A Fast Scheme for Blind Identification of Channel Codes

Reza Moosavi and Erik G. Larsson

Reza Moosavi and Erik G. Larsson, A Fast Scheme for Blind Identification of Channel Codes, 2011, accepted The 54th IEEE Global Communications Conference (GLOBECOM).

Preprint available at: Linköping University Electronic Press
http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-68072

A Fast Scheme for Blind Identification of Channel Codes

Reza Moosavi and Erik G. Larsson
Dept. of Electrical Engineering (ISY), Linköping University, Linköping, Sweden. Email:{reza,egl}@isy.liu.se

***Abstract*—We present a fast mechanism for determining which channel code that was used on a communication link. In the proposed scheme, the receiver does not need to receive the entire data to determine the actual code. Moreover, the proposed scheme can also be used to determine the interleaving/scrambling sequence that was used at the transmitter. We investigate the performance of the scheme for some standard convolutional codes.**

I. Introduction

Adaptive modulation and coding (AMC) is used to meet high demands on throughput in modern wireless systems [1]. The idea is to change the modulation format and coding rate on the fly in order to adapt to a changing channel quality. This adaptation mechanism is typically supported by a control channel on which the currently used modulation and coding parameters are signaled. These control channels themselves are quite information heavy in a modern wireless system and would benefit from the use of AMC in order to conserve channel resources in favor of payload data. Then in principle the modulation and coding parameters of these control channels would need to be sent over a "control-channel for the control channel", and so on. However, instead of explicitly signaling the AMC parameters, one can use so-called *blind decoding*.

The basic idea of blind decoding is to blindly try to decode the data collected from the channel by trying different combinations of modulation formats, channel codes and code block lengths. The set of valid combinations to try is agreed upon on beforehand. The blind decoding is supported by a cyclic redundancy check (CRC) added to the information sequence. If the CRC matches after a decoding attempt then it is assumed that the correct modulation format, channel code and block length have been found and that the data is uncorrupted. In some multiuser wireless systems such as 3GPP long-term evolution (LTE), the CRC check is also used to pinpoint the intended recipient of the transmitted information, by using user specific CRC codes [2]. As an illustration of how blind decoding is implemented in practice, the Appendix describes the procedure for the physical downlink control channel (PDCCH) decoding in LTE.

This work was supported in part by Ericsson, VINNOVA and the Excellence Center at Linköping-Lund in Information Technology (ELLIIT). E. Larsson is a Royal Swedish Academy of Sciences (KVA) Research Fellow supported by a grant from the Knut and Alice Wallenberg Foundation.

The blind decoding type of adaptive modulation and coding comes at the price of a decoding delay and more importantly energy consumption in the decoder on the receiver side. Given that the receiver is a mobile device with limited battery capacity, the latter is of some concern and any reduction in the decoding complexity incurred by the blind decoding strategy would be valuable.

II. Related Work and Contribution

In [3] a solution to decrease the computational effort of the blind decoding for LTE is proposed. The idea is to limit the number of combinations in which the control data blocks may be arranged and located in the control channel elements (CCE), hence reducing the search space. For example, a tree-based concatenation of CCEs is proposed, where the largest-sized CCE aggregation is a concatenation of smaller-sized CCE aggregations. To find the correct aggregation of CCEs, a terminal starts with the set having the smallest-size of CCE aggregation and continues with the combinations of those smaller-size CCE aggregations to search for a larger size CCE aggregation and so forth. In [4], a solution to decrease the number of blind decoding attempts for high-speed downlink packet access (HSDPA) is proposed. The idea is to decode the received data partially for each parameter/location combination in the search space and early terminate the decoders that yield low quality metrics. The quality metric can be cumulative log-likelihood ratios for instance. In [5], an algorithm to estimate the parameter of a convolutional code from noisy observations in a binary-symmetric channel (BSC) is proposed. The algorithm is based on so-called *Expectation Maximization* (EM). The authors showed that the computations can be simplified by using the concept of log-likelihood ratio algebra [6]. A solution to decrease the detection errors of blind detection for the LTE standard was proposed in [7]. A PDCCH transmission employs circular buffer based rate matching for a rate-1/3 tail-biting convolutional code (See the Appendix). Due to repetition of coded bits and search space overlapping between different CCE aggregation levels, multiple aggregation levels may pass the CRC checking. The idea therein is to modify the circular buffer, for instance by excluding at least one coded bit from the circular buffer, such that the control information can be decoded unambiguously by the users.

Contribution: In this paper, we present an idea that facilitates a fast mechanism that determines which channel code

that was used. In the proposed scheme, the receiver does not need to receive the entire data to determine the actual code. Moreover, the proposed scheme can also be used to determine the interleaving/scrambling sequence that was used at the transmitter. We investigate the performance of the scheme for a class of standard convolutional codes.

III. Preliminaries: Log-Likelihood Ratio Algebra

Let us first introduce the notation that we will use throughout the paper. For a binary random variable X, let

$$L(X) = \frac{\Pr(X=0)}{\Pr(X=1)}$$

be the *a priori likelihood ratio* of X. Given another random variable Y, the *a posteriori likelihood ratio* of X given Y is defined as

$$L(X|Y) = \frac{\Pr(X=0|Y)}{\Pr(X=1|Y)}.$$

Similarly, the *a priori log-likelihood ratio* (LLR) of X and the *a posteriori log-likelihood ratio* of X given Y are defined as $\Lambda(X) = \log(L(X))$ and $\Lambda(X|Y) = \log(L(X|Y))$, respectively. Note that by the Bayes' rule,

$$\begin{aligned} L(X|Y) &= \frac{\Pr(X=0|Y)}{\Pr(X=1|Y)} \\ &= \frac{\Pr(Y|X=0)\Pr(X=0)/\Pr(Y)}{\Pr(Y|X=1)\Pr(X=1)/\Pr(Y)} \\ &= \frac{\Pr(Y|X=0)}{\Pr(Y|X=1)}\frac{\Pr(X=0)}{\Pr(X=1)} = L(Y|X)L(X) \end{aligned}$$

and thus $\Lambda(X|Y) = \Lambda(Y|X) + \Lambda(X)$. Therefore, if X is an equiprobable binary random variable, then $L(X) = 1$ and thus $\Lambda(X|Y) = \Lambda(Y|X)$. Moreover if $Y_1, Y_2, \ldots, Y_n$ are independent random variables, then for a binary random variable X,

$$\Lambda(X|Y_1, \ldots, Y_n) = \sum_{i=1}^{n} \Lambda(Y_i|X) + \Lambda(X).$$

Suppose that X_1, X_2 are binary random variables and that Y_1, Y_2 are random variables and let $\oplus$ denote the binary addition over $\mathbb{F}_2$. It can be shown that

$$\Lambda(X_1 \oplus X_2|Y_1, Y_2) = \Lambda(X_1|Y_1) \boxplus \Lambda(X_2|Y_2) \qquad (1)$$

where $\boxplus$ denotes the *box-plus* operation [6]. More precisely,

$$\ell_1 \boxplus \ell_2 \triangleq \log\left(\frac{1+\tanh(\ell_1/2)\tanh(\ell_2/2)}{1-\tanh(\ell_1/2)\tanh(\ell_2/2)}\right)$$

with $\ell \boxplus \infty = \ell$, $\ell \boxplus -\infty = -\ell$ and $\ell \boxplus 0 = 0$.

By using induction, one can further prove that for binary random variables $X_1, X_2, \ldots, X_n$ and random variables $Y_1, Y_2, \ldots, Y_n$ we have

$$\Lambda(X_1 \oplus \cdots \oplus X_n|Y_1, \cdots, Y_n) = \boxplus_{i=1}^{n} \Lambda(X_i|Y_i) = \log\left(\frac{1+\prod_{i=1}^{n}\tanh\left(\Lambda(X_i|Y_i)/2\right)}{1-\prod_{i=1}^{n}\tanh\left(\Lambda(X_i|Y_i)/2\right)}\right). \qquad (2)$$

The box-plus operator has the associative property, that is

$$\ell_1 \boxplus \ell_2 \boxplus \ell_3 = (\ell_1 \boxplus \ell_2) \boxplus \ell_3,$$

which can be used to compute (2) recursively. Finally, it is worth mentioning that in [6], the well-known approximation of the box-plus operation is presented,

$$\boxplus_{i=1}^{n} \ell_i \approx \left(\prod_{i=1}^{n} \text{sign}(\ell_i)\right) \min_{i=1,\ldots,n} |\ell_i|. \qquad (3)$$

Also in [8], other methods to approximate (2) were proposed which provide a better approximation than (3). These approximation methods can be used to find (2) more efficiently.

IV. Proposed Scheme

Let $b_1, b_2, \ldots, b_M$ denote the information bearing bits and let $c_1, c_2, \ldots, c_N$ denote the corresponding coded bits obtained from the channel encoder. The coded bits are transmitted to the receiver through a communication channel. Let $y_1, y_2, \ldots, y_N$ denote the corresponding received sequence at the receiver. We assume that the channel code which is used at the transmitter is unknown to the receiver, but we assume that the code has been chosen from a set of possible codes which we call the *candidate set*. Thus the receiver wants to determine which of the channel codes in the candidate set was used by the transmitter to encode the data.

Equation (2) suggests an algorithm that might be applied in order to determine whether a specific code was used at the transmitter to encode the data or not. The key observation is that for any code we will have parity check relations of the form

$$c_{i_1} \oplus c_{i_2} \oplus, \ldots \oplus c_{i_P} = 0,$$

for some i and P[1] (to be defined later on). Now given that the propagation channel is not bad (i.e., the received signal to noise ratio (SNR) is high enough), then the "syndrome posterior probability"

$$\gamma_i \triangleq \boxplus_{j=1}^{P} \Lambda(c_{i_j}|y_{i_j})$$

should be large. Hence by collecting enough observations i and combining the corresponding conditional LLRs γ_i, one can decide if a given code was used. As discussed earlier, equation (2) can be efficiently implemented to compute the conditional LLRs fast.

We exemplify the proposed scheme using the standard rate-1/2 convolutional code with constraint length 4, depicted in Figure 1. For this code, at each time instant i, we have

$$c_i^{(1)} = b_i \oplus b_{i-1} \oplus b_{i-3}$$

and

$$c_i^{(2)} = b_i \oplus b_{i-1} \oplus b_{i-2} \oplus b_{i-3}.$$

[1] In general for any convolutional code, these relations can be obtained using the *syndrome former* of the code [9]. For block codes, these relations are directly obtained from parity check matrix [10].

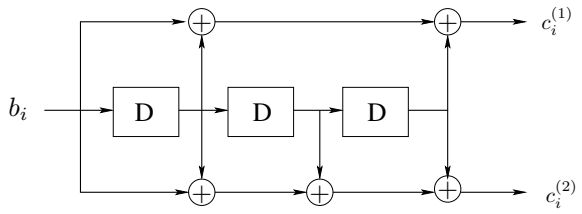

Fig. 1. The standard rate-1/2 convolutional code with constraint length 4. The generators for this code are $g_1 = 15$ and $g_2 = 17$ in octal.

Herein, we assume that the coded bits are labeled as

$$c_1^{(1)}, c_1^{(2)}, \ldots, c_i^{(1)}, c_i^{(2)}, \ldots$$

rather than the conventional labeling (that is the sequence $c_1, c_2, \ldots$). Let

$$y_1^{(1)}, y_1^{(2)}, \ldots, y_i^{(1)}, y_i^{(2)}, \ldots$$

denote the corresponding received sequence at the receiver.

Using the syndrome former of the code, it is easy to see that

$$c_{i-1}^{(2)} \oplus c_{i-1}^{(1)} \oplus c_i^{(1)} \oplus c_{i+1}^{(1)} \oplus c_{i+1}^{(2)} \oplus c_{i+2}^{(1)} \oplus c_{i+2}^{(2)} = 0. \quad (4)$$

Therefore, the syndrome posterior probability,

$$\gamma_i \triangleq \ell_{i-1}^{(2)} \boxplus \ell_{i-1}^{(1)} \boxplus \ell_i^{(1)} \boxplus \ell_{i+1}^{(1)} \boxplus \ell_{i+1}^{(2)} \boxplus \ell_{i+2}^{(1)} \boxplus \ell_{i+2}^{(2)} \quad (5)$$

where $\ell_i^{(j)} = \Lambda(c_i^{(j)}|y_i^{(j)})$, would most probably take on high values. Therefore by observing, say K pairs at the channel decoder, and computing the syndrome posterior probability vector $\boldsymbol{\gamma} = [\gamma_1, \gamma_2, \ldots, \gamma_K]^T$ we may decide if the transmitter had used the given convolutional code to encode the data or not.

V. Statistical Test for Detection

In this section, we will propose two detection algorithms that can be used to determine whether a certain channel code was used to encode the data.

A. A Simple Approach

As a simple test, one may compare the cumulative metric

$$\gamma(K) \triangleq \sum_{i=1}^{K} \gamma_i$$

with a threshold, say η, to determine whether a given code was used at the transmitter to encode the data, that is,

$$\gamma(K) \underset{H_0}{\overset{H_1}{\gtrless}} \eta \quad (6)$$

where the hypothesis H_1 means the correct code was used at the transmitter and H_0 means that the transmitter used some other code.

B. A GLRT-Based Approach

As a more systematic but still heuristic approach to the test, one can design a statistical test based on the observed sequence $\boldsymbol{\gamma} = [\gamma_1, \gamma_2, \ldots, \gamma_K]^T$. In order to do so, one needs to know the probability distribution of $\boldsymbol{\gamma}$ under the two hypotheses. Obtaining the exact distribution of $\boldsymbol{\gamma}$ is not a trivial problem. However inspired by much of the coding theory literature, we will assume that $\boldsymbol{\gamma}$ has a Gaussian distribution under the two hypotheses. More precisely, we approximate each γ_i as i.i.d. Gaussian random variables of the form

$$\begin{cases} \gamma_i \sim \mathrm{N}(\lambda, \sigma_1^2), & \text{Under } H_1 \\ \gamma_i \sim \mathrm{N}(0, \sigma_0^2), & \text{Under } H_0 \end{cases}, \text{ for } i = 1, 2, \ldots, K \quad (7)$$

where λ, σ_1^2 and σ_0^2 are nuisance parameters of the statistical test. The assumption of having an i.i.d distribution can be justified with increasing the interval between each observation. Now we can write the distribution of the observed vector $\boldsymbol{\gamma}$ under the two hypotheses as

$$\begin{cases} p_{\boldsymbol{\gamma}|H_1}(\boldsymbol{\gamma}|H_1) = \prod_{i=1}^{K} \frac{1}{\sqrt{2\pi}\sigma_1} \exp\big(-\frac{(\gamma_i-\lambda)^2}{2\sigma_1^2}\big), & \text{Under } H_1 \\ p_{\boldsymbol{\gamma}|H_0}(\boldsymbol{\gamma}|H_0) = \prod_{i=1}^{K} \frac{1}{\sqrt{2\pi}\sigma_0} \exp\big(-\frac{\gamma_i^2}{2\sigma_0^2}\big), & \text{Under } H_0. \end{cases} \quad (8)$$

A final step to design the test is to find/estimate the nuisance parameters. This can be done for instance by marginalization of the probability distributions with respect to the nuisance parameters. This approach is referred to as the Bayesian approach [11] and it requires a priori information on the distributions of the nuisance parameters. Alternatively a generalized likelihood ratio test (GLRT) may be used to distinguish between H_0 and H_1 [11]:

$$\Delta(\boldsymbol{\gamma}) = \frac{\max\limits_{\lambda,\sigma_1} \; p_{\boldsymbol{\gamma}|H_1}(\boldsymbol{\gamma}|H_1)}{\max\limits_{\sigma_0} \; p_{\boldsymbol{\gamma}|H_0}(\boldsymbol{\gamma}|H_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \eta. \quad (9)$$

We will use the GLRT-based approach in this paper. A direct calculation shows that the GLRT test (9) can be expressed equivalently as

$$\frac{\hat{\sigma_0}^2}{\hat{\sigma_1}^2} \underset{H_0}{\overset{H_1}{\gtrless}} \eta^{\frac{2}{K}} \quad (10)$$

where

$$\hat{\sigma_0}^2 \triangleq \frac{1}{K}\sum_{i=1}^{K} \gamma_i^2, \quad \hat{\sigma_1}^2 \triangleq \frac{1}{K}\sum_{i=1}^{K} (\gamma_i - \hat{\lambda})^2$$

with

$$\hat{\lambda} \triangleq \frac{1}{K}\sum_{i=1}^{K} \gamma_i.$$

VI. Illustration

We evaluate the performance of the proposed scheme for rate-1/2 convolutional codes with four different constraint lengths C. We assume that the transmitter picks one of the codes with equal probability to encode the data. We form two hypotheses H_1 and H_0 where under the hypothesis H_1, the *true code* with $C = 4$ is used at the transmitter to encode

the data and under the hypothesis H_0, one of the rate-1/2 convolutional codes with constraint lengths $C = 3$, $C = 6$ or $C = 8$ is chosen to encode the data. The coded bits are transmitted over an additive white Gaussian noise (AWGN) channel using binary phase shift keying (BPSK) modulation. Following the notation of the paper, let $\boldsymbol{c} = [c_1, \cdots, c_N]$ be the coded bits obtained from the channel encoder and let $\boldsymbol{y} = [y_1, \cdots, y_N]$ be the corresponding received vector at the receiver corrupted by additive white Gaussian noise with variance $N_0/2$.

At the receiver, we first compute the posterior LLR $\Lambda(c_i|y_i)$, for $i = 1, \cdots, N$ and we use the proposed algorithm to determine whether the true code was used at the transmitter to encode the data. We recall that, for the rate-1/2 convolutional code with constraint length $C = 4$, the syndrome posterior probability is given by (5). Therefore, the syndrome posterior probability vector $\boldsymbol{\gamma} = [\gamma_1, \cdots, \gamma_K]$ is obtained for the two hypotheses which would be used to determine if the true channel code was used to encode the data.

Figures 2 and 3 show the cumulative metric $\gamma(K)$ as a function of the observed interval K for different codes. Results are plotted for two random (anecdotal) channel realizations. The SNR is 5 dB for all curves in Figure 2 whereas the SNR is 10 dB for all curves in Figure 3. The dashed lines illustrate the mean values of $\gamma(K)$. We can see that the cumulative metric $\gamma(K)$ is a noisy linear function of the observed interval K for the true code $C = 4$ but not for the other codes. Also as expected, we see that by increasing SNR, the mean value as well as the cumulative metric for the true code increase.

For a more quantitative comparison we show the receiver operating characteristic (ROC). That is we plot the probability of correctly detecting the true code (probability of detection) versus the probability of mistaking one of the wrong codes for the true code (probability of false alarm) for the two detection algorithms defined in Section V. Figures 4 and 5 show the ROC of the scheme for two different values of SNR and also four different values of the observed interval K. As we see from comparing the figures, increasing the SNR improves the detection performance. Also we see that for all cases, by increasing the observed interval K a better performance can be achieved. We can also see that the test based on the first scheme outperforms the GLRT based approach in this example.

VII. Conclusion

We have proposed an algorithm that facilitates fast blind detection of channel codes. The algorithm does not need to know the exact length of the coded block in advance and hence it can be applied in any system that uses blind decoding (LTE for instance). Continued work on this idea may include the characterization of asymptotic performance of the scheme when SNR grows as well as generalizations to arbitrary channel codes and also the evaluation of the scheme in fading channels with imperfect channel state information.

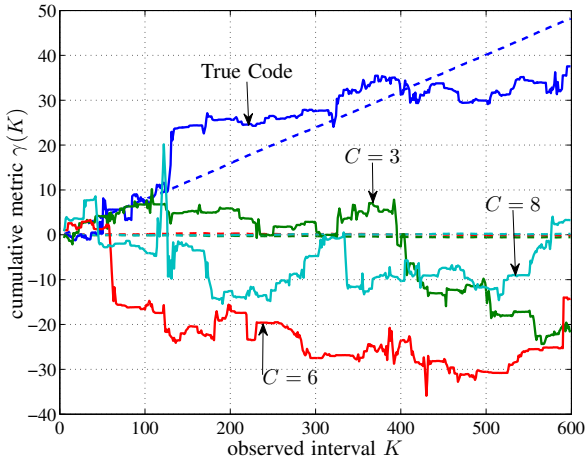

Fig. 2. Comparison of cumulative metrics for rate-1/2 standard convolutional code with different constraint lengths, for a random channel realization with SNR = 5 dB. The dashed lines represent the corresponding mean values.

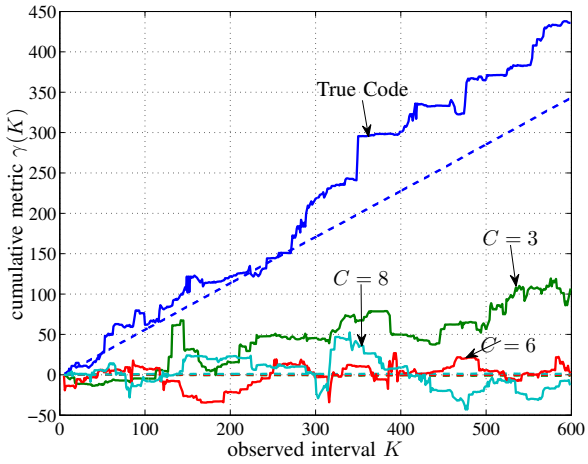

Fig. 3. The same as Figure 2 but for SNR = 10 dB.

Appendix
Blind Decoding Mechanism in LTE

In LTE, the physical downlink control channel (PDCCH) supports different transmission formats for the downlink control information (DCI), which are a priori unknown to the terminals. Each terminal will find its information by blindly decoding the incoming information by trying a set of possible formats. More precisely, the transmission of control information in LTE can be described as follows. There are five DCI formats with different message sizes. Based on the factors such as cell-coverage, the number of terminals in the cell and the scheduling granularity, one format is chosen as the downlink control information format. Prior to transmission, a terminal-specific CRC is appended to each control message. The attached CRC is used by each terminal to find the control information. After attaching the CRC, the control information bits are encoded with a rate-1/3 tail-biting convolutional code and the rate is matched to fit the amount of resources available for PDCCH transmission by using a circular buffer. The mapping of PDCCHs to physical resource elements is subject to a

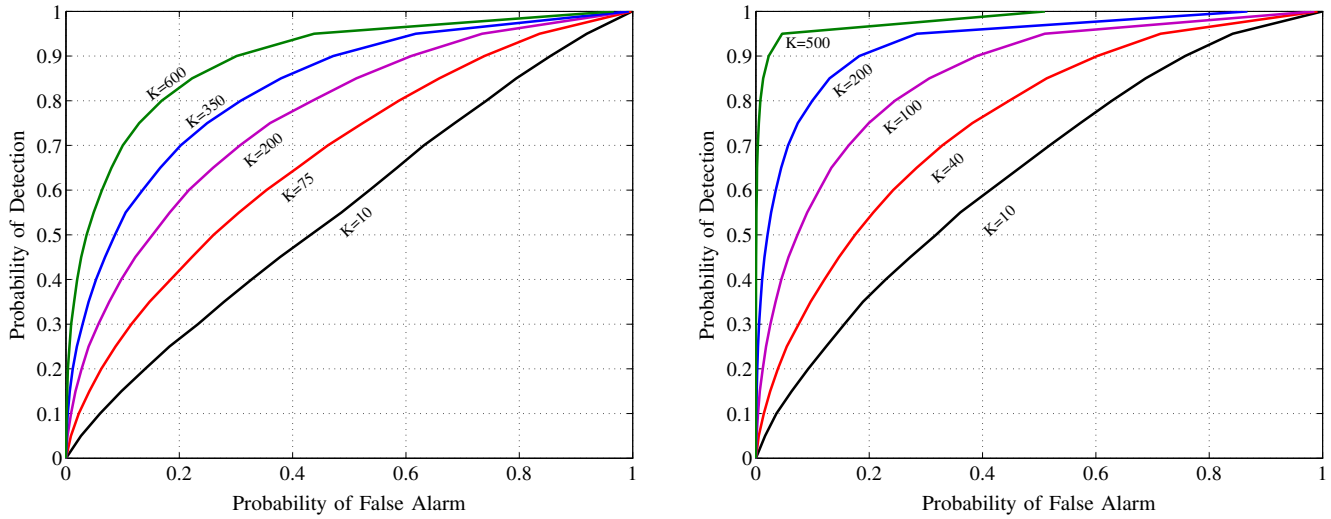

Fig. 4. Receiver Operating Characteristic according to the scheme defined in Section V-A (comparing cumulative metric with a threshold). The left-hand figure is for SNR = 5 dB whereas the right-hand figure is for SNR = 10 dB.

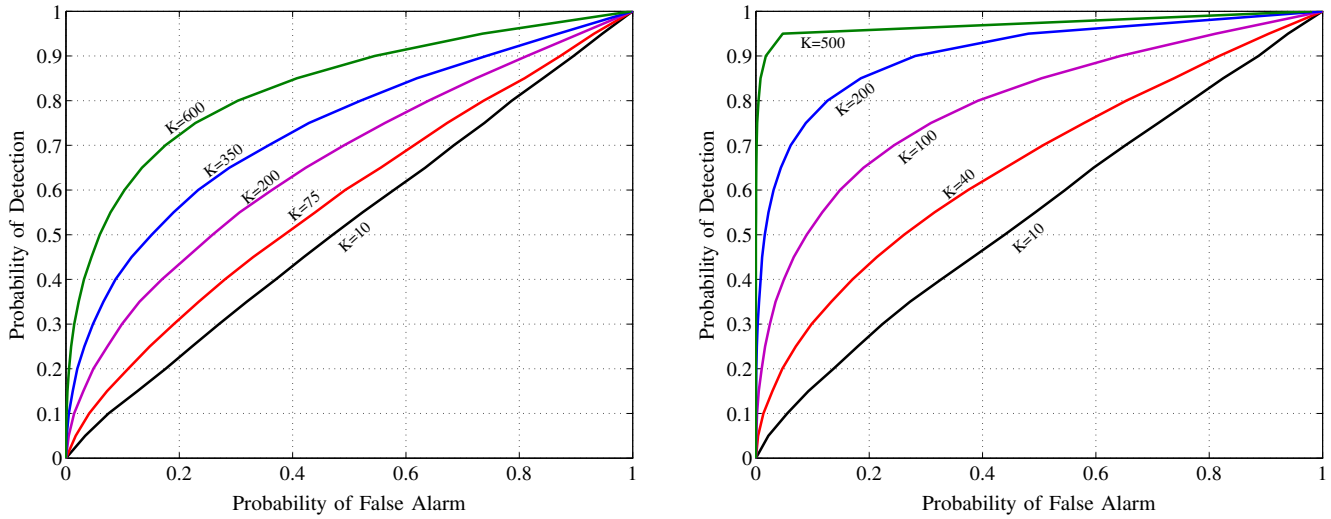

Fig. 5. The same as Figure 4 but for the GLRT based approach defined in Section V-B.

certain structure which is based on so-called *control channel elements* (CCE). Each CCE consists of 36 physical resource elements. Based on the instantaneous channel condition and the DCI format, the PDCCH for each terminal is mapped onto a set of CCEs. Since various aggregations of the CCEs may be used for the transmission of control information, the terminal needs to blindly detect the format of the PDCCHs by testing different CCE combinations. To reduce the complexity of the blind decoding process in LTE, the *search space* of each terminal which describes the set of CCEs that the terminal is supposed to monitor for possible control message is limited to 44 possibilities per frame [2, Section 16.4].

REFERENCES

[1] A. J. Goldsmith and S. G. Chua, "Adaptive coded modulation for fading channels", *IEEE Trans. Commun.*, vol. 46, no. 5, pp. 595-602, MAY 1998.

[2] E. Dahlman, S. Parkvall, J. Sköld and P. Beming, *3G Evolution HSPA and LTE for Mobile Broadband*, 2nd edition Academic Press 2008.

[3] D. P. Malladi, J. Montojo and S. Sarkar, *Methods and systems for PDCCH blind decoding in mobile communications*, United States Patent Application Publication 2009/0168922, Jul. 2, 2009.

[4] A. Reial and L. Andersson, *HS-PDSCH blind decoding*, United States Patent Application Publication 2009/003301, Jan. 1, 2009.

[5] J. Dingel and J. Hagenauer, "Parameter estimation of a convolutional encoder from noisy observations," *in Proc. of IEEE ISIT*, pp. 1776-1780, Jun. 2007.

[6] J. Hagenauer, E. Offer and L. Papke, "Iterative decoding of binary block and convolutional codes," *IEEE Trans. Info. Theory*, vol. 42, pp. 429-445, Mar. 1996.

[7] J. F. Cheng, *System and method for removing PDCCH detection errors in a telecommunications network*, United States Patent Application Publication 2010/0050059, Feb. 25, 2010.

[8] T. Clevorn and P. Vary, "Low-complexity belief propagation by approximations with lookup-tables", *5th Internantional ITG Conference on Source and Channel Coding (SCC)*, Erlangen, Germany, Jan. 2004.

[9] R. Johannesson and K. Sh. Zigangirov, *Fundamentals of Convolutional Coding*, IEEE Press, 1999.

[10] J. G Proakis and M. Salehi, *Digital Communication*. 5th Edition McGraw-Hill International Edition 2008.

[11] H. L. Van Trees, *Detection, Estimation, and Modulation Theory*, A Wiley-Interscience Publication, 2001.