ISSN XXXX XXXX © 2016 IJESC

Research Article Volume 6 Issue No. 12

Turbo Encoding and Decoding Techniques for Secure and Reliable Data Transmission in Wireless Networks

K.Sreenivasulu[1], K.Aparna[2]
Master of technology[1], Assistant Professor[2]
JNTUA college of Engineering Pulivendula, Andhrapradesh, India

Abstract:
Turbo codes are a standout amongst the most capable sorts of superior forward error correction codes and error control codes right now available. They will be utilized later as a part of the proposition as intense building blocks in our search for better bandwidth proficient code plans. Turbo codes rose in 1993 and have subsequent to wind up a popular area of communications research. This paper gives a portrayal of three turbo codes algorithms. Soft-output Viterbi algorithm, logarithmic maximum a posteriori turbo algorithm and maximum-logarithmic-maximum a posteriori turbo decoding algorithms are the three candidates for disentangling turbo codes. . Soft-input soft-output (SISO) turbo decoder in view of soft-output Viterbi algorithm (SOVA) and the logarithmic forms of the MAP calculation, specifically, Log-MAP disentangling calculation. The bit error rate (BER) exhibitions of these calculations are analyzed.

Keywords: LOG-MAP, MAX-LOG-MAP, Turbo encoder, Threshold and MAX-LOG-MAP

I. INTRODUCTION:

The hypothesis of error revising codes has introduced countless developments with relating disentangling algorithms. Be that as it may, for applications where exceptionally solid error adjusting capabilities are required these developments all outcome in far excessively complex decoder arrangements. The way to combat this is to utilize concatenated coding, where two (or more) constituent codes are utilized after each other or as a part of parallel - usually with some sort of interleaving. The constituent codes are decoded with their individual decoders, yet the final decoded result is usually problematic. This means that better results may be achieved with a more complicated decoding algorithm - like the Brute-power attempting of all conceivable code words. In any case, concatenated coding offers a pleasant trade of between blunder rectifying capabilities and decoder many-sided quality. On the off chance that the codes are working in parallel, we don't have this additional parity. The idea of concatenated coding fits well with Shannon's channel coding hypothesis, stating that the length of we stay on the right half of the channel capacity we can rectify everything - if the code is sufficiently long. This also means that if the code is long, it doesn't have to be optimal. The length in itself gives great blunder redressing capabilities, and concatenated coding is only a way of developing - and especially unravelling - long codes.

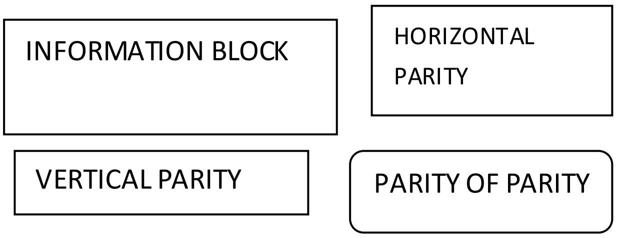


Figure.1.Concatenated Coding

II. CODING IN COMMUNICATION SYSTEM:

The main aim of any communication plans is to give blunder free data transmission. In a communication framework, information can be transmitted by analog or digital signals. At that point two distinct signals will be utilized to speak to "0" and "1" individually. As can be alluded to the accompanying illustration, the main advantage of utilizing digital signal is that errors presented by noise during transmission can be identified and potentially redressed. For communication utilizing cables, the random movement of charges in directing (e.g. resistors), known as thermal noise, is the major source of noise. For wireless communication channels, commotion can be presented in various ways. On account of mobile phones, commotion incorporates the signals sent by other mobile telephone clients in the framework.

Figure 1 shows the flow of a simple digital communication system:

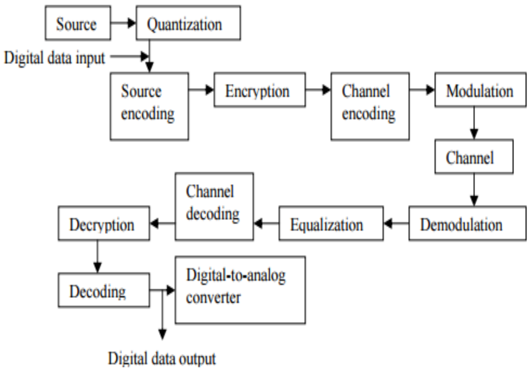


Figure 1: The flow of a simple digital communication system

Prior to this information can be transmitted to the channel, it is initially translated into a stream of bits ('0' and '1'). The procedure is called source coding. There are many generally utilized ways to translate that. For example, if ASCII code is utilized, each alphabet will be spoken to by 7-bit so called the code word. Notwithstanding, in the perspective of productive communication, the event of "Z" is not as often as that of "e" and 'a'. On the off chance that there is a way of encoding information to such an extent that the alphabets with higher probability of event are assigned with shorter code words, and more for alternate letters which from time to time turn out, then on the entire it may have the capacity to save the quantity of bits .This is what the variable length code can do. The accompanying illustrates the Huffman Codes, which was produced by David Huffman in 1951

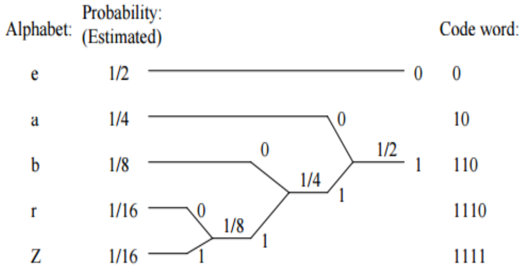


Figure 3: The process of coding the word 'Zebra' by Huffman Code

1.1. Channel Coding (Error Control Coding):

Error control coding is a technique to identify and conceivably redress blunders by acquainting redundancy with the stream of bits to be sent to the channel. The Channel Encoder will add bits to the message bits to be transmitted systematically. After passing through the channel, the Channel decoder will distinguish and redress the blunders. Because of clamour in the channel, they got bits may get to be '001'. In any case, subsequent to either "000" or "111" could have been sent. By majority logic decoding plan, it will be decoded as "000" and accordingly the message has been a '0'.Two types of Error Correction codes are there

1. Block Codes
2. Convolutional codes

1.2 Block codes:

A block code is a code in which k bits (or, all the more generally, images) are info and n bits (or, all the more generally images) are yield. We designate the code as a (n, k) code. We will start with bits, components from the field GF(2); later we will consider components from a field GF(q) (after we recognize what this means). On the off chance that we enter k bits, then there are 2k particular messages (or, all the more generally q k). Each message of n images associated with a with each information block is called a codeword. We could, in general, basically have a query table with k inputs and n yields. Be that as it may, as k gets large, this rapidly gets to be infeasible. (Attempt k = 255, for example.) We in this manner confine our attention to linear codes. Definition 1 A block code C of length n with 2k code words is called a linear (n, k) code if and just if its 2k code words shape a k-dimensional subspace of the vector space of all n-tuples over the field GF(2). All the more generally, with a greater field, a square code C of length n with q k is called a linear (n, k) code if and just if its q k code words frame a k-dimensional subspace of the vector space of all n-tuples over the field GF(q). ✷We help ourselves to remember what a vector space is: we have an addition characterized that is commutative and shut; we have scalar multiplication that is shut, distributive, and associative. We will formalize these properties somewhat further, yet this suffices for the present purposes. We will see (later) that we have a group structure on the addition operation. So what does this mean for code words: the sum of any two code words is a codeword. Being a linear vector space, there is some basis, and all cod ords can be obtained as linear combinations of the basis. We can designate {g0, g1, . . . , gk−1} as the basis vectors. In a nutshell, it means that we can represent the coding operation as matrix multiplication, as we have already seen. We can formulate a generator matrix as G=[g0, g1, . . . , gk−1].

1.3. Convolutional codes: We now introduce binary linear convolutional codes, which like binary linear block codes are useful in the power-limited (low-SNR, low-ρ) regime. In this chapter we will concentrate on rate-1/n binary linear time-invariant convolutional codes, which are the simplest to understand and also the most useful in the power-limited regime. Here is a canonical example: Example 1. Figure 1 shows a simple rate-1/2 binary linear convolutional encoder. At each time k, one input bit uk comes in, and two output bits (y1k, y2k) go out. The input bits enter a 2-bit shift register, which has 4 possible states (uk−1, uk−2). The output bits are binary linear combinations of the input bit and the stored bits.

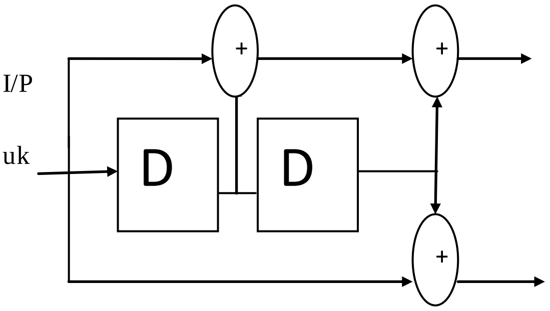


Figure .3. Four stateRate-1/2 binary linear convolutional encoder

III. TURBO CODES:

2.1 Encoding:

The termination tail is then appended to the encoded information and utilized as a part of the decoder. The framework is illustrated in Figure 2.We can regard the turbo code as a large piece code. The performance relies on upon the weight circulation - the base distance as well as the quantity of words with low weight. Convolutional codes have usually been encoded in their food forward structure, as

(G1,G2)=(1+D2,1+D+D2).

Notwithstanding, for these codes a solitary 1, i.e. the succession ...0001000..., will give a code word which is exactly the generator vectors and the heaviness of this codeword will in general be low. Plainly a solitary 1 will propagate through any interleaver as a solitary 1, so the conclusion is that on the off chance that we utilize the codes in the food forward structure in the turbo plan the subsequent code will have countless with low weight. The trap is to utilize the codes in their recursive systematic structure where we separate with one of the generator vectors.
Our example gives

(1,G2/G1)=1,(1+D+D2)/(1+D2)).

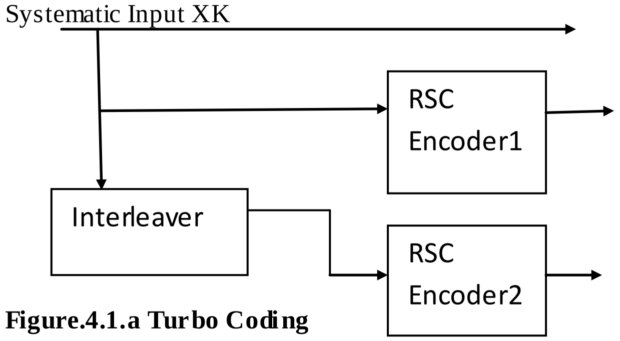


Figure.4.1.a Turbo Coding

Interleaving: It is a device for reordering a sequence of bits or symbols. A familiar role of interleavers in communications is that of the symbol interleaver which is used after error control coding and signal mapping to ensure that fading bursts affecting blocks of symbols transmitted over the channel are broken up at the receiver by a de-interleaver, prior to decoding.

2.2 Turbo codes Decoding:

These decoders ought to deliver soft-yields to enhance the interpreting performance. Such a decoder is called a Soft-Input Soft-Output (SISO) decoder. Each decoder operates all alone contribution as well as on alternate decoders not entirely decoded yield which takes after the operation guideline of turbo motors..Turbo deciphering procedure can be explained as takes after: Encoded information grouping X_k is transmitted over an Additive White Gaussian Noise (AWGN) channel and a loud got arrangement Y_k is obtained.

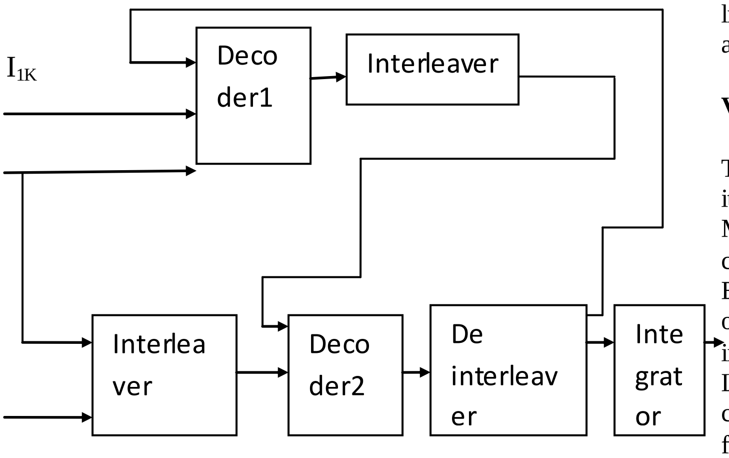


Figure.5.2.a Iterative Turbo Decoding

The MAP algorithm looks for the in all probability data arrangement whereas SOVA, which is a changed form of the Viterbi algorithm, looks for the in all likelihood associated path through the encoder trellis. The accompanying segments explain the MAP algorithm and its disentangled forms Log-MAP and Max-Log-MAP algorithms.

IV.1 . MAP ALGORITHM:

The MAP algorithm is an optimal however computationally complex SISO algorithm. The Log-MAP and Max-Log-MAP algorithms are rearranged adaptations of the MAP algorithm. MAP algorithm calculates LLRs for each information bit as

$$L(d_k)=\ln\left[\frac{\sum\limits_{S_k}\sum\limits_{S_{k-1}}\gamma_1(S_{k-1},S_k)\alpha(S_{k-1})\beta(S_k)}{\sum\limits_{S_k}\sum\limits_{S_{k-1}}\gamma_0(S_{k-1},S_k)\alpha(S_{k-1})\beta(S_k)}\right]$$

Recursive calculation of forward state metrics is performed as

$$\alpha_k(S_k)=\sum_{j=0}^{1}\alpha_{k-1}(S_{k-1})\gamma_j(S_{k-1},S_k)$$

Similarly, the backward state metrics are calculated by a backward recursion
from trellis time k = N to, k = 1 as

$$\beta_k(s_k)=\sum\beta_{k+1}(s_{k+1})\mathrm{Y}j(s_k.s_{k+1})$$

Branch metrics are calculated for each possible trellis transition.

3.2The Log-MAP Algorithm:

To evade complex numerical estimations of MAP decoding, computations can be performed in the logarithmic space. Furthermore, logarithm and exponential calculations can be wiped out by the accompanying estimate
$\mathrm{Max}^*(XY)==\ln(e^x+e^y)=\max(X,Y)+\log(1+e^{-y-x})$
The last term in max*(.) operation can easily be calculated by using alook-up table (LUT).

3.3 The Max-Log-MAP Algorithm:

The correction function
This simplification eliminates the need for an LUT required to find the
$f_c = \log(1+ e^{-|y-x|})$ in the max (.) operation can be implemented in different ways.
$\ln(e^x+e^y)\approx\approx \max(x,y)$
at the expense of some performance degradation.

V. SIMULATION RESULTS:

The simulation curve exhibited demonstrates the impact of iteration number,. In figures (4-5) BER for SOVA and LOG MAP as a component of Eb/No bends are appeared for constituent codes of constraint length three and code rate ½. Eight interpreting iterations were performed for Block length of 1024. Also the change achieved when the piece length is increased from 1024 to 4096 for both algorithms. For figure 6, LOG MAP indicates preferred performance over SOVA for constraint length of three and for square length of 1024.And from the figure7,we can watch the BER performances of LOG MAP and MAX-LOG MAP algorithms. The MAX-LOG MAP algorithm gives better BER performance.

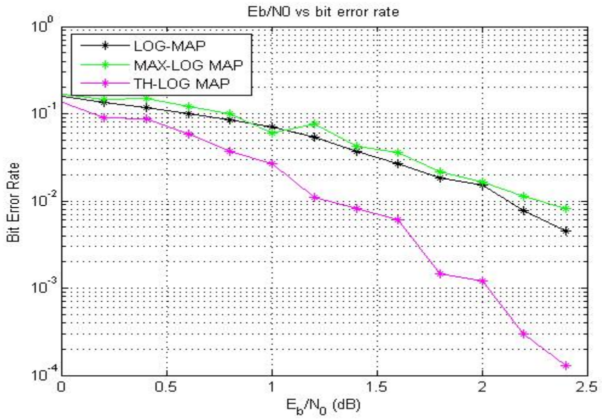


Figure.6.Comparison between Log map, Max-logmap, Threshold-logmap.

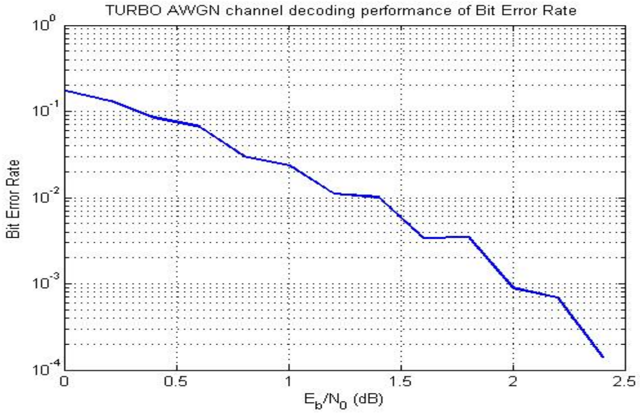


Figure.7. **BER performance with SNR for Log map**

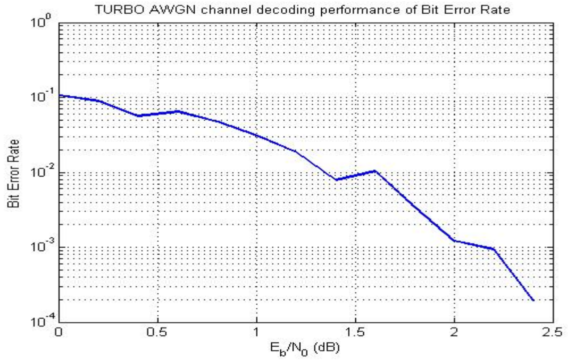


Figure.8. BER performance with SNR for Max-log map

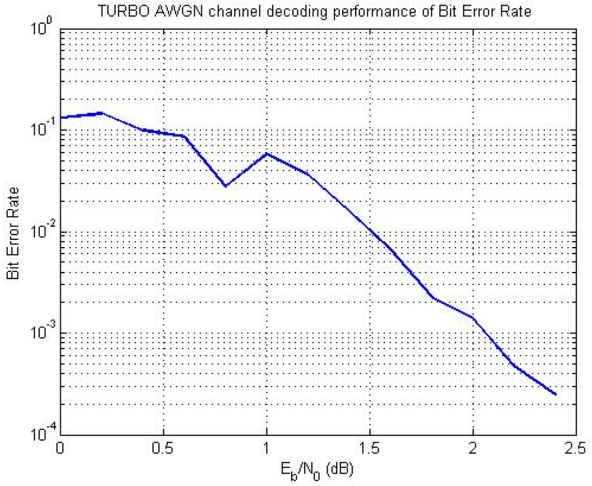
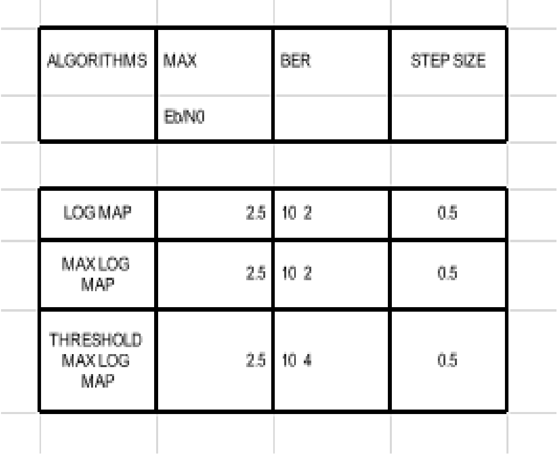


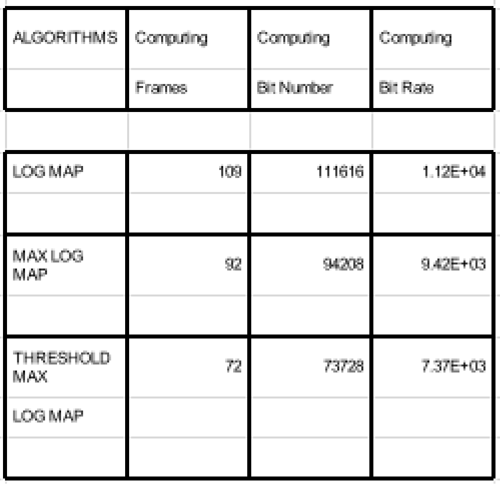
Figure.9. BER performance with SNR for Threshold-log map.

Table.1: Comparison



ALGORITHMS	MAX Eb/N0	BER	STEP SIZE
LOG MAP	2.5	10 2	0.5
MAX LOG MAP	2.5	10 2	0.5
THRESHOLD MAX LOG MAP	2.5	10 4	0.5

Table.2: Comparison



length=10s Cutting length=1024 Iteration=2

ALGORITHMS	Computing Frames	Computing Bit Number	Computing Bit Rate
LOG MAP	109	111616	1.12E+04
MAX LOG MAP	92	94208	9.42E+03
THRESHOLD MAX LOG MAP	72	73728	7.37E+03

VI. APPLICATIONS:

Turbo codes are utilized widely as a part of 3G and 4G mobile communication standards; Communication framework, for example, DVB-RC Sand DVB-RCS2.New NASA missions, for example, Mars Reconnaissance Orbiter now utilize turbo codes, as an alternative to RS-Viterbi codes.

VII. CONCLUSION:

In this chapter, standards of turbo coding and its applications in wireless communications have been talked about. The emphasis has been given on an algorithm modification to enhance the BER performance of the Max-Log-MAP algorithm which is the reduced complexity adaptation of the Log-MAP algorithm. This modification in the Max-Log-MAP algorithm can be executed basically by increasing the extrinsic information by a scaling factor. The adjusted Max-Log-MAP algorithms simulated by picking this scaling factor as a constant as well as picking the best scaling factors for various SNRs and disentangling iterations. Simulation results demonstrate that there is almost no performance gain when we adaptively change the scaling factor with various channel conditions and for various deciphering iterations.

VIII. REFERENCES:

[1].Grace Oletu, PredragRapajic," The Performance of Turbo codes for Wireless Communication Systems,IEEE2011.

[2]. C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon Limit Error-Correcting Coding and Decoding: Turbo Codes, "Proceeding of IEEE ICC 93, pp. 1064-1070.

[3]. S. Benedetto, G. Montorsi, "Design of Parallel Concatenation Convolutional Codes: IEEE Trans. on communication, vol. 44,No.5, May 1996.

[4]. C. Berrou, "The Ten-Year-Old Turbo Codes are Entering into Service," IEEE Commun. Mag. vol. 41, no. 8, pp.110-116, Aug 2003.

[5]. L. Bahi, J. Cocke, F. Jelinek, and J. Raviv, "Optimum decoding of linear codes for minimizing symbol error rate," IEEE Trans.on Inf. Theory, vol. IT-20, pp. 284-287, Mar. 1974.

[6]. T.A. Summers and S.G. Wilson, "SNR Mismatch and Online Estimation in Turbo Decoding, "IEEE Trans. On Comm. vol.46, no.4, pp. 421-424, April 1998.

[7]. P. Robertson, P. Hoeher, and E. Villebrun, "Optimal and Sub-Optimal Maximum A Posteriori Algorithms Suitable for Turbo Decoding,"European Trans. on Telecomm. vol. 8, no. 2, pp. 119-126, March-April 1997.

[8]. P. Robertson, E. Villebrun, and P. Hoeher, "A Comparison of Optimal and Sub-optimal MAP Decoding Algorithms Operating in the Log Domain," International Conference on Communications, pp.1009-1013, June 1995.

[9]. S. Benedetto, G. Montorsi, D. Divsalr, and F. Pollara "Soft- Output Decoding Algorithm in Iterative Decoding of Turbo Codes," TDA Progress Report 42-124, pp. 63-87, February 15, 1996.

[10]. J. Hagenauer, and P. Hoeher, "A Viterbi Algorithm with Soft-Decision Outputs and Its applications, "Proc. Of GLOBECOM, pp.1680-1686, November 1989.