Int. J. Electron. Commun. (AEÜ) 65 (2011) 1015–1022

Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

journal homepage: www.elsevier.de/aeue

Multilevel/AES-LDPCC-CPFSK with channel equalization over WSSUS multipath environment

Hakan Cam[a], Osman N. Ucan[b], Volkan Ozduran[c,*]

[a] Turkish Air Force Academy, 34149 Yesilyurt, Istanbul, Turkey
[b] Istanbul Aydin University, Faculty of Engineering and Architecture, Department of Electrical and Electronics Engineering, Florya, Kucukcekmece, Istanbul, Turkey
[c] Istanbul University, Faculty of Engineering, Department of Electrical and Electronics Engineering, 34320 Avcilar, Istanbul, Turkey

ARTICLE INFO

Article history:
Received 13 December 2010
Accepted 24 March 2011

Keywords:
Advanced Encryption Standard
Low density parity check codes
Continuous Phase Frequency Shift Keying
WSSUS
Channel equalization

ABSTRACT

In this paper, in order to ensure secure and robust communication, a new type of data encryption and error correction mechanism called Multilevel/Advanced Encryption Standard-Low Density Parity Check Coded-Continuous Phase Frequency Shift Keying (Multilevel/AES-LDPCC-CPFSK) is carried out. Here, we have chosen AES for data encryption, LDPC codes for error correction and CPFSK for modulation. We have evaluated error performance of this scheme over Wide-Sense Stationary Uncorrelated Scattering (WSSUS) multipath channels with channel equalization. We have simulated 5-level AES, 2-level LDPC for 4CPFSK and 16CPFSK over WSSUS channels modeled by Cooperation in the field of Science & Technology, Project #207 (COST207). We have concluded that our proposed structure has promising results compared to Turbo Codes for all SNR values in WSSUS channels.

1. Introduction

Encryption and error correction mechanisms are required for secure and robust communication. AES algorithm is a symmetric block cipher providing secure sensitive information. 128, 192 or 256 bits of data blocks can be processed by AES using key lengths of 128, 196 and 256 bits. It is based on round functions which are Byte Substitution, Row Shifting, Column Mixing and Key Addition [1–3]. LDPC codes are well known error correction codes, providing low encoder and decoder complexity [4]. Many authors have investigated LDPC codes; Zyablov and Pinkster [5], Margulis [6], Tanner [7], MacKay and Neal [8], Wiberg [9]. These studies have defined the basic principles of LDPC codes. There also can be found many studies in literature which have expanded the range of LDPC code usage by Haley et al. [10], Cui et al. [11], Luby et al. [12], Johnson [13], Bing and Jun [14], Abematsu et al. [15], Nik and Fekri [16].

Bandwidth efficiency is one of the main performance criteria in multipath channels. CPFSK, a special kind of Continuous Phase Modulation (CPM) [17], provides a good bandwidth efficiency and bit error performance with its additional memory unit. Various studies have been investigated about the different aspects of CPFSK by the following authors; Osman [18], Sakamoto et al. [19], Altay [20], Cheng and Lu [21]. Continuous Phase Encoder (CPE) and Memoryless Mapper (MM) are two components of CPFSK. CPE is a convolutional encoder. It produces codeword sequences that are mapped onto waveforms by MM, which creates continuous phase signals. CPE provides not only power efficiency but also phase continuity.

WSSUS is a basic multipath channel model to describe the fading dispersive channels. It has two main parameters for characterizing of fading and multipath effects, which are propagation delay and Doppler shift [8]. WSSUS channels can be modeled as in Cooperation in the field of Science & Technology, Project #207 (COST207) with standard profiles such as Typical Urban (TU), Bad Urban (BU) and Hilly Terrain (HT). Since COST207 is a severe fading channel, various channel equalizers such as Least Mean Squares (LMS) and Recursive Least Squares (RLS) are employed.

In this paper, a new joint scheme, "Multilevel/Advanced Encryption Standard-Low Density Parity Check Coded-Continuous Phase Frequency Shift Keying (ML/AES-LDPCC-CPFSK)" is simulated over WSSUS multipath environment with channel equalization. The basic idea of using multilevel encryption and encoding is to partition information bits into several levels and encrypt and encode each level separately by AES cipher and LDPC encoder. In this approach, "ML/AES cipher" encrypts information bits, then "ML/LDPC encoder" [22] encodes these parallel bits, after that, the coded bits are turned into serial to parallel according to the type of modulation. CPE encodes the last level of these bits to provide phase continuity, then, MM maps the coded bits into M-ary CPFSK signals and these signals are sent to channel. CPFSK demodulator demodulates the noisy signals at the receiver side. Then, "Signal constellation and probability calculation block" processes

* Corresponding author. Tel.: +90 5358415755.
E-mail address: volkan@istanbul.edu.tr (V. Ozduran).

1434-8411/$ – see front matter © 2011 Elsevier GmbH. All rights reserved.
doi:10.1016/j.aeue.2011.03.020

these signals, and one and zero probabilities of received signals are evaluated. In every level "LDPC decoder" decodes these signals and input bits are estimated from these bits. Finally, "ML/AES decryption block" decrypts these bit streams.

Organization of this paper is as follows: In Section 2, a brief overview of AES algorithm is given. Then LDPC codes and CPFSK modulation are described in Sections 3 and 4, respectively. ML/AES-LDPCC-CPFSK systems are investigated in Section 5. Finally, error performance of the proposed scheme is discussed in Section 6.

2. Advanced Encryption Standard

AES is known worldwide as Rijndael symmetric-key block cipher which designed by Joan Daemen and Vincent Rijmen. The block size of AES is 128 bits, and the key lengths can be 128, 192 or 256 bits [3]. The key size determines the number of rounds to be performed. For instance, for the key size of 128, 192 and 256 bits, the number of rounds are 10, 12 and 14, respectively.

In our proposed scheme, we use the version of Rijndael that has a 128-bit key, operates on 128-bit plaintexts and has 10 rounds. Multiple of 128 bits (5×128 bits) are fed into AES Encryption block. The input level of ML/LDPC block determines the input level of AES. It is both possible to operate on long size data blocks and provide bandwidth-efficient transmission at the same time with multilevel inputs.

3. Low Density Parity Check Codes

LDPC codes are the members of binary linear block codes family. These codes can be described as very sparse parity check matrix H, which contains many zeros and only few ones. It is possible to represent a LDPC code as a graph, namely bipartite graph, whose node-set can be partitioned into two non-empty sets V and C and every edge connects a node in V with a node in C. The variable and check nodes correspond to the columns and rows of parity check matrix H and represent a bit symbol in the code words and a parity equation of code, respectively. An edge between each variable node and check node can be represented by a "1" in corresponding row and column in the parity-check matrix. In this paper only regular LDPC codes are investigated. In regular LDPC codes, every column of H contains j amount of "1" and every row of H is filled with k amount of "1", which j and k denote variable node degree and check node degree, respectively. There are two kinds of LDPC codes: regular and irregular [23]. Here regular LDPC codes are investigated. In regular LDPC codes all rows and columns of the parity check matrix H has the same degree which corresponds to the number of "1" bits in these rows and columns. All variable nodes have degree j and all check nodes have degree k in a bipartite graph of regular LDPC code. The bipartite graph of a regular (3,4) LDPC code is depicted in Fig. 1 and the corresponding parity check matrix of this code is described as an example.

$$H = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix} \quad (1)$$

3.1. Encoding of LDPC codes

LDPC codes can be represented with two parameters: (n, k), where n corresponds to information bits and k corresponds to codewords. A LDPC code with a parity check matrix H, which has $n-k$ rows and k columns, encodes k information bits into n codewords. Codewords of this LDPC code satisfy the following relation:

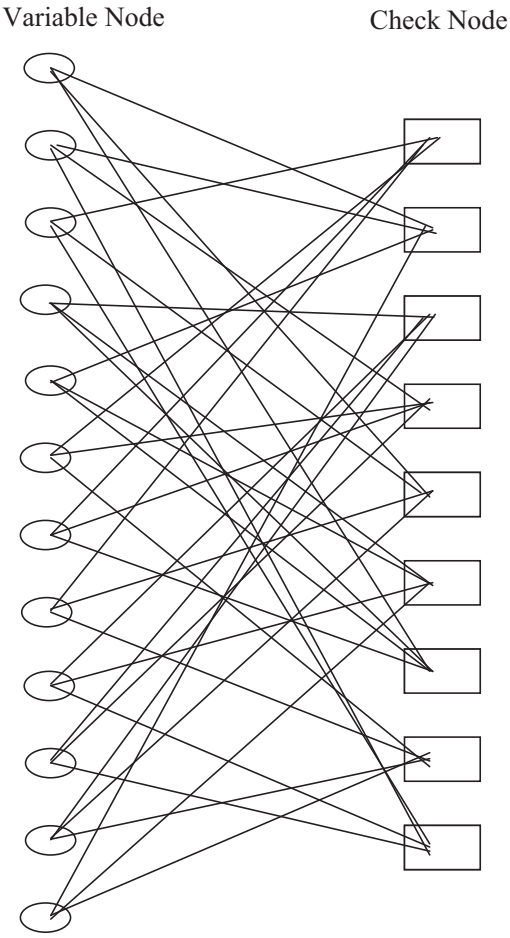

Fig. 1. Bipartite graph representation of regular (3,4) LDPC code.

$$Hx^T = 0 \quad (2)$$

where H, x and T refers to parity check matrix, codeword and transpose operation, respectively. The parity check matrix H of an LDPC code can be defined as:

$$H = [H_p | H_u] \quad (3)$$

where H_p is parity bits submatrix and H_u is information bits submatrix. Likewise codewords can be defined as:

$$X = [X_p | X_u] \quad (4)$$

where x_p is a set of parity bits and x_u is a set of information bits. The following relation can be defined:

$$b = H_u X_u^T \quad (5)$$

With this equality, encoding of a binary systematic (n, k) LDPC code becomes equivalent to solving the following equation:

$$b = H_p X_p^T \quad (6)$$

From this equation the following relation can be defined:

$$X_p^T = H_p^{-1} b \quad (7)$$

3.2. Decoding of LDPC codes

LDPC codes can be decoded by Message Passing Algorithm (MPA), which iteratively updates the probabilities of bit nodes.

Some authors have called different names for this algorithm like Sum Product Algorithm (SPA) or Belief Propagation Algorithm (BPA) at the same time. At this point, some terms and formulations which we used in MPA are defined as follows:

y_i: set of received signal
c_i: set of bit node
b: 0,1
$q_{ij}(b)$: the probability of message to be passed from bit node c_i to the check node f_j
$r_{ji}(b)$: the probability of message to be passed from check node f_j to the bit node c_i
R_j = set of column locations of the 1s in the jth row
$R_{j/i}$: set of column locations of 1s in the jth row, excluding the variable node i
C_j = set of row locations of the 1s in the ith column
$C_{i/j}$: set of row locations of 1s in the ith column, excluding the check node j
K_{ij}: constant values
$Q_i(b)$: posterior probability of the code bit c_i
$p_i = prob(c_i = 1|y_i)$

Decoding process of LDPC Codes can be explained step by step in the following section.

Step 1: Initialization

All bit nodes send their $q_{ij}(0)$ and $q_{ij}(1)$ messages. Since no other information is available at this step, the probabilities of messages ($q_{ij}(0)$ and $q_{ij}(1)$) can be computed using Eqs. (8) and (9).

$$q_{ij}(0) = 1 - p_i = prob(c_i = 0|y_i) = \frac{1}{1 + e^{-2y_i/\sigma^2}} \tag{8}$$

$$q_{ij}(1) = p_i = prob(c_i = 1|y_i) = \frac{1}{1 + e^{2y_i/\sigma^2}} \tag{9}$$

Step 2: Parity node updates (first half round iteration)

The check nodes calculate their $r_{ji}(0)$ and $r_{ji}(1)$ response messages according to Eqs. (10) and (11).

$$r_{ji}(0) = \frac{1}{2} + \frac{1}{2} \prod_{i' \in R_{j/i}} (1 - 2q_{i'j}(1)) \tag{10}$$

$$r_{ji}(1) = 1 - r_{ji}(0) \tag{11}$$

Step 3: Bit node updates (second half round iteration)

The bit nodes update their response messages to the check nodes. So, the probabilities of messages ($q_{ij}(0)$ and $q_{ij}(1)$) can be updated using Eqs. (12) and (13).

$$q_{ij}(0) = K_{ij}(1 - p_i) \prod_{j' \in C_{i/j}} r_{j'i}(0) \tag{12}$$

$$q_{ij}(1) = K_{ij} p_i \prod_{j' \in C_{i/j}} r_{j'i}(1)) \tag{13}$$

where constants k_{ij} are selected to ensure $q_{ij}(0) + q_{ij}(1) = 1$

Step 4: Soft decision

All the bit nodes calculate the $Q_i(0)$ and $Q_i(1)$ posterior probabilities of the code bit c_i using Eqs. (14) and (15).

$$Q_i(0) = K_i(1 - p_i) \prod_{j \in C_i} r_{ij}(0) \tag{14}$$

$$Q_i(1) = K_i p_i \prod_{j \in C_i} r_{ij}(1) \tag{15}$$

where constants k_i are selected to ensure $Q_i(0) + Q_i(1) = 1$

Step 5: Hard decision

Finally, all the bit nodes update their current estimation $c_i\psi$ of their variable $c_i\psi$ by calculating the probabilities for 0ψ and 1ψ and voting for the bigger one as in Eq. (16).

$$\hat{c}_i = \begin{cases} 1 & Q_i(1) > \frac{1}{2} \\ 0 & \text{other} \end{cases} \tag{16}$$

Step 6: If $\hat{c}H^T = 0$ or the number of iterations reaches the maximum limit, then the algorithm terminates, otherwise it returns to step 2.

4. Continuous Phase Frequency Shift Keying

CPFSK is a special kind of CPM [23], which has an M-dimensional form. At this point some terms and formulations which are used in CPFSK are defined as follows:

$\phi(t,Y)$: tilted-phase representation of CPM
Y: input sequence of M-ary symbols, $Y_i \in \{0, 1, 2, \ldots, M-1\}$.
h: modulation index $h = J/P$, where J and P are relatively prime integers
T: channel symbol period
$q(t)$: phase response function
L: integer
$g(t)$: frequency pulse
$s(t)$: transmitted signal
f_1: asymmetric carrier frequency where $f_1 = f_c - h(M-1)/2T$
f_c: carrier frequency
E_s: energy per channel symbol
ϕ_0: initial carrier phase

Tilted-phase representation of CPM was derived by Rimoldi in [17], with the information-bearing phase given by

$$\phi(t, Y) = 4\pi h \sum_{i=0}^{\infty} Y_i\, q(t - iT) \tag{17}$$

Here, J is generally chosen as 1 and P is calculated as 2 to the power of the number of memories in CPE. Modulation index can be computed from the equation of $h = 1/P$. The phase response function $q(t)$ is a continuous and monotonically increasing function subject to the following inequalities:

$$q(t) = \begin{cases} 0 & t \le 0 \\ 1/2 & t \ge LT \end{cases} \tag{18}$$

The phase response is can be described as in

$$q(t) = \int_{-\infty}^{t} g(\tau)\, d\tau \tag{19}$$

Transmitted signal $s(t)$ can be computed from the following equation:

$$s(t, Y) = \sqrt{\frac{2E_s}{T}} \cos(2\pi f_1 t + \phi(t, Y) + \phi_0) \tag{20}$$

where $f_1 T$ is assumed as an integer for simplification when using the equivalent representation of the CPM waveform.

5. Wide-Sense Stationary Uncorrelated Scattering enviroment and equalization

In digital communication systems multipath fading is the most important factor for system performance. Due to various objects surrounding, scattering, diffraction and reflection cause the multipath fading which has frequency and time dispersive nature. Since

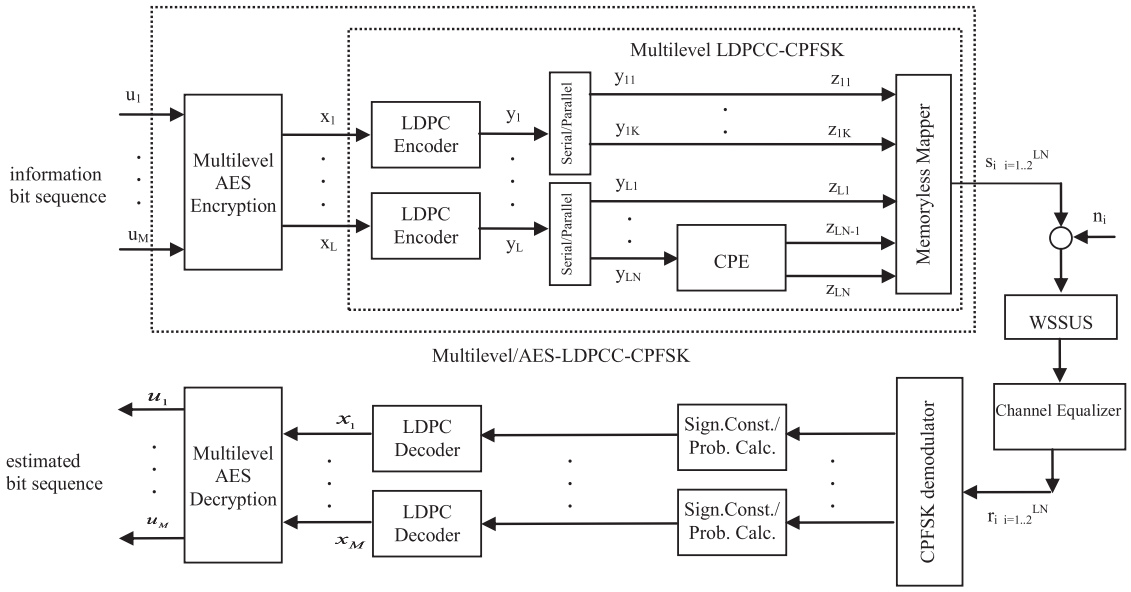

Fig. 2. General Multilevel/AES-LDPCC-CPFSK scheme.

changing characteristics of channel due to the movement of the mobile station it can be assumed as a time-variant and multipath fading channel and this channel can be described as statistical WSSUS channel. This channel model can be characterized by a two dimensional scattering function which has two parameters; Doppler frequency due to the mobile movement and echo delay due to multipath effects. Fading statistics of this channel model are assumed to be constant for a short time interval. Since severe transmission conditions of WSSUS channels and the added noise, signals are corrupted and need to be regenerated by using channel equalizers. Under severe conditions receivers require the characteristics of a transmission channel for channel identification. But these characteristics are not always available and channel's equivalent impulse response has to be estimated. It is impossible to estimate information bits without channel equalization. Thus channel equalizer block is necessary for all schemes in WSSUS channels for performance improvement.

6. Proposed scheme

In Fig. 2, block diagram of designed joint ML/AES-LDPCC-CPFSK model is depicted. As can be seen from this figure, there exists a "ML/AES Encryption block" for the encryption of message bit sequences. Multilevel inputs to this block are multiple of 128 bits ($M \times 128$ bits) and are dependent on the input level of "ML/LDPC block" [22]. After the encryption block, there is a LDPC encoder at every level of the system model and a CPE which is serially connected to the LDPC encoder at the last level. Encoded message bit sequence is converted from serial to $\log_2 M$ parallel branch in the multilevel scheme according to the type of M-ary CPFSK modulation. Then, each LDPC encoder processes the information sequence simultaneously. The level of "ML/LDPC block" determines the level of "ML/AES Encryption block" (i.e. 2, 3 and 4 levels of LDPC, the levels of AES are 5, 7 and 10, respectively). The output of the last LDPC encoder is run through the CPE. CPE is used to shape the modulated signal's spectrum for phase continuity. Finally, all encoder outputs and CPE output are mapped to CPFSK signals by a memoryless mapper according to partitioning rule. In the partitioning rule, signal set is divided into two subsets by the MSB of Serial to Parallel (S/P) converter output. If the first output z_{11} is 0, then the first subset is chosen, if z_{11} is 1, then the second subset is chosen. The second output z_{12} bit divides the subsets into two groups as the similar way. This partitioning process continues until the last partitioning level. These signals are run through the channel. Noise is added according to the channel model. Channel Equalizer block processes these corrupted and noise added signal sequence. At the receiver side of the communication channel, "CPFSK demodulator" demodulates the corrupted noisy signals. Then "Signal constellation and probability calculation block" processes these signals to evaluate one and zero probabilities of received signals. After that "LDPC decoder" decodes these signals and input bits are estimated from decoded bits in every partitioning level. Finally, these bit streams are gone through the "ML/AES decryption process" and estimated bit sequences can be decrypted. For a better bit error performance, some of the message bit sequences which will be known by receiver block as in pilot symbol communication [24], can be used in the last level of AES to estimate channel parameters.

In Fig. 3, the partitioning mechanism for 4CPFSK system is depicted in order to explain the partitioning of ML/AES-LDPCC-CPFSK. In the first partitioning level z_1 defines which subset is chosen. If $z_1 = 0$, then first subset $\{s_0,s_1,s_4,s_5\}$ is chosen, if $z_1 = 1$, then the second subset $\{s_2,s_3,s_6,s_7\}$ is chosen. At the second partitioning level, if we assume that the first subset is chosen in first partitioning level, z_2z_3 bits specify which signal will be transmitted to the channel. Similarly, in the first partitioning level, if the second subset is chosen, z_2z_3 bits specify which signal will be transmitted to the channel. Table 1 summarizes this process.

It can be seen from Fig. 3 that initial and ending phase of transmitted signal will take $(0,\pi)$ values if modulation index h of an LDPCC-4CPFSK system is chosen as 1/2. Input–output data and signal constellations for this system are summarized in Table 1. Here,

Table 1
Input–output and signal constellation for 4CPFSK.

θ_n	β_n	$z_1\ z_2\ z_3$	θ_{n+1}	4CPFSK
0	0	0 0 0	0	s_0
0	1	0 0 1	π	s_1
0	2	0 1 0	0	s_2
0	3	0 1 1	π	s_3
π	0	1 0 0	π	$s_4 = -s_0$
π	1	1 0 1	0	$s_5 = -s_1$
π	2	1 1 0	π	$s_6 = -s_2$
π	3	1 1 1	0	$s_7 = -s_3$

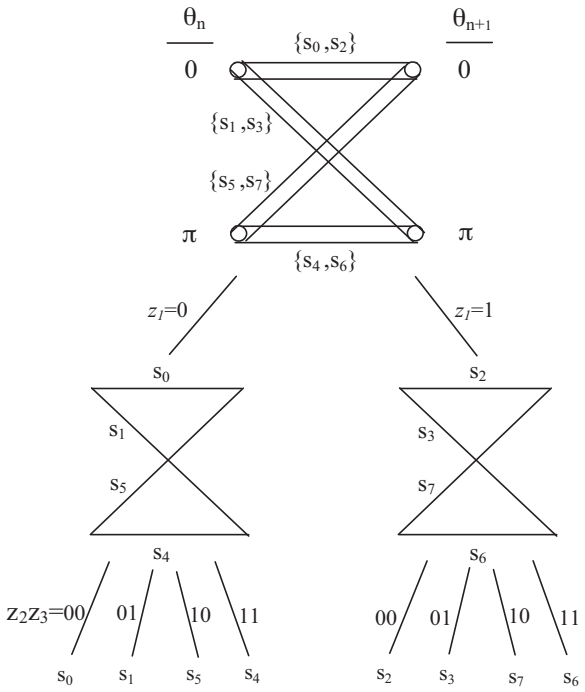

Fig. 3. 4CPFSK $h = 1/2$ signal phase diagram.

z_1 is systematic bit, z_2 and z_3 are the bits encoded by CPE. Here, z_2 helps to show us at which phase the signal will start at the next coding interval. If the initial phase (θ_n) is "0" and "z_2" is 0, the ending phase of the instant signal and the starting angle of the next signal phase (θ_{n+1}) is "0", if $\theta_n = 0$ and $z_2 = 1$, $\theta_{n+1} = \pi$, if $\theta_n = 1$ and $z_2 = 0$, $\theta_{n+1} = \pi$, if $\theta_n = 1$ and $z_2 = 1$, θ_{n+1} is 0. If the initial phase is "0", then the signal is positive, if the initial phase is "1", then the signal is negative. Only if these conditions are met is continuity granted. According to Fig. 3 and Table 1, the transmitted signals at the phase transitions are as follows: from 0 phase to 0 phase, s_0, s_2; from 0 phase to π phase, s_1, s_3; from π phase to 0 phase, s_5, s_7 and from π phase to π phase, s_4, s_6.

Message passing algorithm is used for decoding at the receiver side of LDPC codes. One and zero probabilities of received signal are used in this algorithm. For every decoding interval, these probabilities are firstly evaluated for all parallel input branch sequences according to partitioning rule. At this point, some terms and formulations are defined as follows:

r_k: received signal
L: partitioning level
s_i: transmitted M-ary CPFSK signal
P_i^j: probability where i denotes 0 or 1

One and zero probabilities of received signal are computed from the following equations:

$$P_0^L = \frac{1}{M}\left[\sum_{i=0}^{M-1}\frac{1}{(r_k - s_{2i})^2}\right] \tag{21}$$

$$P_1^L = \frac{1}{M}\left[\sum_{i=0}^{M-1}\frac{1}{(r_k - s_{2i+1})^2}\right] \tag{22}$$

Then received signal is mapped to one dimensional BPSK signal as can be described in below.

$$\gamma^L = 1 - \frac{2 \cdot P_0^L}{P_0^L + P_1^L} \tag{23}$$

In Fig. 3, it can be shown that in every partitioning level probability computations and mapping are executed according to signal set. These probabilities are calculated as in Eqs. (24)–(27) for partitioning level 1 and 2.

$$P_0^1 = \frac{1}{4}\left[\sum_{i=0}^{3}\frac{1}{(r_k - s_{2i})^2}\right] \tag{24}$$

$$P_1^1 = \frac{1}{4}\left[\sum_{i=0}^{3}\frac{1}{(r_k - s_{2i+1})^2}\right] \tag{25}$$

$$P_0^2 = \frac{1}{4}\left[\sum_{i=0}^{1}\frac{1}{(r_k - s_i)^2} + \frac{1}{(r_k - s_{i+4})^2}\right] \tag{26}$$

$$P_1^2 = \frac{1}{4}\left[\sum_{i=0}^{1}\frac{1}{(r_k - s_{i+2})^2} + \frac{1}{(r_k - s_{i+6})^2}\right] \tag{27}$$

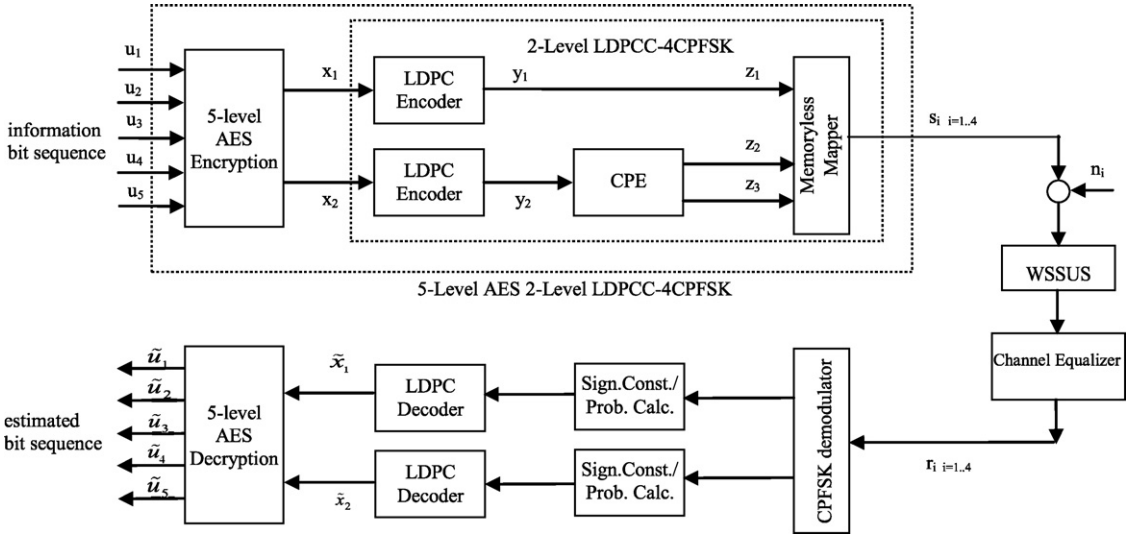

Fig. 4. Five level AES two level LDPCC-4CPFSK scheme.

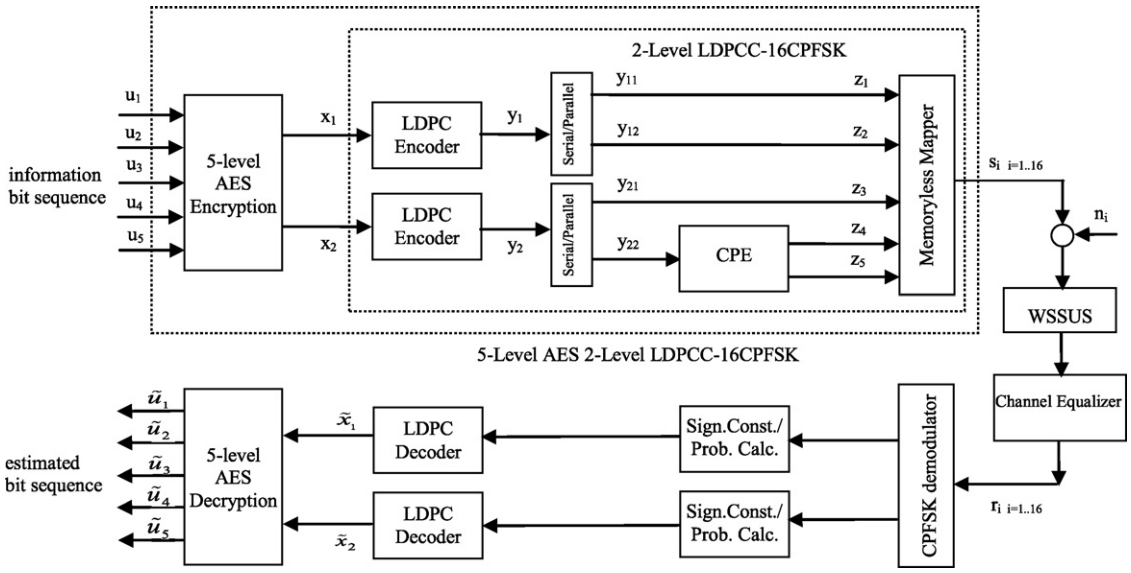

Fig. 5. Five level AES two level LDPCC-16CPFSK scheme.

These one and zero probabilities of received signal are evaluated and then $\hat{c}_i$ is estimated from Eqs. (9)–(13) for every partitioning level.

Partitioning mechanism for 16CPFSK system has the same property as in 4CPFSK.

6.1. Five-level AES two-level LDPC coded 4CPFSK

In Fig. 4, five-level AES two-level LDPC coded 4CPFSK system model is depicted. First of all "5-level AES Encryption block" encrypts 5 parallel message bit sequences which are multiple of 5×128 bits and thus 5×128 bits long input data can be processed simultaneously. Five-level inputs are dependent on the number of two-level LDPC. After the encryption process, two-level LDPC encoder encodes these encrypted parallel bit sequences. At this stage, LSB bits are encoded by CPE for phase continuity. Then memoryless mapper maps these coded bits into 4CPFSK signals. These signals are sent to the WSSUS multipath channel. Noise is added according to the channel model. Channel Equalizer block processes these corrupted and noise added signal sequence. At the receiver side of the communication channel, "CPFSK demodulator block", "Signal constellation and probability calculation block", "LDPC decoder block" and "5-level AES decryption block" work like in "Five-level AES two-level LDPC coded 4CPFSK". Finally, estimated bit sequences can be decrypted.

6.2. Five-level AES two-level LDPC coded 16CPFSK

In Fig. 5, five-level AES two-level LDPC coded 16CPFSK system model is depicted. In this scheme "AES Encryption block" and "LDPC Encoder block" work like in "Five-level AES two-level LDPC coded 4CPFSK" as described in Section 6.1. Then encoded bits are turned into serial to parallel with two branches for each output of "LDPC Encoder block". Here, LSB bits are encoded by CPE again for phase continuity. Then memoryless mapper maps these coded bits into 16CPFSK signals. These signals are sent to the WSSUS multipath channel. Noise is added according to the channel model. Channel Equalizer block processes these corrupted and noise added signal sequence. At the receiver side of the communication channel, "CPFSK demodulator block", "Signal constellation and probability calculation block", "LDPC decoder block" and "5-level AES decryption block" work like in "Five-level AES two-level LDPC coded 4CPFSK". Finally, estimated bit sequences can be decrypted.

7. Performance analysis and discussion

Here, we investigate multilevel AES encryption, multilevel LDPC coded CPFSK structures and join these schemes as "Multilevel/Advanced Encryption Standard-Low Density Parity Check Coded-Continuous Phase Frequency Shift Keying (ML/AES-LDPCC-CPFSK)". Thus a real communication environment is achieved employing both data encryption and channel encoding. We study on two different modulation techniques; "Five level AES two level LDPCC-4CPFSK" and "Five level AES two level LDPCC-16CPFSK" over WSSUS channels with RLS, LMS equalization. We use regular (3,4) LDPC codes with a block length of 302 bits, and maximum 100 iterations. The Bit Error Ratio (BER) versus Signal to Noise Ratio (SNR) curves of the proposed systems are obtained for BU, TU and HT types of COST207 (Figs. 6–8). In our simulation we use seventeen

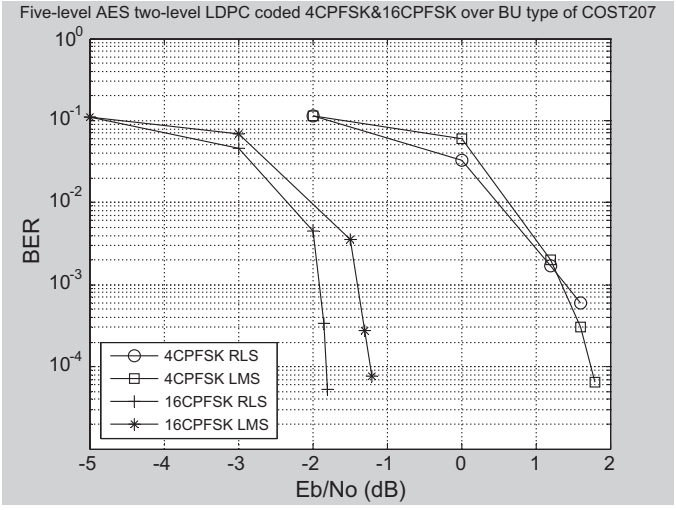

Fig. 6. Performance of five-level AES two-level LDPC coded 4CPFSK&16CPFSK scheme over BU type of COST207 channel.

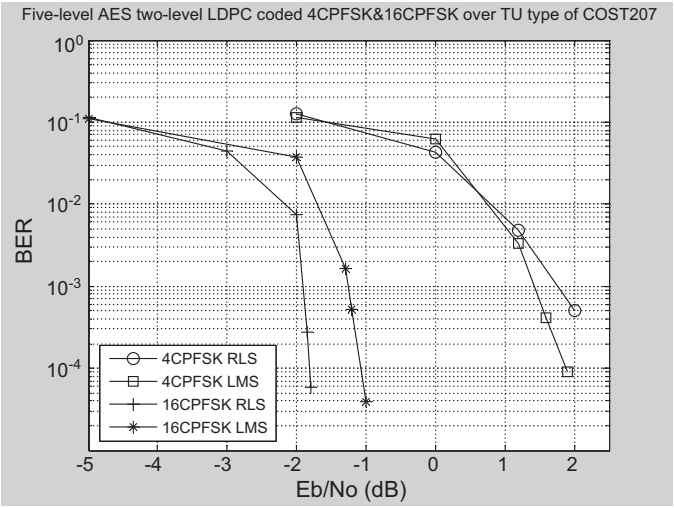

Fig. 7. Performance of five-level AES two-level LDPC coded 4CPFSK&16CPFSK scheme over TU type of COST207 channel.

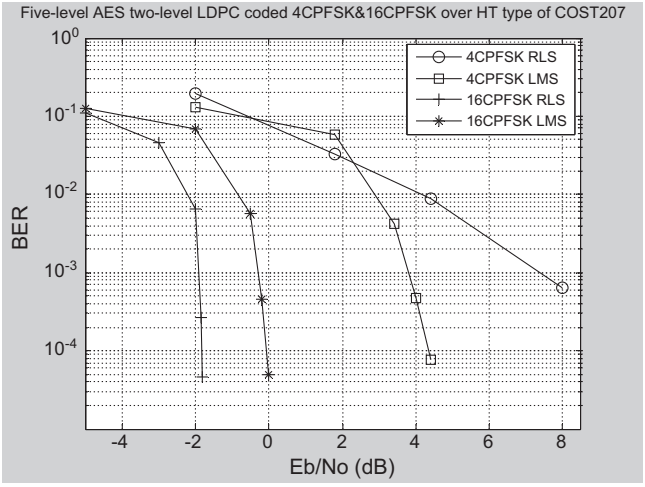

Fig. 8. Performance of five-level AES two-level LDPC coded 4CPFSK&16CPFSK scheme over HT type of COST207 channel.

channel coefficients for BU, TU and HT as can be seen from Table 2. We assume the velocity of the mobile radio communication terminal as 100 km/h. The carrier frequency of COST207 channel is taken as 950 MHz. The maximum Doppler Shift is taken as 88 Hz and minimum Doppler period is chosen as 11.4 ms. Finally, the symbol period is assumed as 3.7 μs.

Although ideal data encryption is assumed in most of the related compared models [18,20,23,24] we include data encryption block. We have simulated our schemes for various SNR values over WSSUS channel models. As it can be seen from Tables 3 and 4, Five level AES two level LDPCC-4CPFSK&16CPFSK systems show higher BER performance in all SNR values over 2 Level-Turbo Codes 4 Phase Shift Keying (2L-TC 4PSK) [24] for TU, BU, HT type of COST207 with RLS, LMS. Thus, both higher coding gain and reduction in the number of CPFSK levels are achieved.

Table 2
Channel coefficients of BU, TU and HT types of COST207.

BU	TU	HT
−0.0484 − 0.2943*i*	−0.1651 + 0.5534*i*	−1.0607 + 0.2118*i*
−0.0000 − 0.4282*i*	−0.0506 + 0.7480*i*	−1.3775 − 0.0015*i*
0.0447 − 0.5339*i*	0.0849 + 0.9113*i*	−1.5213 − 0.1868*i*
0.0815 − 0.6063*i*	0.2169 + 1.0292*i*	−1.4957 − 0.3254*i*
0.1064 − 0.6414*i*	0.3215 + 1.0907*i*	−1.3252 − 0.4056*i*
0.1162 − 0.6368*i*	0.3778 + 1.0881*i*	−1.0507 − 0.4232*i*
0.1090 − 0.5919*i*	0.3702 + 1.0178*i*	−0.7242 − 0.3814*i*
0.0839 − 0.5077*i*	0.2910 + 0.8806*i*	0.4014 − 0.2902*i*
0.0418 − 0.3872*i*	0.1403 + 0.6815*i*	−0.1342 − 0.1641*i*
−0.0152 − 0.2351*i*	−0.0733 + 0.4294*i*	0.0356 − 0.0203*i*
−0.0835 − 0.0577*i*	−0.3338 + 0.1373*i*	0.0820 + 0.1237*i*
−0.1582 + 0.1375*i*	−0.6196 − 0.1790*i*	−0.0021 + 0.2523*i*
−0.2335 + 0.3418*i*	−0.9057 − 0.5011*i*	−0.2047 + 0.3541*i*
−0.3030 + 0.5460*i*	−1.1663 − 0.8090*i*	−0.4962 + 0.4224*i*
−0.3599 + 0.7407*i*	−1.3771 − 1.0820*i*	−0.8341 + 0.4562*i*
−0.3978 + 0.9165*i*	−1.5177 − 1.3001*i*	−1.1686 + 0.4600*i*
−0.4108 + 1.0649*i*	−1.5736 − 1.4452*i*	−1.4497 + 0.4420*i*

Table 3
Comparison of BER-SNR (in dB) values of 2L-TC 4PSK [24] and five level AES two level LDPCC-4CPFSK[a] for TU, BU, HT type of COST207 with RLS, LMS.

	TU						BU						HT					
	RLS			LMS			RLS			LMS			RLS			LMS		
BER	[24]	[a]	Gain	[24]	[a]	Gain	[24]	[a]	Gain	[24]	[a]	Gain	[24]	[a]	Gain	[24]	[a]	Gain
1.00E−01	2	−2	4	0	−2	2	3	−2	5	4	−2	6	5	−2	7	7	−2	9
1.00E−02	3	0	3	4	0	4	5	0	5	6	0	6	7	1.8	5.2	9	1.8	7.2
1.00E−03	4	1.2	2.8	5	1.2	3.8	6	1.2	4.8	7	1.2	5.8	9	4.4	4.6	10	3.4	6.6
1.00E−04	5	2	3	6	1.6	4.4	7	1.6	5.4	8	1.6	6.4	10	8	2	11	4	7
1.00E−05	7			8	1.9	6.1	8			9	1.8	7.2	12			12	4.4	7.6

[24]: 2L-TC 4PSK.
[a] Five level AES two level LDPCC-4CPFSK.

Table 4
Comparison of BER-SNR (in dB) values of 2L-TC 4PSK [24] and five level AES two level LDPCC-16CPFSK[a] for TU, BU, HT type of COST207 with RLS, LMS.

	TU						BU						HT					
	RLS			LMS			RLS			LMS			RLS			LMS		
BER	[24]	[a]	Gain	[24]	[a]	Gain	[24]	[a]	Gain	[24]	[a]	Gain	[24]	[a]	Gain	[24]	[a]	Gain
1.00E−01	2	−5	7	0	−5	5	3	−5	8	4	−5	9	5	−5	10	7	−5	12
1.00E−02	3	−3	6	4	−2	6	5	−3	8	6	−3	9	7	−3	10	9	−2	11
1.00E−03	4	−2	6	5	−1.3	6.3	6	−2	8	7	−1.5	8.5	9	−2	11	10	−0.5	10.5
1.00E−04	5	−1.85	6.85	6	−1.2	7.2	7	−1.85	8.85	8	−1.3	9.3	10	−1.85	11.85	11	−0.2	11.2
1.00E−05	7	−1.8	8.8	8	−1	9	8	−1.8	9.8	9	−1.2	10.2	12	−1.8	13.8	12	0	12

[24]: 2L-TC 4PSK.
[a] Five level AES two level LDPCC-16CPFSK.

As it can be seen from simulation results, ML/AES-LDPCC-CPFSK schemes have better error performance than 2L-TC 4PSK [24] models.

8. Conclusion

In this paper, we present a new joint encryption and error correction structure to ensure secure and robust communication in WSSUS channels without additional complexity. For this purpose, we introduce Multilevel/Advanced Encryption Standard-Low Density Parity Check Coded-Continuous Phase Frequency Shift Keying and we evaluate error performance over WSSUS channels for TU, BU and HT type of COST207 with RLS, LMS equalization. It is shown that our proposed system provides secure, reliable data transmission with high error capability, bandwidth efficiency and reduction of transmission power usage. Thus, our system has important power and bandwidth advantages and is very suitable for low power and band limited applications.

References

[1] Daemen J, Rijmen V. The block cipher Rijndael. SmartCard Research and Applications, LNCS 1820. Berlin: Springer; 2000. pp. 288–296.
[2] Daemen J, Rijmen V. AES proposal: Rijndael AES algorithm submission, September 3, 1999.
[3] FIPS 197. Advanced Encryption Standard, Federal Information Processing Standard (FIPS). Washington, D.C.: National Bureau of Standards, U.S. Department of Commerce; November 26, 2001 [Publication 197].
[4] Gallager RG. Low-density parity-check codes. Cambridge, MA: MIT Press; 1963.
[5] Zyablov V, Pinkster M. Estimation of the error-correction complexity of Gallager low-density codes. Probl Pered Inform 1975;11(January):23–6.
[6] Margulis GA. Explicit construction of graphs without short cycles and low density codes. Combinatorica 1982;2(1):71–8.
[7] Tanner R. A recursive approach to low complexity codes. IEEE Trans Inform Theory 1981;IT-27(September):533–47.
[8] MacKay DJC, Neal RM. Near Shannon limit performance of low density parity check codes. Electron Lett 1996;32(August):1645–6.
[9] Wiberg N. Codes and decoding on general graphs. Dissertation on. 440. Linköping, Sweden: Dept Elect. Linköping Univ.; 1996.
[10] Haley D, Gaudet V, Winstead C, Grant A, Schlegel C. A dual-function mixed-signal circuit for LDPC encoding/decoding. Integration VLSI J 2008, doi:10.1016/j.vlsi.2008.09.006.
[11] Cui Y, Si X, Shen Y. A novel algorithm of constructing LDPC codes with graph theory. In: CIS. 2008.
[12] Luby MG, Mitzenmacher M, Shrokrollahi MA, Spielman D, Stemann V. Practical loss-resilient codes. In: Proc 29th Annu ACM Symp Theory of Computing. 1997. p. 150–9.
[13] Johnson SJ. Burst erasure correcting LDPC codes. IEEE Trans Commun 2009;57(March (3)).
[14] Bing D, Jun Z. Design and optimization of joint network-channel LDPC code for wireless cooperative communications. ICCS 2008.
[15] Abematsu D, Ohtsuki T, Kashima T, Jarot SPW. LDPC codes for high data rate multiband OFDM systems over 1 Gbps. PACRIM'07.
[16] Nik HP, Fekri F. Results on punctured low-density parity-check codes and improved iterative decoding techniques. IEEE Trans Inform Theory 2007;53(February (2)).
[17] Rimoldi BE. A decomposition approach to CPM. IEEE Trans Inform Theory 1988;34(March):260–70.
[18] Osman O. Blind equalization of multilevel turbo coded-continuous phase frequency shift keying over MIMO channels: research articles. Int J Commun Syst 2007;20(January (1)):103–19.
[19] Sakamoto T, Kawanishi T, Izutsu M. Continuous-phase frequency-shift keying with external modulation. IEEE J Sel Top Quantum Electron 2006;12(July/August (4)).
[20] Altay G. Performance of systematic distance-4 binary linear block codes with continuous phase frequency shift keying over MIMO systems. Wireless Pers Commun 2008;44:403–13, doi:10.1007/s11277-007-9364-2.
[21] Cheng CC, Lu CC. Space-time code design for CPFSK modulation over frequency-nonselective fading channels. IEEE Trans Commun 2005;53(September (9)).
[22] Limpaphayom P, Winick KA. Power and bandwidth-efficient communications using LDPC codes. IEEE Trans Commun 2004;52(March (3)):350–4.
[23] Hekim Y, Odabasioglu N, Ucan ON. Performance of low density parity check coded continuous phase frequency shift keying (LDPCC-CPFSK) over fading channels. Int J Commun Syst 2007;20:397–410.
[24] Ucan ON, Buyukatak K, Gose E, Osman O, Odabasioglu N. Performance of multilevel-turbo codes with blind/non-blind equalization over WSSUS multipath channels. Int J Commun Syst 2006;19:281–97.