CYCLIC CODES RECONSTRUCTION FROM UNSYNCHRONIZED BITSREAM WITH GAUSSIAN NOISE

[1]A. SUBHASH DEEPTHI, [2]E. V. NARAYANA
Dept of ECE, University College of Engineering Kakinada, JNTU-K, AP, India.

Abstract: **A solution to blind reconstruction of binary cyclic codes is proposed here. Here we consider the problem of finding unknown length of channel codes from unsynchronized bit stream. For this we identify the correct synchronization, length and factors of the generator polynomial of the code. Towards this we study the distribution of the syndromes of the received polynomials with respect to a candidate factors of the generator polynomial. Also we prove that the probability of zero syndrome is maximum. Using this result the problem of blind reconstruction of cyclic codes is formulated and solved as a hypothesis testing problem. In this paper MATLAB15.0 is used.**

Index Terms**- blind reconstruction, candidate factor, channel codes, cyclic codes**

I. INTRODUCTION

In most cases of digital communications, forward error correcting coding is used to protect the transmitted information against noisy channels to reduce errors which occur during transmission. Cyclic codes are one class of the most important error-correcting codes applied in communication area. The problem of identifying the channel codes from the received sequence of noise affected code words is known as the blind reconstruction of channel codes [1], [2]. Cyclic code is a block code, where the circular shift of each code word gives another code word that belongs to the code. If the location of the code word boundaries is not known then it is called as unsynchronized bit stream. Additive white Gaussian noise is a basic noise model used in information theory to mock the effect of random process [3], [4]. In this paper, we consider a non-cooperative scenario where an eavesdropper does not have the knowledge of the underlying channel code and has access to a sequence of noise-affected code words. The aim of the eavesdropper is to identify the channel code that has generated this sequence (see Fig. 1). This problem of reconstructing the channel code corresponding to a given sequence of noise-affected code words is commonly known as blind reconstruction of channel codes [5], [6]. Blind reconstruction of channel codes can be used in military surveillance applications to identify the decoding of an adversary received data when the underlying channel code is not known. The blind reconstruction of channel codes could be used to identify the channel code.

Blind reconstruction has also been used to study the structure of DNA sequence [7].

For identifying the cyclic codes, it is sufficient to identify the length n_0 of the code and the generator polynomial g(X) that has generated the code [8].

II. SYSTEM MODEL FOR BLIND RECONSTRUCTION PROBLEM OF CHANNEL CODES

Generator polynomial g(X) is a factor of$X^{n_0} + 1$ can be factored as,

$$g(X) = \prod_{I} [f_I(X)]^{m_i}$$

Where $f_i(X)$ are irreducible factors of g(X) and mi are their respective multiplicities. Thus to find g(X) we need to find all its irreducible factors along with their multiplicities. For blind reconstruction we need to identify the boundaries of code words i.e. identify correct synchronization of the received data (see Fig. 2).

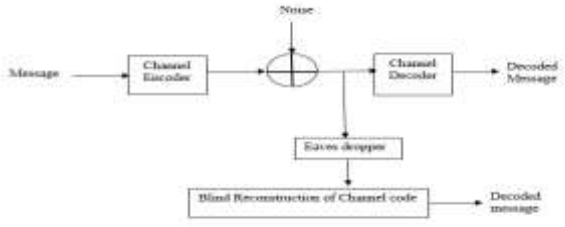

Fig 1 A System model for blind reconstruction of channel codes

Let C(n,g) be binary cyclic code of length n generated by the generator polynomial g(X).For binary cyclic codes if the code word is represented by v. The polynomial representation of $v=[v_0\ v_1 \ldots v_{n-1}]$will be $v(X)=v_0+v_1\ X+\ldots+v_{n-1}\ x^{n-1}$.Thus any code word polynomial v(X) can be written as a product of message polynomial u(X) and generator polynomial g(X), i.e., v(X) = u(X) g(X). F2 denotes the finite field with two elements 0 and 1. F2[X] denotes the polynomial ring with coefficients

from F2. The greatest integer less than or equal to n is denoted by ⌊n⌋. Let Pm denotes the set of polynomials in F2(X) of degree less than m, i.e.

$$Pm= \{f(X) \varepsilon F2(X) \mid \deg (f(X)) \leq m-1\}$$

According to this notation any code word polynomial $v(X) \varepsilon$ Pk. We assume through out that the message polynomials are uniformly distributed over Pk. For the correct length n_0 and correct synchronization s_0, each y_j (n_0, s, X) is a noise affected code word polynomial in C (n_0, g) given by

$$y_j(n_0, s_0, X) = v_j (X) + e_j(X),$$

$$= u_j(X) g (X) + e_j(X)$$

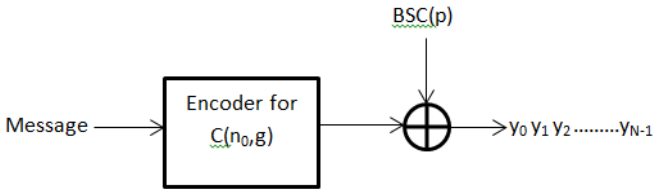

Fig 2 Synchronization of received sequence

III. RESULTS

In this section we present simulation results for the performance of the proposed method and compare it with the existing methods available in the literature for blind reconstruction of binary cyclic codes. For the simulation we generate a sequence of code words of the true cyclic codes C(n_0,g), where each code word is chosen independently with a uniform distribution. Each bit in the sequence is flipped independently with probability p, which corresponds to the crossover probability of the BSC (binary symmetric channel).

The BSC is a binary channel it can transmit only one of two symbols. It can be used to analyse the noisy channels. Many problems in communication theory can be reduced to a BSC. Conversely being able to transmit effectively over the BSC can give rise to solutions for more complicated channels. To introduce a delay or synchronization error, an integer s_0 is chosen with a uniform distribution on the set {0, 1, n_0-1} and the initial s0 bits of the sequence are ignored to obtain the received noise affected sequence $y_0, y_1, \ldots y_{N-1}$.

Let us assume the length n and synchronization $0 \leq s < n$ and consider the corresponding polynomials. For each factor f(X) of X^{n+1}, find the probability of f(X) being a factor of the received polynomials. For all possible values factors of X^{n+1} the histogram is plotted. If the plot is not uniform distribution then the assumed length and synchronization are correct. If each candidate polynomial will have an equal probability of being a factor of received polynomial, i.e., the histogram will have uniform distribution then the length and synchronization are incorrect. After finding the histogram plot the different values in the histogram is declared as factors of the generator polynomial.

A. SYNDROME DISTRIBUTION

Suppose the j th received polynomial $y_j(X)$ is given

$$y_j (X) = w_j (X) + e_j (X)$$

where $w_j(X)$ is the noise free polynomial and $e_j(X)$ is the error polynomial. The syndrome distribution for noise free polynomial is given by

$$w_j (X) \bmod f (X).$$

Syndrome distribution for noise affected received sequence is

$$y_j (X) \bmod f (X)$$

where f(X) is irreducible factor for X^{n_0+1}

B. SYNDROME CALCULATION

It can be implemented using minimal polynomials

$$r(X) = M_i (X) Q_i (X) + B_i (X)$$

where B is remainder , Q is quotient, M is divisor received code word is given by

$$r(X) = r_0+r_1 X+\ldots..+r_{n-1} X_{n-1}$$

Syndrome is given by $Si = r (\alpha^i) = r_0+r_1 \alpha^i+r_2 \alpha^{2i}+\ldots..+r_{n-1} \alpha^{n-1}$when i=2t then four syndromes can be generated S1,S2,S3,S4

Receiver example

1101001 changed to 11011101

$$\begin{array}{r} x^3+x^2+x+1 \\ x^3+x+1 \overline{)\, x^6+x^5+x^3+x^2+1} \\ \underline{x^6+x^4+x^3} \\ x^5+x^4+x^2 \\ \underline{x^5+x^3+x^2} \\ x^4+x^3+1 \\ \underline{x^4+x^2+x} \\ x^3+x^2+x+1 \\ \underline{x^3+x+1} \\ x^2 \end{array}$$

In the decoding of a linear code, the first step is to compute the syndrome $s= r \cdot H^T$, where H is the parity check matrix. If the syndrome = 0, r is a code vector and decoder accepts r as the transmitted code vector. If the syndrome ≠0, r is not a code vector and the presence of errors has been detected. The errors can be detected and corrected by syndrome table (see Fig. 3)

by using this table we can find the position of the error and correcting them.

e	e(x)	s(x)
(0000000)	0	0
(0000001)	1	1
(0000010)	x	x
(0000100)	x^2	x^2
(0001000)	x^3	x+1
(0010000)	x^4	x^2+x
(0100000)	x^5	x^2+x+1
(1000000)	x^6	x^2+1

Fig 3 Syndrome table

C. SIMULATION PARAMETERS

Mobility caching placement strategy (MCPS):

In this paper, we extend this approach by proposing a sliding-window full-duplex model allowing decisions to be taken on a sample-by- sample basis. We also derive the access-latency for both the existing and the proposed schemes. Now we are design Mobility caching placement strategy (MCPS) algorithm to transfer more no of data a time in full duplex communication (see Fig.4). The MCPS is more accuracy compared to existing technologies. And here using OFDMA methodology for long distance communication in device to device communication for both half and full duplex communication networks. No of bits-increase up to 10^5;Channel length- 64;Channel size- 64;Tx= 2 or 3;Rx=2 or 3;SNR- 25dB (see Fig. 5,Fig 6).

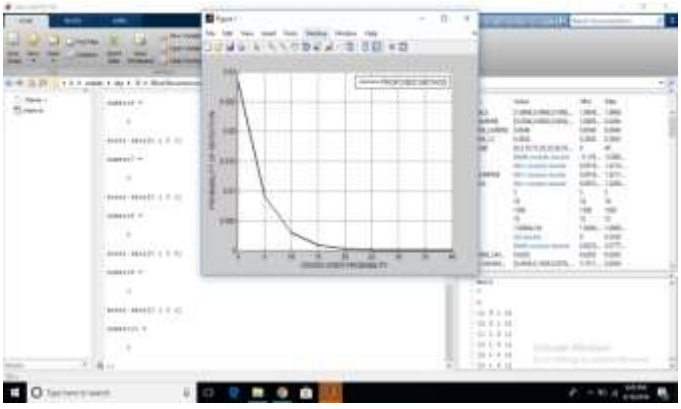

Fig 4 Plot of probability of detection (P_D) versus crossover probability (p)

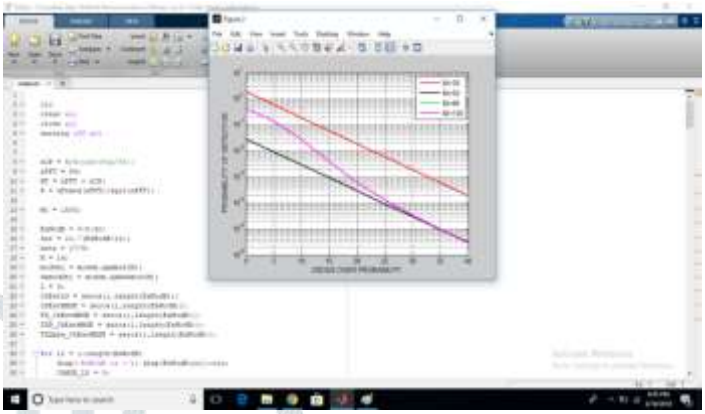

Fig 5 Performance of proposed method

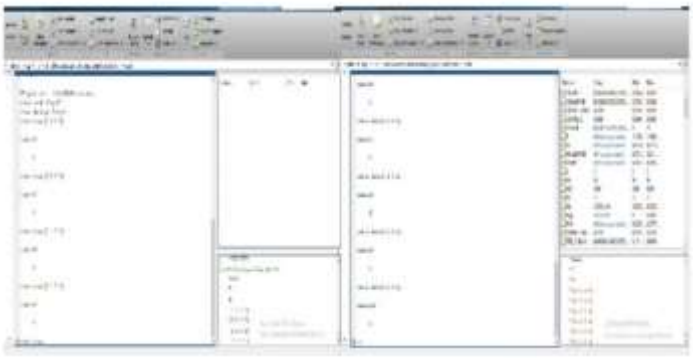

Fig 6 Performance of proposed method for C (51, g3)

IV. CONCLUSION

A solution for blind reconstruction of binary cyclic codes is proposed in this paper. It is observed that, it covers more signals to noise ratio 60db for military applications. The parameters like cross over probability, syndrome calculation, probability of detection are observed. It reconstructs the received bits up to 1000000.

V. REFERENCES

[1] G. Planquette, "Identification de trains binaires codes PhD. Thesis, Universitite de Rennes I, France, 1996.
[2] E. Filiol, "Reconstruction of convolutional encoder GF(q),"in cryptography and coding. Springer 1997, pp,101-109.
[3] A. Valembois, " Detection and recognition of a binary linear code," Discrete Applied Mathematics, vol. 111,pp.199-218, july 2001.
[4] G. Rosen , "Examining coding structure and redundancy Seattle, USA, July 2006,pp,2269-2273.

[5] M.Cluzeau, "Block code reconstruction using iterative decoding techniques, " in proceedings of IEEE ISIT,Seattle, USA, July 2006,pp,2269-2273.
[6] J. Wang, Y. Yue, and J. Yao, "Statistical Recognition method of binary BCH code."Communication and networks , vol. 3, pp.17-22- 2011.
[7] Z. Jing, H. Zhipping, L. Chunwu, S.Shaojing, and Z.Yimeng, "Information –dispersion-entropy-based Blind recognition of binary BCH codes in soft Decision situations,"Entropy, vol. 15, no. 5, pp.1705-1725, 2013.
[8] R. Moosavi and E. Larsson, " Fastblind recognition Of channel codes," IEEE Transmission Communications,vol. 62, no. 5, pp. 1393-1405,2014.