Vojnotehnicki glasnik/Military Technical Courier
ISSN: 0042-8469
vojnotehnicki.glasnik@mod.gov.rs
University of Defence
Serbia

LDPC CODES FOR PHYSICAL LAYER SECURITY

Sonja R. Kuljanski Marić

Serbian Armed Forces, General Staff,
Department for Telecommunication and Informatics (J-6),
Center for Applied Mathematics and Electronics,
Belgrade, Republic of Serbia,
e-mail: sonjakuljanski@gmail.com,
ORCID iD: http://orcid.org/0000-0003-4625-1035

DOI: 10.5937/vojtehg66-14776; https://doi.org/10.5937/vojtehg66-14776

FIELD: Applied Mathematics
ARTICLE TYPE: Professional Paper
ARTICLE LANGUAGE: English

Summary:

Wireless communication is ubiquitous in today's society. Unfortunately, wireless transmission is by the nature of broadcasting suitable for eavesdropping. These links are usually secured by encryption protocols that rely on cryptographic algorithms whose security is based on complexity of calculation and inability to calculate in real time. The hypothesis in the field of information theory is that the eavesdropper has unlimited computer capabilities, and the use of common cryptographic protocols is uncertain. Instead, it is assumed that the legitimate recipient of the message has a better communication channel than the intrusion listening. Based on this physical advantage, it is possible to use random encoding schemes for the transmission of information at the physical level. These schemes function without the prior exchange of secret keys securely, so protection at this layer tends to significantly simplify key management in communication systems. At the end of the last and the beginning of this century, there was an idea that LDPC codes should be applied to protect data at the physical layer. In this paper, the Wyner model of the communication channel was used, and LDPC codes were constructed for the transmission of information through this channel. A comparison of the basic algorithm and its modification was made based on the following parameters: transmission of mutual information, bit-error rate and execution time. An algorithm for different sizes of LDPC codes was also performed based on the above parameters.

Key words: LDPC codes, Physical layer security, Wyner wiretap channel.

Introduction

Protection at the physical layer in the OSI model is independent of data encryption and authentication. An important feature of this protection is that secure communication can be established without the exchange of keys that have been performed in advance. In recent years, with the increasing use of mobile phones, wireless sensory networks and radio frequency identification (RFID) systems, security at the physical layer has gained significance. However, the implementation of sachems which rely on protection at the physical layer can be significantly more expensive than the implementation of security features based on cryptography. Currently, it is believed that it is best to combine cryptographic algorithms with physical layer protection. The use of security at the physical layer is recommended only for the transmission of the most sensitive information, such as key transport, key agreement or exchange of public key certificates. After the exchange of keys, the entities move to symmetric or asymmetric cryptographic algorithms.

Shannon's perfect security

In 1948, Shannon published a work (Shannon, 1948), which is considered the beginning of both the theory of information and coding theory. The diagram for transmitting information through a communication channel was described for the first time.

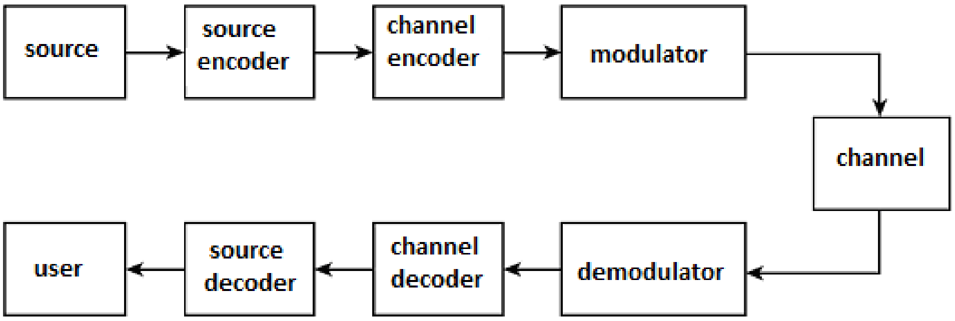

Figure 1 – Basic digital communication block by Shannon
Рис. 1 – Главная цифровая блок-диаграмма по Shannon
Слика 1 – Основни дигитални комуникациони блок-дијаграм по Shannon-у

The channel components are as follows:

1. Source as a series of bits.

2. Encoder converts the original information bit string into an alternate bit information series with a more efficient presentation of information. This operation is also called compression. Depending on the source, compression can be with loss or lossless. The source decoder returns the received alternative information to the original.

3. The channel encoder preserve a number of bits that are transmitted through a channel vulnerable to noise, signal distortion, and interference. It works by converting its input into a new sequence that has redundancy. The ratio of the number of bits that enters the channel encoder and the number of bits output from it is called code radio and is denoted by R, 0 <R <1. The role of the channel decoder is the detection of a series of bits that entered the encoder of the channel.

4. The modulator converts the output string of the encoder of the channel into a form corresponding to the given channel. For example, for a wireless communication channel, a series of bits must be represented by a high-frequency signal to allow transmission with an antenna of a reasonable size. The demodulator does the opposite of the modulator, and it detects the sequence that entered the modulator.

5. Channel is the physical medium through which the modulator sends its output. The channel can add noise to the signal that passes through it, and it can interfere with other signals.

Shannon introduced the notion of perfect security in (Shannon, 1949), which means that any intercept signal does not give the attacker more information than a random signal. According to this theory, Shannon discovered that for the purpose of secure transmission, the sender and the receiver in advance need to exchange the relevant key. Moreover, this pre-shared key should be changed during each data transfer. This result represents the theoretical basis for a symmetric key cryptography.

Let the source be completely defined by the list of symbols $S(s_1, s_2, \dots, s_q)$ and the set of appropriate probabilities $P(s_i), i \in \{1, \dots, q\}$, whereby it is assumed that the symbols represent a complete set of mutually exclusive events, $\sum P(s_i) = 1$ Shannon defines entropy as the amount of uncertainty involved in the value of a random variable or the outcome of a random process

$$H(S) = \sum_{i=1}^{q} P(s_i) \log_2 \frac{1}{P(s_i)} = -\sum_{i=1}^{q} P(s_i) \log_2 P(s_i) \qquad (1)$$

Perfect security is achieved if it is valid

$$H(M \mid X) = H(M) \quad (2)$$

otherwise if code word X is statistically independent of the message M.

In order to be able to broadcast information, the source must have at least two symbols available. Such a source is called a binary source of information. It is common to label these symbols as 0 and 1. If $P(0) = p$, then $P(1) = 1 - p$, so the entropy of the binary source is $H(S) = -p\log_2 p - (1-p)\log_2(1-p)$ information bits. It is clear that entropy is maximal when the probabilities of the both symbols are equal, $p = 1 - p = 0.5$ and then entropy is 1.

Let X and Y be random variables. It is then possible to define their mutual entropy as $H(X;Y) = E[-\log_2 p_{X,Y}(X,Y)]$, where $p_{X,Y}(X,Y)$ is mutual probability of the density function X and Y then their mutual information is defined as

$$I(X,Y) = \sum_{x \in X, y \in Y} p_{X,Y}(x,y) \log_2 \frac{p_{X,Y}(x,y)}{p_X(x) p_Y(y)} \quad (3)$$

ie, mutual information for X and Y can be presented as

$$I(X,Y) = H(X) - H(X \mid Y) \quad (4)$$

where $H(X \mid Y)$ is conditional entropy which is defined as $H(X \mid Y) = \sum p_Y(y) H(X \mid Y = y)$.

Shannon showed that channels can be categorized according to the parameter C, called channel capacity, which measures the amount of information that can be transmitted through the given channel. Although C can be presented in several different units, in the context of the channel code rate R whose unit is bit information on the channel bit, Shannon showed that there are codes that provide arbitrary reliable communication if the code rate meets the condition $R < C$. He also showed that, for $R > C$, there is no code that provides reliable communication.

The channel capacity is defined as

$$C = \max_{P(x)} I(X,Y). \quad (5)$$

That is, the capacity is the maximum common information where the maximization is done through the distribution of the probability of the channel input $P(x)$.

The transmission system meets Shannon's definition of perfect security if the mutual information between the sent signal X (plain text) and the intercepted signal Y (encrypted text) is equal to zero, i.e. $I(X,Y) = 0$.

It is not easy to construct a security system that meets the above criteria. Shannon has proven that one-time pad systems satisfy the criterion if the key space entropy is greater than or equal to the entropy of the message space, i.e. $H(K) \geq H(X)$.

Wyner *wiretap* channel

In 1975, Wyner introduced a wiretap channel in (Wyner, 1975) and established the ability to create almost perfectly secure communications without relying on cryptographic keys. He found the difference between the two types of noise, one that got the legitimate receiver and the other that received the wiretapper and showed that it was possible to reach non-zero secret capacity. He introduced a wiretap channel notation.

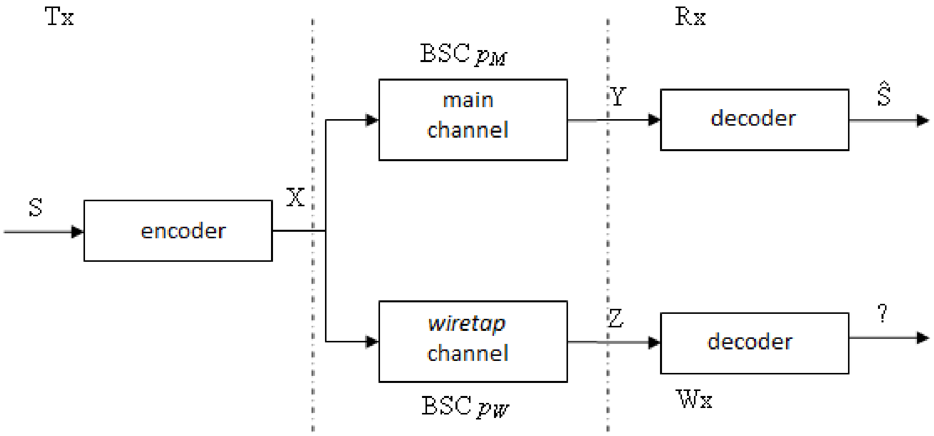

Figure 2 – Wyner's wiretap channel (Ghen & Gong, 2012)
Рис. 2 – Канал *Wyner wiretap (Ghen & Gong, 2012)*
Слика 2 – Wyner-ов wiretap канал (Ghen & Gong, 2012)

Secret capacity of the data transmission sistem is defined as

$$C = H(S \mid Z) - H(S \mid Y) \tag{6}$$

According to Shannon, perfect security requires that $I(S,Z) = 0$. Since $I(S,Z) = H(S) - H(S \mid Z)$, perfect security is achieved when $H(S \mid Z)$ is maximal, and that is exactly what Wyner's security required. The Wiretap channel does not require the exchange of keys in advance, and it is enough that the main channel has less noise than the wiretap channel so that the secrecy of the data transmission system is attainable.

The first question is how practical the implemention of this approach is. In some applicable scenarios, such as Radion Frequency Identification (RFID), a channel between an RFID reader and a valid tag is better than the channel between the tag and the illegal reader, since the illegal reader must be at a certain distance to avoid detection of the system.

The second question is how to design an encoder that is efficient, reliable and secure and how to choose a wiretap code. LDPC and Polar codes approach Shannon's channal capacity and meet the required conditions which can be mathematically defined.

LDPC codes

Wyner and Ozarow used a coset coding strategy (Ozarow & Wyner, 1984, pp.2135-2157) to show that perfect secrecy can be achieved when there are no errors in the main channel and when the imput alphabet is binary.

In the 1960s, Gallager (Gallager, 1962) developed low-density parity-check codes (LDPC codes); however, they were ignored for a long time because their computer complexity was too great for technology of that time. LDPC codes have very good decoding performance. In addition, they have the ability to parallellate in decoding and simple operations to calculate. The low complexity of computability combined with parallelism and good performance to correct errors are the main reasons why LDPC codes attract so much attention.

Despite these advantages, finding good methods for constructing LDPC codes and their efficient hardware implementation is still a challenge. Approaching the capacity of the channel implies that infinitely long codes are used. Different system applications have different decoding, delay, power and costing performance. These requirements limit the size of the code and its hardware implementation. As a result, different code lengths are recommended for different applications in order to get good performance and to meet the hardware requirements. LDPC codes can be applied in wireless, wired and optical communication systems, as well as on magnetic and compact discs. These are the reasons why it is a challenge to find ways to construct a fixed-length LDPC code and speed with good performance.

Implementation of LDPS codes in Wyner's wiretap channel

Wiretape encoding maps k message bit into the entire n-dimensional space. Therefore, there are 2^{n-k} code words for each message. One of them is randomly selected and transmitted through a wiretap channel. This coincidence is essential in securing the secrecy of the transmission through the wiretap channel.

Let there be a linear correcting code that has G as a matrix generator. The code C is a subspace of space $\{0,1\}^n$ with 2^k elements. According to the theory of error correction codes, every coset has cardinality 2^k, and there are 2^{n-k} total of them, so cosets completely divide the n-dimensional space into nonoverlapping subspaces.

Let Alice and Bob want to secretly exchange messages in Wyner's wiretap channel and let Eva want to listen to the exchange of messages. Alisa starts the communication procedure by choosing the message m length of the syndrome k. It is a secret message to be transmitted to Bob, and Eva cannot reconstruct it. Alisa finds a matrix base G for the complementary subspace C of the subspace of the code C. C and its complement C together make up the entire n-dimensional space of binary vector lengths n, i.e. $C \cup C = \{0,1\}^n$ Alice then generates a random sequence of lengths $n-k$. This is a uniformly distributed random vector, generated so that neither Bob nor Eva have any information about it. Alice then performs the following coding procedure

$$x = [mu]\begin{bmatrix} G \\ G \end{bmatrix} = mG + uG$$

the code word x is then transmitted via the wiretap channel. According to the definition, uG is the valid code word of the code C, while the message m determines one coset of the code C the cardinality of which is 2^k . Alisa sends x throught the wiretap channel. Bob receives the code word x without error. Its goal is to decode the message m , so he applies the following procedure

$$Hx^T = H(mG \quad + uG)^T = H(mG \quad)^T \ .$$

Note that Bob does not need to use information about a random vector u . He is in a favorable situation because the message is a syndrome and that each of the 2^{n-k} words in the coset serves equally well to get the message. Eve's goal is the same as Bob's, but her channel is worse than Bob's, so she gets a code word with the noise X . The randomized code schema along with a careful code design ensures that the noisy code word x reveals to Eva very little or no information about the sent message m .

The parity check matrix H is of a form $[A \quad B]$, where the matrix B has to be non-singular (i.e. inverse must exist. There is an evidence that every linear code C with the generating matrix G is equivalent to a linear code C' whose generating matrix G' is derived from matrix G by bringing in reduced row echelon form - RREF), (Hofman et al, 1992).

This allows us to select a unity matrix for the matrix B without additional constraints. The generating matrix G can be constructed as

$$G = \left[I_{n-1} \quad \left(B^{-1}A\right)^T\right]$$

If the code C is self-dual then $G \quad = H$ and the matrix A must have a trait $AA^T = 0$. If the matrix A is randomly generated, then it is necessary to calculate the matrix G before starting the coding.

For simplicity, suppose that the matrix $G = [I \quad P]$, then $H = \left[P^T \quad I\right]$. It is necessary to calculate the matrix G. By definition,

$x = [m \quad u]\begin{bmatrix} G \\ G \end{bmatrix} = mG \quad + uG.$ When decoding, we need to get $xH^T \ = m$, respectively

$$\left(mG^* + uG\right)H^T = mG^*H^T + \underbrace{uGH^T}_{0} = mG^*H^T = m$$

follows is that $G \ H^T = I$. Let the matrix be $G \quad = \left[G_1 \quad G_2\right]$, then

$$G\,H^T = [G_1 \quad G_2]H^T = [G_1 \quad G_2]\cdot[P^T \quad I]^T = [G_1 \quad G_2]\begin{bmatrix}P\\ I\end{bmatrix} =$$

$$G_1P + G_2I = G_1P + G_2 = I$$

That is, there is a mutual dependance between the matrices G_1 and G_2. If the matrix G_1 is generated in a random way, we can calculate the matrix G_2 as $G_1P + I$.

It has been experimentally shown that for the parity check matrix of the form $m \times 2m$ as the matrix G_1 unity matrix can be chosen without increasing mutual information, that speed up encryption since the matrix multiplication is eliminated. This significantly reduces the execution time of the algorithm in the case of a large matrix. In this case, the matrix G_2 is calculated as $IP + I = P + I$.

The construction of the self-dual code requires more time in the design of the generating and parity check matrix, but allows faster encoding. On the other hand, for non-self-dual codes, it is possible to construct the generating and verification matrix more quickly, but it takes extra time to generate a matrix G necessary for successful encryption.

The advantage of Wyner's wiretap coding in relation to other types of secret information transmission is that the attacker knows the code process as well as the legitimate participants in the communication and there is no pre-established secret key. The only condition is that legitimate participants have a better channel than an attacker.

Experimental results

For the needs of the simulation, wiretap codes are based on the use of the coset code scheme. The generating codes and the parity check matrix are constructed as follows:

$H = [P \quad I]$ i $G = [I \quad P^T]$

For such constructed matrices, the bit error rate, mutual information and the rate of execution of the encoding are experimentally checked. Particular cases were considered for different constructions of the matrix G. For an arbitrary size of the code $C(n,m)$, the matrix G is constructed in the following way $G = \left[A \quad \left(P^T A + I\right)^T\right]$, where the matrix P is a matrix from $H = [P \quad I]$, and a matrix A is randomly generated. For the code of forms $C(2m,m)$, it is possible to construct a matrix G as $G=[I \quad P+I]$.

Three cases are considered:

1. Code C has $C(n,m)$ form,

2. Code C has $C(2m,m)$ form and the matrix G has $G=\left[A \quad \left(P^T A+I\right)^T\right]$ form.

3. Code C has $C(2m,m)$ form and the matrix G has $G=[I \quad P+I]$ form.

Description of simulation

To modulate the messages in the simulation, QPSK (Quadrature Phase Shift Keying) modulation was selected. The selected channel is AWGN (additive White Gaussian Noise). The simulation is conceived as follows:

1. A random message of 1024 bits is generated. Then, depending on the used code, it takes the multiplication of the number of bits that is taken in the given wiretap code as information content.
2. Define the number of passes per signal-to-noise ratio in the channel in order to obtain the mean values and to obtain correct results. The number of passes is 50.
3. A simulation of the transmission of information content is initiated, with the signal-to-noise ratio going from 01 to 14 ($S/Nratio$).
   a. A channel with the current signal-to-noise ratio is created.
   b. Message is coded by a chosen code.
   c. Message is modulated by QPSK modulation.
   d. Transmission over the AWGN channel is simulated.
   e. The demodulation of the received signal is performed.
   f. An error is calculated at the transmission layer.
   g. The received message is decoded.
   h. An end-to-end error is calculated.
   i. The mutual information between sent and received message is calculated.
   j. The time of encoding initial message is calculated.
4. The mean error value at the transmission layer and the end-to-end error for each value $S/Nratio$ for the selected code is calculated

5. The mean value of the mutual information for each value $S / Nratio$ for the selected code is calculated.
6. The coding time for the selected code is calculated.
7. Draw graphics.

LDPC codes of the form $C(n,m)$

Among the codes of the form $C(n,m)$ the next codes are compared $C(512,32)$, $C(512,64)$, $C(512,128)$, $C(512,256)$, $C(512,384)$, $C(512,448)$, $C(512,480)$ i $C(512,496)$.

Bit error rate for the codes of the form $C(n,m)$

This feature was compared to pure BER on the channel (between the modulator and the QPSK demodulator) and the total BER on the system from the source of the message to the destination, end-to-end.

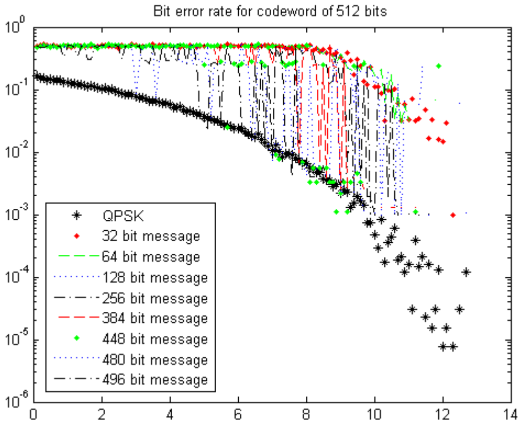

Figure 3 – BER for the code $C(512,m)$, $m < 512$ depending on the syndrom length

Рис. 3 – BER для кода формы $C(512,m)$, $m < 512$, в зависимости от продолжительности синдрома

Слика 3 – BER за код облика $C(512,m)$, $m < 512$, у зависности од дужине синдрома

As expected, the best BER has the code $C(512,32)$, while the code $C(512,496)$ has the worst BER.

Mutual information for the codes of the form $C(n,m)$

Figure 4 shows an increase in transformation as the signal-noise ratio increases. If the recipient has a signal-to-noise ratio above 12, which according to work (Baldi, 2014) is expected from the main channel, and the eavesdropper has a degraded channel, then the secrecy capacity could be calculated as the difference of these two transformations multiplied by the signaling speed that would have been used.

The bigest slope has the code $C(512,32)$, while the code $C(512,496)$ has the smallest slope.

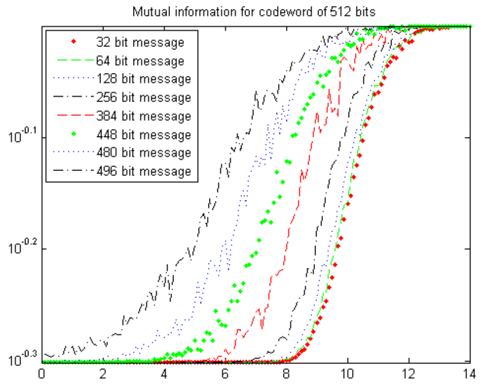

Figure 4 – Mutual information for the codes $C(512,m)$, $m < 512$ depending on the syndrom length

Рис. 4 – Совместная информация по коду формы $C(512,m)$, $m < 512$ в зависимости от продолжительности синдрома

Слика 4 – Заједничка информација за код облика $C(512,m)$, $m < 512$ у зависности од дужине синдрома

Execution speed for the codes of the form $C(n,m)$

Encoding execution time increases with increasing the length of basic information. Based on the measurement of BER and common information, it is clear that the best code is $C(512,32)$. However, this code takes the most time to encode, as shown in Figure 5.

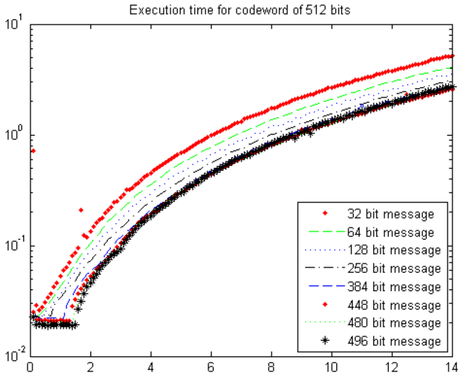

Figure 5 – Execution time for the codes $C(512,m)$, $m < 512$ depending on the syndrom length

Рис. 5 – Время выполнения по коду формы $C(512,m)$, $m < 512$ в зависимости от продолжительности синдрома

Слика 5 – Време извршавања за код облика $C(512,m)$, $m < 512$ у зависности од дужине синдрома

LDPC codes of the form $C(2m,m)$

For the codes of the form $C(2m,m)$, it is possible to make certain changes in the creation of the matrix G that lead to a significant speed up in the execution of the encoding function. Among the codes of the form $C(2m,m)$ codes $C(32,16)$, $C(64,32)$, $C(128,64)$, $C(256,128)$, $C(512,256)$ and $C(1024,512)$ are compared.

For each of these codes, two matrices G are created. One in a standard way, and the other in a simplified form for speeding up the encoding process.

Bit error rate for the codes of the form $C(2m,m)$

In Figures 6 and 7, it can be noticed hat there is no increase in the bit error rate if the matrix G is constructed simpler for the codes of the form $C(2m,m)$.

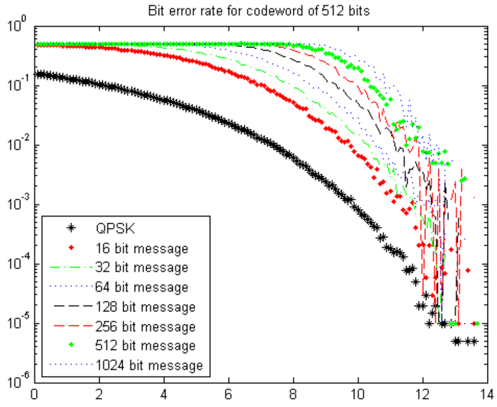

FIgure 6 – BER for the code $C(2m,m)$; $m < n$ depending on the codeword length for the matrix G^* constructed in the standard way

Рис. 6 – BER для кода формы $C(2m,m)$; $m < n$ в зависимости от величины кодового слова для стандартного создания матрицы G^*

Слика 6 – BER за код облика $C(2m,m)$; $m < n$ у зависности од дужине кодне речи за стандардан начин креирања матрице G^*

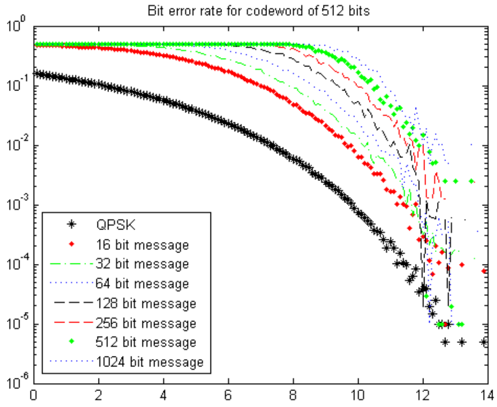

Figure 7 – BER forthe codes $C(2m,m)$; $m < n$ depending on the codeword length for the matrix G^* constructed in a simplified way

Рис. 7 – BER для кода формы $C(2m,m)$; $m < n$ в зависимости от величины кодового слова для упрощенного создания матрицы G^*

Слика 7 – BER за код облика $C(2m,m)$; $m < n$ у зависности од дужине кодне речи за поједностављен начин креирања матрице G^*

Mutual information for the codes of the form $C(2m,m)$

Also, in Figures 8 and 9, it is seen that mutual information does not increase for different constructions of the matrix G.

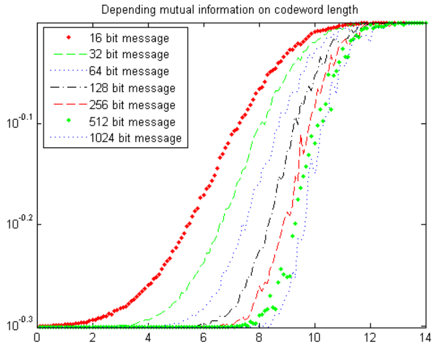

Figure 8 – Mutual information for the code $C(2m,m)$; $m<n$ depending on the codeword length for the matrix G^* constructed in the standard way
Рис. 8 – Совместная информация по коду формы $C(2m,m)$; $m<n$ в зависимости от величины кодового слова для стандартного создания матрицы G^*
Слика 8 – Заједничка информација за код облика $C(2m,m)$; $m<n$ у зависности од дужине кодне речи за стандардан начин креирања матрице G^*

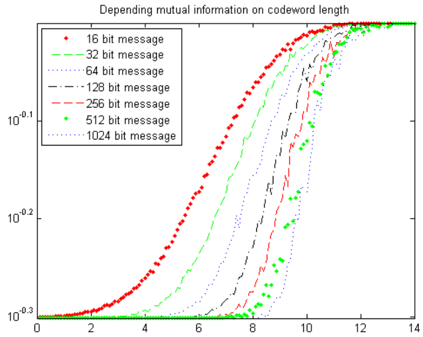

Figure 9 – Mutual information for the codes $C(2m,m)$; $m<n$ depending on the codeword length for the matrix G^* constructed in a simplified way
Рис. 9 – Совместная информация по коду формы $C(2m,m)$; $m<n$ в зависимости от величины кодового слова для упрощенного создания матрицы G^*
Слика 9 – Заједничка информација за код облика $C(2m,m)$; $m<n$ у зависности од дужине кодне речи за поједностављен начин креирања матрице G^*

Execution time for the codes of the form $C(2m,m)$

In Figures 10, 11 and 12, it can be noticed that the execution time in the standard matrix G creation is greater than the execution time if a simplified matrix G is used. This feature is more noticeable for codes for a longer codeword.

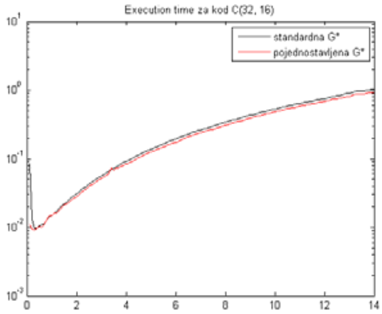

Figure 10 – Execution time for the codes $C(32{,}16)$ depending on the codeword length for the matrix G^* constructed in the standard way and the matrix G^* constructed in a simplified way

Рис. 10 – Время выполнения по коду $C(32{,}16)$ для стандартного создания матрицы G^* и упрощенного создания матрицы G^*

Слика 10 – Време извршавања за код $C(32{,}16)$ за стандардан начин креирања матрице G^* и поједностављен начин креирања матрице G^*

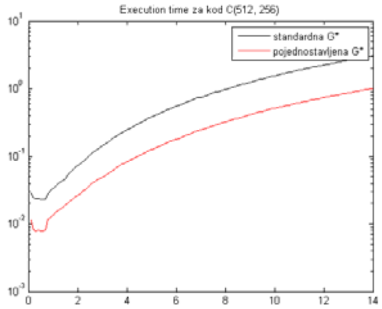

Figure 11 – Execution time for the codes $C(512{,}256)$ depending on the codeword length for the matrix G^* constructed in the standard way and the matrix G^* constructed in a simplified way

Рис. 11 – Время выполнения по коду $C(512{,}256)$ для стандартного создания матрицы G^* и упрощенного создания матрицы G^*

Слика 11 – Време извршавања за код $C(512{,}256)$ за стандардан начин креирања матрице G^* и поједностављен начин креирања матрице G^*

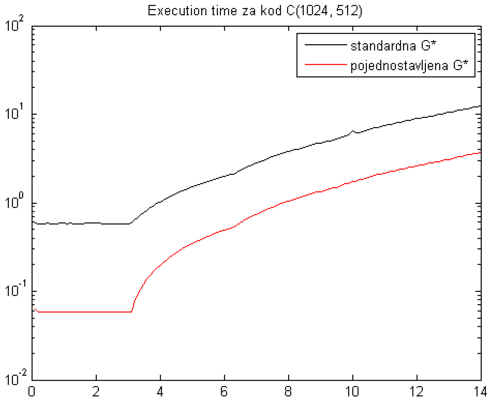

Figure 12 – Execution time for the codes $C(1024,512)$ depending on the codeword length for the matrix G^{*} constructed in the standard way and the matrix G^{*} constructed in a simplified way

Рис. 12 – Время выполнения по коду $C(1024,512)$ для стандартного создания матрицы G^{*} и упрощенного создания матрицы G^{*}

Слика 12 – Време извршавања за код $C(1024,512)$ за стандардан начин креирања матрице G^{*} и поједностављен начин креирања матрице G^{*}

Conclusion

Progress in wireless communication over the past two decades, especially at the physical layer, enables error control techniques. The aim of the paper was to present LDPC codes and their practical implementation as well as some modulations of implementation that lead to acceleration. These codes, together with Turbo codes, represent the basis of the digital and mobile revolution (3G and 4G networks) that began at the beginning of this century.

During the experimental comparison of differently constructed codes, what is measured is the error rate bit, the mutual information for the plain text and the encoded text, as well as the execution time for different lengths of the code. The expected conclusion is that the error rate bit is better when the syndrome is shorter, and the code word is longer. The same applies to mutual information. However, codes with a longer syndrome are performed faster. Accordingly, one must find the trade-off between the speed of execution on the one hand and the transmission of common information and the bit error rate on the other.

The scientific research process could be aimed at constructing and checking the properties of Gallager's, MacKay's and protograph codes as the main representatives of randomly constructed LDPC codes. The methods for the construction of codes based on Euccidal geometry and on combinatorial designs could also be studied, as the representatives of structured constrained LDPC codes.

References

Baldi, M. 2014. *QC-LDPC Code-Based Cryptography: Chapter Low-Density Parity-Check Codes.* Springer, pp.5-23.

Gallager, R.G. 1962. Low-density parity-check codes. *IRE Transactions on Information Theory*, January, pp.21-28.

Ghen, L., & Gong, G. 2012. *Communication System Security: Chapter Physical-Layer Security.* CRC Press, pp.583-611.

Ozarow, L.H., & Wyner, A.D. 1984. Wire-tap channel II. *AT&T Bell Laboratories Technical Journal*, 63(10), pp.2135-2157. Available at: https://doi.org/10.1002/j.1538-7305.1984.tb00072.x.

Shannon, C.E. 1948. A mathematical theory of communication. *The Bell System Technical Journal*, 27(3), pp.379-423.

Shannon, C.E. 1949. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4), pp.656-715.

Wyner, A.D. 1975. The wire-tap channel. *The Bell Systems Technical Journal*, 54(8), pp.1355-1387.

НИЗКОПЛОТНОСТНЫЕ КОДЫ ДЛЯ ЗАЩИТЫ ДАННЫХ НА ФИЗИЧЕСКОМ УРОВНЕ

Соня Р. Кулянски Марич

Вооруженные силы Республики Сербия, Генеральный штаб,
Управление информатики и телекоммуникаций (J-6),
Центр прикладной математики и электроники,
г. Белград, Республика Сербия

ОБЛАСТЬ: прикладная математика
ВИД СТАТЬИ: профессиональная статья
ЯЗЫК СТАТЬИ: английский

Резюме:

Беспроводная коммуникация стала неотъемлемой частью современного мира. К сожалению, беспроводная передача данных имеет и свои недостатки, так например, такой вид связи очень удобен для прослушивания. Беспроводная связь обычно защищена протоколами шифрования потока данных, которые основаны на криптографических алгоритмах. Безопасность данных обеспечивается за счет сложных вычислений, которые невозможно произвести в реальном времени. В области теории *информаций существует гипотеза о том, что прослушивающее устройство имеет неограниченные вычислительные возможности, поэтому в данном случае использование обычных криптографических протоколов не совсем надежно. Вместо этого предполагается, что у законного получателя сообщения коммуникационный канал лучше, чем канал с которого ведется прослушивание. И это физическое преимущество дает возможность применения схемы случайного кодирования для передачи информации на физическом уровне. Эти схемы функционируют без предварительного обмена ключами безопасным методом, таким образом защита этого уровня стремится к значительному упрощению управления ключами в коммуникационной системе. В конце прошлого и начале этого века родилась идея о применении низкоплотностных кодов для защиты на физическом уровне. В данной статье применена модель Wyner коммуникационного канала, а для передачи информации по этому каналу были разработаны низкоплотностные коды.*

Приведен сравнительный анализ главного алгоритма и его модификаций на основании следующих параметров: передача совместной информации, частота ошибок по битам (BER) и скорости выполнения. Также проведен сравнительный анализ работы алгоритма с различными величинами низкоплотностных кодов, на основании вышеприведенных параметров.

Ключевые слова: низкоплотностные коды, защита данных на физическом уровне, канал Wyner wiretap.

LDPC КОДОВИ ЗА ПОТРЕБЕ ЗАШТИТЕ ПОДАТАКА НА ФИЗИЧКОМ НИВОУ

Соња Р. Куљански Марић

Војска Србије, Генералштаб,
Управа за телекомуникације и информатику (J-6),
Центар за примењену математику и електронику,
Београд, Република Србија

ОБЛАСТ: примењена математика
ВРСТА ЧЛАНКА: стручни чланак
ЈЕЗИК ЧЛАНКА: енглески

Сажетак:

Бежична комуникација је свеприсутна у данашњем свету. Нажалост, бежични пренос података је по природи емитовања погодан за прислушкивање. Ове везе су обично осигуране протоколима за енкрипцију који се ослањају на криптографске алгоритме и чија се безбедност заснива на сложености израчунавања и немогућности израчунавања у реалном времену.

Хипотеза у области теорије информација јесте да прислушкивач има неограничене рачунарске могућности, па је коришћење уобичајених криптографских протокола несигурно. Уместо тога уводи се претпоставка да легитимни прималац поруке има бољи комуникациони канал од ентитета који прислушкује. На основу ове физичке предности могуће је користити шеме за случајно кодирање за пренос информација на физичком нивоу. Ове шеме функционишу без претходне размене тајних кључева сигурним путем, па заштита на овом нивоу тежи да значајно поједностави управљање кључевима у комуникационим системима. Крајем прошлог и почетком овог века јавила се идеја да се LDPC кодови примене приликом заштите на физичком нивоу. У раду је коришћен Wyner-ов модел комуникационог канала, а за пренос информација кроз овај канал конструисани су LDPC кодови. Вршено је поређење рада основног алгоритма и његове модифкације на основу следећих параметара: преноса заједничке информације, bit-error rate-а и брзине извршавања. Такође, вршено је поређење рада алгоритма за различите величине LDPC кодова на основу наведених параметара.

Кључне речи: LDPC кодови, заштита података на физичком нивоу, Вајнеров wiretap канал.

Paper received on / Дата получения работы / Датум пријема чланка: 10.08.2017.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 03.07.2018.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 05.07.2018.