Research of Different Turbo Code Speeds, Types of Modulations, Decoding Methods and their Compatibility with Encryption Techniques

Stanimir Parvanov
National Military University "Vasil Levski",
Faculty "Artillery Air Defense and
Communication and Information Systems"
Shumen, Bulgaria
ssparvanov@gmail.com

***Abstract*. Turbo codes are widely used to perform reliable information transfer over noisy communication connections with limited bandwidth or latency. The focus of the report is the analysis of different turbo encoder speed of the code, types of modulations, decoding methods and their joint use with information covert transmission methods. Realization of the communication channels is realized via Matlab/Simulink software. The effectiveness of communication systems is a matter of constant analysis and research by experts in the field of communication technologies.**

Keywords: turbo codes, error correction, encryption, communication systems.

I. INTRODUCTION

Turbo codes do a simple but incredible thing: they let engineers design systems that come extremely close to the so-called channel capacity - the absolute maximum capacity, in bits per second, of a communications channel for a given power level at the transmitter. This threshold for reliable communications was discovered by the famed Claude Shannon, the brilliant electrical engineer and mathematician who worked at Bell Telephone Laboratories in Murray Hill, N.J., and is renowned as the father of information theory [1]. Nowadays, Turbo codes are widely used from the ground or terrestrial systems of data storage, Asymmetric Digital Subscriber Line (ADSL) modems and fiber optic communications. Subsequently, it moves up to the air channel applications by employing to wireless communication systems, systems operating on the principle of secondary radar systems, [9] and then flies up to the space by using in digital video broadcasting and satellite communications. Undoubtedly, with the excellent error correction potential, it has been selected to support data transmission in space exploring system as well [2],[3]. Also, communication over the public network infrastructure like Internet brings potential threat which necessitating the use of encrypted algorithms [4], [5], [6].

The main purpose of this study is to build different communication models, with different speed of the turbo encoders, precisely different generating polynomial, with different codeword length, to combine them with different types of modulation, and examine and summarize the results obtained with different types of algorithms to decode in to decoders [11].

II. MODEL AND METHODS

There are many ways to implement a communication channel, but in most case's, this requires a large amount of funds. In this report, the focus is on communication simulation models implemented in the Simulink simulation environment.

Figure 1 depicts the first communication model considered. Its composition includes the following blocks. Message Source, Matrix Interleaver, Turbo Encoder, 64-QAM Modulator, AWGN Channel, 64-QAM Demodulator, Turbo Decoder, Matrix Deinterleaver, Bit Error Rate Calculator, Display, Spectrum Analyzer and Constellation Diagram Block. The specific thing about this simulation model is that, unlike standard turbo encoders, a matrix interleaver is added before it, which adds a percentage of hiddenness in the task of secret transmission of the information, which, in principle is achieved by encrypting the message. The phase manipulated (PM) signals, possessing a crest factor equal to one and a thumbtack autocorrelation function (ACF), are very important for many types of radio-communication systems (RCSs), because they provide the maximal possible resolution of the objects and diminish the negative effects, caused by the multipath spread of the electromagnetic waves [12].

Print ISSN 1691-5402
Online ISSN 2256-070X
https://doi.org/10.17770/etr2024vol2.8037

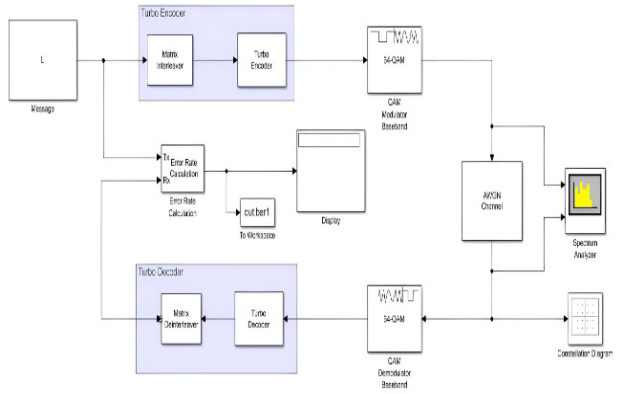

Fig. 1. Communication channel with Turbo coding and 64-QAM modulation

The communication channel of Figure 1 works as follows: From the message source, a text is generated, which is encrypted via RSA algorithm and converted into a binary form containing a cryptotext and a public key from a written code in the command window of Matlab (code is almost similar as in source [5]), the binary message is passed through a matrix interleaver, where an additional shift by rows and columns takes place, then the series of 0‘s and 1‘s is encoded with the turbo encoder with different generating polynomials (different length and code rate), then the encoded ciphertext is modulated by 64-QAM modulator, the modulated signal is received at AWGN channel, where noise is added, after that the signal is demodulated, decoded and received by bit error calculator, which compare the real message with the received one and, also the send signal is received by “ber1” block which is connected with Matlab environment and the final result can by decrypted from the written RSA code. More about RSA algorithm in [6].

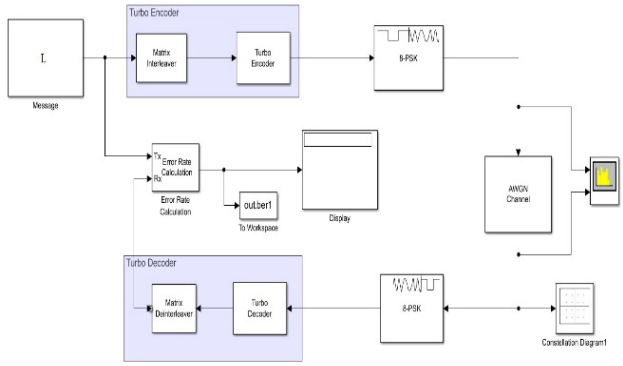

Fig. 2. Communication channel with Turbo coding and 8-PSK modulation

For the simulations are made 2 more models shown in fig.2 and fig.3 that are similar to the one illustrated in fig 1, the difference being that the modulation blocks are set to: different modulations and the poly2trellis structure in turbo encoder/decoder, are also other. Table 1 shows the parameters of the simulation models.

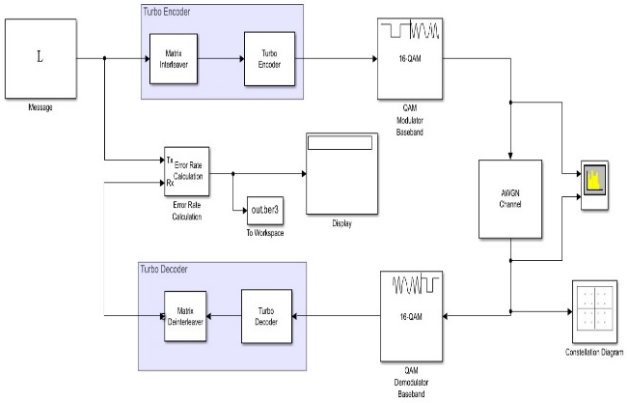

Fig. 3. Communication channel with Turbo coding and 16-QAM modulation

- *Adds White Gaussian noise channel (AWGN)*

The relationship between Ratio of symbol energy to noise power spectral density (Es/N0) and Ratio of bit energy to noise power spectral density (Eb/N0), both expressed in [dB], is as follows:

$$E_s / N_0(dB) = E_b / N_0(dB) + 10\,log_{10}(k) \quad (1)$$

where “k” is the number of information bits per symbol.

In a communications system, “k” might be influenced by the size of the modulation alphabet or the code rate of an error-control code. For example, in a system using a rate 1/2 code and 8-PSK modulation, the number of information bits per symbol “k” is the product of the code rate and the number of coded bits per modulated symbol. Specifically,

$$(1/2)\,log_2(8) = 3/2 \quad (2)$$

in such a system, three information bits correspond to six coded bits, which in turn correspond to two 8-PSK symbols [6].

- *Encoder/Decoder Trellis structure*

Trellis construction = poly2trellis (Constraint Length, Code Generator, Feedback Connection) returns the trellis structure description corresponding to the conversion for a rate k/n feedback encoder. “k” is the number of input bit streams to the encoder, and “n” is the number of output connections. Constraint length specifies the delay for the input bit streams to the encoder. Code Generator specifies the output connections for the input bit streams to the encoder. Feedback connection specifies the feedback connection for each of the “k” input bit streams to the encoder. You can find more information about trellis structures in [8].

TABLE 1 PARAMETERS OF THE MODELS

№	Parameters of the models		
	poly2trellis structure	*modulation*	*R, K*
1.	poly2trellis(4,[13,15],13)	8-PSK	1/2, 4
2.	poly2trellis(4,[13,15,17],13)	8-PSK	1/3, 4
3.	poly2trellis(7,[23,12,7],170)	8-PSK	1/3, 7
4.	poly2trellis(4,[13,15],13)	16-QAM	1/2, 4
5.	poly2trellis(4,[13,15,17],13)	16-QAM	1/3, 4
6.	poly2trellis(7,[23,12,7],170)	16-QAM	1/3, 7
7.	poly2trellis(4,[13,15],13)	64-QAM	½, 4
8.	poly2trellis(4,[13,15,17],13)	64-QAM	1/3, 4
9.	poly2trellis(7,[23,12,7],170)	64-QAM	1/3, 7

III. RESULTS AND DISCUSSION

The first results shown in (fig. 4, 5, 6) claim from a simulation model with 8-PSK modulation, with parameters shown in table 1.

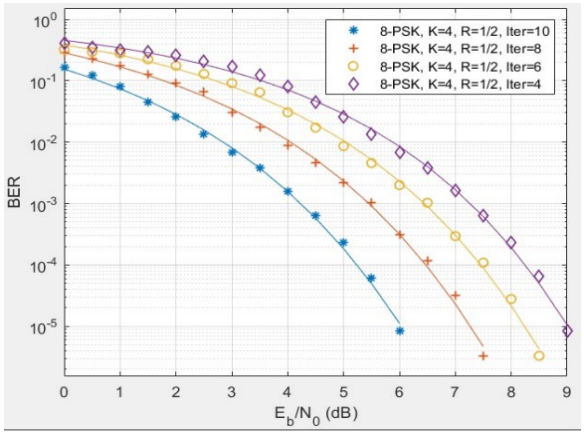

Fig. 4. Communication channel with Turbo coding and 8-PSK modulation and poly2trellis(4,[13,15],13), R = 1/2, K = 4

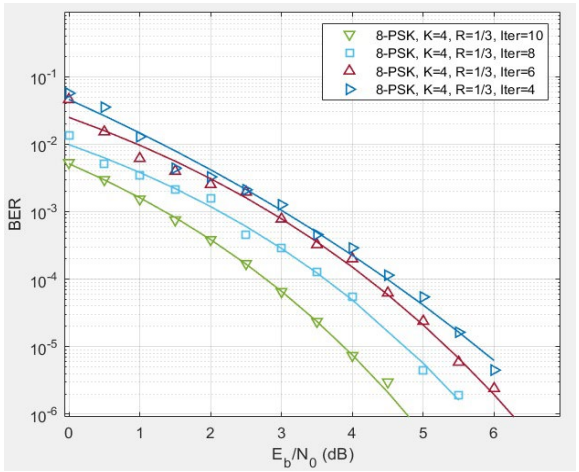

Fig. 5. Communication channel with Turbo coding and 8-PSK modulation and poly2trellis(4,[13,15, 17],13), R = 1/3, K = 4

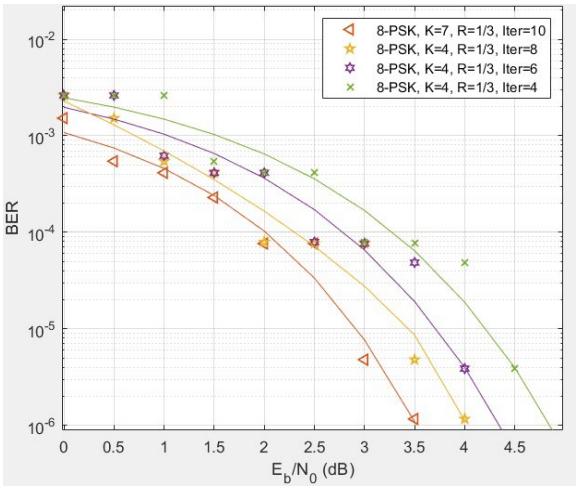

Fig. 6. Communication channel with Turbo coding and 8-PSK modulation and poly2trellis(7,[23,12,7],170), R = 1/3, K = 7

The model with 8-PSK modulation give the following results: for poly2trellis (7, [23,12,7],170), R=1/3, K=7 and 10 iterations in turbo decoder as the best signal to noise ratio is 3,5 [dB]. The lowest score was obtained with poly2trellis (4, [13,15],13), R=1/2, K=4 and 4 iterations in decoder and signal to noise ratio 9 [dB].

The second results (fig. 7, 8, 9) that are illustrated are obtained from a simulation model with 16-QAM modulation, with parameters shown in table 1.

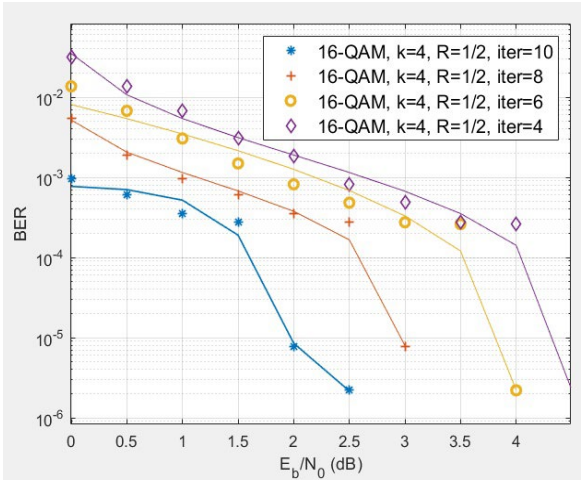

Fig. 7. Communication channel with Turbo coding and 16-QAM modulation and poly2trellis(4,[13,15,],13), R = 1/2, K = 4

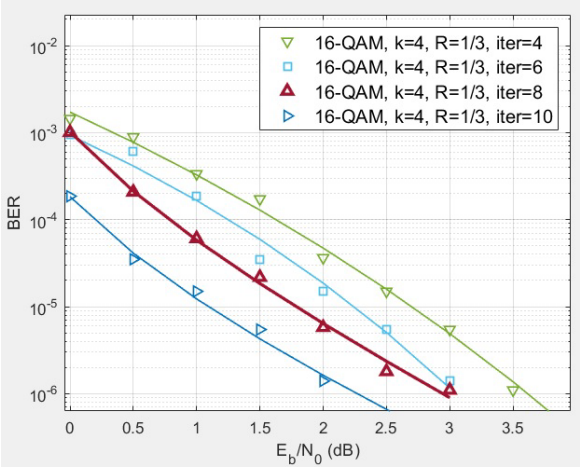

Fig. 8. Communication channel with Turbo coding and 16-QAM modulation and poly2trellis(4,[13,15, 17],13), R = 1/3, K = 4

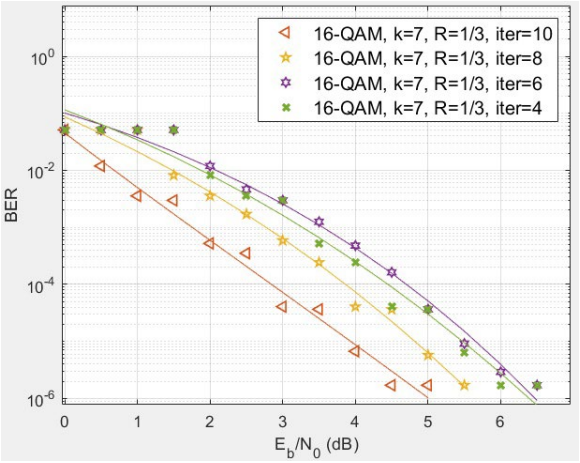

Fig. 9. Communication channel with Turbo coding and 16-QAM modulation and poly2trellis (7,[23,12,7],170), R = 1/3, K = 7

The best results are for model with 16-QAM modulation and parameters: poly2trellis (4, [13,15,17],13), R=1/3, K=4 and 10 iterations in turbo decoder as the best signal to noise ratio is 2,5 [dB]. The worst results were obtained with poly2trellis (7, [23,12,7],170), R=1/3, K=7, K=4 and 4 iterations in turbo decoder and SNR = 6,5 [dB].

The last results (fig. 10, 11, 12) which is simulated was from a model with 64-QAM modulation, with settings specified in table 1.

The best indicators for model with 64-QAM modulation is for: poly2trellis (4, [13,15,17],13), R=1/3, K=7 and 10 iterations in turbo decoder as the best signal to noise ratio is 2,3 [dB]. The worst results were obtained with poly2trellis (4, [13,15],13), R=1/2, K=4, K=4 and 4 iterations in turbo decoder and SNR = 6,5 [dB].

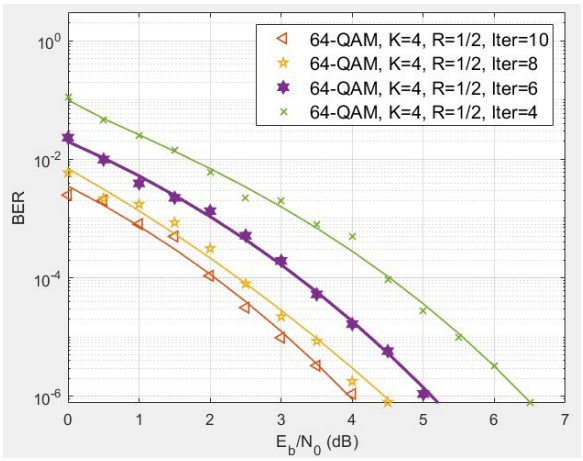

Fig. 10. Communication channel with Turbo coding and 64-QAM modulation and poly2trellis(4,[13,15,],13), R = 1/2, K = 4

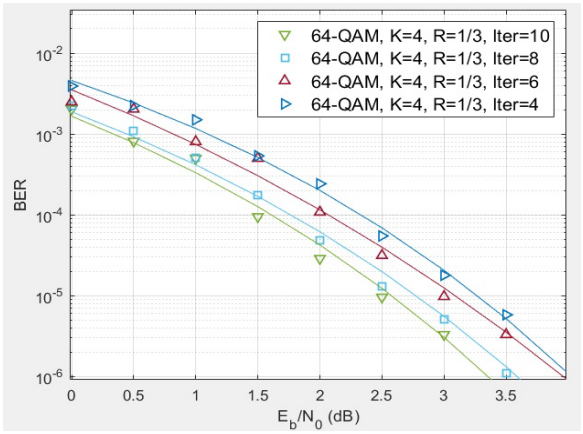

Fig. 11. Communication channel with Turbo coding and 64-QAM modulation and poly2trellis(4,[13,15, 17],13), R = 1/3, K = 4

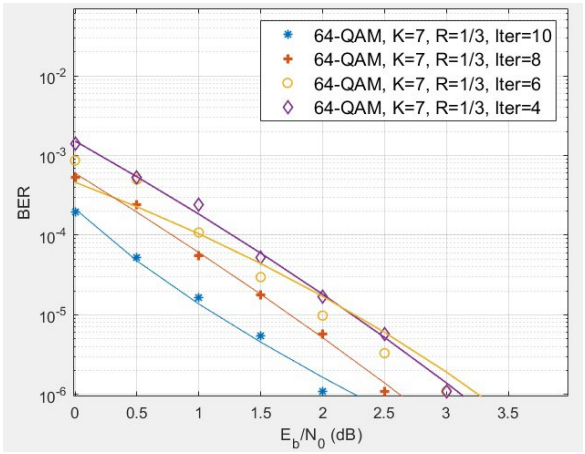

Fig. 12. Communication channel with Turbo coding and 64-QAM modulation and poly2trellis (7,[23,12,7],170), R = 1/3, K = 7

IV. CONCLUSION

The following conclusions can be drawn from the examined results:

1. As the length of the codeword increases, the chance of correcting erroneous bits increases.

2. Increasing the code rate improves the signal-to-noise ratio.

3. As the codeword length, code rate, and iterations in the decoder increase, the data rate slows down significantly.

4. To increase the data transfer rate, it is necessary to use a shorter code word, a smaller code rate and fewer iterations in the turbo decoder.

If you need a streaming communication system you should use short code word length and low code rate, if signal to noise ratio is need to be optimal then the longer the code word is, the faster the code rate and more iterations in the decoder are needed at the expense of the data transfer rate, or if you want to keep the data transfer rate you must use more powerful computing device such as a system of multiprocessor systems consisting of a number of independent processors connected to each other by a system of buses, organized in a certain way with a single operating system, shared operative memory and external devices [10], if this is cost effective.

ACKNOWLEDGMENT

This paper is supported by the National Scientific Program "Security and Defense", approved with Decision № 171/21.10.2021, task 3.1.9 of the Ministry Council of Republic of Bulgaria.

REFERENCES

[1] Erico Guizzo, "Closing In On The Perfect Code", [Online], Available: https://spectrum.ieee.org/turbo-codes, [Accessed March 1, 2004].

[2] Keattisak Sripimanwat, "Turbo Code Applications - A Journey from a Paper to Realization", National Electronics and Computer Technology Center (NECTEC), Pathumthani, Thailand, 2005;

[3] K. O. Slavyanov, "Contemporary Synthetic Aperture Radar Systems.Market Situation", International Scientific Conference "Defense Technology" at "Artillery, Aircraft Defense and CIS" Shumen, Bulgaria, 2017;

[4] L. Nikolov, R. Dimov, B. Zlatinov, "Malware in Social Engineering", "Scientific-Technical Union Of Mechanical Engineering - Industry 4.0", Borovets Winter Resort, Bulgaria, 2020;

[5] Suriyanath, RSA algorithm, MATLAB Central File Exchange, [Online], Available:.https://nl.mathworks.com/matlabcentral/fileexchange/46824-rsa-algorithm; [Accessed: April 12, 2024];

[6] Z. J. Luo, R. Liu, A. Mehta, "Understanding the RSA algorithm", 2023;

[7] Mathworks support centre, Documentation, [Online], Available: https://nl.mathworks.com/help/comm/ug/awgn-channel.html, [Accessed: 1994-2024 The MathWorks, Inc.]

[8] Mathworks support centre, Documentation, [Online], Available: https://nl.mathworks.com/help/comm/ref/poly2trellis.html?searchHighlight=poly2trellis&s_tid=srchtitle_support_results_1_poly2trellis, [Accessed: 1994-2024 The MathWorks, Inc.]

[9] D. Dimitrov, M. Kirov, "Methods For Increasing Information Authenticity by Knowing Objects for Identification System "IFF"", Sientific Session - Part I, National Military University "Vasil Levski", V. Tarnovo, 2010;

[10] T. G. Peshev, "Types of processor architectures for signal processing in inverse antenna aperture synthesis radar", Sientific Session - Part I, National Military University "Vasil Levski", V. Tarnovo, 2010;

[11] J. Kenea, K. Kulatb, "Soft Output Decoding Algorithm for Turbo Codes Implementation in Mobile Wi-Max Environment", "2nd International Conference on Communication, Computing & Security", [Online] Available: https://www.sciencedirect.com/science/article/pii/S2212017312006251, [Accessed: November 12, 2012 [ICCCS-2012], DOI: 10.1016/j.protcy.2012.10.080;

[12] B. Bedzhev, D. Dimitrov, "Application Of Quasi Complementary Pairs Of Phase Manipulated Signals In Radio-Communication Systems", Proceedings of "International Scientific Conference - Defense Technologies", DefTech, Shumen, Bulgaria, 2023.