

# Novel Blind Identification of LDPC Codes Using Average LLR of Syndrome *a Posteriori* Probability

Tian Xia and Hsiao-Chun Wu, *Senior Member, IEEE*

**Abstract**—Blind signal processing methods have been very popular recently since they can play crucial roles in the prevalent cognitive radio research. Blind encoder identification has drawn research interest lately. In this paper, we would like to tackle the blind identification of binary low-density parity-check (LDPC) codes for binary phase-shift keying (BPSK) signals. We propose a novel blind identification system which consists of three components, namely expectation-maximization (EM) estimator for signal amplitude and noise variance, log-likelihood ratio (LLR) estimator for syndrome *a posteriori* probabilities, and maximum average LLR detector. Monte Carlo simulation results demonstrate that our proposed blind LDPC encoder identification scheme is very promising even for low signal-to-noise ratio conditions.

**Index Terms**—Blind signal processing, low-density parity-check (LDPC) codes, expectation maximization (EM), cognitive radio.

## I. INTRODUCTION

ADAPTIVE modulation and coding (AMC) techniques can adjust the quality of service for communication sessions through time varying channels so as to seek the tradeoff between data rate (throughput) and bit-error-rate performance. Based on the feedback channel state information (CSI), the AMC transmitter dynamically selects an appropriate combination of modulator and channel encoder from the predefined candidate pool [1]–[6]. In conventional AMC techniques, a *control channel* is necessary to be facilitated to coordinate the changes in modulation/demodulation and coding/decoding mechanisms at both transmitter and receiver. Although this strategy makes the receiver easy to synchronize with the transmitter changes, either additional spectral resource or spectral efficiency reduction is definitely required thereupon.

On the other hand, *blind signal processing* techniques would be very useful for modern communication applications if the training sequences or the aforementioned control channel is absent from any AMC transceiver. One example is *blind equalization* for cognitive radio receivers [7]. Besides, receivers can

rely on *blind classification* techniques to determine the modulation types of the transmitted signals directly from the received signal data [8], [9]. Furthermore, *blind identification* of channel encoders was also investigated in [10]–[15] at the primitive stage lately. This paper will be dedicated to the study on blind channel-encoder identification as well.

The blind encoder identification may play a significant role in cognitive radio or wireless sensor networks (WSNs). In a WSN, individual sensor nodes (transmitters) can adopt AMC techniques to choose different encoders of different rates and codeword-lengths. In order to reduce energy consumption, the sensor nodes would prefer not to frequently transmit overheads to specify these changes because the transmitting data rates of the sensor nodes are already quite low. Sometimes, the overhead transmission may not even be feasible since the sensor nodes cannot be built upon sophisticated protocols. In this scenario, the sink (receiver) with sufficient power supply and computational capacity has to blindly identify the encoder used by each individual sensor node from time to time.

Since no *a priori* knowledge about the transmitted data is given at the receiver, the receiver has to utilize the redundancy introduced by the channel encoder of the transmitter to identify which kind of encoder the transmitter actually employs. The statistical characteristics, say the *log-likelihood ratios* (LLRs) of the received signals, are usually invoked to extract the essential information in the existing blind channel-encoder identification approaches [10]–[12]. In addition, for *space-time block codes* (STBCs), which can be considered as a special kind of channel codes, the *space-time redundancy* of the received signal samples is exploited to distinguish coding schemes [10]. For most channel coding schemes involving parity-check symbols, the mathematical structures inferred by the parity check symbols over the *Galois field* are explored for identifying the original encoder at the receiver [11].

Recently, a fast blind identification scheme of channel codes was proposed in [11]. The *parity-check relations* inferred by the *syndrome former* were investigated; the log-likelihood ratio function arising from the syndrome *a posteriori* probability (APP) was established and two detection algorithms were based on the cumulative metric of LLRs [11]. The detection performances were evaluated by the receiver-operating characteristics for some commonly-used convolutional codes [11]. In [12], a fast algorithm was proposed to detect an *additional lonely bit* (ALB) by identifying two different linear codes. The idea is that the value of the ALB (“0” or “1”) is used to determine which encoder is adopted; thus identifying the encoder would lead to the value of the ALB without decoding it. In [11], [12],

Manuscript received December 19, 2012; revised April 13, 2013 and June 18, 2013; accepted November 10, 2013. Date of publication December 03, 2013; date of current version January 14, 2014. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Rong-Rong Chen. This work was supported in part by Alcatel-Lucent Bell Labs, National Science Foundation of USA (NSF-CNS-NeTS: 0963793), and by the Louisiana Board of Regents (LEQSF-EPS(2013)-OPT-IN-26, LEQSF-EPS(2011)-OPT-IN-03, LEQSF(2011)-PFUND-242).

The authors are with the School of Electrical Engineering and Computer Science, Louisiana State University, Baton Rouge, LA 70803 USA (e-mail: txia5@lsu.edu; wu@ece.lsu.edu).

Digital Object Identifier 10.1109/TSP.2013.2293975

the blind encoder detection was illustrated only for the binary hypothesis (two encoder candidates were considered).

As blind channel-encoder identification recently emerges as an important topic, we would like to dedicate research endeavors to innovative methods in this field. We would like to focus on blind identification of *low-density parity-check* (LDPC) codes because there exists no detailed blind identification scheme tailored for multiple LDPC encoders so far to the best of our knowledge. LDPC codes, first introduced by pioneer Gallager (see [16]) and then revived after more than thirty years of hibernation (see [17]), are believed to be capable of approaching Shannon-capacity [18] and outperform prevalent turbo codes when codeword block lengths get sufficiently large [19]. Since the revivification of LDPC coding techniques, there has been a considerable amount of research work dedicated to the pertinent studies over the last two decades, including [20]–[22]. Due to their superior error-correction performance and high code-rates, LDPC codes are becoming more and more favorable in the future wireless communication standards. For example, IEEE 802.11n standard has specified the LDPC codes as a forward error-correction (FEC) option for high-performance, high-throughput networks [23].

In this paper, we extend and modify the idea in [11] to blindly identify binary LDPC codes for binary phase-shift keying (BPSK) signals over the additive white Gaussian noise (AWGN) channel. The underlying assumption is that the receiver has the knowledge of the complete encoder candidate set. The contributions of this paper can be highlighted as follows. First, our new blind identification method incorporates blind estimators for the received signal amplitude and the noise variance. Specifically, two statistical signal processing methods, namely the *second-order/fourth-order moment* method ( $M_2/M_4$ ) (see [24]) and the *expectation-maximization* (EM) algorithm (see [25]) are adopted and benchmarked with the corresponding Cramer-Rao lower bounds (CRLBs). Second, other than the cumulative LLRs used for threshold detection in [11], we propose to use the average LLR metric which is normalized by the number of parity-check bits so as to improve the identification performance for the encoders with different codeword lengths and different coding rates.

The rest of this paper is organized as follows. The basic transceiver system diagram and the signal model are introduced in Section II. The blind LDPC encoder identification problem and our proposed solution are presented in Section III. How to blindly estimate two crucial parameters, namely signal amplitude and noise variance, are discussed in Section IV, where the corresponding Cramer-Rao lower bounds are also derived. Monte Carlo simulation results are demonstrated in Section V to evaluate the effectiveness of our proposed new scheme. Conclusion will be drawn in Section VI.

#### A. Nomenclature

A *vector* is represented as a bold-face lower-case symbol such as  $\mathbf{x}$ , while a *matrix* is represented as a bold-face upper-case symbol such as  $\mathbf{X}$ . The superscript  $(\ )^T$  denotes the transpose of a vector or a matrix.  $P_r\{\mathcal{A}\}$  represents a *cumulative distribution function* (CDF) where  $\mathcal{A}$  is the underlying event or condition, while  $p(x)$  denotes the *probability density function* (PDF) of a

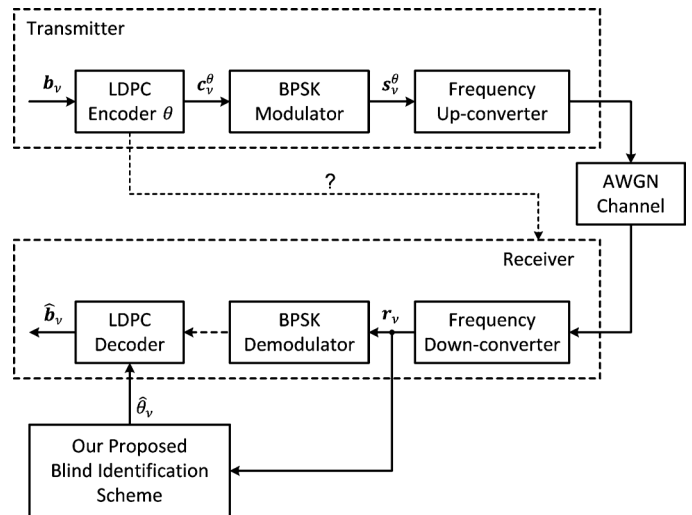


Fig. 1. The system diagram of a basic transceiver model.

random variable  $x$ .  $\mathbb{E}\{\ \}$  stands for the statistical expectation. The Galois field of an integer  $q$  is denoted by  $\mathbb{GF}(q)$ . The set of all integers is denoted by  $\mathcal{Z}$ , the set of all positive integers is denoted by  $\mathcal{Z}^+$ , and the set of real numbers is denoted by  $\mathcal{R}$ . If a set  $\mathcal{S}$  has a finite number of elements, then  $|\mathcal{S}|$  denotes the total number of its elements. A *zero matrix* or *zero vector*  $\mathbf{0}$  has all zero elements.

## II. BASIC TRANSCIVER MODEL

In this section, we will introduce the basic system model for the transceivers involving LDPC coder/decoder. The block diagram of the transceiver involving our proposed new blind LDPC channel-encoder identification mechanism is depicted in Fig. 1. Without loss of generality, let's not consider source encoder/decoder here. Denote the sets  $\mathcal{Z}_2 \stackrel{\text{def}}{=} \{0, 1\}$  and  $\mathcal{B} \stackrel{\text{def}}{=} \{-1, 1\}$ . At the transmitter, original information bits are grouped in blocks, each of which consists  $k$  consecutive bits, say  $\mathbf{b}_\nu \in \mathcal{Z}_2^{k \times 1}$ , where  $\nu \in \mathcal{Z}$  is the *block index*. This block of information bits are passed to the "LDPC encoder  $\theta$ " to generate a corresponding block of "codeword" or "coded bits", say  $\mathbf{c}_\nu^\theta \in \mathcal{Z}_2^{n \times 1}$ , where  $\theta$  denotes a particular type of LDPC encoder. Obviously the corresponding code rate is  $R = k/n$ . Then, the codeword  $\mathbf{c}_\nu^\theta$  should be modulated by BPSK modulator and the corresponding block of modulated symbols are denoted by  $\mathbf{s}_\nu^\theta \in \mathcal{B}^{n \times 1}$ . These modulated BPSK symbols will undergo a "frequency up-converter" to engender the *pass-band signals* for actual transmission.

The transmitted pass-band signals travel through the channel and arrive at the receiver. They will go through the "frequency down-converter" first to come back to the baseband. In this paper, we assume that both frequency and frame synchronizations are properly carried out prior to encoder identification. It is possible that joint frequency synchronization, frame synchronization, and encoder identification can be accomplished blindly using the techniques in [26], [27] and the proposed encoder identification scheme here in this paper. Nevertheless, we focus on the new blind encoder identification scheme throughout this paper. The received baseband signal symbols are also collected in blocks, say  $\mathbf{r}_\nu \in \mathcal{R}^{n \times 1}$ ,  $\nu \in \mathcal{Z}$ . Instead of passing  $\mathbf{r}_\nu$  to

the ‘‘BPSK demodulator’’ as in the standard receivers, we propose to feed  $\mathbf{r}_\nu$  to our new ‘‘blind identification scheme’’ to identify  $\theta$ , the unknown LDPC encoder adopted in the transmitter. Once the encoder type is identified by our proposed scheme as  $\hat{\theta}_\nu$ , where the subscript  $\nu$  means that it is estimated from the  $\nu^{\text{th}}$  block of received signal samples, then the appropriate LDPC decoder can be employed to construct the information symbol estimates  $\hat{\mathbf{b}}_\nu$ .

Consider the AWGN channel here. Each element of the  $\nu^{\text{th}}$  block of received baseband signal samples,  $\mathbf{r}_\nu \stackrel{\text{def}}{=} [r_{\nu,0}, r_{\nu,1}, \dots, r_{\nu,j}, \dots, r_{\nu,n-1}]^T$ , can be expressed as

$$r_{\nu,j} = a_\nu s_{\nu,j}^\theta + w_{\nu,j}, \quad j = 0, 1, \dots, n-1, \quad (1)$$

where  $a_\nu$  is the unknown signal amplitude accounting for the processing gain and the channel gain,  $s_{\nu,j}^\theta \in \mathcal{B}$  is the modulated BPSK signal generated from the encoder  $\theta$ , and  $w_{\nu,j}$  is the zero-mean AWGN with the variance  $\mathbb{E}\{w_{\nu,j}^2\} \stackrel{\text{def}}{=} \sigma_\nu^2$  for the  $j^{\text{th}}$  signal sample within the  $\nu^{\text{th}}$  block. Consequently, the *signal-to-noise ratio* (SNR) per coded bit for the  $\nu^{\text{th}}$  block of modulated signals is given by

$$\rho_\nu = \frac{a_\nu^2}{\sigma_\nu^2}. \quad (2)$$

On the other hand, according to (2), the SNR per uncoded bit for the  $\nu^{\text{th}}$  block of modulated signals is given by

$$\eta_\nu = \frac{\rho_\nu}{R} = \frac{a_\nu^2}{R\sigma_\nu^2}, \quad (3)$$

where  $R$  is the code rate.

According to Fig. 1, the receiver has no idea about the exact encoder  $\theta$  the transmitter adopts. Therefore, it needs to identify the encoder before any received signal can be decoded. Often, an LDPC encoder would have a very large parity-check matrix, and it is impossible for any receiver to blindly reproduce the exact parity-check matrix without any *a priori* knowledge. In practice, the AMC transceivers would not change their modulators and encoders arbitrarily. Therefore, one may restrict the modulation/encoder options within a given set. In this paper, we assume that a pre-determined LDPC encoder candidate set, say  $\Theta$ , which contains multiple encoder candidates, is known to both transmitter and receiver, and obviously  $\theta \in \Theta$ . We also assume that the encoders in  $\Theta$  are different from each other so that the parity-check matrices of any two encoders do not have identical row(s). It is the usual constraint for AMC schemes. Thus, we can pick up its estimate  $\hat{\theta}_\nu$  from this given set  $\Theta$  as well. We will present a new method to blindly identify the LDPC encoder adopted in the transmitter in the subsequent sections.

### III. BLIND LDPC ENCODER IDENTIFICATION

Since each LDPC code has a unique parity-check matrix, the encoder  $\theta$  can be unambiguously identified if we can successfully establish the corresponding underlying *parity-check relations* directly from the received signal data samples. The parity-check relations are manifested by that the sums of certain coded bits in the codeword block over the Galois field  $\mathbb{GF}(2)$  are zero. To achieve this, we first formulate the log-likelihood

ratio (LLR) of the syndrome *a posteriori* probability (APP) in this section. The similar LLR metric was used for the iterative convolutional decoder in [28]. Henceforth, we propose a novel blind LDPC encoder identification scheme, which is based on this feature, the average LLR of the LDPC syndrome APP. The details are established in the following subsections.

#### A. Log-Likelihood Ratio

Since we need to rely on the LLR metric for the blind LDPC encoder identification in this paper, a preliminary introduction on the log-likelihood ratio formulation for a binary random process is provided here. The log-likelihood ratio of a binary random variable  $X$  can be facilitated as

$$\mathcal{L}_X(x) = \ln \frac{P_r\{x=0\}}{P_r\{x=1\}}, \quad (4)$$

which is the natural logarithm of the ratio between the probabilities of  $X$  taking values 0 and 1, respectively. Given another random variable, say  $Y$ , then the LLR of  $X$  conditioned on  $Y$  is given by

$$\mathcal{L}_{X|Y}(x|y) = \ln \frac{P_r\{x=0|y\}}{P_r\{x=1|y\}}. \quad (5)$$

According to the Bayes’s Theorem, we get

$$\begin{aligned} \mathcal{L}_{X|Y}(x|y) &= \ln \frac{P_r\{y|x=0\}}{P_r\{y|x=1\}} + \ln \frac{P_r\{x=0\}}{P_r\{x=1\}} \\ &= \mathcal{L}_{Y|X}(y|x) + \mathcal{L}_X(x). \end{aligned} \quad (6)$$

Without any ambiguity, we hereafter simplify the notations of  $\mathcal{L}_X(x)$ ,  $\mathcal{L}_{X|Y}(x|y)$ , and  $\mathcal{L}_{Y|X}(y|x)$  as  $\mathcal{L}(x)$ ,  $\mathcal{L}(x|y)$ , and  $\mathcal{L}(y|x)$ , respectively. Let  $\oplus$  denote the addition over Galois field  $\mathbb{GF}(2)$  (or exclusive-OR operation). A *box-plus* operation, denoted by  $\boxplus$ , can be formulated according to [28] as follows:

$$\begin{aligned} &\mathcal{L}(x_1 \oplus x_2 \oplus \dots \oplus x_n) \\ &\stackrel{\text{def}}{=} \boxplus_{j=1}^n \mathcal{L}(x_j) \\ &\stackrel{\text{def}}{=} \mathcal{L}(x_1) \boxplus \mathcal{L}(x_2) \boxplus \dots \boxplus \mathcal{L}(x_n) \\ &= 2 \tanh^{-1} \left( \prod_{j=1}^n \tanh \left( \mathcal{L}(x_j)/2 \right) \right). \end{aligned} \quad (7)$$

#### B. LDPC Codes Identification

Given an encoder  $\theta' \in \Theta$ , one can determine its parity-check matrix  $\mathbf{H}_{\theta'} \in \mathbb{Z}_2^{(n-k) \times n}$ , and obtain

$$\mathbf{H}_{\theta'} \mathbf{c}_\nu^\theta = \mathbf{0}, \quad \text{if and only if } \theta' = \theta, \quad (8)$$

where  $\mathbf{c}_\nu^\theta$  is the coded sequence from encoder  $\theta$  with length  $n$ , and  $\mathbf{0}$  is the  $(n-k) \times 1$  zero vector. The ‘‘only if’’ implication in (8) holds because the encoders in the candidate set  $\Theta$  are assumed to be different from each other as stated in the end of Section II. That is, the candidate LDPC encoder  $\theta'$  is exactly the encoder  $\theta$  adopted at the transmitter within the  $\nu^{\text{th}}$  block. Equation (8) describes the so-called parity-check relations.

Denote the locations of the non-zero elements at the  $i^{\text{th}}$  row of the parity check matrix  $\mathbf{H}_{\theta'}$  by a vector

$\mathbf{l}_i^{\theta'} = [l_{i_1}, l_{i_2}, \dots, l_{i_{N_i}}]^T$  ( $0 \leq l_{i_1} < l_{i_2} < \dots < l_{i_{N_i}} \leq n-1$ ), where  $N_i$  is the total number of the non-zero elements in the  $i^{\text{th}}$  row of  $\mathbf{H}_{\theta'}$ . Note that the location of the first element in any row of  $\mathbf{H}_{\theta'}$  is indexed as “0” instead of “1”. Denote  $\mathbf{c}_\nu^{\theta'} \stackrel{\text{def}}{=} [c_{\nu,0}, c_{\nu,1}, \dots, c_{\nu,n-1}]^T$ . Thus, we can rewrite (8) as

$$c_{\nu,l_{i_1}} \oplus c_{\nu,l_{i_2}} \oplus \dots \oplus c_{\nu,l_{i_{N_i}}} = 0, \quad \forall 1 \leq i \leq n-k, \quad (9)$$

if and only if  $\theta' = \theta$  (the estimated encoder at the receiver is exactly the encoder adopted at the transmitter).

According to (6), we can have

$$\begin{aligned} \mathcal{L}(c_{\nu,j}|r_{\nu,j}) &= \mathcal{L}(r_{\nu,j}|c_{\nu,j}) + \mathcal{L}(c_{\nu,j}) \\ &= \mathcal{L}(r_{\nu,j}|c_{\nu,j}), \quad 0 \leq j \leq n-1, \end{aligned} \quad (10)$$

where  $\mathcal{L}(c_{\nu,j}) = 0$  because each bit in any LDPC codeword is assumed to have equal probabilities of taking value 0 or 1. Consider  $\mathcal{L}(c_{\nu,j}|r_{\nu,j})$  as the messages which are assumed to be conditionally independent of each other [18]. If an encoder candidate  $\theta'$  is picked at the receiver, according to (7)–(10), we obtain the LLR of the syndrome *a posteriori* probability (APP) for the  $i^{\text{th}}$  parity check bit ( $i = 1, 2, \dots, n-k$ ) in the  $\nu^{\text{th}}$  block as follows:

$$\begin{aligned} \gamma_{\nu,i}^{\theta'} &\stackrel{\text{def}}{=} \mathcal{L}(c_{\nu,l_{i_1}} \oplus c_{\nu,l_{i_2}} \oplus \dots \oplus c_{\nu,l_{i_{N_i}}} | r_{\nu,l_{i_1}} r_{\nu,l_{i_2}} \dots r_{\nu,l_{i_{N_i}}}) \\ &= \boxplus_{j=1}^{N_i} \mathcal{L}(c_{\nu,l_{i_j}} | r_{\nu,l_{i_j}}) \\ &= 2 \tanh^{-1} \left( \prod_{j=1}^{N_i} \tanh \left( \mathcal{L}(r_{\nu,l_{i_j}} | c_{\nu,l_{i_j}}) / 2 \right) \right). \end{aligned} \quad (11)$$

According to the LLR definition given by (4) and the parity check relations given by (9), the LLR of the syndrome APP,  $\gamma_{\nu,i}^{\theta'}$ , is expected to be a positive value when  $\theta' = \theta$ . One may take the average over the individual LLRs  $\gamma_{\nu,i}^{\theta'}$ ,  $\forall i$ , for the entire block  $\nu$ , and the “positiveness” of the average LLR will be more substantial when  $\theta' = \theta$ . On the other hand, if  $\theta' \neq \theta$ , individual LLRs  $\gamma_{\nu,i}^{\theta'}$  within the same block  $\nu$  may be sometimes positive and sometimes negative and they often cancel each other when we calculate the corresponding average LLR. The average LLR for the  $\nu^{\text{th}}$  block of received signal data subject to the encoder candidate  $\theta'$  is thus given by

$$\Gamma_\nu^{\theta'} \stackrel{\text{def}}{=} \frac{1}{n-k} \sum_{i=1}^{n-k} \gamma_{\nu,i}^{\theta'}. \quad (12)$$

Note that different encoders  $\theta'$  have different values of  $n$  and  $k$  so that the values of  $n-k$  (the number of parity-check bits) appear different. Consequently, according to (11) and (12), the underlying LDPC encoder for the  $\nu^{\text{th}}$  block of received signals can be identified as

$$\hat{\theta}_\nu = \arg \max_{\theta' \in \Theta} \Gamma_\nu^{\theta'}, \quad (13)$$

where  $\Theta$  is the collection of all possible candidates for the LDPC encoders adopted in the transmitter. Note that one needs to carry out  $\Gamma_\nu^{\theta'}$  for every possible candidate  $\theta'$  in  $\Theta$  according to (12). Alternatively, in order to facilitate the relationship between the

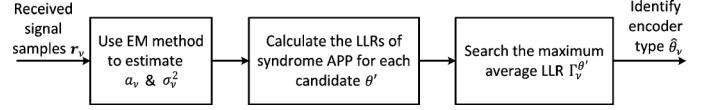


Fig. 2. The block diagram of our proposed new blind LDPC encoder identification system.

average LLR and the number of parity-check bits, the average LLR for the first  $\iota$  parity-check bits of the  $\nu^{\text{th}}$  block of received signal samples subject to the encoder candidate  $\theta'$  is given by

$$\Gamma_\nu^{\theta'}(\iota) \stackrel{\text{def}}{=} \frac{1}{\iota} \sum_{i=1}^{\iota} \gamma_{\nu,i}^{\theta'}, \quad \iota = 1, 2, \dots, n-k. \quad (14)$$

It can be easily seen that (12) is a special case of (14) when  $\iota = n-k$ . According to the system model given by (1), we can write

$$\mathcal{L}(r_{\nu,l_{i_j}} | c_{\nu,l_{i_j}}) = \ln \frac{\exp \left[ -\frac{(r_{\nu,l_{i_j}} - a_\nu)^2}{2\sigma_\nu^2} \right]}{\exp \left[ -\frac{(r_{\nu,l_{i_j}} + a_\nu)^2}{2\sigma_\nu^2} \right]} = \frac{2a_\nu r_{\nu,l_{i_j}}}{\sigma_\nu^2}. \quad (15)$$

To carry out (13), one needs to calculate (15) first. However, the receiver has no *a priori* knowledge of the signal amplitude  $a_\nu$  and the noise variance  $\sigma_\nu^2$ . Therefore, they need to be *blindly* estimated prior to the calculation of the LLRs of syndrome APP  $\gamma_{\nu,i}^{\theta'}$ . We propose the blind estimators for  $a_\nu$  and  $\sigma_\nu^2$  in the following section, which can serve as the frontend mechanism to complete our new blind LDPC encoder identification system, as depicted in Fig. 2.

#### IV. BLIND PARAMETER ESTIMATION

As discussed in Section III, signal amplitude and noise variance are two parameters one needs to estimate first for blind LDPC-encoder identification. Since we focus on the blind scheme, the corresponding estimators have to be blind as well. There exist several *non-data aided* methods to estimate signal amplitude and noise variance, such as the  $M_2/M_4$  estimator [24] and the EM (expectation maximization) estimator [25], [29]. The  $M_2/M_4$  method works well for *constant modulus modulations* such as phase-shift keying (PSK). The received signals formulated by (1) constitute a Gaussian mixture where the EM algorithm can be used to estimate the associated essential parameters. Therefore, we propose to use these two methods to estimate the signal amplitude  $a_\nu$  and the noise variance  $\sigma_\nu^2$ , and then compare their performances with the corresponding CRLBs. In the next subsection, we will present the formulae for the CRLBs of  $a_\nu$  and  $\sigma_\nu^2$ , respectively.

##### A. CRLBs

It is well known that for any underlying statistical parameter to be estimated, among all unbiased estimators, the CRLB facilitates the minimum variance. Hence we can use the CRLB as the benchmark to evaluate any estimator. As mentioned in Section III-B, LDPC coded bits can take either 0 or 1 with equal probability and they are assumed statistically independent of

each other. According to (1), the PDF of a received signal block  $\mathbf{r}_\nu$  can thus be represented by

$$p(\mathbf{r}_\nu) = \prod_{j=0}^{n-1} \frac{1}{2} \frac{1}{\sqrt{2\pi\sigma_\nu^2}} \left[ \exp\left(-\frac{(r_{\nu,j} - a_\nu)^2}{2\sigma_\nu^2}\right) + \exp\left(-\frac{(r_{\nu,j} + a_\nu)^2}{2\sigma_\nu^2}\right) \right]. \quad (16)$$

The associated log-likelihood function is thus given by

$$\ln p(\mathbf{r}_\nu) = -\frac{n}{2} \ln(2\pi\sigma_\nu^2) - \frac{1}{2\sigma_\nu^2} \sum_{j=0}^{n-1} (r_{\nu,j}^2 + a_\nu^2) + \sum_{j=0}^{n-1} \ln \left( \cosh\left(\frac{a_\nu r_{\nu,j}}{\sigma_\nu^2}\right) \right). \quad (17)$$

Denote  $\boldsymbol{\lambda} \stackrel{\text{def}}{=} [a_\nu, \sigma_\nu^2]^T$  the vector of the unknown parameters. According to [30], the inverse of the *Fisher information matrix* can thus be expressed as

$$\mathbf{I}^{-1}(\boldsymbol{\lambda}) = \frac{2\sigma_\nu^2}{n g(\rho_\nu)} \begin{bmatrix} \frac{1}{2} - \rho_\nu f(\rho_\nu) & -a_\nu f(\rho_\nu) \\ -a_\nu f(\rho_\nu) & \sigma_\nu^2 - \sigma_\nu^2 f(\rho_\nu) \end{bmatrix}, \quad (18)$$

where  $\rho_\nu$  is defined by (2),

$$g(\rho_\nu) \stackrel{\text{def}}{=} 1 - f(\rho_\nu) - 2\rho_\nu f(\rho_\nu), \quad (19)$$

and

$$f(\rho_\nu) \stackrel{\text{def}}{=} \frac{\exp(-\frac{\rho_\nu}{2})}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \frac{u^2 \exp(-\frac{u^2}{2})}{\cosh(u\sqrt{\rho_\nu})} du. \quad (20)$$

The CRLBs for the signal amplitude  $a_\nu$  and the noise variance  $\sigma_\nu^2$  are found as the diagonal elements of  $\mathbf{I}^{-1}(\boldsymbol{\lambda})$  such that

$$CRLB_{a_\nu} = \frac{\sigma_\nu^2(1 - 2\rho_\nu f(\rho_\nu))}{n g(\rho_\nu)}, \quad (21)$$

$$CRLB_{\sigma_\nu^2} = \frac{2\sigma_\nu^4(1 - f(\rho_\nu))}{n g(\rho_\nu)}. \quad (22)$$

The corresponding *normalized CRLBs* are defined as

$$NCRLB_{a_\nu} \stackrel{\text{def}}{=} \frac{CRLB_{a_\nu}}{a_\nu^2} \quad (23)$$

and

$$NCRLB_{\sigma_\nu^2} \stackrel{\text{def}}{=} \frac{CRLB_{\sigma_\nu^2}}{\sigma_\nu^4}, \quad (24)$$

respectively.

### B. The $M_2/M_4$ Estimator

From (1), the second-order moment of the received signal sample  $r_{\nu,j}$  is given by

$$M_2 \stackrel{\text{def}}{=} \mathbb{E}\{r_{\nu,j}^2\} = a_\nu^2 + \sigma_\nu^2, \quad (25)$$

while the fourth-order moment of  $r_{\nu,j}$  is given by

$$M_4 \stackrel{\text{def}}{=} \mathbb{E}\{r_{\nu,j}^4\} = a_\nu^4 + 6a_\nu^2\sigma_\nu^2 + 3\sigma_\nu^4. \quad (26)$$

Solving both (25) and (26) together with respect to the two variables  $a_\nu$  and  $\sigma_\nu^2$ , one can get

$$a_\nu = \frac{\sqrt{6M_2^2 - 2M_4}}{\sqrt{2}} \quad (27)$$

and

$$\sigma_\nu^2 = M_2 - \frac{\sqrt{6M_2^2 - 2M_4}}{2}, \quad (28)$$

where  $a_\nu$  is assumed to be non-negative. In practice,  $M_2$  and  $M_4$  have to be estimated by the sample averages over the  $\nu^{\text{th}}$  block such that

$$\hat{M}_2 = \frac{1}{n} \sum_{j=0}^{n-1} r_{\nu,j}^2 \quad (29)$$

and

$$\hat{M}_4 = \frac{1}{n} \sum_{j=0}^{n-1} r_{\nu,j}^4. \quad (30)$$

Substituting (29) and (30) into (27) and (28), we can obtain the  $M_2/M_4$  estimators for  $a_\nu$  and  $\sigma_\nu^2$ .

### C. The EM Estimator

EM estimators have recently been applied for the parameter estimation in wireless communication systems [31], [32]. Here we will establish a EM estimator for determining the signal amplitude  $a_\nu$  and the noise variance  $\sigma_\nu^2$ . According to the system model given by (1), it is obvious that the received signal symbols  $r_{\nu,j}$  constitute a double-modal Gaussian mixture. Upon receiving  $r_{\nu,j}$ ,  $j = 0, 1, \dots, n-1$ , our proposed EM algorithm is presented below.

First, initialize the parameters  $a_\nu$  and  $\sigma_\nu^2$  using *K-means* clustering method for a few iterations. The weight of each Gaussian mode is fixed to 1/2 as we assume that each bit in any LDPC codeword has equal probability for taking value of either 0 or 1.

At the E-step, compute

$$\hat{\beta}_{j,m} = \frac{p_m(r_{\nu,j}|\hat{a}_\nu, \hat{\sigma}_\nu^2)}{\sum_{m=1}^2 p_m(r_{\nu,j}|\hat{a}_\nu, \hat{\sigma}_\nu^2)}, \quad (31)$$

where

$$p_m(r_{\nu,j}|\hat{a}_\nu, \hat{\sigma}_\nu^2) \stackrel{\text{def}}{=} \frac{1}{\sqrt{2\pi\hat{\sigma}_\nu^2}} \exp\left(-\frac{(r_{\nu,j} - \hat{a}_\nu x_m)^2}{2\hat{\sigma}_\nu^2}\right),$$

where  $x_1 \stackrel{\text{def}}{=} 1$ ,  $x_2 \stackrel{\text{def}}{=} -1$  for  $m = 1, 2$ .

At the M-step, compute the new estimates

$$\hat{a}_\nu = \frac{1}{n} \sum_{j=0}^{n-1} \sum_{m=1}^2 \hat{\beta}_{j,m} x_m r_{\nu,j}, \quad (32)$$

$$\hat{\sigma}_\nu^2 = \frac{1}{n} \sum_{j=0}^{n-1} \sum_{m=1}^2 \hat{\beta}_{j,m} (r_{\nu,j} - \hat{a}_\nu x_m)^2. \quad (33)$$

Take several iterations of E-step and M-step recursively until the pre-determined convergence criterion is satisfied.

#### D. Normalized Mean-Square-Error

To evaluate the performances of the above-mentioned estimators in Sections IV-B and IV-C, one may use the *normalized mean-square-error* (NMSE) as the measure. The NMSEs for  $a_\nu$  and  $\sigma_\nu^2$  are given by

$$NMSE_{a_\nu} \stackrel{\text{def}}{=} \mathbb{E} \left\{ \left( \frac{\hat{a}_\nu - a_\nu}{a_\nu} \right)^2 \right\} \approx \frac{1}{N} \sum_{t=1}^N \left( \frac{\hat{a}_\nu^{(t)} - a_\nu}{a_\nu} \right)^2 \quad (34)$$

and

$$NMSE_{\sigma_\nu^2} \stackrel{\text{def}}{=} \mathbb{E} \left\{ \left( \frac{\hat{\sigma}_\nu^2 - \sigma_\nu^2}{\sigma_\nu^2} \right)^2 \right\} \approx \frac{1}{N} \sum_{t=1}^N \left( \frac{\hat{\sigma}_\nu^{2(t)} - \sigma_\nu^2}{\sigma_\nu^2} \right)^2, \quad (35)$$

where the superscript  $(t)$  indicates the trial index;  $N$  is the total number of Monte Carlo trials;  $a_\nu$  and  $\sigma_\nu^2$  are true values;  $\hat{a}_\nu$  and  $\hat{\sigma}_\nu^2$  are the corresponding estimates, respectively.

### V. SIMULATION

The performance of our new blind LDPC-encoder identification scheme is evaluated by computer simulations in this section. The performance metric we choose is the *probability of detection*. It is the probability that the receiver can correctly identify the types of the LDPC encoders the transmitter adopts, i.e.,  $P_D = P_r\{\hat{\theta}_\nu = \theta_\nu\}$ . The LDPC parity-check matrices defined in the IEEE 802.11n standard are used in our simulations [23]. Accordingly, three codeword block lengths  $n = 648, 1296, \text{ and } 1944$  are defined therein. For each block length  $n$ , four different parity-check matrices are specified corresponding to four different code-rates  $R = 1/2, 2/3, 3/4, \text{ and } 5/6$ . Hence, there are totally twelve types of LDPC encoders defined in [23]. The corresponding encoding techniques can refer to [33] for details. The simulation results will be presented in the following subsections.

#### A. Comparative Study on Blind Parameter Estimators

In this subsection, at first, we need to evaluate different estimators for signal amplitude and noise variance stated in Section IV. Ten thousand Monte Carlo trials ( $N = 10,000$ ) are taken for statistical average. In each trial, we consider only a single signal block. We fix the LDPC encoder  $\theta : n = 648$  and  $R = 1/2$  across all different trials. The modulated BPSK symbols  $s_{\nu,j}^\theta$  have constant amplitudes, while  $a_\nu$  varies subject to a uni-variance AWGN  $w_{\nu,j}$  so as to change the SNR  $\eta_\nu$ . For each trial  $t$ , we obtain the estimates  $\hat{a}_\nu^{(t)}$  and  $\hat{\sigma}_\nu^{2(t)}$  using either  $M_2/M_4$  or EM method (executed for five iterations) as described in Section IV. Then we carry out the NMSE measures for these estimates over 10,000 trials. Besides, we calculate the normalized CRLBs as given by Section IV-A.

The NMSEs for the signal amplitude  $a_\nu$  and the noise variance  $\sigma_\nu^2$  together with the corresponding normalized CRLBs are depicted in Figs. 3 and 4, respectively. It is obvious that the  $M_2/M_4$  estimators can achieve reasonably good performances only when  $\eta_\nu > 4$  dB. If  $\eta_\nu < 4$  dB, the term  $6\hat{M}_2^2 - 2\hat{M}_4$

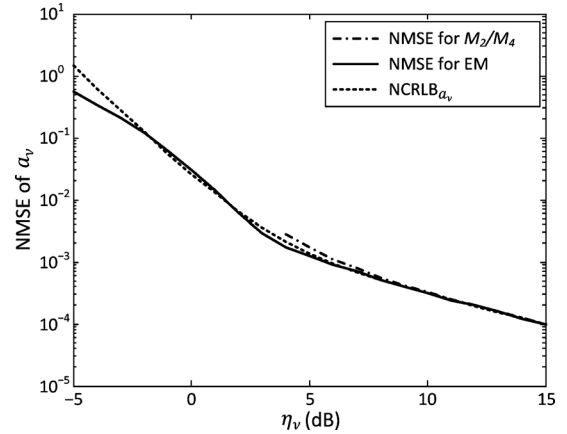


Fig. 3. The NMSEs of  $M_2/M_4$  and EM estimates of  $a_\nu$  and the corresponding CRLBs with respect to  $\eta_\nu$ .

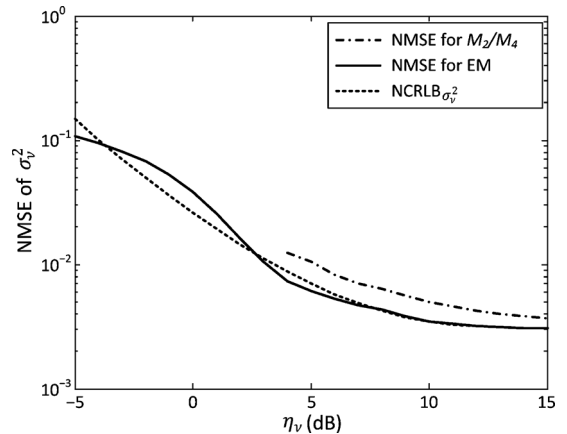


Fig. 4. The NMSEs of  $M_2/M_4$  and EM estimates of  $\sigma_\nu^2$  and the corresponding CRLBs with respect to  $\eta_\nu$ .

substituted in (27) is not necessarily always positive so that the resultant estimates would appear to be complex values, which cannot be used as legitimate parameters. Besides, the EM estimates provide us the lower NMSEs than the  $M_2/M_4$  estimators when  $\eta_\nu > 4$  dB.

Note that the NMSEs of the EM estimates sometimes fall below the NCRLBs when  $\eta_\nu < 6$  dB. Similar phenomenon was also observed in [25], [29]. As a matter of fact, the estimates produced by the EM algorithm may not always be unbiased. To study the *average biases* of the EM estimates, we have carried out 10,000 Monte Carlo simulations to measure their *normalized biases*, which are

$$NB_{a_\nu} \stackrel{\text{def}}{=} \mathbb{E} \left\{ \frac{\hat{a}_\nu - a_\nu}{a_\nu} \right\} \approx \frac{1}{N} \sum_{t=1}^N \frac{\hat{a}_\nu^{(t)} - a_\nu}{a_\nu}, \quad (36)$$

$$NB_{\sigma_\nu^2} \stackrel{\text{def}}{=} \mathbb{E} \left\{ \frac{\hat{\sigma}_\nu^2 - \sigma_\nu^2}{\sigma_\nu^2} \right\} \approx \frac{1}{N} \sum_{t=1}^N \frac{\hat{\sigma}_\nu^{2(t)} - \sigma_\nu^2}{\sigma_\nu^2}. \quad (37)$$

Fig. 5 demonstrates that the normalized biases  $NB_{a_\nu}$  and  $NB_{\sigma_\nu^2}$  are not negligible when  $\eta_\nu < 6$  dB. This explains why the NMSEs of the EM estimates can be lower than the NCRLBs in poor signal quality. Similar trends can be found

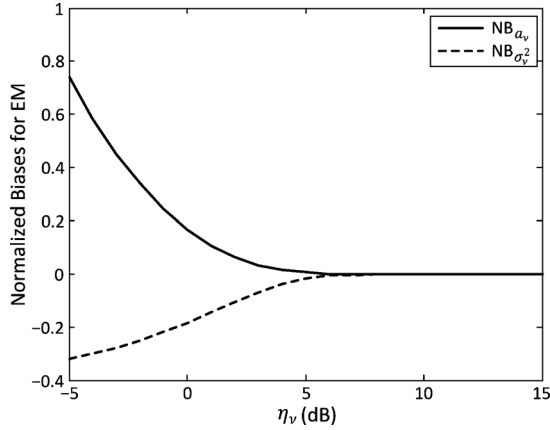


Fig. 5. The normalized biases for the EM estimates of  $a_\nu$  and  $\sigma_\nu^2$  with respect to  $\eta_\nu$ .

when different  $(n, k)$  encoders are applied for Monte Carlo simulations.

### B. Average LLRs

According to the discussion in Section V-A, we choose the EM estimators in our blind LDPC encoder identification scheme. Based on the estimates  $\hat{a}_\nu$  and  $\hat{\sigma}_\nu^2$  resulting from the EM method, the LLRs of syndrome APP are calculated and the corresponding average LLRs  $\Gamma_\nu^{\theta'}$  can be investigated. The signals and noises are generated in a similar manner to Section V-A subject to a fixed SNR  $\eta_\nu = 8$  dB. For illustration, we just fix the codeword block length to  $n = 648$  and examine the average LLRs  $\Gamma_\nu^{\theta'}$  for four different code-rates  $R = 1/2$ ,  $R = 2/3$ ,  $R = 3/4$ , and  $R = 5/6$ . Thus, we have four encoder candidates, i.e.,  $|\Theta| = 4$ . For each received signal block  $\nu$ , the receiver calculates the average LLR  $\Gamma_\nu^{\theta'}$  for each candidate  $\theta' \in \Theta$ .

To investigate the variations of the average LLRs  $\Gamma_\nu^{\theta'}(\iota)$ , each of which is constructed from the first  $\iota$  parity-check bits of the  $\nu^{\text{th}}$  block of received signal samples subject to the encoder candidate  $\theta'$ , as given by (14), we delineate Fig. 6. Each sub-figure consists of the average LLRs for four different candidates, namely  $\theta' : R = 1/2$ ,  $\theta' : R = 2/3$ ,  $\theta' : R = 3/4$ , and  $\theta' : R = 5/6$ . For different code-rates  $R$ , the numbers of parity check bits,  $n - k$ , are surely different.

According to Fig. 6, the average LLRs for  $\theta' = \theta$  reach the maximum and always stay positive among all candidates  $\theta' \in \Theta$ , that is, a correct encoder identification can be undertaken. On the contrary, for  $\theta' \neq \theta$ , the average LLRs fluctuate around zero and tend to be close to 0 as  $\iota$  increases. In addition, one may desire to use as many parity-check bits (large  $\iota$ ) as possible to reach a satisfactory encoder identification performance. If we may collect the entire received signal block to build the LLRs, the average LLR formula  $\Gamma_\nu^{\theta'}$  given by (12) is used for blind encoder identification instead. The average LLRs for the block lengths  $n = 1296$  and  $n = 1944$  have also been investigated and similar phenomena can be observed.

### C. Probability of Detection per Block

The evaluation of the probability of detection  $P_D$  per block is carried out in the same simulation set-up as Section V-B. Once

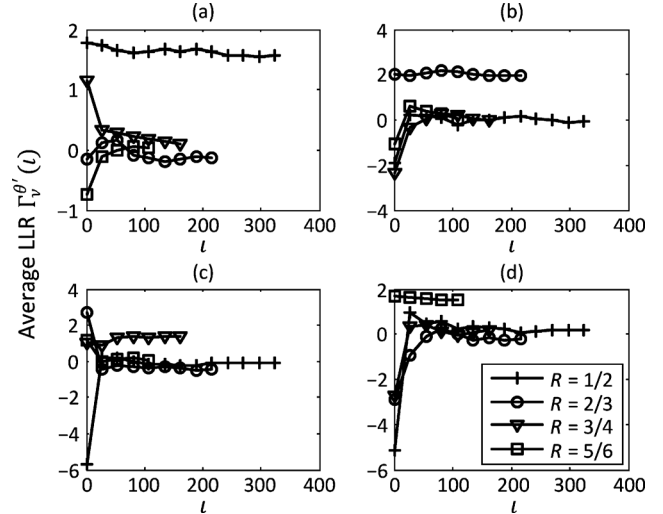


Fig. 6. The average LLRs  $\Gamma_\nu^{\theta'}(\iota)$  with respect to  $\iota$  when  $\eta_\nu = 8$  dB and  $n = 648$  for (a) the true LDPC encoder  $\theta : R = 1/2$ , (b) the true LDPC encoder  $\theta : R = 2/3$ , (c) the true LDPC encoder  $\theta : R = 3/4$ , and (d) the true LDPC encoder  $\theta : R = 5/6$ .

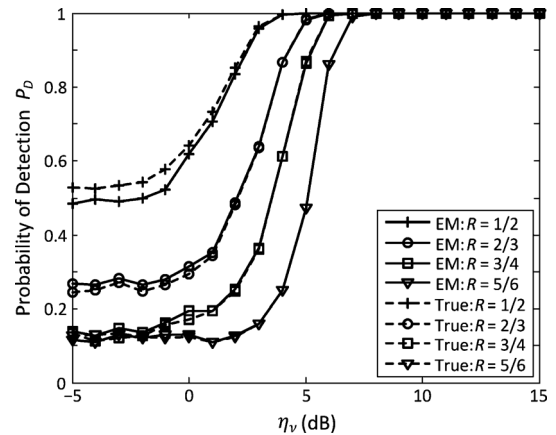


Fig. 7. The probabilities of detection  $P_D$  with respect to  $\eta_\nu$  for the codeword block length  $n = 648$  and different code-rates  $R$ .

the average LLRs are computed, the blind identification can be performed using (13).

Fig. 7 demonstrates  $P_D$  per block versus  $\eta_\nu$  for four different code-rates when the codeword length is fixed as  $n = 648$ . We also investigate the effect of the EM estimators for signal amplitude and noise variance on  $P_D$  by comparing the identification results from the estimates (denoted by “EM” in the figure) and the true values of parameters (denoted by “True” in the figure). According to Fig. 7, the EM estimators perform very well and hence they lead to very similar identification performances to those from the true values of parameters. Moreover, the lower the code-rate, the higher the probability of detection. For example, when  $\eta_\nu = 5$  dB,  $P_D$  can reach close to 100% for the code-rate  $R = 1/2$ , while  $P_D$  can only attain about 50% for the code-rate  $R = 5/6$ .

On the other hand, we fix the code-rate  $R = 5/6$  and change the codeword block length  $n$  to depict Fig. 8. According to the results shown in Fig. 7, we use the EM estimators here to facilitate a completely blind encoder identification scheme since they can lead to outstanding performances. Fig. 8 exhibits  $P_D$

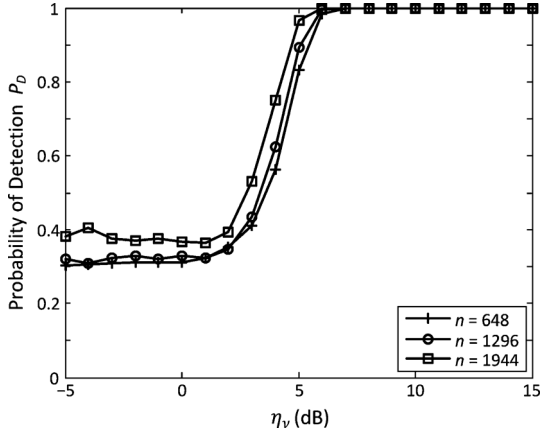


Fig. 8. The probabilities of detection  $P_D$  with respect to  $\eta_\nu$  for the code-rate  $R = 5/6$  and different codeword block lengths  $n$ .

per block versus  $\eta_\nu$  for three different codeword block lengths  $n$  ( $|\Theta| = 3$ ) for the code-rate  $R = 5/6$ . The larger the codeword block length, the higher the probability of detection  $P_D$ . Note that  $P_D$  for the codeword block length  $n = 648$  depicted in Fig. 8 is different from  $P_D$  for the same code rate  $R = 5/6$  shown in Fig. 7. The reason is simply because these two figures are based on different candidate sets  $\Theta$  and the encoder identification performance highly depends on the particular candidate set  $\Theta$ .

#### D. Probability of Detection for Multiple Blocks

Both Figs. 7 and 8 demonstrate the fact that the more parity-check bits one uses to construct the average LLRs, the better  $P_D$  performance one can expect. Therefore, it is expected that  $P_D$  would be yet higher if we collect multiple blocks jointly for blind encoder identification. In practice, the transmitter is likely to retain the same encoder for a while spanning over several consecutive codeword blocks. Assume that each encoder  $\theta$  lasts for  $M$  consecutive blocks ( $M \in \mathcal{Z}^+$ ). It yields

$$\theta_\nu = \theta_{\lfloor \nu/M \rfloor \times M}, \quad \forall \nu \in \mathcal{Z}, \quad (38)$$

where  $\lfloor \cdot \rfloor$  denotes the “integer rounding-down” operation. For instance, when  $M = 5$ , one gets  $\theta_0 = \theta_1 = \theta_2 = \theta_3 = \theta_4$ . According to (38), one can compute a single average LLR  $\bar{\Gamma}_M^{\theta'}$  over  $\Gamma_\nu^{\theta'}$ s for  $M$  consecutive blocks, which is given by

$$\bar{\Gamma}_M^{\theta'} \stackrel{\text{def}}{=} \frac{1}{M} \sum_{\nu=\tau}^{\tau+M-1} \Gamma_\nu^{\theta'}, \quad (39)$$

where  $\tau$  specifies the very first block of these  $M$  consecutive blocks. Consequently, the encoder can be blindly identified as

$$\hat{\theta}_\nu = \arg \max_{\theta' \in \Theta} \bar{\Gamma}_M^{\theta'}, \quad \text{for } \nu = \tau, \tau + 1, \dots, \tau + M - 1. \quad (40)$$

Since the signal amplitude  $a_\nu$  and the noise variance  $\sigma_\nu^2$  change with the block index  $\nu$ , the average SNR per uncoded bit over  $M$  received signal blocks,  $\eta_{\text{ave}}$ , is defined as

$$\eta_{\text{ave}} \stackrel{\text{def}}{=} \mathbb{E}\{\eta_\nu\} \approx \frac{1}{M} \sum_{\nu=\tau}^{\tau+M-1} \eta_\nu. \quad (41)$$

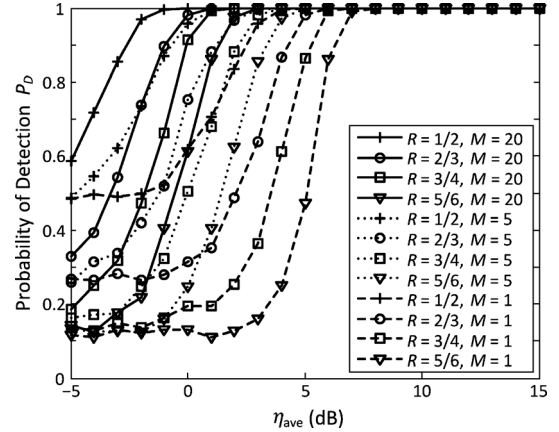


Fig. 9. The probabilities of detection  $P_D$  with respect to  $\eta_{\text{ave}}$  for the codeword block length  $n = 648$  and different code-rates  $R$  when different numbers of blocks,  $M = 1, 5,$  and  $20$ , are collected jointly for blind encoder identification.

We retain the same simulation set-up as Fig. 7 except that we use the new identification method given by (40) to depict the results in Fig. 9. Fig. 9 shows  $P_D$  versus  $\eta_{\text{ave}}$  for  $M = 1, 5,$  and  $20$ . The more the number of blocks  $M$ , the higher  $P_D$  one can expect from the blind identification results.

## VI. CONCLUSION

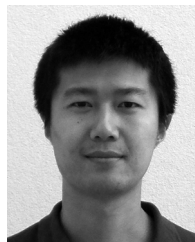
In this paper, we propose a novel blind identification method for binary LDPC encoders. Our proposed scheme is based on the log-likelihood ratios (LLRs) of the syndrome *a posteriori* probability. The average LLRs over the entire block of parity-check bits are used as the essential features to dynamically identify the LDPC encoder adopted at the transmitter. Signal amplitude and noise variance involved in the construction of the LLRs need to be blindly estimated first. Besides, we establish the Cramer-Rao lower bounds for these two parameters and compare two corresponding blind estimators, namely  $M_2/M_4$  and EM techniques. Monte Carlo simulation results in compliance with the IEEE 802.11n standard are provided to evaluate the effectiveness of our proposed scheme. The simulation results show that the probability of detection for a single block can achieve 100% when the signal-to-noise ratio per uncoded-bit is larger than 8 dB. In addition, we also design a blind encoder identification method using multiple consecutive signal blocks jointly and the probability of detection can reach 100% when the signal-to-noise ratio per uncoded-bit is as low as 3 dB for a collection of twenty blocks. As the proposed scheme focuses on BPSK signals, future research can be undertaken to extend this scheme to higher-order modulations.

## REFERENCES

- [1] A. Goldsmith and S.-G. Chua, “Adaptive coded modulation for fading channels,” *IEEE Trans. Commun.*, vol. 46, no. 5, pp. 595–602, May 1998.
- [2] X. Huang, H.-C. Wu, and Y. Wu, “Novel pilot-free adaptive modulation for wireless OFDM systems,” *IEEE Trans. Veh. Technol.*, vol. 57, no. 6, pp. 3863–3867, Nov. 2008.
- [3] X. Wang, A. Marques, and G. Giannakis, “Power-efficient resource allocation and quantization for TDMA using adaptive transmission and limited-rate feedback,” *IEEE Trans. Signal Process.*, vol. 56, no. 9, pp. 4470–4485, Sep. 2008.



- [4] H.-C. Wu and S. Y. Chang, "Constellation subset selection: Theories and algorithms," *IEEE Trans. Wireless Commun.*, vol. 9, no. 7, pp. 2248–2257, Jul. 2010.
- [5] S.-K. Ahn and K. Yang, "Adaptive modulation and coding schemes based on LDPC codes with irregular modulation," *IEEE Trans. Commun.*, vol. 58, no. 9, pp. 2465–2470, Sep. 2010.
- [6] S. C.-H. Huang, H.-C. Wu, and S. Y. Chang, "Fast approximation algorithms for symmetric constellation subset selection," *IEEE Trans. Wireless Commun.*, vol. 11, no. 5, pp. 1655–1665, May 2012.
- [7] H.-C. Wu, Y. Wu, J. Principe, and X. Wang, "Robust switching blind equalizer for wireless cognitive receivers," *IEEE Trans. Wireless Commun.*, vol. 7, no. 5, pp. 1461–1465, May 2008.
- [8] H.-C. Wu, M. Saquib, and Z. Yun, "Novel automatic modulation classification using cumulant features for communications via multipath channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 8, pp. 3098–3105, Aug. 2008.
- [9] F. Hameed, O. Dobre, and D. Popescu, "On the likelihood-based approach to modulation classification," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 5884–5892, Dec. 2009.
- [10] V. Choqueuse, M. Marazin, L. Collin, K. Yao, and G. Burel, "Blind recognition of linear space-time block codes: A likelihood-based approach," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1290–1299, Mar. 2010.
- [11] R. Moosavi and E. Larsson, "A fast scheme for blind identification of channel codes," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM'2011)*, Houston, TX, Dec. 2011, pp. 1–5.
- [12] E. Larsson and R. Moosavi, "Piggybacking an additional lonely bit on linearly coded payload data," *IEEE Wireless Commun. Lett.*, vol. 1, no. 4, pp. 292–295, Aug. 2012.
- [13] Y. Debessu, H.-C. Wu, and H. Jiang, "Novel blind encoder parameter estimation for turbo codes," *IEEE Commun. Lett.*, vol. 16, no. 12, pp. 1917–1920, 2012.
- [14] T. Xia and H.-C. Wu, "Novel blind identification of LDPC codes using average LLR of syndrome *a posteriori* probability," in *Proc. IEEE Int. Conf. Intell. Transport Syst. Telecommun. (ITST'2012)*, Taipei, Taiwan, Nov. 2012, pp. 12–16.
- [15] T. Xia and H.-C. Wu, "Blind identification of nonbinary LDPC codes using average LLR of syndrome *a posteriori* probability," *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1301–1304, Jul. 2013.
- [16] R. G. Gallager, *Low Density Parity Check Codes*. Cambridge, MA: MIT Press, 1963.
- [17] D. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 399–431, Mar. 1999.
- [18] T. Richardson and R. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 599–618, Feb. 2001.
- [19] T. Richardson, M. Shokrollahi, and R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 619–637, Feb. 2001.
- [20] J. Gunther, M. Ankapura, and T. Moon, "A generalized LDPC decoder for blind turbo equalization," *IEEE Trans. Signal Process.*, vol. 53, no. 10, pp. 3847–3856, Oct. 2005.
- [21] S. Sharifi Tehrani, S. Mannor, and W. Gross, "Fully parallel stochastic LDPC decoders," *IEEE Trans. Signal Process.*, vol. 56, no. 11, pp. 5692–5703, Nov. 2008.
- [22] A. Cohen and K. Parhi, "A low-complexity hybrid LDPC code encoder for IEEE 802.3an (10GBase-T) ethernet," *IEEE Trans. Signal Process.*, vol. 57, no. 10, pp. 4085–4094, Oct. 2009.
- [23] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput*, IEEE Std. 802.11n-2009, 2009, IEEE Std. 802.11n-2009.
- [24] D. Pauluzzi and N. Beaulieu, "A comparison of SNR estimation techniques for the AWGN channel," *IEEE Trans. Commun.*, vol. 48, no. 10, pp. 1681–1691, Oct. 2000.
- [25] A. Wiesel, J. Goldberg, and H. Messer, "Non-data-aided signal-to-noise-ratio estimation," in *Proc. IEEE Int. Conf. Commun. (ICC'2002)*, New York, NY, Apr. 2002, pp. 197–201.
- [26] R. Imad, G. Sicot, and S. Houcke, "Blind frame synchronization for error correcting codes having a sparse parity check matrix," *IEEE Trans. Commun.*, vol. 57, no. 6, pp. 1574–1577, Jun. 2009.
- [27] R. Imad, S. Houcke, and M. Ghogho, "Blind estimation of the phase and carrier frequency offsets for LDPC-coded systems," *EURASIP J. Adv. Signal Process.*, vol. 2010, pp. 1–13, Feb. 2010.
- [28] J. Hagenauer, E. Offer, and L. Papke, "Iterative decoding of binary block and convolutional codes," *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 429–445, Mar. 1996.
- [29] A. Das, "NDA SNR estimation: CRLBs and EM based estimators," in *Proc. IEEE Region 10 Conf. (TENCON'2008)*, Hyderabad, India, Nov. 2008, pp. 1–6.
- [30] N. Alagha, "Cramer-Rao bounds of SNR estimates for BPSK and QPSK modulated signals," *IEEE Commun. Lett.*, vol. 5, no. 1, pp. 10–12, Jan. 2001.
- [31] H.-C. Wu and X. Huang, "Joint phase/amplitude estimation and symbol detection for wireless ICI self-cancellation coded OFDM systems," *IEEE Trans. Broadcast.*, vol. 50, no. 1, pp. 49–55, Mar. 2004.
- [32] H.-C. Wu, X. Huang, and D. Xu, "Pilot-free dynamic phase and amplitude estimations for wireless ICI self-cancellation coded OFDM systems," *IEEE Trans. Broadcast.*, vol. 51, no. 1, pp. 94–105, Mar. 2005.
- [33] Z. Cai, J. Hao, P. Tan, S. Sun, and P. Chin, "Efficient encoding of IEEE 802.11n LDPC codes," *Electron. Lett.*, vol. 42, no. 25, pp. 1471–1472, Dec. 2006.



**Tian Xia** received the B.S. and M.S. degrees from the University of Electronic Science and Technology of China, Chengdu, China, in 2008 and 2011, respectively.

He is currently working towards the Ph.D. degree in electrical and computer engineering at Louisiana State University, Baton Rouge. His research interests are in the areas of wireless communications and signal processing.



**Hsiao-Chun Wu** (M'00–SM'05) received the B.S.E.E. degree from National Cheng Kung University, Taiwan, in 1990, and the M.S. and Ph.D. degrees in electrical and computer engineering from University of Florida, Gainesville, in 1993 and 1999, respectively.

From March 1999 to January 2001, he had worked for Motorola Personal Communications Sector Research Labs as a Senior Electrical Engineer. Since January 2001, he has been with the Department of Electrical and Computer Engineering, Louisiana State University, Baton Rouge. From July to August 2007, he was a visiting assistant professor at Television and Networks Transmission Group, Communications Research Centre, Ottawa, Canada. From August to December 2008, he was a visiting associate professor with the Department of Electrical Engineering, Stanford University, CA. He has published more than 180 peer-refereed technical journal and conference articles in electrical and computer engineering. His research interests include the areas of wireless communications and signal processing.

Dr. Wu is an IEEE Distinguished Lecturer. He currently serves as an Associate Editor for the IEEE TRANSACTIONS ON BROADCASTING and a Technical Editor for IEEE COMMUNICATIONS MAGAZINE. He was an Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and IEEE SIGNAL PROCESSING LETTERS. He has also served for numerous textbooks, IEEE/ACM conferences and journals as the technical committee, symposium chair, track chair, or the reviewer in signal processing, communications, circuits and computers.