International Journal of Innovative
Computing, Information and Control
Volume 8, Number 3(B), March 2012
 ISSN 1349-4198
pp. 2329–2337

# BLIND DETECTION OF PSK SIGNALS

Yong Jin, Shuichi Ohno and Masayoshi Nakamoto

Graduate School of Engineering
Hiroshima University
1-4-1 Kagamiyama, Higashi-Hiroshima-shi, Hiroshima 739-8527, Japan
{ jinyong2009; ohno; msy }@hiroshima-u.ac.jp

Received March 2011; revised July 2011

Abstract. *In this paper, a blind detection method is proposed to evaluate the information that can be drawn from the received phase shift keying (PSK) signals without channel knowledge at the receiver. First, we develop a method to determine the decision regions for detecting PSK symbols based on the maximum a posterior (MAP) criterion. Then, to reduce the numerical complexity, an approximated MAP criterion equivalent to a least squares criterion is derived. Numerical simulations are conducted to evaluate the performance of our proposed methods in terms of the mean squared error (MSE) and the bit error rate (BER).*
**Keywords:** PSK, MAP, Least squares, Bit error rate, Mean squared error

1. **Introduction.** For an unknown system where only the output signal is known, the blind equalization technique can be used to recover the input signals. The technique has been studied for single-input single-output (SISO) systems since 1980s (see, e.g., [1] and the references therein). It has been explored also for multiple-input multiple-output (MIMO) systems, where it is commonly referred to as independent components analysis (ICA) [2] or blind signal separation [3, 4]. Many applications based on blind equalization have been developed, e.g., in medical engineering, signal analysis and wireless communication.

It has been shown that under some conditions, blind equalization for SISO systems can recover the original signal up to an unknown complex value. This means that, if there are no noises then the recovered signals are scaled and rotated in two-dimensional signal space.

Blind equalization technique has received much attention in wireless communication, since it does not require estimation of the unknown channel. However, at least phase information is required for coherent detection of digitally modulated signals. Incoherent detection is possible for some digital modulation when at least one symbol (usually the first transmitted symbol) is known (e.g., see [5]).

Despite the advantages of blind equalization, it may be still used, e.g., by eavesdropping a wireless communication. Due to the presence of this disadvantage, we need to pay more attention to the security issue of communication systems especially in wireless communication. Usually, the security is maintained by using secret-key sharing only by a specific pair of transmitter and receiver. The disadvantage of the secret-key sharing is the development of a method to share the secret-key before data communication. Recently, new techniques based on information theory have been proposed in [6, 7] for secret communication. However, it remains unclear whether they are robust to blind equalization.

In this paper, we study the blind detection of phase shift keying (PSK) signals to know the extent of the information that can be eavesdropped and the corresponding probability.

Using the maximum a posterior (MAP) criterion, we develop a method to determine the decision regions for detecting PSK symbols, which is equivalent to estimating the unknown phase of the received PSK symbols after blind equalization. Since the proposed method requires many logarithmic and exponential computations, to reduce the computational complexity, we use the approximation of the log-sum-exp function, as an approximate MAP based method which can also be considered as a least squares (LS) based estimator.

By taking quadrature PSK (QPSK) and 8PSK signaling as examples, the mean squared error (MSE) of the phase and gain estimates are numerically evaluated and the bit error rate (BER) of the detection using the phase estimates is also given to assess the performances of our estimators.

This paper studies the security aspect of blind equalization. Comparing with other works on blind equalization and separation such as [8, 9], where their objects are to equalize signals blindly under the assumption that the prior knowledge of the transmitted signals is available at the receiver (which is usually obtained through pilot or training symbols) and to separate signals blindly, our proposed methods detect and recover digitally modulated signals as possible as it can without any prior knowledge of the transmitted signals at the receiver. By using our method, we can numerically evaluate to what extent information is eavesdropped.

## 2. Problem Formulation.

Suppose that a transmitter transmits $K$ $M$-ary phase shift keying (MPSK) signals for a specified time duration. Let $s_k$ be the symbol from the transmitter at the $k$th time-slot, which is assumed to be a PSK symbol.

After some processing at the receiver, let the received baseband signal corresponding to $s_k$ be

$$y_k = re^{j\theta}s_k + w_k, \quad k = 1, \dots, K \tag{1}$$

where $j$ is the imaginary unit, $r(\geq 0)$ and $\theta$ are unknown gain and phase respectively, and $w_k$ is a complex Gaussian noise with zero mean and variance $\sigma_w^2$. Let us define the received signal vector $\boldsymbol{y}$ as

$$\boldsymbol{y} = [y_1, y_2, \dots, y_K]. \tag{2}$$

From (1), we consider a case where the receiver does not know the channel and a blind equalization is conducted as in [1]. It is well-known that if $s_k$ is non-Gaussian and $w_k$ is absent, then the transmitted signals can be recovered up to the unknown amplitude $r$ and phase $\theta$. Thus, if the transmitter sends a pilot symbol known to the receiver, then the phase can be estimated based on the received pilot symbol and the detection of $s_k$ becomes possible.

Figure 1 plots the received signal points when the signal to noise ratio (SNR) is 10dB and $\theta = \pi/8$ (radian). One can guess the existence of quadrature PSK (QPSK) signals but cannot estimate $\theta$ without additional information.

Suppose that there is an eavesdropper that can blindly equalize the transmitted symbols up to the unknown amplitude $r$ and phase $\theta$. We would like to evaluate how much information is eavesdropped from $y_k$ in (1).

Since all PSK signals have constant amplitude, then the amplitude $r$ is not necessary for the detection of PSK signals. Thus, we mainly study the estimation of $\theta$ to obtain information from the received signals. Note that, even if there are no noises, there is still an ambiguity on estimating $\theta$ due to the symmetry of MPSK signal points. To avoid this, without loss of generality, we assume that

$$-\frac{\pi}{M} \leq \theta < \frac{\pi}{M}. \tag{3}$$

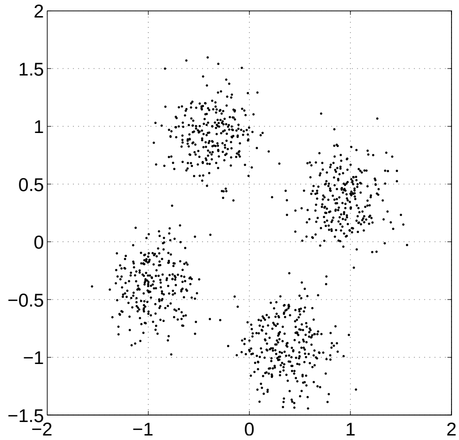


FIGURE 1. Received signal points (10dB)

3. **Symbol Detection with Phase Estimation.** Now we consider the detection of the transmitted symbols. We utilize the maximum a posterior (MAP) criterion to estimate the unknown phase $\theta$ for symbol detection. For the simplicity of presentation, we only consider QPSK signaling; however, our method can be easily extended to general MPSK signals.

QPSK signals can be represented by 4 constellation points $(1,0),(0,j),(-1,0),(0,-j)$ in the two-dimensional complex signal space. Using complex values, we denote the constellation as $\mathcal{C} = \{e^{j\cdot 0\cdot\frac{\pi}{2}}, e^{j\cdot 1\cdot\frac{\pi}{2}}, e^{j\cdot 2\cdot\frac{\pi}{2}}, e^{j\cdot 3\cdot\frac{\pi}{2}}\}$. In this case, phase differences are a multiple of $\pi/2$. And there are 4 possible cases:

$$y_k = re^{j\theta} + w_k \tag{4}$$

$$y_k = -re^{j\theta} + w_k \tag{5}$$

$$y_k = jre^{j\theta} + w_k \tag{6}$$

$$y_k = -jre^{j\theta} + w_k. \tag{7}$$

Let us assume that the 4 constellation points are taken with equal probability and $\theta$ is uniformly distributed between $[0, 2\pi)$. Since $\theta$ and $s_k$ are independent, the joint probability density function (PDF) of $y_k$ can be expressed as

$$p(y_k, \theta, r, s_k) = p(\theta)p(r)p(s_k)p(y_k|\theta, r, s_k) \tag{8}$$

where $p(x)$ denotes the PDF of $x$. Since the noise is Gaussian, then marginalizing $p(y_k, \theta, r, s_k)$ over $s_k$ leads to

$$p(y_k, \theta, r) = \frac{p(r)}{8\pi^2\sigma_w^2} I(y_k, \theta, r) \tag{9}$$

where

$$I(y_k, \theta, r) = \sum_{s_k \in \mathcal{C}} \exp\left(-\frac{|y_k - re^{j\theta}s_k|^2}{\sigma_w^2}\right) \tag{10}$$

We assume that the transmitted symbols $s_1, \ldots, s_K$ are independent of each other. Then we obtain

$$p(\boldsymbol{y}, \theta, r) = \Pi_{k=1}^K p(y_k, \theta, r) = \frac{p(r)}{8\pi^2\sigma_w^2} \Pi_{k=1}^K I(y_k, \theta, r). \tag{11}$$

By taking the logarithm of $p(\boldsymbol{y}, \theta, r)$ and ignoring the constant terms, the MAP estimates of $\theta$ and $r$ can be obtained by maximizing

$$J_{MAP}(\theta, r) = \sum_{k=1}^{K} \log I(y_k, \theta, r) + \log p(r). \tag{12}$$

The criterion function $J_{MAP}(\theta, r)$ is non-linear. Moreover, the computational complexity of (12) is higher due to the presence of logarithmic and exponential functions. To reduce the complexity, we develop an approximate of $J_{MAP}(\theta, r)$ in the following.

As $K$ gets larger, the first term in the R.H.S. of (12) gets larger, while the last term is constant (for a given $r$). Thus, for large $K$, we can ignore the last term in the R.H.S. of (12). Applying the approximation of the log-sum-exp function such as

$$\log(e^{x_1} + e^{x_2} + \cdots + e^{x_N}) \approx \max(x_1, x_2, \ldots, x_N) \tag{13}$$

to $\log I(y_k, \theta, r)$, we obtain

$$J_{MAP}(\theta, r) \approx \sum_{k=1}^{K} \max_{s_k \in \mathcal{C}} \left(-|y_k - re^{j\theta}s_k|^2\right) = J(\theta, r) \tag{14}$$

where

$$J(\theta, r) = \sum_{k=1}^{K} \min_{s_k \in \mathcal{C}} |y_k - re^{j\theta}s_k|^2 \tag{15}$$

This shows that the maximization of $J_{MAP}(\theta, r)$ can be approximately achieved by the minimization of $J(\theta, r)$.

The criterion function $J(\theta, r)$ has another important interpretation: If we resort to the least squares to estimate $\theta$ and $r$ for our model (1), then it follows that the LS estimates of $\theta$ and $r$ are given by minimizing $J(\theta, r)$.

Let us define

$$\tilde{J}(\theta) = \sum_{k=1}^{K} \min\left(\pm\Re\{y_k^* e^{j\theta}\}, \pm\Im\{y_k^* e^{j\theta}\}\right), \tag{16}$$

where $\Re\{\cdot\}$ is the real part of the argument, while $\Im\{\cdot\}$ is the imaginary part. It should be noted that the selection of the minimum of $\Re\{y_k^* e^{j\theta}\}, -\Re\{y_k^* e^{j\theta}\}, \Im\{y_k^* e^{j\theta}\}, -\Im\{y_k^* e^{j\theta}\}$ corresponds to the estimation of $s_k$.

Using $\tilde{J}(\theta)$, we re-express $J(\theta, r)$ as

$$J(\theta, r) = 2r\tilde{J}(\theta) + C(r) \tag{17}$$

where

$$C(r) = Kr^2 + \sum_{k=1}^{K} |y_k|^2. \tag{18}$$

Since $\tilde{J}(\theta)$ does not depend on $r$, all we have to do is to minimize $\tilde{J}(\theta)$ to find the optimal $\theta$ such as

$$\hat{\theta} = \arg\min_{\theta} \tilde{J}(\theta). \tag{19}$$

Unfortunately, (16) cannot be solved analytically, since the metric above is non-linear in $\theta$. Thus, we resort to the line search to find the optimal $\theta$.

The decision regions for $y_k$ are determined by $\hat{\theta}$ obtained from the corresponding symbols in the selection of the minimum of $\Re\{y_k^* e^{j\theta}\}, -\Re\{y_k^* e^{j\theta}\}, \Im\{y_k^* e^{j\theta}\}, -\Im\{y_k^* e^{j\theta}\}$. However, there is still an ambiguity in the phase rotation of the estimated symbols.

Although the detection of PSK signals does not require the estimation of the unknown amplitude $r$, suppose that one may need to estimate the unknown amplitude. Then, (17) shows that the joint minimization of $J(\theta, r)$ can be decoupled into two-step minimization. It follows from (17) that

$$\frac{\partial J(\theta, r)}{\partial r} = 2\tilde{J}(\theta) + 2Kr. \tag{20}$$

Thus, the optimal $\hat{r}$ is given by

$$\hat{r} = -\frac{1}{K}\tilde{J}(\hat{\theta}). \tag{21}$$

4. **Simulation Results.** To demonstrate performance of our proposed methods, we define signal energy as $E\{|s_k|^2\} = \mathcal{E}_s$ (where $E\{\cdot\}$ is called the expected value operator) and set the noise variance to be $\sigma_w^2 = \mathcal{N}_0$, and define signal to noise ratio (SNR) as $10 \log(\mathcal{E}_s/\mathcal{N}_0)$ in dB.

For the simplicity of illustration, we only consider QPSK and 8PSK signals as examples, although our methods can be extended to the detection of any PSK modulation scheme.

Since (12) depends on $\theta$ and $r$, we fix $r = 1$ to evaluate the performance of our MAP phase estimates obtained by maximizing (12). We generate $10^4$ uniform random phases between $[-\frac{\pi}{M}, \frac{\pi}{M})$. For each realization, the cost function in (16) is evaluated at $10^3$ points that are uniform in $[-\frac{\pi}{M}, \frac{\pi}{M})$. In other words, the distance of two neighboring search points is $2\pi/(M \cdot 10^3)$. Then, we select the best among $10^3$ values of the cost function to obtain the estimate of $\theta$.

Figure 2 presents the mean squared error (MSE) of the estimated $\hat{\theta}$ for different values of $K$ received signals for QPSK symbols. MSE curves are represented by using two different criterion functions (12) and (16). We have small MSE even at relatively low SNR with (12). For the same SNR, the performance gets better as $K$ increases. In terms of MSE, the approximated criterion does not seem to work well and its performance slightly improves with increasing $K$ compared with the MAP criterion. However, as which can be shown later in Figure 4, in terms of BER, it works as good as the MAP criterion. Similar phenomena can be seen in Figure 3 which demonstrates the MSE of estimated $\hat{\theta}$ on 8PSK symbols.

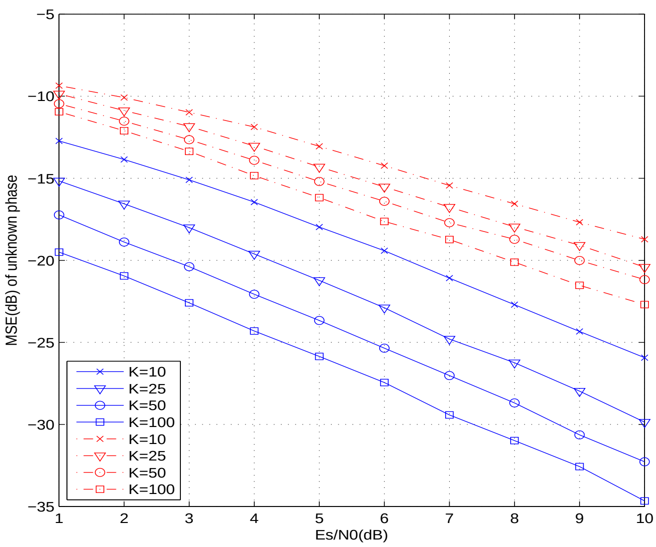


FIGURE 2. MSE of phases estimated by (12) (dash-dot curves) and by (16) (solid curves) for QPSK

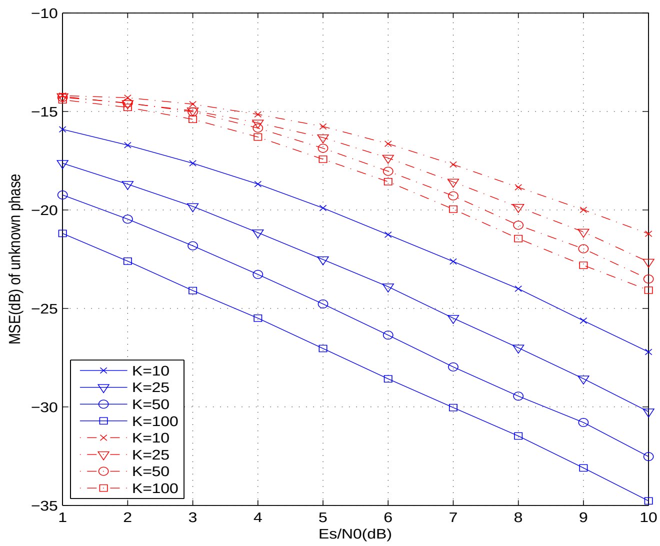


FIGURE 3. MSE of phases estimated by (12) (dash-dot curves) and by (16) (solid curves) for 8PSK

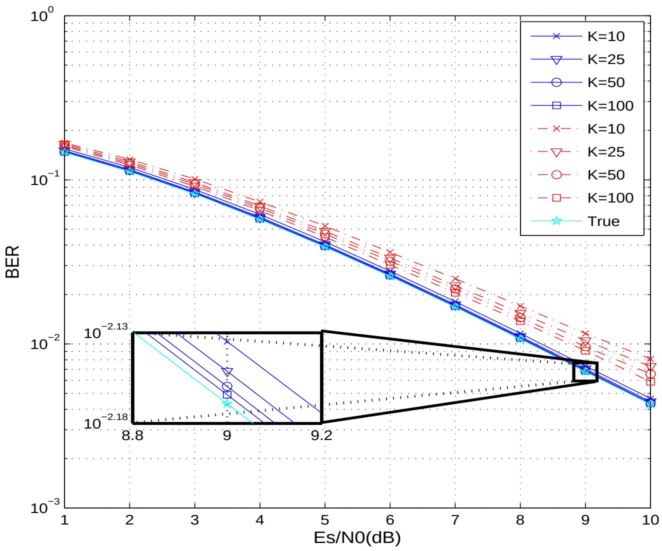


FIGURE 4. BER using phases estimated by (12) (dash-dot curves) and by (16) (solid curves) for QPSK

In the following, from the estimated $\hat{\theta}$, we compute $e^{-j\hat{\theta}}y_k$ to detect the symbols with the conventional decision regions. Figure 4 and Figure 5 show bit error rate (BER) performance for different $K$ for QPSK and 8PSK symbols respectively, where the curves with $\star$ are the BER with the true value of $\theta$, that is, when the value of $\theta$ is known at the receiver.

Again, two different cost functions, the MAP given by (12) and the approximated MAP (16) are considered. Unlike MSE, BER with phases estimated using the approximated criterion is comparable to BER with phases estimated using the MAP criterion. Meanwhile BER improvements with the increase of $K$ are not significant. This implies that

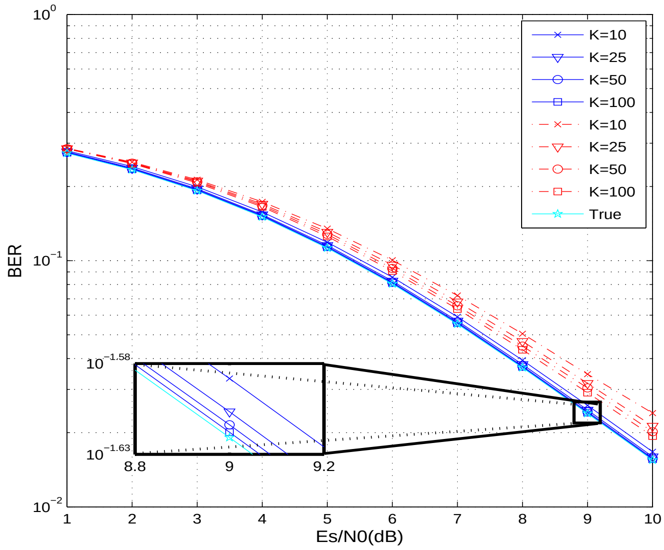


FIGURE 5. BER using phases estimated by (12) (dash-dot curves) and by (16) (solid curves) for 8PSK

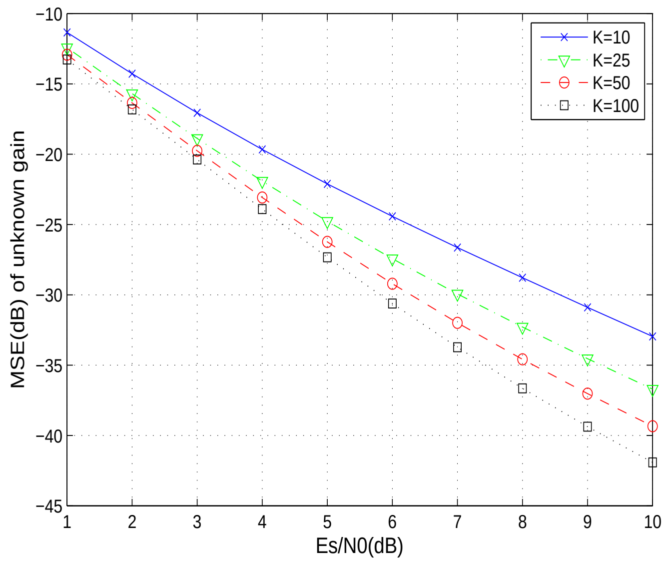


FIGURE 6. MSE of gain estimates for QPSK

sufficiently good phase estimates are obtained even with small $K$. This is also verified by the comparison of the BER of the estimated phases with the BER of the known phase, that is, the performance limit, where BERs obtained by using estimated phases are close to the performance limit.

Since PSK modulations have a constant modulus, their gains are not necessary for the detection. However, other modulations like quadrature amplitude modulations (QAM), both phase and gain are needed for their detection. Since we would like to extend our method to other modulations, we evaluate the gain estimates obtained by (21) for PSK signals.

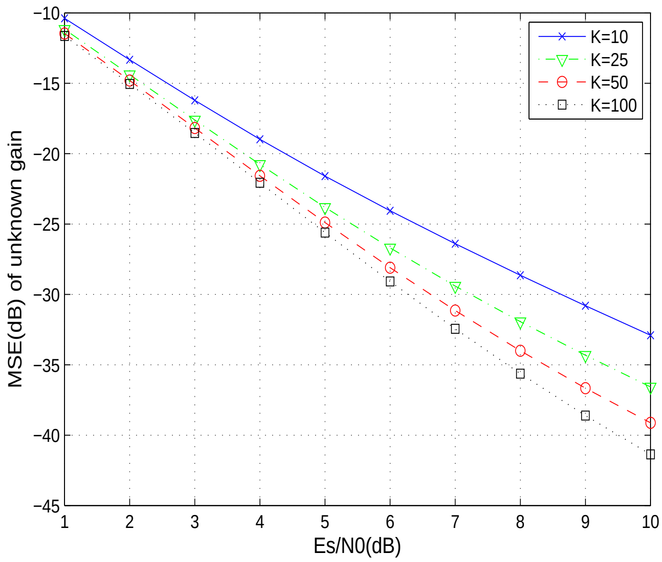


Figure 7. MSE of gain estimates for 8PSK

Figure 6 illustrates the MSE of estimated $\hat{r}$ of QPSK symbols for different $K$. It can be observed that small MSE is also obtained at low SNR even for small $K$. As $K$ increases, the performance gets better. The same conclusion can be drawn from the MSE of estimated $\hat{r}$ for different $K$ on 8PSK as described in Figure 7.

5. **Conclusions.** The problem of blind detection of PSK signals is studied. Different from other works on blind separation, we detect and recover digitally modulated signals as possible as we can without any prior knowledge of transmitted signals at the receiver (which is commonly obtained through pilot or training symbols). By using our method, we can also numerically evaluate the extent that information is eavesdropped. We have designed a method to determine the decision regions to detect PSK symbols based on the MAP criterion. We have also presented another method by approximating the MAP criterion, which is equivalent to the least squares based determination of decision regions. The MSE of the phase estimates and the BER of the detection using the estimated phases have been also provided to assess the performance of our estimator. The accuracy of estimated amplitude is also demonstrated by its MSE performance.

## REFERENCES

[1] S. Haykin et al., *Unsupervised Adaptive Filtering, Volume II Blind Deconvolution*, John Wiley & Sons, 2000.
[2] P. Comon, Independent component analysis, a new concept? *Signal Processing*, vol.36, pp.287-314, 1994.
[3] J. F. Cardoso, Sources separation using higher order moments, *Proc. of Internat. Conf. Acoust. Speech Signal Process.*, pp.2109-2112, 1989.
[4] C. Jutten and J. Herault, Blind separation of sources, Part I: An adaptive algorithm based on neuromimatic architecture, *Signal Processing*, vol.24, no.1, pp.1-10, 1991.
[5] B. Sklar, *Digital Communications*, 2nd Edition, Prentice Hall, 2001.
[6] X. Li and E. P. Ratazzi, MIMO transmissions with information-theoretic secrecy for secret-key agreement in wireless networks, *Proc. of IEEE Military Communications Conference*, vol.3, pp.1353-1359, 2005.
[7] X. Tang, R. Riu, P. Spasojevic and H. V. Poor, The Gaussian wiretap channel with a helping interfere, *Proc. of IEEE International Symposium on Information Theory*, pp.389-393, 2008.

[8] M. Khosravy, M. R. Asharif, M. Khosravi and K. Yamashita, An optimum pre-filter for ICA based mulit-input multi-output OFDM system, *International Journal of Innovative Computing, Information and Control*, vol.7, no.6, pp.3499-3508, 2011.

[9] G. R Naik and D. K Kumar, Dimensional reduction using blind source separation for identifying sources, *International Journal of Innovative Computing, Information and Control*, vol.7, no.2, pp.989-1000, 2011.