducing the error-correction capability. Indeed, this result is predictable for M-LRPC and Gabidulin code since the rank metric codes are more efficient when the errors are confined in the rows or in the columns. This is the reason of using a convolutional code to reduce the channel errors impact. It is obvious that rank code performance varies slightly when $N_E = 6$. The performance of Gabidulin codes deteriorates significantly compared to M-LRPC when rank errors is equals to 12.

Fig. 6b shows the Packet Error Rate (PER) of the two codes as a function of SNR when nodes x-or three packets at least and decode using convolutional code. We can observe that the concatenated M-LRPC and convolutional code is about 2.5 dB better than the concatenated code in Fig. 6a. The coding gain of the concatenated M-LRPC and convolutional code code is very large compared to that of the concatenated Gabidulin and convolutional code whose performance becomes very poor when $N_E = 12$. Indeed, it becomes no longer able to efficiently correct errors; only M-LRPC-convolutional code succeed in the error recovery in this case.

VII. Conclusions

In this paper, we proposed a novel efficient decoding algorithm based on rank code concatenated with convolutional code for Random Linear Network Coding, and we have modeled the problem as a constrained multi-source network in the presence of Additive White Gaussian Noise. We have proved that the proposed approach allows the Base station to recover packets using the M-LRPC algorithm. Besides, we have derived analytically the expression of the decoding probability. Numerical results have shown that both the simulation and the theoretical expression for the decoding probability of M-LRPC are very tight and accurately predict the decoding probability at the BS. Our analysis has also exposed the clear benefits of the M-LRPC in terms of recovery accuracy compared to Gabidulin codes.

Note that at the source nodes, only simple operations are done to encode packets. The complex decoding task is achieved by BS, which does not have limited calculation capacity in contrast with the sensor nodes. At the relay nodes, only a simple convolutional code together with packet x-oring using RLNC are accomplished. Therefore the complexity at relay level are very low and acceptable for a realistic WSN.

References

[1] R. Arroyo-Valles, A. Simonetto, and G. Leus, "Consistent sensor, relay, and link selection in wireless sensor networks," *Signal Processing*, 2017.

[2] R. Ahlswede, N. Cai, S. yen Robert Li, and R. W. Yeung, "Network information flow," *IEEE TRANSACTIONS ON INFORMATION THEORY*, vol. 46, no. 4, pp. 1204–1216, 2000.

[3] T. Ho, R. Koetter, M. Medard, D. R. Karger, and M. Effros, "The benefits of coding over routing in a randomized setting," in *Information Theory, 2003. Proceedings. IEEE International Symposium on*. IEEE, Jun. 2003, pp. 442+.

[4] I. El qachchach, A. K. Yazbek, O. Habachi, J. P. Cances, and V. Meghdadi, "New concatenated code schemes for data gathering in WSN's using rank metric codes," in *2018 IEEE Wireless Communications and Networking Conference (WCNC) (IEEE WCNC 2018)*, Barcelona, Spain, Apr. 2018.

[5] A. Fiandrotti, R. Gaeta, and M. Grangetto, "Simple countermeasures to mitigate the effect of pollution attack in network coding-based peer-to-peer live streaming," *IEEE Transactions on Multimedia*, vol. 17, no. 4, pp. 562–573, April 2015.

[6] T. Ho, B. Leong, R. Koetter, M. Medard, M. Effros, and D. R. Karger, "Byzantine modification detection in multicast networks with random network coding," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2798–2803, June 2008.

[7] S. Plass, G. Richter, and A. H. Vinck, "Coding schemes for crisscross error patterns," *Wireless Personal Communications*, vol. 47, no. 1, pp. 39–49, 2008.

[8] P. Gaborit, G. Murat, O. Ruatta, and G. Zémor, "Low rank parity check codes and their application to cryptography," in *Proc. WCC*, 2013, pp. 168–180.

[9] R. Koetter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3579–3591, Aug 2008.

[10] I. El qachchach, O. Habachi, J.-P. Cances, and V. Meghdadi, "Efficient multi-source network coding using low rank parity check code," in *2018 IEEE Wireless Communications and Networking Conference (WCNC) (IEEE WCNC 2018)*, Barcelona, Spain, Apr. 2018.

[11] S. Arabi, S. Handouf, E. Sabir, and M. Sadik, "A green coalitional store-and-forward scheme for delay tolerant networks," in *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Sept 2016, pp. 1–7.

[12] A. S. Khan and I. Chatzigeorgiou, "Performance analysis of random linear network coding in two-source single-relay networks," in *Communication Workshop (ICCW), 2015 IEEE International Conference on*. IEEE, 2015, pp. 991–996.

[13] E. Tsimbalo, A. Tassi, and R. J. Piechocki, "Novel performance analysis of network coded communications in single-relay networks," in *2016 IEEE Global Communications Conference (GLOBECOM)*, Dec 2016, pp. 1–6.

[14] A. S. Khan and I. Chatzigeorgiou, "Opportunistic relaying and random linear network coding for secure and reliable communication," *IEEE Transactions on Wireless Communications*, vol. 17, no. 1, pp. 223–234, 2018.

[15] W. B. Abbas, P. Casari, and M. Zorzi, "Controlled flooding of fountain codes," *IEEE Transactions on Wireless Communications*, vol. 16, no. 7, pp. 4698–4710, 2017.

[16] S. T. Basaran, S. Gokceli, G. K. Kurt, E. Ozdemir, and E. Yaraneri, "Error performance analysis of random network coded cooperation systems," *IEEE Transactions on Wireless Communications*, vol. 16, no. 8, pp. 5325–5337, 2017.

[17] E. M. Gabidulin, "Theory of codes with maximum rank distance." *Problems of Information Transmission (English translation of Problemy Peredachi Informatsii)*, vol. 21, no. 1, 1985.

[18] A. K. Yazbek, I. EL Qachchach, J.-P. Cances, and V. Meghdadi, "Low rank parity check codes and their application in power line communications smart grid networks," *International Journal of Communication Systems*, 2017.

[19] O. Ore, "On a special class of polynomials," *Transactions of the American Mathematical Society*, vol. 35, no. 3, pp. 559–584, 1933.

[20] M. Gadouleau and Z. Yan, "Complexity of decoding gabidulin codes," in *2008 42nd Annual Conference on Information Sciences and Systems*, March 2008, pp. 1081–1085.

[21] R. Lidl, H. Niederreiter, and P. Cohn, "Encyclopedia of mathematics and its applications 20: Finite fields," 1996.

[22] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov, "Ideals over a noncommutative ring and their applications to cryptography," 1991.

[23] A. W. Kabore, V. Meghdadi, J. P. Cances, P. Gaborit, and O. Ruatta, "Performance of gabidulin codes for narrowband plc smart grid networks," in *2015 IEEE International Symposium on Power Line Communications and Its Applications (ISPLC)*, March 2015, pp. 262–267.

[24] G. Richter and S. Plass, "Fast decoding of rank-codes with rank errors and column erasures," in *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*. IEEE, 2004, pp. 398–398.