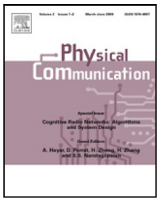
Physical Communication 39 (2020) 100975

Contents lists available at ScienceDirect

Physical Communication

journal homepage: www.elsevier.com/locate/phycom



Full length article

Index modulation aided multi carrier power line communication employing rank codes from cyclic codes

Raghavendra M.A.N.S. *, U. Shripathi Acharya

Department of Electronics and Communication Engineering, National Institute of Technology Karnataka Surathkal, India

ARTICLE INFO

Article history:
Received 12 June 2019
Received in revised form 26 October 2019
Accepted 16 December 2019
Available online 24 December 2019

Keywords:
Full rank codes
Index modulation
OFDM
Power line communication
Rank-metric
Maximum rank distance codes

ABSTRACT

In a multi-carrier power line communication (mPLC) with dominant Narrowband and Impulse noise, *crisscross* errors can be clearly observed. In this work, mPLC employing Rank codes with Index modulation (mPLC-IM) has been considered to provide a reliable high data rate communication over the powerline channel. The rank codes required for this implementation have been derived from cyclic codes over $GF(q^m)$ viewed as $m \times n$ matrices over $GF(q)$. Encoding has been performed by employing the Galois Field Fourier Transform (GFFT) domain description of cyclic codes. This scheme is able to correct a variety of *crisscross* errors in mPLC-IM The GFFT approach provides an additional degree of freedom that is offered by choice of free transform component indices. It can be used to design an index key scheme which can enhance the physical layer security of an mPLC system. In the absence of knowledge of the index key, it is observed that the probability of error reaches an error floor of $\approx 10^{-2}$, highlighting the need for index key for appropriate decoding. Further, a novel check matrix construction is proposed and used in devising a decoding strategy. It is observed that the proposed decoder is capable of correcting any errors of rank $\leq \lfloor \frac{m-1}{2} \rfloor$. In mPLC-IM with OFDM, the proposed codes over $GF(2^4)$ provide an asymptotic gain of approximately 3 dB when compared to the uncoded system. For mPLC-IM with multi-tone Frequency Shift Keying (FSK), the proposed RC over $GF(2^4)$ provides a 25% improvement in symbol error rate (SER) at lower values of p (probability of occurrence of narrowband noise) when compared to Reed-Solomon (RS) based Constant Weight (CW) $CW(13, 6, 5)_2 \circ RS[15, 14, 2]_{16}$ codes. Further, a SER improvement of around 30% is achieved using rank codes (RCs) over $GF(2^8)$ when compared with $CW(9, 4, 4)_2 \circ RS[15, 14, 2]_{16}$. In the presence of dominant background noise, the BER graphs show that the proposed codes are equivalent (slightly superior) in performance as that of Low Rank Parity Check (LRPC)/Gabidulin based designs. In the presence of dominant impulse noise, the proposed system is providing significant gain when compared with the Linearly Pre-coded Orthogonal Frequency Division Multiplexing (LP-OFDM) system and LRPC based scheme. Additionally, simulation results show that, in the absence of an index key, the probability of error reaches the error floor, highlighting the need for index key for appropriate decoding. This can be viewed as the code capable of providing an additional layer of security.

1. Introduction

Spectrum management has been of primary importance with growing demand for seamless services and connectivity. The amount of devices that are required to be connected using the wireless medium is increasing disproportionately when compared to the available spectrum. Hence there is a need to look into alternate technologies that support communication between devices. Power line communication (PLC) is one such technology that is gaining importance. It can support data transfer between devices that are connected through power lines and thus make use of existing physical infrastructure. Some of the notable examples of PLC include in-vehicular power line communication (in which devices inside vehicles can communicate through power lines of vehicles), aircraft power line communication [1,2], and smart grid & Internet of Things (IoT) [3,4]. However, the existing infrastructure of the power line, its band-limited nature and noise impairments are factors that hinder the performance and speed of communication (data rate) [3]. One possible way of achieving high speed data transfer is by transmitting information using multiple carriers (Multi-carrier PLC) [4]. In a multicarrier PLC system, information is generally communicated in 2-D arrays, where symbols along a given row are modulated onto a particular subcarrier assigned to that row. Thus at any instant of time, the

* Corresponding author.
E-mail addresses: mans.raghavendra@rediff.com (Raghavendra M.A.N.S.), sripati.acharya1@gmail.com (U. Shripathi Acharya).

https://doi.org/10.1016/j.phycom.2019.100975
1874-4907/© 2019 Elsevier B.V. All rights reserved.

$$N_b \longrightarrow \begin{bmatrix} \mathbf{e} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{e} & \mathbf{e} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{e} & 0 & 0 & 0 \end{bmatrix}$$

Fig. 1. Error Patterns due to background noise [6].

$$N_{nb} \longrightarrow \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ \mathbf{e} & \mathbf{e} & \mathbf{e} & \mathbf{e} & \mathbf{e} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \qquad N_i \longrightarrow \begin{bmatrix} 0 & 0 & 0 & 0 & \mathbf{e} \\ 0 & 0 & 0 & 0 & \mathbf{e} \\ 0 & 0 & 0 & 0 & \mathbf{e} \\ 0 & 0 & 0 & 0 & \mathbf{e} \end{bmatrix}$$

Fig. 2. Error Patterns due to narrow band noise, impulse noise and frequency selective nature of PLC channel [6].

information is conveyed using group of subcarriers. In addition, the involvement of Index modulation can achieve the same data rate by using a subset of carriers [5]. The choice of subcarriers (active) is dependent on the incoming data.

However, due to the frequency selective nature of the PLC channel, information that is transmitted through PLC using multiple carriers may get corrupted. In addition to this, the presence of narrowband noise, impulse noise and background noise, will result in additional errors induced in the received information stream [6]. Various authors have studied the effect of impairments induced by power line channel on the multicarrier transmission and have proposed models that mimic channel behaviour It has been shown that the PLC channel impairments can broadly result in two types of errors in received data: Random errors (due to background noise) and *crisscross* errors (due to narrowband noise or impulse noise).

1. *Errors due to the presence of dominant Background noise (N_b)*: These errors are also referred to as random errors. The baseband 2D error matrix pertaining to background noise is shown in Fig. 1.

   As shown in Fig. 1, the background noise disturbs the symbols randomly resulting in errors that are spread across the matrix.
2. *Errors due to the presence of dominant Narrowband noise* (N_{nb}) *or Impulse noise* (N_i)*:* These errors are classified as burst errors, and crisscross errors. The baseband 2D error matrix pertaining to narrowband noise and impulse noise is as shown

As shown in Fig. 2, impulse noise (N_i) disturbs all frequencies at a particular instant of time resulting in column errors, and narrowband noise (N_{nb}) disturbs a specific frequency or a set of frequencies resulting in row errors.

Various methods have been proposed in literature to mitigate the effects of dominant impulse noise and enhance the reliability and throughput of the PLC system. These include the use of precoded Orthogonal Frequency Division Multiplexing (OFDM) or Wavelet based OFDM (WOFDM) [7], Wavelet OFDM [8], error control codes [9,10] and crosslayer approaches [4,11].

In this work we consider the communication enhancement using error control codes that are capable of correcting errors in PLC. We observed that the use of suitable error control code (rank correcting code) can overcome errors induced by narrow band, impulse and background noise and increase the reliability of communication even under harsh channel conditions. Random errors can be corrected by employing conventional Hamming metric based random error correcting codes or convolutional codes [12]. Burst errors can be corrected using the Reed Solomon codes [9] or product codes. However, in the presence of dominant narrowband and impulse noise, that result in crisscross errors, the use of burst error correcting codes were observed to exhibit noise floor [9]. To mitigate crisscross errors and reduce the noise floor one possible solution is to employ hamming metric based product codes and a complex interleaver [13]. However it was shown that, crisscross errors can be corrected or by using codes designed with good rank distance propertied [14,15]. The use of rank metric codes in PLC eliminates the need for complex interleavers and multi-level code constructions. Further, the use of full rank codes provide additional diversity gain and enhance the reliability. The authors in [16] have analysed the performance of Gabidulin codes employed for the correction of crisscross errors in narrowband power line communications. In [12], authors have proposed the use of Low-Rank Parity Check codes (an equivalent of LDPC codes) for smart grids and proposed a check matrix based decoding algorithm for LRPC codes. To improve the performance, LRPC codes were used in concatenation with convolutional codes. The decoding is based on the construction of parity check matrix. In [11], authors proposed the use of network codes for enhancing reliability and throughput of the PLC network. The approach was similar to that of Gabidulin codes used for distributed storage. In this approach, message symbols (packets), generator matrix symbols and encoded symbols(symbols) assume values over $GF(q)$. The relay node is assumed to receive information that can help receiver decode the transmitted message in the presence of loss of symbols (packets) at the receiver.

In Gabidulin, and LRPC constructions, the codeword length n is chosen such that $n \leq m$, where m represents the order of field extension [14,17]. A method of constructing rank-distance codes over F_{q^m}, for $n \geq m$ and $n|q^m - 1$, was given by *Sripati* et al. in [18]. This approach uses the transform domain description of cyclic codes. These constructions are characterized by $n \geq m$. Unlike the constructions proposed in [12,14,15], the construction proposed in [18] has the following advantages

1. It can be used to construct full rank cyclic codes (rank equal to m), for $k > 1$ [19].
2. The choice of free transform component indices offers an additional degree of freedom, which can be used in enhancing the security of the communication.

In this work we consider the use of error control codes based on the rank metric and analyse their performance in multicarrier PLC. Design of codes over rank metric were first introduced by Gabidulin [14] in 1985.

Motivated by the use of rank codes in PLC [12,16] and considering the advantages offered by the GFFT approach of constructing (n, k) rank metric codes cyclic codes [18,19], in this work we consider the use of codes proposed in [19] at the physical layer of multicarrier PLC system employing index modulation. These codes will be designated as rank codes (RC). It can be noted that the proposed rank codes can be used for network coding in PLC with additional advantage mentioned above in point 2 [11]. However in this work the use of rank codes is confined to physical (PHY) layer. To the best of author's knowledge the rank metric based decoding strategies proposed in literature [14–20], cannot efficiently decode the RC codes. This is mainly because of the constraint $n \geq m$. This lacuna has been addressed in this paper, and a strategy for decoding rank errors in RC codes has been proposed.

The major contributions of this work are as follows:

- We have proposed an Index Modulation based Multi-carrier power line communication (mPLC-IM) system employing the proposed RC.
- A method to enhance security of the communication system has been proposed. The approach exploits additional degree of freedom offered by choice of free transform component indices.

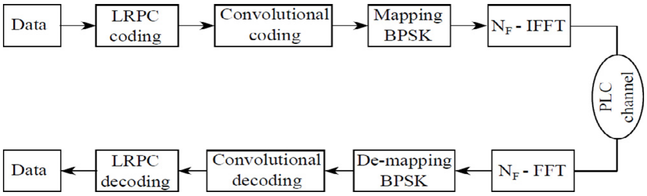


Fig. 3. Block diagram of OFDM based PLC [21].

- We have proposed a new rank-metric based decoding strategy for decoding RC codes over $GF(q^m)$ and showed that the proposed decoder can correct *crisscross* errors of rank $\le \lfloor\frac{m-1}{2}\rfloor$.

The rest of the paper has been organized as follows. Section 2 revisits the details of Power Line Communication using OFDM and Low Rank Parity Check (LRPC) codes. Section 3 discusses the construction of rank codes (RCs) over $GF(q^m)$, starting from transform domain description of cyclic codes. A brief description of the Maximum Rank distance (MRD) separable cyclic codes is provided. Later we propose a decoding strategy for these MRD codes. To derive the decoding strategy, we have first shown that every $(n, 1)$ codeword in an RC over $GF(q^m)$ has the property that the codeword elements are in geometric progression. Using this result, we have formulated a decoding strategy based on the use of the parity check matrix and provide a brief analysis of the rank error correctability of the proposed decoder. We further show that the decoder can correct *crisscross* errors of rank $\le \left\lfloor\frac{m-1}{2}\right\rfloor$. Section 4 presents the details of the proposed PLC system employing OFDM, Index Modulation, and rank-metric based cyclic codes. In Section 5 we provide details of the computational complexity of the proposed scheme. Section 6 discusses the performance of the proposed scheme in the presence of dominant background and impulse noise. We consider a 4−path frequency selective PLC channel. A fair comparison has been done with the support of RC codes over $GF(2^m)$ with $m = 4,\ 6, \&\ 8$. Section 7 concludes the work by comparing the performance of RC based schemes with conventional schemes [4,6,7,12,16] and quantifying the improvements obtained.

2. Coded PLC system with OFDM revisited

Fig. 3 shows the block diagram of the OFDM based PLC system that employ a low-rank parity check (LRPC) codes proposed by [21]. LRPC coding ensures the mitigation of crisscross errors. The input data is encoded using Rate-1/2 LRPC encoder over $GF(2)$. The LRPC coded output is encoded using convolutional coder, to mitigate the random errors due to background noise. The convolutional encoder of rate 1/2 is chosen to match the rate of LRPC encoder. The encoded symbols, which are over base field $GF(2)$, are mapped onto symbols in BPSK constellation and then passed onto 256 point IFFT module, for OFDM modulation. The OFDM modulated data is then sent through the low voltage PLC channel. At the receiver, a soft decision Viterbi decoder is used to overcome the random errors due to background noise and LRPC decoder mitigates the effect of rank errors induced by narrowband noise and Impulse Noise. We now discuss the details of the secure multicarrier PLC system proposed in this paper.

3. Preliminaries

3.1. Notions and definitions

In this paper bold and small letters denote vectors. Bold and capital letters indicate matrices.

- $\mathbf{u} = (u_0, u_1, \ldots, u_1) \rightarrow m-$ tuple data (message) vector.
- $\beta \rightarrow nth$ root of unity in $GF(q^m)$.
- For any positive integer f, $[f] = \left\{f, fq, \ldots, fq^r, \ldots, fq^s, \ldots, fq^{r+s}, \ldots, fq^{e_f-1}\right\}$ represents the $q-$ cyclotomic coset of size e_f.
- Separation between two elements fq^l and fq^{l+s} of a $q-$ cyclotomic coset of f is defined as the difference in powers of q associated with the elements fq^l and fq^{l+s},i.e. $l+s-l = s$
- $\mathscr{C} \longrightarrow$ RC over F_{q^m}
- $\mathbf{c} = (c_0, c_1, \ldots, c_{m-1}, c_m, \ldots, c_{n-2}, c_{n-1}) \in \mathscr{C}$ represents codeword vector over $GF(q^m)$. This implies that each symbol c_i, $0 \le i \le (n-1) \in GF(q^m)$
- If $c_i \in GF(q^m)$, then c_i can be represented as $m-$tuple vector over the base field $GF(q)$ as $\left(c_{i,0}, c_{i,1}, c_{i,2}, \ldots, c_{i,m-1}\right)$. For any $\mathbf{c}$ in $\mathscr{C}$, representing each element in $\mathbf{c}$ by its equivalent $m-$ tuple representation we get,

$$\boldsymbol{C} = \begin{bmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,m} & \cdots & c_{0,n-1} \\ c_{1,0} & c_{1,1} & \cdots & c_{1,m} & \cdots & c_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ c_{m-1,0} & c_{m-1,1} & \cdots & c_{m-1,m} & \cdots & c_{m-1,n-1} \end{bmatrix}$$

Here, $\boldsymbol{C}$ represent the $m\times n$ matrix over $GF(q)$, corresponding to a codeword vector $\mathbf{c} \in \mathscr{C}$.
Rank of codeword vector $\mathbf{c}$ is now defined as the rank of its corresponding codeword matrix $\mathbf{C}$

- $R_q\,(\boldsymbol{c}) \rightarrow$ rank of vector $\boldsymbol{c}$ corresponding to matrix $\boldsymbol{C}$.
- $R_q\left(\boldsymbol{c} - \mathbf{c}'\right) \rightarrow$ rank distance between any pair of codewords $\boldsymbol{c}, \boldsymbol{c}' \in \mathscr{C}$ and $\boldsymbol{c} \ne \mathbf{c}'$
- $R_q\,(\mathscr{C})$ $\rightarrow$rank of code $\mathscr{C}$ given by, $R_q\,(\mathscr{C}) = min\left\{R_q\left(\mathbf{c} - \mathbf{c}'\right),\ \forall\, \mathbf{c}, \mathbf{c}' \in \mathscr{C} : \mathbf{c} \ne \mathbf{c}'\right\}$.
- $\boldsymbol{E} \rightarrow m \times n$ error matrix corresponding to $n-$ length error vector $\boldsymbol{e}$,
- $\boldsymbol{R} = \boldsymbol{C} + \boldsymbol{E}$ denotes the received matrix corresponding to received vector $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$.
- $\boldsymbol{s}$ is the syndrome vector.
- $[\cdot]^T$ represents the transpose.
- $w_H[\cdot]$ denotes the hamming weight.

3.2. Construction of rank-metric cyclic codes

In this section we revisit the theorems used in [19]. We present theorems, that are useful in synthesizing rank codes for PLC and then use these theorems for constructing a decoding strategy that is used in correcting *crisscross* errors.

3.2.1. Transform domain description of cyclic codes

The DFT of vector $\boldsymbol{v} = \{v_i,\ 0 \le i \le n-1\}, v_i \in GF(q^m)$ is defined as [18]

$$V_\ell = \textstyle\sum_{i=0}^{n-1} v_i\beta^{-i\ell} \qquad 0 \le \ell \le n-1 \qquad (1)$$

Here β is the primitive nth root of unity in F_{q^m}. The inverse DFT (IDFT) of $\boldsymbol{V} = \{V_\ell,\ 0 \le \ell \le n-1\}$ is given by,

$$v_i = (n \bmod q)^{-1} \textstyle\sum_{\ell=0}^{n-1} V_\ell\beta^{-i\ell} \qquad 0 \le i \le n-1 \qquad (2)$$

Following usual terminology, $\boldsymbol{v} = (v_0, v_1, \ldots, v_{n-1})$ is called the time domain vector and $\boldsymbol{V} = (V_0, V_1, \ldots, V_{n-1})$ is called the DFT vector of $\mathbf{v}$.

We now state theorems pertaining to the rank-distance properties of cyclic code $\mathscr{C}$ obtained using Eq. (2).

3.3. Rank-distance properties of cyclic codes

Lemma 1 ([19]). *If a polynomial y_1 with degree of r_1 is a minimal polynomial of α_1 and polynomial y_2 with degree r_2 is the minimal polynomial of α_2, then the degree e_j of the minimal polynomial y having both α_1 and α_2 as roots is,*

- $e_j = r_1$ *if* $y_1 = y_2$
- $e_j = r_1 + r_2$ *if* $y_1 \neq y_2$.

Theorem 1 (*[19]*). *Let $\mathscr{C}$ be a cyclic code obtained using $k-$ free transform components $\{C_{j_1}, C_{j_2}, \dots, C_{j_k}\}$ with indices $j_1 \neq j_2 \neq j_3 \neq \dots \neq j_{n-1}$ and other transform components constrained to zero (transform components with other indices). If $y_{j_1}, y_{j_2}, \dots, y_{j_k}$ with degrees $r_{j_1}, r_{j_2}, \dots, r_{j_k}$ are minimal polynomials of $\beta^{j_1}, \beta^{j_2}, \dots, \beta^{j_k}$ respectively then for any vector $\mathbf{c} \in \mathscr{C}$ the set of elements from location e_j (i.e. each element of the set $\{c_{e_j}, c_{e_j+1}, \dots, c_{n-1}\}$) is a linear combination of the first e_j elements $\{c_0, c_1, \dots, c_{e_j-1}\}$.*

Theorem 2 (*[19]*). *Let $\mathscr{C}$ be a cyclic code designed using k free transform components $C_J = \{C_{j_1}, C_{j_2}, \dots, C_{j_k}\}$, with indices $J = \{j_1, j_2, \dots, j_k\}$ (The other transform domain components are explicitly set equal to zero),*

1. *If $j_1 \neq j_2 \neq \dots \neq j_k$ belong to the same cyclotomic coset $[j]_n$ of size r_j. then*

   $$R_q(\mathscr{C}) = r_j - (k-1)g$$

   Here g is chosen such that $g|\mathscr{G}_1, g|\mathscr{G}_2, \dots, g|\mathscr{G}_k, g|m$ where $\mathscr{G}_i = gcd(s_i, r_j)$, $1 \leq i \leq k$. and $GF(q^g) \subseteq GF(q^{\mathscr{G}_i})$ $1 \leq i \leq k$.
2. *If $j_i \in [j_i]_n$ of size r_{j_i}, (i.e $j_1 \in [j_1]_n$ of size r_{j_1}, $j_2 \in [j_2]_n$ of size r_{j_2} and so on) then*

   $$R_q(\mathscr{C}) = min(r_{j_1}, r_{j_2}, \dots, r_{j_k}).$$

Theorem 1 implies that if we construct code $\mathscr{C}$ using only one free transform domain component, we obtain codeword vectors $\mathbf{c} \in \mathscr{C}$ with rank at least equal to the size of cyclotomic coset from which the index of the transform domain coefficient is chosen. Theorem 2 implies that the rank of the cyclic code $\mathscr{C}$ constructed using more than one free transform domain component depends on the choice of free transform component indices. If the indices belong to the same q-cyclotomic coset of size r_j then the rank of cyclic code $\mathscr{C}$ drops to value less than r_j and if all the indices belong to different q-cyclotomic cosets then rank depends on the minimum size of the q-cyclotomic cosets from which the free transform indices are chosen. Since the maximum value of the size of a $q-$ cyclotomic coset over the field $GF(q^m)$ is m, the rank of the code $\mathscr{C}$ will be less than or equal to m depending on the choice of free transform component indices.

3.4. MRD Cyclic codes and their decoding

Following Theorems 1 and 2 we see that for full rank codes with transform domain indices chosen from different q-cyclotomic cosets of size m, the value of $e_j = km$. Since the rank error correctability of code depends on its rank distance, full rank codes that are maximum rank distance separable are desirable for communication over channels inducing *crisscross* errors. According to Theorem 2 if k free transform components are chosen from same $q-$ cyclotomic coset mod n then the codeword matrices are of dimension $e_j \times m$. If $e_j = m$, we obtain an (m, k) MRD cyclic code with $m \times m$ codeword matrices with rank at least d_R. These codes are analogous to the Gabidulin codes with a generator matrix representation as shown below.

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \beta^{-j} & \beta^{-2j} & \cdots & \beta^{-(m-1)j} \\ 1 & \beta^{-jq} & \beta^{-2jq} & \cdots & \beta^{-(m-1)jq} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta^{-jq^{(m-1)}} & \beta^{-2jq^{(m-1)}} & \cdots & \beta^{-(m-1)jq^{(m-1)}} \end{bmatrix} \tag{3}$$

The codewords of code $\mathscr{C}_p$ are obtained by multiplying the generator matrix with the corresponding transform vector, given as

$$\mathbf{c} = \mathcal{C} \times \mathbf{G} \tag{4}$$

With $\mathcal{C} = DFT(\mathbf{c}) = \{C_0, C_1, \dots, C_{m-1}\}$ and $C_i \in GF(q^m)$.

From now on we consider $\mathscr{C}_p$ over $GF(q^m)$ constructed with indices of the free transform domain components chosen from cyclotomic cosets of size $e_j = m$ (maximum size of the cyclotomic coset).

Decoding of MRD cyclic codes

In this section, we present the details of the proposed decoding strategy used for correcting burst errors or correcting *crisscross* errors. We initially discuss the details pertaining to the construction of the check matrix. Later we discuss the details of the proposed decoding based on the constructed check matrix.

Construction of Check matrix

Proposition 1. *If $\mathscr{C}$ is an RC with V_{jq^s} as the free transform component, then*

- *Any non-zero codeword vector $\mathbf{c}$ is an $n-$length geometric series with common ratio β^{-jq^s}.*

Proof. Consider Eq. (2). Eq. (2) now reduces to

$$v_i = (n \bmod q)^{-1} V_{jq^s} \beta^{-ijq^s} \qquad 0 \leq i \leq n-1 \tag{5}$$

From (5) we have vector $\boldsymbol{c}$ as,

$$\mathbf{c} = \boldsymbol{v} = \frac{1}{n \bmod q} V_{jq^s} \left(1, \beta^{-jq^s}, \beta^{-2jq^s}, \dots, \beta^{-(n-1)jq^s}\right), \tag{6}$$

where $jq^s \in [j]$.

From (6), we see that $\forall\ V_{jq^s} \in F_{q^m}$, the term $\left(1, \beta^{-jq^s}, \beta^{-2jq^s}, \dots, \beta^{-(n-1)jq^s}\right)$ on the RHS remain same and the ratio between two successive elements is β^{-jq^s}. Hence any non-zero codeword vector $\boldsymbol{c} \in \mathscr{C}$ has geometric progression with common ratio β^{-jq^s}.

From Theorems 1 and 2 we see that the first e_j elements of any codeword vector are linearly independent and the rest $n - e_j$ elements linearly depend on these e_j elements. This results in punctured codeword vectors $\mathbf{c}_p$ without altering their rank. The resulting punctured code $\mathscr{C}_p$ has same rank as $\mathscr{C}$. In case of full row rank code $\mathscr{C}$ the punctured code has codewords of dimension $m \times m$.

Check matrix for FRC MRD codes

Let $\mathbf{c}_p$ denote a codeword in $\mathscr{C}_p$ constructed using algorithm 1. Following Theorems 1, 2 and Proposition 1, if $\mathscr{C}_p$ is $(m, 1)$ then we have.

$$\begin{pmatrix} \beta^{-jq^s} & -1 & 0 & \cdots & 0 & 0 \\ 0 & \beta^{-jq^s} & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & 0 & \cdots & \beta^{-jq^s} & -1 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{e_j-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{7}$$

Since $\mathbf{H} \cdot \boldsymbol{c}^{\mathbf{T}} = \mathbf{0}$, the $m - 1 \times m$ circulant matrix on LHS of (7) can be considered as check matrix for $\mathscr{C}$

We now extend the analysis for $(m, k \geq 2)$ codes. From the definition of IFFT and Proposition 1, we see that the codewords of $(m, k \geq 2)$ can be thought of as linear combination of codewords of different $(m, 1)$ codes obtained using different free-transform domain components. For example if C_1 is $(m, 1)$ MRD obtained using transform domain component V_1 with $v_i = V_1\beta^{-j}$ and C_2 is $(m, 1)$ MRD code obtained using transform domain component V_2

with $v_i = V_2\beta^{-2j}$. Then the MRD C obtained using free transform components V_1 and V_2 with $v_i = V_1\beta^{-1j} + V_2\beta^{-2j}$ will have codewords which are linear combinations of codewords of C_1 and C_2. We now formulate the decoding strategy for proposed MRD codes using mathematical induction, we first consider the case of two free transform components and then extend to the case of k free transform components: Consider two free transform domain components, V_1, V_2, Eq. (5) becomes

$$v_i = V_1\beta^{-i} + V_2\beta^{-2i} \tag{8}$$

Let

$$v_i' = \beta^{-1}v_i - v_{i+1}, 0 \leq i \leq m-2; \tag{9}$$

Substituting for v_i and v_i, we get,

$$v_i' = \beta^{-1}\left(V_1\beta^{-i} + V_2\beta^{-2i}\right) - V_1\beta^{-i-1} - V_2\beta^{-2i-2}, 0 \leq i \leq m-2; \tag{10}$$

$$v_i' = \beta^{-1}\left(V_1\beta^{-i} + V_2\beta^{-2i}\right) - V_1\beta^{-i-1} + V_2\beta^{-2i-2}, 0 \leq i \leq m-2; \tag{11}$$

$$v_i' = V_1\beta^{-i-1} + V_2\beta^{-2i-1} - V_1\beta^{-i-1} - V_2\beta^{-2i-2}, 0 \leq i \leq m-2; \tag{12}$$

$$v_i' = V_2\beta^{-2i-1} - V_2\beta^{-2i-2}, 0 \leq i \leq m-2; \tag{13}$$

$$v_i' = V_2\beta^{-2i}\left(\beta^{-1} - \beta^{-2}\right), 0 \leq i \leq m-2; \tag{14}$$

From Eq. (14) we infer that

$$\beta^{-2}v_i' - v_{i+1}' = 0, 0 \leq i \leq m-2; \tag{15}$$

Substituting for v_i' and v_{i+1}', we get

$$\begin{aligned}&\beta^{-2}\left\{V_2\beta^{-2i}\left(\beta^{-1} - \beta^{-2}\right)\right\}\\ &\quad - \left\{V_2\beta^{-2i-2}\left(\beta^{-1} - \beta^{-2}\right)\right\} = 0, 0 \leq i \leq m-2;\end{aligned} \tag{16}$$

Expanding above equation for all values of i and expressing in terms of product of matrices we get

$$\begin{aligned}&\begin{bmatrix} \beta^{-2} & -1 & 0 & \cdots & 0 & 0 \\ 0 & \beta^{-2} & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0\cdots & \beta^{-2} & -1 \end{bmatrix}\\ &\times \begin{bmatrix} \beta^{-1} & -1 & 0 & \cdots & 0 & 0 & 0 & \\ 0 & \beta^{-1} & -1 & \cdots & 0 & 0 & 0 & \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \\ 0 & 0 & 0 & 0 & \cdots & \beta^{-1} & -1 & 0 \\ 0 & 0 & 0 & 0\cdots & 0 & \beta^{-1} & -1 & \end{bmatrix}\\ &\times \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-2} \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ 0 \end{bmatrix}\end{aligned} \tag{17}$$

The product of $m-2 \times m-1$ and $m-1 \times m$ matrix is given by

$$\begin{bmatrix} \beta^{-3} & -(\beta^{-2}+\beta^{-1}) & 1 & 0\cdots & 0 & 0 & 0 \\ 0 & \beta^{-3} & -(\beta^{-2}+\beta^{-1}) & 1\cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots\ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0\cdots & \beta^{-3} & -(\beta^{-2}+\beta^{-1}) & 1 \end{bmatrix} \tag{18}$$

In the above matrix it can be observed that the consecutive non-zero entries in each row are convolution of $\left\{\beta^{-2}, -1\right\}$ and $\left\{\beta^{-1}, -1\right\}$. In general, if cyclic code is designed by using k free transform components $\{j_1, j_2, j_3, \ldots, j_k\}$, then the non-zero entries along each row of the parity check matrix can be obtained convolving the sequences $\left\{\beta^{-j_1}, -1\right\}, \left\{\beta^{-j_2}, -1\right\}, \left\{\beta^{-j_3}, -1\right\}, \ldots, \left\{\beta^{-j_k}, -1\right\}$. Thus, the number of non-zero entries along each row of the parity check matrix is given by $2 + (k-1) * (2-1) = k+1 < n$. If $\{h_0, h_1, \ldots, h_{k-1}\}$ is the sequence obtained by convolution, then the parity check matrix is given by

$$\mathbf{H} = \begin{bmatrix} h_0 & h_1 & h_2 & h_3 & \cdots & h_k & 0 & 0 \\ 0 & h_0 & h_1 & h_2 & \cdots & h_{k-1} & h_k & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & h_{k-2} & h_{k-1} & h_k \end{bmatrix} \tag{19}$$

Thus, any codeword $\{c_0, c_1, \ldots, c_{n-1}\} \in \mathscr{C}$ satisfies

$$\begin{bmatrix} h_0 & h_1 & h_2 & h_3 & \cdots & h_k & 0 & 0 \\ 0 & h_0 & h_1 & h_2 & \cdots & h_{k-1} & h_k & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & h_{k-2} & h_{k-1} & h_k \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{m-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{20}$$

We now formulate the decoding algorithm. Since the number of rows is greater than the number of columns, there exist multiple solutions.

Decoding in rank-metric :

Let $\mathbf{R} = \mathbf{C} + \mathbf{E}$ be the received matrix with elements over $GF(q)$. Equivalently, let $\mathbf{r} = \mathbf{c} + \mathbf{e}$ be the received vector with elements over $GF(q^m)$. We now propose a decoding algorithm that can correct *crisscross* errors. The decoding strategy is based on syndrome decoding and hence decoding complexity increases exponentially with higher values of k and m. Due to the availability of high speed computation processing platforms and taking into account the data rate requirement of PLC communication, we have employed syndrome decoding strategy in this work. The decoding algorithm is given in Algorithm 1. From Eq. (20) and the decoding algorithm we can see that there exists q^{km} solutions for a particular syndrome vector $\mathbf{s}$. Out of these, we consider the solution (error pattern) possessing minimum rank as the most likely perturbing matrix. This is accepted as the error pattern actually introduced by the channel.

Algorithm 1 Decoding algorithm

```
Input: $\mathbf{R}$; Output: $\hat{\mathbf{u}}, \hat{\mathbf{e}}$
if $\mathbf{H} \cdot \mathbf{r}^T \neq 0$ then
W = $\left\{\boldsymbol{w_j} = \hat{\boldsymbol{e}}_j | \boldsymbol{H} \cdot \hat{\boldsymbol{e}}_{\boldsymbol{j}}^T = \boldsymbol{s}, 0 \leq j \leq q^{km} - 1\right\}$
    for $j$ from 0 to $q^{km} - 1$ do
        if $R_q(\boldsymbol{w_j}) \leq \lfloor \frac{m-1}{2} \rfloor$ then $\hat{\mathbf{c}} = \mathbf{r} - \mathbf{w_j}$
            if $\mathbf{H}_1 \cdot \hat{\mathbf{c}} = \mathbf{0}$ then
                $\hat{\mathbf{e}} = \mathbf{w}_j$; break
else $\hat{\mathbf{c}} = \mathbf{r}$
$\hat{\mathbf{u}} = (\hat{u}_0, \hat{u}_1, \hat{u}_2, \cdots \hat{u}_{m-1}) = \Phi^{-1}(\hat{\mathbf{c}})$
```

In the algorithm Φ denotes the mapping function that maps $m-$ length data vector to symbols in $GF(q^m)$. In the following proposition we show that the solution (error pattern) obtained by the above decoding algorithm is unique if the rank of the error pattern introduced by the channel is $R_q(\mathbf{e}) \leq \lfloor \frac{m-1}{2} \rfloor$

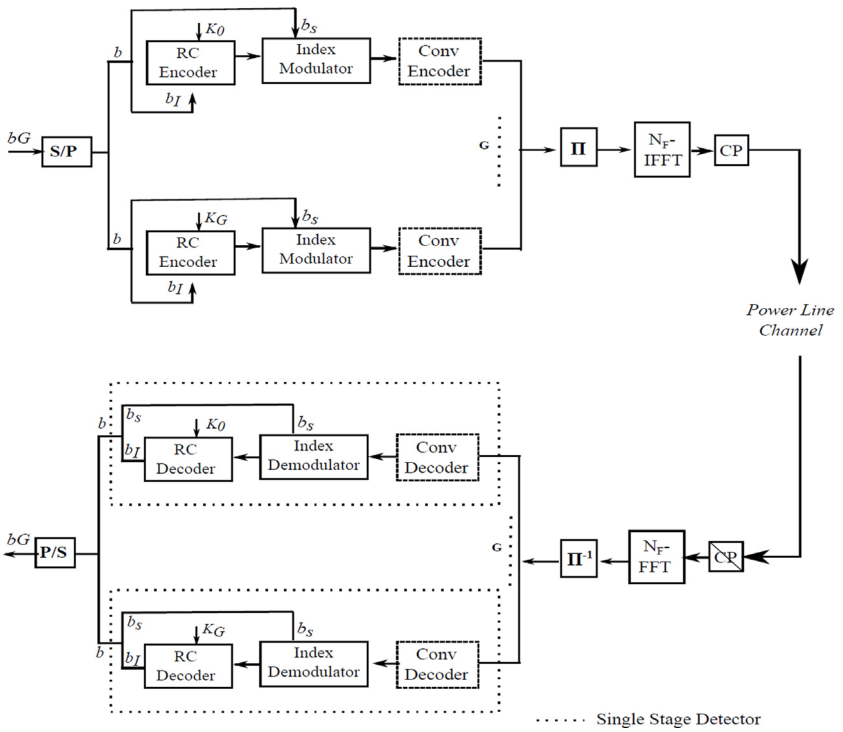


Fig. 4. Proposed Secure PLC with index modulation.

Proposition 2. *The solution of the decoding algorithm is unique if* $R_q(\mathbf{e}) \le \lfloor \frac{m-1}{2} \rfloor$

Proof. Without loss of generality let $\boldsymbol{x_1}$, $\boldsymbol{x_2}$ be two solutions of rank $\le \lfloor \frac{m-1}{2} \rfloor$ such that $\mathbf{H} \cdot (\boldsymbol{x_1}) = \mathbf{H} \cdot (\boldsymbol{x_2}) \implies \mathbf{H} \cdot (\boldsymbol{x_1} - \boldsymbol{x_2}) = 0$. This is true only if $(\boldsymbol{x_1} - \boldsymbol{x_2}) = 0$ which means $x_1 = x_2$ or $(\boldsymbol{x_1} - \boldsymbol{x_2}) \in \mathscr{C}$, thus $R_q(\boldsymbol{x_1} - \boldsymbol{x_2}) = m$. However, according to the rank inequality we have $R_q(\boldsymbol{x_1} - \boldsymbol{x_2}) \le R_q(\boldsymbol{x_1}) + R_q(\boldsymbol{x_2})$. Since $R_q(\boldsymbol{x_1}) = R_q(\boldsymbol{x_2}) \le \lfloor \frac{m-1}{2} \rfloor, R_q(\boldsymbol{x_1} - \boldsymbol{x_2}) \le 2\lfloor \frac{m-1}{2} \rfloor < m$ contradicting the condition $R_q(\boldsymbol{x_1} - \boldsymbol{x_2}) = m$. Hence $\boldsymbol{x_1} = \boldsymbol{x_2}$.

Hence the proposed decoding algorithm gives unique solution if $R_q(\mathbf{e}) \le \lfloor \frac{m-1}{2} \rfloor$. It is to be noted that the decoding is possible if and only if the receiver has knowledge of $jq^s \in [j]$ chosen at the transmitter.

4. Secure multicarrier PLC system with index modulation

4.1. Construction of index key

In Section 3, we have seen that a full rank code $\mathscr{C}_p$ can be synthesized by the appropriate choice of free transform component indices. From the definition of cyclotomic coset, we see that there are multiple choices of free transform component indices, each leading to the synthesis of a different full rank code $\mathscr{C}_p$. Using this additional degree of freedom (freedom to chose the transform component indices) the transmitter and receiver can jointly establish an arrangement to follow through the set of component codes in a particular order. This arrangement is called the index key, given by $\{\mathbf{k_0}, \mathbf{k_1}, \dots, \mathbf{k_{G-1}}\}$. To illustrate this idea we consider the following example.

Example 1. Let $n = 15$. The $2-$ cyclotomic cosets *mod* 15 are given by:

$[0]_{15} = \{0\}$,
$[1]_{15} = \{1, 2, 4, 8\}$,
$[3]_{15} = \{3, 6, 12, 9\}$,
$[5]_{15} = \{5, 10\}$
$[7]_{15} = \{7, 14, 13, 11\}$

Following case 2 of Theorem 2 we see that $(4, 1)$ cyclic codes of rank 4 can be obtained by choosing any one index from the cyclotomic cosets $[1]_{15}, [3]_{15}, [7]_{15}$. There are 12 possible choices and these choices can be used in random to construct an index key. An example index key can be given by $\{\mathbf{k_0}, \mathbf{k_1}, \dots, \mathbf{k_{11}}\} = \{\mathbf{3}, \mathbf{1}, \mathbf{7}, \mathbf{4}, \dots, \mathbf{11}, \mathbf{13}\}$.

Similar to the cryptographic keys, the level of security of communication increases with randomness in the order of selection and length of the index key. In addition to this, communication security can be enhanced by dynamically changing the key during communication.

4.2. Transmitter

The block diagram of the proposed secure multicarrier PLC system is shown in Fig. 4. Initially, the incoming bG bit stream is split into G parallel streams of length b (serial to parallel conversion). At each RC Encoder (RCE), $b_I = \lfloor m \cdot log_2(q) \rfloor$ bits out of b bits are considered to obtain codeword matrix. The remaining $b_s = \lfloor log_2 \binom{N}{m} \rfloor$ bits out of b bits are considered for subcarrier selection. The b_I information bits at the encoder are encoded into $m \times m$ RC codeword by using the appropriate value of index key element $(\mathbf{k}_i)$. The RC encoding algorithm used at branch i $(0 \le i \le G - 1)$ is as given in Algorithm 2.

Each encoder branch is assigned with $N = N_F/G$ number of subcarriers in a predetermined order. Index modulator (IM) at each branch considers the b_s selection bits to select m subcarriers out of available N subcarriers, for transmitting symbols along each column of RC codeword. To maintain constant minimum weight (CW) and improve the performance, the m carriers chosen will be the same for the entire $m \times e_j$ RC codeword. This results in $(N \times e_j)$ Index Modulated RC (Im-RC) codeword. An example

Algorithm 2 Encoding algorithm

```
Input: $\mathbf{u_i} = \left(u_{i,0}, u_{i,1}, \cdots, u_{i,b_I-1}\right)$;
        $j_i = \mathbf{k_i}$
Output: $\mathbf{C}$
Map $\Phi : (\mathbf{u_i}) \rightarrow F_{q^m}$.
Let $\left\{\begin{matrix} \mathcal{C}_{\mathscr{J}} = \Phi\left(\mathbf{u_i}\right) & \mathscr{J} = j_i \\ 0 & Otherwise \end{matrix}\right\}$.
Compute $\mathbf{c} = \mathcal{C} \times \mathbf{G}$
$\mathbf{c} = (c_0, c_1, \cdots, c_{e_j-1}) \leftrightarrow \mathbf{C} = \begin{bmatrix} c_{0,0} & \cdots & c_{0,m-1} \\ c_{1,0} & \cdots & c_{1,m-1} \\ \vdots & \ddots & \vdots \\ c_{m-1,0} & \cdots & c_{m-1,m-1} \end{bmatrix}$
```

representation of IM-RC can be given by.

$$\mathbf{C}_{IM} = \begin{bmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,m-1} \\ 0 & 0 & \cdots & 0 \\ c_{1,0} & c_{1,1} & \cdots & c_{1,m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \\ c_{N-2,0} & c_{N-2,1} & \cdots & c_{N-2,m-1} \\ c_{N-1,0} & c_{N-1,1} & \cdots & c_{N-1,m-1} \end{bmatrix} \tag{21}$$

The $N \times m$ Im-RC codeword is then fed to the convolutional encoder. The convolutional encoder (CE) considers each row of the index modulated RC and encodes the data along each row. The convolutionally encoded Im-RC is as given as

$$\mathfrak{C}_{IM} = \begin{bmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,m-1} & \cdots & c_{0,n-1} \\ 0 & 0 & \cdots & 0 & \cdots & 0 \\ c_{1,0} & c_{1,1} & \cdots & c_{1,m-1} & \cdots & c_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 \\ c_{N-2,0} & c_{N-2,1} & \cdots & c_{N-2,m-1} & \cdots & c_{N-2,n-1} \\ c_{N-1,0} & c_{N-1,1} & \cdots & c_{N-1,m-1} & \cdots & c_{N-1,n-1} \end{bmatrix} \tag{22}$$

Traditionally the input to the OFDM modulator is a sequence of symbols obtained from a two-dimensional complex number plane. However, the elements of convolutionally encoded Im-RC are over $GF(q)$ with q taking integer values. Hence, there is a need for one-to-one and onto-map to obtain a codeword with symbols over the complex plane. In case of codeword matrices over binary symbols $\{0, 1\}$ a rank preserved space time block code (STBC) can be obtained by mapping symbol 0 to -1 and mapping symbol 1 to 1. In case of codewords over non-binary symbols, two well-know rank preserving maps have been defined: Gaussian Integer map and Eisenstein–Jacobi Integer map. In this work we use codes constructed over $\mathbb{F}_{2^m}$ with codeword matrices over $GF(2)$, hence we use binary phase shift keying (BPSK) mapping. After mapping the symbols of Im-RC codeword using the rank preserving maps, the resulting Index modulated NSTBC (NSTBC-IM) codeword is given as,

$$\mathbf{X}_{IM} = \begin{bmatrix} x_{0,0} & x_{0,1} & \cdots & x_{0,m-1} & \cdots & x_{0,n-1} \\ 0 & 0 & \cdots & 0 & \cdots & 0 \\ x_{1,0} & x_{1,1} & \cdots & x_{1,m-1} & \cdots & x_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 \\ x_{N-2,0} & x_{N-2,1} & \cdots & x_{N-2,m-1} & \cdots & x_{N-2,n-1} \\ x_{N-1,0} & x_{N-1,1} & \cdots & x_{N-1,m-1} & \cdots & x_{N-1,n-1} \end{bmatrix} \tag{23}$$

Where $x_{i,j} = \zeta(c_{i,j})$; $0 \leq i \leq m-1, 0 \leq j \leq m-1$, and ζ is either Gaussian Integer map of Eisenstein-Integer map.

Each branch of the transmitter results in a corresponding $\mathbf{X}_{IM}$. Since there are G branches, $G-$ such $\mathbf{X}_{IM}$ matrices are considered by the interleaver (Π). The interleaver (Π) stacks corresponding rows of G codewords one below the other (in row dimension). Each column of the interleaved codeword S is considered as one frame. Since there are n columns, n interleaved frames are obtained. Since there are G IM-RC codewords, the dimension of S is $NG \times e_j = N_F \times e_j$. The N_F point IFFT block considers interleaved frames one by one and then outputs the corresponding OFDM frames containing complex symbols. The OFDM-IM block is represented as $\mathfrak{X}$ (collection of n OFDM-IM frames). A cyclic prefix of suitable length is padded at the end of each N length OFDM frame (column of $\mathfrak{X}$) and then transmitted through PLC channel frame by frame.

4.2.1. Rate of codes

Following [6], the rate is defined as

$$\mathcal{R} = \mathcal{R}_{IM-RC} \cdot \mathcal{R}_{conv} = \frac{G\left(log_2\left(q^{km}\right) + log_2\binom{N}{m}\right)}{m\left(N_F + N_{CP}\right)} R_{conv}$$

Here $\mathcal{R}_{IM-RC}$ represents overall rate of the RC and IM block together.

$\mathcal{R}_{conv}$ represents the rate of convolutional encoder.

4.3. Power line channel

The multipath power line channel is shown to be frequency selective with a complex frequency response given by [22,23].

$$H(f) = \sum_{i=1}^{N} g_i e^{-(\alpha_0+\alpha_1 f^{\kappa})\mathrm{D}_i} . e^{-2\pi f(\mathrm{D}_i/\mathscr{V}_i)} \tag{24}$$

Here, g_i is the weighting parameter. α_0, α_1 are the attenuation parameters. D_i is the length of ith path. $\mathscr{V}_i$ is the velocity of the wave propagating through ith path. κ is the exponent. Besides frequency selective fading (η_f), noise in the PLC channel has three main components:

- Background noise (N_b): The background noise is assumed to be additive. The effect of background noise is most commonly characterized by Nakagami-m distribution [24,25].
- Narrowband noise (N_{nb}): In case of PLC, narrowband interference is caused by ingress of signals from broadcast stations that are transmitting in Medium wave (MW), Short wave (SW) and Very High Frequency (VHF) bands. Various models have been proposed in the literature to model the effect of narrowband noise. In this work, we use the model described in [13] with narrowband interference probability p.
- Impulsive noise (N_i)- Impulse noise occurs mainly due to switching or surge in voltage. Based on the nature of the occurrence, the impulse noise can be periodic and asynchronous to mains, or periodic and synchronous to mains, or Asynchronous to mains. The most widely used channel description is Middleton class A model, with a probability density function (pdf) given by, [26,27].

$$p_\eta(v) = \sum_{k=0}^{\infty} \frac{e^{-A}A^k}{k!} \frac{1}{\sqrt{2\pi\sigma_k^2}} exp(-v^2/2\sigma_k^2) \tag{25}$$

Here, A is impulse index.
$\sigma_k^2 = \left(1 + \frac{1}{\Gamma}\right)\left(\frac{k/A+\Gamma}{1+\Gamma}\right)\sigma_b^2$ σ_b^2 is the background noise variance.
Γ is the Background to impulse noise ratio.
In this work, the value of impulse index A is chosen to be 0.3 and the value of background to impulse noise ratio Γ as 0.1.

4.4. Receiver

At the receiver, the received block matrix corresponding to OFDM-IM block $\mathfrak{X}$ is represented by $\mathbf{Y}_S$. After the removal of CP and applying FFT, the signal can be given by:

$$\mathbf{Y} = FFT(\mathbf{Y_S}) = \mathbf{H}S + N \tag{26}$$

Where N is the additive noise comprising of narrowband noise N_{nb}, background noise N_b and impulse noise N_i. $\mathbf{H}$ is the FFT of the channel matrix, given by

$$\mathbf{H} = diag(H(f_0), H(f_1), \ldots, H(f_{N_F-1})) \tag{27}$$

The effect of various noise components (N_b, N_{nb}, N_i) on the proposed codewords is as discussed in Section 1. Since FFT is a linear process, following central limit theorem and the analysis given in [28], the Noise matrix $\mathbb{N} = FFT(N_b + N_{nb} + N_i)$ will have entries following Gaussian distribution with mean $\mu = \mu_x$ and variance $\sigma^2 = \sigma/\sqrt{(N_F)}$. After the removal of CP and performing N_F point FFT, the deinterleaver rearranges the interleaved IM-RC codewords, before passing onto the Index demodulator block. The output of FFT block is a $N_F \times n$ matrix corresponding to transmitted OFDM block S. The deinterleaver & demapper block (Π^{-1}) splits the OFDM block into $G-$ $(N \times n)$ $\hat{\mathbf{X}}_{IM}$s, finds the estimate of the transmitted complex symbols, inverse maps these complex symbols to symbols over $GF(q)$ and then passes the resulting estimate $\hat{\mathfrak{C}}_{IM}$ onto the bank of convolutional decoders. The convolutional decoder considers the $(N \times n)$ $\hat{\mathfrak{C}}_{IM}$ codeword and finds an estimate of the transmitted Im-RC codeword $\hat{\mathbf{C}}$. This estimated codeword is then fed to Index Demodulator. The index demodulator considers $N \times e_j$ Im-RC matrix and uses majority logic to estimate the carrier selection bits assigned to a particular RC. The resulting $m \times m$ matrix is then fed to the proposed rank metric decoder. Following [6], the $m \times m$ matrix at the input of proposed decoder, corresponding to $m_j \times m$ RC, can be modelled using the following equation:

$$\zeta^{-1}(\mathbf{Y}) \triangleq \mathbf{R} = \mathbf{C} + E \tag{28}$$

The decoder now refers to the index key value and estimates the transmitted RC using the proposed decoder. The corresponding b_s length binary data is then estimated. At this point, it can be noted that the binary data at the output of the decoder will be a correct estimate of the corresponding binary data used at the transmitter, only if the index key value used at both encoder and corresponding decoder is same.

5. Computational complexity

In this section we present the complexity comparison of decoding in the presence and absence of index key. The decoding complexity is in terms of number of multiplications required in estimating information pertaining to one transmitted RC codeword. We consider two scenarios: (1) Receiver employing the proposed decoder. (2) Receiver employing sphere decoder. In case of the proposed decoder the computational complexity depends on the list of codewords that satisfy $\mathbf{H}.\hat{\mathbf{e}}_{\mathbf{j}}^{T} = \mathbf{s}$. In case of sphere decoding, the number of codewords in the search space depend on the sphere radius, and for the case of large radius (which includes all codewords), the complexity attains to that of ML decoding complexity.

Referring to Fig. 4 and Section 4, we have rate 1/2 convolutional encoder at the transmitter. The convolutional decoder at a particular branch outputs the estimated row of the codeword by using trellis decoding. Since the symbols of codeword are from the field $GF(2)$ for the rate $\frac{1}{2}$ convolutional code, the computation involves 2^2 multiplications per bit and there are 2 bits per branch, therefore the number of computations per bit is given by 2.2^2. If the constraint length is L_c, the number of computations per bit is 2^{3+L_c}. There are e_j bits per row of the and m rows per codeword. Thus total number of computations required to estimate the RC codeword over $GF(2)$ is $me_j2^{3+L_c}$. Since the m rows can be independently (parallel) decoded the mathematical complexity is of the order $O(2^{(3+L_c)})$. We now consider the complexity of the proposed rank metric based decoder. Referring to Algorithm 1, the first step consists of computing 2^{km} solutions with each solution requiring $(m-k)$ multiplications (since in $GF(q)$ division is considered to be multiplication with inverse). Since complexity involved in multiplication is of primary importance, the worst case computational complexity of rank decoder can be given by $O((m-k)2^{km})$. Thus the overall complexity of the decoder can be given by $O(2^{(3+L_c)}) + O((m-k)2^{km})$. At this point it can be noted that this is the maximum complexity and if the decoder can find the solution in the first attempt then the complexity can be given by $O(2^{(3+L_c)}) + O((m-k))$. Since the decoder can be implemented in a way to stop when the solution is found, the complexity is close to the minimum complexity if the errors are of minimum rank (in the presence of dominant impulse noise). From this it can be inferred that the computational complexity of the proposed decoder is proportional to the number of solutions that satisfy the syndrome equations. In the presence of dominant impulse noise, for small values of k and m, the complexity of the proposed approach is comparable to that of the approach proposed in [4] which is dependent on the number of subcarriers used and is given by $\frac{N}{m}O(Nlog_2(N))$.

Table 1
Computational complexity.

Scheme	Complexity	Order
RC (*With key*)	$\binom{N}{m}2^{km}\left(m^2e_j^2 + m^2\right)$	$\mathcal{O}(2^{km})$
RC (*Without Key*)	$\binom{L}{k}m^k\binom{N}{m}2^{km}\left(m^2e_j^2 + m^2\right)$	$\mathcal{O}(m^k2^{km})$
RC (*With proposed decoding*)	$2m^3e_j + m^2e_j^2 + 2^{km}2m^3/3$	$\mathcal{O}(2^{km}m^3)$

In case of ML decoding since $\mathbf{H}$ is of dimension $m \times me_j$ and $\mathbf{X}_d$ is of dimension $me_j \times n$, the number of complex multiplications required to compute $\mathbf{HX}_d$ is given by $m^2e_j^2$. Since $\mathbf{Y} - \mathbf{HX}_d$ is of dimension $m \times m$, the ML computation of $\|\mathbf{Y_HX}_d\|^2$ requires another m^2 complex multiplications. Total number of multiplications required in computing $Y-$ is $m^2e_j^2 + m^2$. There are $\binom{N}{m}2^{km}$ codewords. Thus, the total number of complex multiplications required in estimating one RC-IM is $\binom{N}{m}2^{km}(m^2e_j^2 + m^2)$. In the absence of index key the search space includes $\binom{L}{k}m^k2^{km}$. Thus, the total number of computations required in estimating one RC-IM in the absence of index key is $\binom{L}{k}m^k\binom{N}{m}2^{km}\left(m^2e_j^2 + m^2\right)$.

Thus we see that the order of complexity in estimating the codeword in the absence of index key is $O(\ m^k2^{km})$. As we go to higher extension fields (high value of m) and higher value of k, the complexity involved in estimating the transmitted codeword increases exponentially making it difficult for the eavesdropper to determine the estimate of the transmitted code word in real time because he does not possess knowledge of the index key.

As can be seen from Table 1, in case of ML decoding the knowledge of index key at the receiver helps the decoder to search right code space and also reduces the search space. At the same time, absence of index key increases the search space, and can reduce the performance of the PLC system. In the case of proposed decoder, the number of computations required in estimating the transmitted information is less if the index key is known at the receiver. In addition to this the absence of index key leads to incorrect decoding as discussed in Section 4.

Table 2
Parameters of 4-path model.

Attenuation parameters					
k=1		$\alpha_0 = 0$			$\alpha_1 = 7.8\ \times 10^{-8}$ m/s
Path parameters					
i	g_i	D_i/m	i	g_i	D_i/m
1	0.64	200	3	−0.15	244.8
2	0.38	222.4	4	0.05	267.5

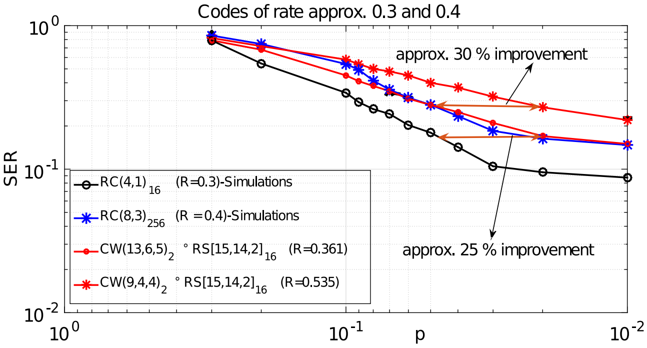


Fig. 5. SER plot of RC(R=0.4,0.5) and CCW(R =0.361,0.535) codes.

Additionally, from Table 1 it can be observed that the complexity becomes significantly with increase in k, making the proposed approach suitable for multicast scenarios only in case of lower dimension codes over lower extension fields). Thus, for PLC multicast scenarios the proposed approach has significantly high complexity when compared with the approach given in [4]. However, the proposed approach facilitates multi user communication through PLC network by providing additional physical layer security.

6. Simulation results

For simulations, we have considered 4-path PLC channel with the parameters given in Table 2. Further, we have considered RC(n, k) over $GF(2^4)$ and $GF(2^8)$, a 4-path PLC model with channel coefficients given in Table 2. Moreover, we have considered OFDM modulation with the number of data sub-carriers as $N_F = 512$. Each branch at the transmitter is assigned with 8 or 16 carriers based on the RC code used.

In the presence of dominant narrowband noise and Impulse noise, the errors are considered to follow crisscross patterns [6, 12] as shown in Fig. 2. In [6], Chee et al. proposed the use of matrix codes for correcting crisscross errors in multitone power line communication. To understand the crisscross error correction capability of the proposed RC codes and also to have a fair comparison with the existing results [6,12], initially, we have considered the simulation of the proposed system by employing only the proposed rank-metric cyclic codes and decoding (i.e. in the absence of convolutional encoder and decoder). The proposed codes are compared with constant column weight (CCW) codes proposed by Chee et al.. Table 3 gives rate comparisons of the proposed codes with the existing CCW codes. Fig. 5 shows the BER performance of the proposed RC(4,1)$_{16}$, RC(8,3)$_{256}$ codes. From the figure, we infer that RC(4,1)$_{16}$ gives approx. 25% improvement in symbol error rate (SER) as compared to $CW(13, 6, 5)_2 \circ RS[15, 14, 2]_{16}$ [6]. Further, the proposed RC(8, 3) codes provide an improvement by about 30%, as compared to $CW(9, 4, 4)_2 \circ RS[15, 14, 2]_{16}$ codes. Table 3. gives the comparison of rates of codes used in Multitone FSK based PLC [6].

Table 3
Comparison of rates of RC and CCW codes.

Code	N	m	$\mathcal{R}$
CW$(13, 6, 5)_2 \circ$ RS$[15, 14, 2]_{16}$	15	13	$log\lvert\mathbb{C}\rvert/nlog\binom{N_f}{m} = 0.36$
Im-RC$(4, 1)_{2^4}$	8	4	0.31
CW$(9, 4, 4)_2 \circ$ RS$[15, 14, 2]_{16}$	15	9	$log\lvert\mathbb{C}\rvert/nlog\binom{N_f}{m} = 0.53$
RC$(6, 3)_{2^6}$	12	6	0.50
RC$(8, 3)_{2^8}$	16	8	≈0.40

Fig. 6 shows the performance of the proposed scheme in the presence of dominant background noise, considerable narrowband noise with probability $p = 0.05$ affecting at most two rows, and impulse noise with probability $p = 0.05$. In the presence of narrowband noise, at a BER of 10^{-4} the proposed RC$(8, 3)_{2^8}$ code in concatenation with rate-1/2 convolutional code provides a gain of approx. 3 dB as compared to the case of rate-2/3 convolutional code. Further, in the case of RC$(8, 4)_{2^8}$ codes with rate-1/3 convolutional code, an additional gain of 0.8 dB is achieved when compared to RC(8, 3) codes. When compared with the Linearly precoded OFDM/ wavelet OFDM (WOFDM) scheme [7], the proposed technique provided significant gain due to the presence of error control codes for both background errors and crisscross errors. In comparison with the performance of Reed Solomon (RS) coded binary frequency shift keying (BFSK), the proposed RC-with rate 2/3 convolutional codes is observed to provide gain of approximately 2dB due to the presence of convolutional code and rank error correcting capability of RC codes. Additionally, it can be seen that in the absence of the exact knowledge of the index key at the receiver, the performance reaches the error floor at a BER of approximately 1×10^{-2}. Thus, the use of the index key provides an additional layer of security. Moreover, when compared with the existing LRPC/Gabidulin based design with rate-1/2 convolutional code, the performance of the proposed scheme is observed to be slightly better. In terms of complexity, the computations required by the constructions in [12,16] are over the Galois field $GF(2^{46})$ whereas our constructions are based on computations over the Galois field $GF(2^8)$. This brings about a significant reduction in the complexity of the encoding and decoding operations. Thus, these codes provide equivalent (slightly better) performance with significantly reduced computational complexity.

Fig. 7 shows the bit error rate (BER) performance of the proposed scheme in case of dominant background noise with narrowband noise (N_{nb}) affecting one, two and three rows with probability $p = 0.05$ and with impulse noise characterized by probability $p = 0.05$. It can be observed that the performance offered by the proposed scheme is similar to LRPC in both cases. However, for appropriate decoding, the proposed codes require knowledge of index key at the receiver, as seen from Fig. 7. Additionally, the proposed approach considers codes over $GF(2^8)$ where as the LRPC codes are constructed over $\mathbb{F}_{2^46}$.

To illustrate the performance of proposed codes in terms of Euclidean distance metric we have evaluated the performance of the proposed scheme (without convolutional codes) in the presence of dominant background noise. In Fig. 8 we have shown the performance of the proposed system in the presence of dominant random errors due to background noise, narrowband noise affecting three rows with probability $p = 0.05$, and impulse noise affecting columns with probability $p = 0.05$. The decoder is a Single stage ML decoder or Sphere decoder. It can be observed that the BER curve for sphere radius $r = 10$ is similar to that of ML decoding. Further, it can be observed that the performance of a single stage ML/Sphere decoder is inferior as compared to two-stage decoding (Figs. 6 and 7), because of the presence of rank errors and background errors. In the presence of errors with rank $< \lfloor m - 1/2 \rfloor$, but spread across all rows of the transmitted

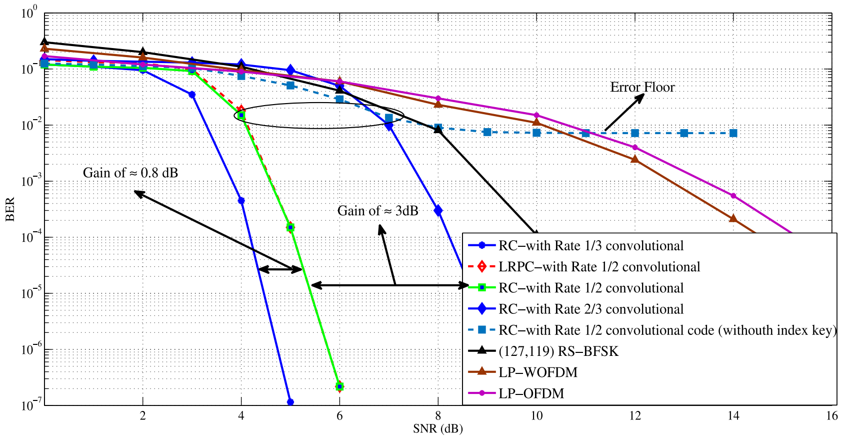


Fig. 6. BER plot of RC-Conv. codes over $GF(2^8)$ and LRPC/Gabidulin-Conv. codes.

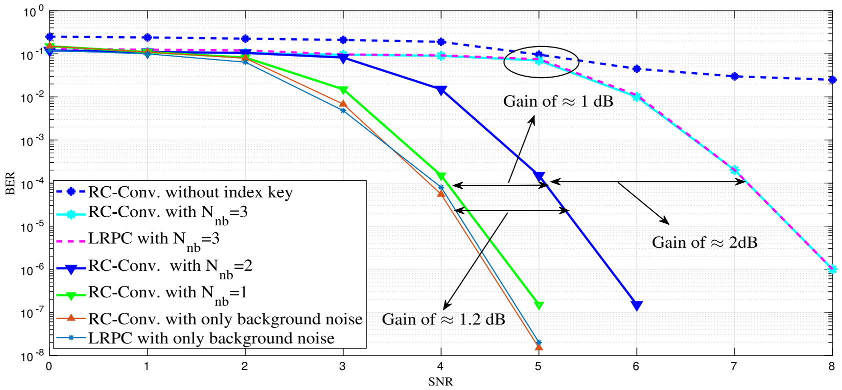


Fig. 7. BER plot of RC-Conv. codes and LRPC/Gabidulin-Conv. codes fro various values of N_{nb}.

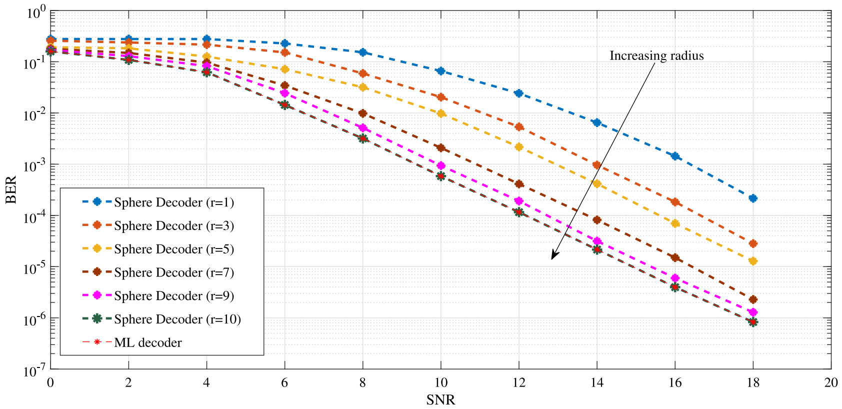


Fig. 8. BER performance of proposed RC-codes in the presence of dominant background noise.

codeword, the proposed rank decoder can still decode without any error, however, the ML decoder can result in the wrong estimate as the decision metric is Euclidean distance and not rank distance, and the search space all possible Im-RC codewords, as evident from Fig. 8.

7. Conclusion

In this paper, we have proposed a PLC communication scheme employing OFDM and Index modulation. The proposed scheme employs cyclic codes with desired rank distance properties for correcting crisscross errors. Also convolutional codes are used in concatenation with the rank codes, for correcting random background errors. We have designed a rank-metric based decoding strategy for correcting *crisscross* errors. Error correcting capability of the proposed rank-metric decoder is discussed and is shown to correct *crisscross* errors of rank $R_q \leq \lfloor \frac{m-1}{2} \rfloor$. To correct random errors we have used Viterbi decoder. Performance of the proposed RC codes with the proposed decoding strategy is evaluated in a multicarrier power line communication system employing OFDM and Index modulation. Simulation results show that a coding gain of approximately 2dB can be achieved with RC over F_{2^8} in the presence of rank-2 errors as compared to the performance in the presence of rank three errors. Additionally, a coding gain of 1dB can be achieved by using the proposed codes with rate-1/3 convolutional code as compared to that using the rate-1/2 convolutional code. Moreover, it was shown that in the absence of index key the receiver could not decode correct information, resulting in the error floor in the BER performance. In the case of PLC with multitone FSK, symbol error rate (SER) graph shows that with RC codes an improvement of about 25%–30% in SER can be achieved when compared with CCW codes proposed by Chee et al.. Simulation results further indicate that the codes proposed in this paper offer an additional layer of security, equivalent (slightly superior) error performance and reduced computational complexity when compared with LRPC/Gabidulin codes. Further, the proposed approach offers significant SNR gain when compared with LP-OFDM/WOFDM method and RS coded BFSK method. The rank-metric codes considered in this approach can be used as network codes and it will be promising to explore the application of these codes as network codes for PLC system.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Virginie Degardin, I. Junqua, Martine Lienard, Pierre Degauque, S. Bertuol, Theoretical approach to the feasibility of power-line communication in aircrafts, IEEE Trans. Veh. Technol. 62 (3) (2013) 1362–1366.

[2] Pierre Degauque, Igor Stievano, Sergio Pignari, Virginie Degardin, Flavio Canavero, Flavia Grassi, Francisco Javier Canete, Power-line communication: Channel characterization and modeling for transportation systems, IEEE Veh. Technol. Mag. 10 (2) (2015) 28–37.

[3] Leonardo de MBA Dib, Victor Fernandes, Mateus de L. Filomeno, Moises V. Ribeiro, Hybrid PLC/wireless communication for smart grids and internet of things applications, IEEE Internet Things J. 5 (2) (2018) 655–667.

[4] Francesco Chiti, Romano Fantacci, Dania Marabissi, Andrea Tani, Performance evaluation of an efficient and reliable multicast power line communication system, IEEE J. Sel. Areas Commun. 34 (7) (2016) 1953–1964.

[5] Ertuğrul Başar, Ümit Aygölü, Erdal Panayırcı, H. Vincent Poor, Orthogonal frequency division multiplexing with index modulation, IEEE Trans. Signal Process. 61 (22) (2013) 5536–5549.

[6] Yeow Meng Chee, Han Mao Kiah, Punarbasu Purkayastha, Matrix codes and multitone frequency shift keying for power line communications, in: Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on, IEEE, 2013, pp. 2870–2874.

[7] Arsla Khan, Soo Young Shin, Linear precoded wavelet OFDM-based PLC system with overlap FDE for impulse noise mitigation, Int. J. Commun. Syst. 30 (17) (2017) e3349.

[8] Ying-Ren Chien, Hao-Chun Yu, Mitigating impulsive noise for wavelet-OFDM powerline communication, Energies 12 (8) (2019) 1567.

[9] Anirban Chattopadhyay, Kalyan Sharma, Aniruddha Chandra, Error performance of RS coded binary FSK in PLC channels with Nakagami and impulsive noise, in: 18th IEEE International Symposium on Power Line Communications and Its Applications, IEEE, 2014, pp. 184–189.

[10] Aniruddha Chandra, Anirban Chattopadhyay, Kalyan Sharma, Sanjay Dhar Roy, Bit error rate of RS coded BFSK in broadband powerline channels with background Nakagami and impulsive noise, Phys. Commun. 14 (2015) 14–23.

[11] Josu Bilbao, Pedro M. Crespo, Igor Armendariz, Muriel Medard, Network coding in the link layer for reliable narrowband powerline communications, IEEE J. Sel. Areas Commun. 34 (7) (2016) 1965–1977.

[12] Abdul Karim Yazbek, Imad E.L. Qachchach, Jean-Pierre Cances, Vahid Meghdadi, Low rank parity check codes and their application in power line communications smart grid networks, Int. J. Commun. Syst. 30 (12) (2017) e3256.

[13] Thokozani Shongwe, A.J. Han Vinck, Interleaving and nulling to combat narrow-band interference in plc standard technologies PLC G3 and PRIME, in: Power Line Communications and Its Applications (ISPLC), 2013 17th IEEE International Symposium on, IEEE, 2013, pp. 258–262.

[14] Ernest M. Gabidulin, Theory of codes with maximum rank distance, Probl. Pereda. Inf. 21 (1) (1985) 3–16.

[15] Ron M. Roth, Maximum-rank array codes and their application to crisscross error correction, IEEE Trans. Inf. Theory 37 (2) (1991) 328–336.

[16] Abraham Wendyida Kabore, Vahid Meghdadi, Jean-Pierre Cances, Philippe Gaborit, Olivier Ruatta, Performance of gabidulin codes for narrowband PLC smart grid networks, in: Power Line Communications and Its Applications (ISPLC), 2015 International Symposium on, IEEE, 2015, pp. 262–267.

[17] Pierre Loidreau, A new rank metric codes based encryption scheme, in: International Workshop on Post-Quantum Cryptography, Springer, 2017, pp. 3–17.

[18] U. Sripati, B. Sundar Rajan, On the rank distance of cyclic codes, in: Information Theory, 2003. Proceedings. IEEE International Symposium on, IEEE, 2003, p. 72.

[19] Raghavendra M.A.N.S., U. Shripathi Acharya, Non orthogonal space-frequency-block codes from cyclic codes for wireless systems employing MIMO-OFDM with index modulation, Phys. Commun. (2019).

[20] Antonia Wachter-Zeh, List decoding of crisscross error patterns, in: Information Theory (ISIT), 2014 IEEE International Symposium on, IEEE, 2014, pp. 1236–1240.

[21] Youbing Zhang, Shijie Cheng, A novel multicarrier signal transmission system over multipath channel of low-voltage power line, IEEE Trans. Power Deliv. 19 (4) (2004) 1668–1672.

[22] Manfred Zimmermann, Klaus Dostert, A multipath model for the powerline channel, IEEE Trans. Commun. 50 (4) (2002) 553–559.

[23] Masaaki Katayama, Takaya Yamazato, Hiraku Okada, A mathematical model of noise in narrowband power line communication systems, IEEE J. Sel. Areas Commun. 24 (7) (2006) 1267–1276.

[24] Aashish Mathur, Manav R. Bhatnagar, PLC performance analysis assuming BPSK modulation over Nakagami-*m* additive noise, IEEE Commun. Lett. 18 (6) (2014) 909–912.

[25] Aashish Mathur, Manav R. Bhatnagar, Bijaya K. Panigrahi, PLC performance analysis over Rayleigh fading channel under Nakagami-*m* additive noise, IEEE Commun. Lett. 18 (12) (2014) 2101–2104.

[26] Luca Di Bert, Peter Caldera, David Schwingshackl, Andrea M. Tonello, On noise modeling for power line communications, in: Power Line Communications and Its Applications (ISPLC), 2011 IEEE International Symposium on, IEEE, 2011, pp. 283–288.

[27] Gaëtan Ndo, Fabrice Labeau, Marthe Kassouf, A Markov-Middleton model for bursty impulsive noise: Modeling and receiver design, IEEE Trans. Power Deliv. 28 (4) (2013) 2317–2325.

[28] H. Meng, Y. Ll Guan, S. Chen, Modeling and analysis of noise effects on broadband power-line communications, IEEE Trans. Power Deliv. 20 (2) (2005) 630–637.

Raghavendra M.A.N.S. (S16) received his M.Tech degree in Communication Engineering from the National Institute of Technology Karnataka (N I T K) Surathkal, India in 2013. He was involved in Secure Turbulence Resistant Free Space Optical FSO links for Broadband Wireless Access Networks project funded by Department of Information Technology India, and Uncoordinated Secure and Energy Aware Access in Distributed Wireless Networks project which was sponsored by Information Technology Research Academy (ITRA) Media Lab Asia. Currently he is a Research scholar in the Department of Electronics and Communication Engineering, National Institute of Technology Karnataka, India. His areas of interest are: Free Space Optic communications, Error control coding and MIMO Wireless communications.

U. Shripathi Acharya (aka U Sripati Acharya) (M'16) is a professor in the Department of Electronics and Communication Engineering, National Institute of Technology Karnataka (N I T K) Surathkal, India. He obtained his Bachelor's and Master's degrees in Electronics and Communication Engineering from Mangalore University in 1989 and 1992 respectively. He obtained his Ph.D degree from the Indian Institute of Science in the area of Error Control Coding in 2005. He has been working with N I T K, Surathkal since 1995. His areas of interest are Error control coding, Wireless Communication (both RF and Optical) and Alternate Energy systems. He has taught courses in Analog and Digital Communication Systems, Mathematical Foundations for Communication Engineering, Error Control Coding, Antennas and Radiating Systems, Electromagnetic Waves, RF circuits and Systems, Detection and Estimation theory and MIMO Wireless Communications. He has completed two major projects supported by agencies of Government of India and has handled a number of consultancy assignments from Public Sector banks and Konkan Railways, India.