Hindawi
Wireless Communications and Mobile Computing
Volume 2017, Article ID 8949430, 8 pages
https://doi.org/10.1155/2017/8949430

Research Article

Collaborative Covert Communication Design Based on Lattice Reduction Aided Multiple User Detection Method

Baoguo Yu,[1,2] Yachuan Bao,[1,2] Haitao Wei,[1,2] Xin Huang,[3] and Yuquan Shu[1,2]

[1]*State Key Laboratory of Satellite Navigation System and Equipment Technology, Shijiazhuang, China*
[2]*The 54th Research Institute of CETC, Shijiazhuang, China*
[3]*Northwestern Polytechnical University, Xi'an, China*

Correspondence should be addressed to Yachuan Bao; baoyachuan@126.com

Received 13 April 2017; Accepted 28 June 2017; Published 6 August 2017

Academic Editor: Xiaoqiang Ma

Spread spectrum communication is a typical scheme for covert communication because of its low detectability and antijam characteristic. However, the associated design concerns multiple factors, such as cochannel multiple access interference (MAI) and spread spectrum gain. In this paper, the lattice reduction theory is applied to MAI cancellation of spread spectrum communication and a novel lattice reduction aided multiple user detection method is proposed. The near maximum likelihood (ML) performance of MAI resistance is verified by simulation and theoretical analysis. The superiority of detection performance in strong MAI scenarios is especially addressed. Based on the algorithm, a collaborative covert communication system design is proposed. Low-power covert signals can be transmitted at a higher bit rate with the same coverage as more high-power cochannel signals. The covert transmission performance can be improved significantly compared to traditional designs.

1. Introduction

For the purposes of information transmission security, covert communication is applied in many special scenarios, including military and national security applications. The development of covert communication systems shows a trend for diversity, where different designs are tailored to different applications. Covert communication systems can be divided into two main groups: covert information transmission and covert signal transmission. The covert transmission of information can be satisfied by securing both the information source and the communication protocol encryption. A typical schema includes information transmission with image and video compression [1] and covert P2P channels over the Internet [2], among others. The covert transmission of signals is realized by signal or transmitter-receiver mode design with low detectability. Typical schemes include designs based on direct antenna modulation (DAM) [3] and spread spectrum (SS) communication.

The most common method for covert communication design based on SS involves reducing the signal power to hide it in noise or transmit the covert signal covered by several high-power signals. An improved method involving frequency and code hopping is proposed in this paper, with an improvement in anticapture performance [4]. SS signals are also designed to transmit coupled with satellite television signals and broadcast signals to achieve covert communication [5].

Transmitting low-power covert signals coupled with high-power signals is an effective way to reduce the detectability of a signal. However, the design will be restricted by multiple access interference (MAI) and wireless link resources. To achieve high imperceptibility, signal power and information rates will be limited.

Research on covert communication based on SS is discussed in this paper. Lattice reduction (LR) is applied to multiple user detection (MUD) of SS communication, and an LR-MUD algorithm is also proposed. Near maximum likelihood (ML) performance of lower power signals is achieved with low complexity in serious MAI scenarios. Based on the LR-MUD algorithm, a novel design of collaborative SS covert communication is proposed. Covert signals

can be transmitted with the coverage of a greater number of high-power signals. Thus, the transmission concealment and robustness of covert communication will be improved significantly.

The remainder of the paper is organized as follows: Section 2 gives the covert communication model based on SS communication, while the traditional MUD method is analyzed in Section 3. The lattice theory and lattice aided MUD algorithm is given in Section 4, followed by simulation experiments of the algorithm in Section 5. The design of a system based on LR-MUD is given in Section 6. Finally, the conclusions are provided in Section 7.

2. Covert Communication Model Based on Spread Spectrum

Consider a covert SS communication system consisting of one low-power covert signal and $N-1$ high-power signals. The received signal at the receiver is

$$r(t) = \sum_{k=1}^{N} A_k(t)\, b_k(t)\, \mathrm{PN}_k(t) + n(t), \tag{1}$$

where A is the signal amplitude, b is the information bit which takes values in the interval $\{-1, +1\}$, and PN is the pseudo noise code used for spread spectrum modulation.

Suppose signal k is the desired signal. Then, the output of the matched filter for signal k is as follows:

$$\begin{aligned} y_k &= \int_0^{T_b} r(t)\, \mathrm{PN}_k(t)\, dt \\ &= \int_0^{T_b} \left[\sum_{k=1}^{N} A_k b_k \mathrm{PN}_k(t) + n(t) \right] \mathrm{PN}_k(t)\, dt \\ &= A_k b_k + \sum_{j=1, j\neq k}^{N} A_j b_j \rho_{jk} + n_k, \end{aligned} \tag{2}$$

where $\rho_{jk} = \int_0^{T_b} \mathrm{PN}_k(t)\mathrm{PN}_j(t)dt$, $n_k = \int_0^{T_b} n(t)\mathrm{PN}_k(t)dt$, and T_b is the time length of the information bit.

The first item is the expected signal, whereas the second item is the correlation sum of the spread spectrum code and other signals, which is the MAI. The third item is the channel noise.

The output of a matched filter of N signals is given below:

$$\begin{aligned} \mathbf{Y} &= [y_1, y_2, \ldots, y_N]^T, \\ \mathbf{Y} &= \begin{bmatrix} \rho_{11} & \rho_{12} & \cdots & \rho_{1N} \\ \rho_{21} & \rho_{22} & \cdots & \rho_{2N} \\ \vdots & \vdots & \vdots & \vdots \\ \rho_{N1} & \rho_{N2} & \cdots & \rho_{NN} \end{bmatrix} \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_N \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_N \end{bmatrix} \\ &\quad + \begin{bmatrix} n_1 \\ n_2 \\ \vdots \\ n_N \end{bmatrix} = \mathbf{RAb} + \mathbf{n}. \end{aligned} \tag{3}$$

Definite $\mathbf{H} = \mathbf{RA}$ and formula (3) can be written as follows:

$$\mathbf{Y} = \mathbf{Hb} + \mathbf{n}. \tag{4}$$

In traditional detection, the output of a matched filter will be sampled at every bit interval, and the bit will be decided on the basis of the decision threshold:

$$\widehat{\mathbf{b}} = \mathrm{dec}(\mathbf{Y}) = \mathrm{dec}(\mathbf{Hb} + \mathbf{n}), \tag{5}$$

where dec( ) represents the decision value of the bit. Getting the bit directly with the decision of the matched filer output, critical errors could possibly be caused by MAI, especially for the covert low-power signal.

3. Multiple User Detection Method for Spread Spectrum Communication

As an effective method to improve the capacity of a spread spectrum communication system, a MAI suppression method has been developed in depth [6, 7]. The typical method includes two types: multiple user detection (MUD) and an interference cancellation method. The foundation of the MUD method is the calculation of correlation between signals, and the interference is suppressed by the decorrelation process. The traditional MUD method includes the zero forcing (ZF) method and the minimum mean square error (MMSE) method, among many other new methods proposed over the years.

Here, a MUD method aided by a Hopfield neural network is proposed [8]. With the method, detection performance can be improved, but the improvement will decrease with an increase in signal number. A weighted orthogonal matched filter method based on quantum signal processing is proposed [9]. With this method, the estimation of noise power is not necessary, but the detection performance is reduced compared to the MMSE method. A blind MUD method based on Schmidt-orthogonalization and subspace-tracking Kalman filtering is also presented, and with this method, the complexity of the blind MUD method is reduced [10]. There are two types of interference cancellation methods: serial interference cancellation (SIC) and parallel interference cancellation (PIC). Based on the correlation computation of signals, the signal interference influence of other signals can be cancelled by the serial or parallel mode. The performance of this kind of method is suboptimal compared with the MUD method. Its performance is limited by the initial detection accuracy of multiple signals. When multiple interference is serious, the platform effect will emerge early and the detection performance will not be ideal [11, 12]. In practical applications, the detection performance can be improved with usage combined with high-gain error correction coding. The benefit from the low computation complexity and flexible processing architecture leads to this interference cancellation method being applied in some satellite communication system designs.

The article is focused on the MUD method. The basic idea of the MUD method is to cancel MAI between signals with

the calculation and transformation of a correlation matrix. Maximum likelihood (ML), ZF, and MMSE methods are typical algorithms applied.

The ML algorithm is the theoretical optimum MUD algorithm. Its principle is shown as follows. Generate a transmit signal traversal set and complete the following operation:

$$\widehat{\mathbf{b}} = \operatorname{argmin}(\mathbf{Y} - \mathbf{Hb}) \quad \mathbf{b} \in \{\mathbf{b}\}. \tag{6}$$

The main process of ZF algorithm involves calculating the inverse matrix G of the correlation matrix $\mathbf{H}$ and then calculating the dot product of $\mathbf{G}$ and the output of the matched filter group. After that, estimation of transmitter signals can be obtained with the following decision [13]:

$$\begin{aligned} \mathbf{G} &= \left(\mathbf{H}^H\mathbf{H}\right)^{-1}\mathbf{H}^H, \\ \widehat{\mathbf{b}} &= \operatorname{dec}(\mathbf{G}(\mathbf{Hb} + \mathbf{n})) = \mathbf{b} + \mathbf{n}'. \end{aligned} \tag{7}$$

$\mathbf{n}'$ is the noise component after ZF conversion and bit decision.

The calculation complexity of the ZF method is relatively low and scales with the number of signals.

The estimation error covariance matrix is as follows:

$$\boldsymbol{\varphi}_{\mathrm{MMSE}} = E\left\{\left(\widehat{\mathbf{b}} - \mathbf{b}\right)\left(\widehat{\mathbf{b}} - \mathbf{b}\right)^H\right\} = \sigma^2\left(\mathbf{H}^H\mathbf{H}\right)^{-1}. \tag{8}$$

σ^2 is the variance of noise. The influence of noise is always increased with the ZF method, which is why ZF performs poorly with a low signal noise ratio (SNR) scenario. $(\mathbf{H}^H\mathbf{H})^{-1}$ can be defined as the demodulation error coefficient for ZF, which measures how the influence of noise is enlarged by the ZF method.

The basic idea of MMSE is to minimize the mean square error between transmit signal and estimation result. Unlike the ZF method, MMSE takes noise suppression into account, and thus the estimation performance is improved to some extent. The process of MMSE is as follows:

$$\begin{aligned} \mathbf{G}' &= \left(\mathbf{H}^H\mathbf{H} + \sigma^2\mathbf{I}\right)^{-1}\mathbf{H}^H, \\ \widehat{\mathbf{b}} &= \operatorname{dec}\left(\mathbf{G}'(\mathbf{Hb} + \mathbf{n})\right) = \mathbf{b} + \mathbf{n}''. \end{aligned} \tag{9}$$

$\mathbf{n}''$ is the noise component after MMSE conversion and bit decision.

The estimation error covariance matrix of MMSE is

$$\begin{aligned} \boldsymbol{\varphi}_{\mathrm{MMSE}} &= E\left\{\left(\widehat{\mathbf{b}} - \mathbf{b}\right)\left(\widehat{\mathbf{b}} - \mathbf{b}\right)^H\right\} \\ &= \sigma^2\left(\mathbf{H}^H\mathbf{H} + \sigma^2\mathbf{I}\right)^{-1}. \end{aligned} \tag{10}$$

Based on formal analysis, it can be shown that the performance of MUD is influenced by noise and the orthogonality of the correlation matrix. If the correlation matrix is orthogonal, the detection performance of MUD will equal that of the performance of a single signal without MAI. In addition, for special users, it is possible to suppress noise with the transformation of the correlation matrix. Searching for a method, which can improve the orthogonality of the matrix, is an important pathway to fulfill enhanced MAI cancellation.

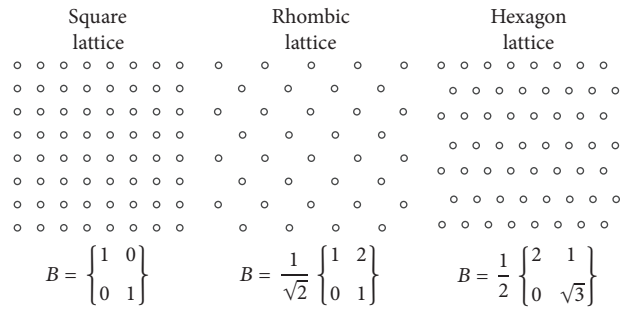

Figure 1: Several typical lattices.

4. Multiple User Detection Methods Based on Lattice Reduction

4.1. Lattice Theory. A lattice is a congregation of scatter points arranged with scheduled rule [14–16]. Any lattice can be generated by a group of linear unrelated vectors. Figure 1 shows several typical types of lattice.

Suppose a group of n dimensional vectors is defined by $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m) \in R_n$. The number of vectors is m and the vectors are linearly independent. The integrated linear combination of the vectors can form an m-dimensional lattice. It can be written as follows:

$$L(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m) = \sum_{i=1}^{m} t_i b_i, \quad t_i \in Z. \tag{11}$$

Vector $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m)$ is one foundation of the lattice, and $\mathbf{t} = [t_1, t_2, \ldots, t_n]^T$ is the coefficient vector composed of integers. It can be written in matrix mode:

$$L = \{\mathbf{l} = \mathbf{Bt}\}. \tag{12}$$

The three different lattices are generated from the basis below the figures. The dimensionality is decided by the number of base vectors. The dimensionality of the base vector is called the rank of the generated lattice.

The basis of a lattice is diversified. A lattice can be denoted by different bases. An m-dimensional space can be generated by any group of m linearly independent vectors, but not any group of m linearly independent vectors can form a lattice.

There is a fixed relation between the different base vectors of one lattice. For the lattice $L(\mathbf{B})$ generated by vector group $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m)$, all of the vectors transformed from $\mathbf{B}$ by an elementary column transfer from the base vectors of the lattice. The product of several elementary column transfer matrices equals one unimodular transfer matrix $\mathbf{T}$. The elements of $\mathbf{T}$ are complex integers and the determinant of $\mathbf{T}$ equals ± 1. As long as $\mathbf{T}$ is a unimodular matrix, the same lattice can be generated by $\mathbf{B}$ and $\mathbf{BT}$.

$$L(\mathbf{B}) = L(\mathbf{BT}). \tag{13}$$

The shortest base vector, that is, the base vector of shortest length, is a common research object for a lattice. If the shortest base vector cannot be reached, the nearest short base vector is always desired. The basis of a lattice has the

Input: $\mathbf{Q}$, $\mathbf{R}$
Reduction process:
Initialization: $\mathbf{Q}' = \mathbf{Q}$, $\mathbf{R}' = \mathbf{R}$, $k = 2$;
While $k \le n$
for $l = k-1, \ldots, 1$
$b = \mathbf{R}'(l,k)/\mathbf{R}'(l,l)$, b rounded to complex integer μ
if $(\mu \neq 0)$
$\mathbf{R}'(1:l,k) = \mathbf{R}'(1:l,k) - \mu\mathbf{R}'(1:l,l)$
$\mathbf{P}(:,k) = \mathbf{P}(:,k) - \mu\mathbf{P}(:,l)$
end
end
if $(\delta\|\mathbf{R}'(k-1,k-1)\|^2 > \|\mathbf{R}'(k,k)\|^2 + \|\mathbf{R}'(k-1,k)\|^2)$
Interchange column $k-1$ and column k of matrix $\mathbf{R}'$ and $\mathbf{P}$.
Calculate the Givens rotation matrix $\boldsymbol{\theta}$, to make $\mathbf{R}'(k,k-1) = 0$:
$\mathbf{R}'\left(k-1:k,k-1:N_t\right) = \boldsymbol{\theta}\mathbf{R}'\left(k-1:k,k-1:N_t\right)$
$\mathbf{Q}'(:,k-1:k) = \mathbf{Q}'(:,k-1:k)\,\boldsymbol{\theta}^H$
$\left(\boldsymbol{\theta} = \begin{bmatrix} \mathbf{c} & \mathbf{s} \\ -\mathbf{s} & \mathbf{c} \end{bmatrix},\ \mathbf{c} = \dfrac{\mathbf{R}'(k-1,k-1)}{\|\mathbf{R}'(k-1:k,k-1)\|},\ \mathbf{s} = \dfrac{\mathbf{R}'(k,k-1)}{\|\mathbf{R}'(k-1:k,k-1)\|}\right)$
$k = \max\{k-1, 2\}$
else
$k = k+1$
end
If $k > n$, export $\mathbf{R}'$ $\mathbf{Q}'$ and transfer matrix $\mathbf{P}$
Reduction completed.

Algorithm 1: Algorithm LLL.

feature that a shorter basis will be more orthometric. Lattice reduction is the process by which the nearest short base vector is found while the orthogonality of the base vector is improved.

4.2. Lattice Reduction Algorithms. Lattice reduction is a process to obtain the nearest short base vector while the orthogonality of the base vector is improved. Common lattice reduction algorithms include the Lenstra–Lenstra–Lovász (LLL) reduction [17] and the Seysen reduction [18, 19].

To measure the orthogonality of a lattice basis, the degree of orthogonality defect is defined. Suppose $(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m)$ is one group of base vectors of lattice L, and the base vector matrix is $\mathbf{H}$. The degree of orthogonality defect of $\mathbf{H}$ is defined as

$$\Delta(\mathbf{H}) = \frac{\prod_{m=1}^{M} \|\mathbf{h}_m\|^2}{\det\left(\mathbf{H}^H\mathbf{H}\right)}. \tag{14}$$

In the formula, M is the column number of $\mathbf{H}$, $\mathbf{h}_m$ is the column m of $\mathbf{H}$, and det( ) is the determinant operator. $\Delta(\mathbf{H}) \ge 1$, and only when $\mathbf{H}$ is an orthogonal matrix, $\Delta(\mathbf{H}) = 1$.

Suppose $\mathbf{H}'$ is the matrix generated by an LLL reduction:

$$\mathbf{H}' = \mathbf{HP}, \quad \mathbf{P} \text{ is a unimodular matrix.} \tag{15}$$

If $\mathbf{R}'$ is found via a QR decomposition of $\mathbf{H}'$, it satisfies the following two conditions:

$$\begin{aligned} \left\|r'_{l,k}\right\| &\le \frac{1}{2}\left\|r'_{l,l}\right\|, \quad 1 \le l \le k \le n, \\ \delta\left\|r'_{k-1,k-1}\right\| &\le \left\|r'_{k,k}\right\| + \left\|r'_{k-1,k}\right\|, \quad k = 2, \ldots, n. \end{aligned} \tag{16}$$

Then, $\mathbf{H}'$ is the matrix processed by LLL reduction.

The basic procedure of LLL [20–22] is shown in Algorithm 1

Compared with the LLL reduction, the main difference in the Seysen reduction is a different definition of the degree of orthogonality defect:

$$S(\mathbf{H}) = \sum_{m=1}^{M} \|\mathbf{h}_m\|^2 \left\|\mathbf{h}_m^{\#}\right\|^2. \tag{17}$$

In the formula, $\mathbf{H}$ has M columns. $\mathbf{h}_m$ is the m column of $\mathbf{H}$, and $\mathbf{h}_m^{\#}$ is the m column of the dual matrix $\mathbf{H}^{\#} = ((\mathbf{H}^H\mathbf{H})^{-1}\mathbf{H}^H)^H$ [12, 13].

When $\mathbf{H}$ is an orthogonal matrix,

$$S(\mathbf{H})_{\min} = M. \tag{18}$$

The Seysen algorithm takes both the raw matrix and dual matrix into account; as a result, a better reduction performance can be achieved.

1: Estimation of signals Y is calculated by matched filters.
Signal power, relative delay, and carrier phase difference of signals are estimated.
2: A correlation matrix between signals $\mathbf{H}$ is calculated.
3: Process $\mathbf{H}$ with lattice reduction algorithm (LLL or Seysen).
Conversion matrix $\mathbf{P}$ and optimized matrix $\mathbf{H}' = \mathbf{HP}$ is obtained.
4: The ZF or MMSE method is implemented

$$\widetilde{\mathbf{Z}}_{\mathrm{LLL\_ZF}} = \left(\mathbf{H}'^{H}\mathbf{H}'\right)^{-1}\mathbf{H}'^{H}\mathbf{Y}$$

$$\widetilde{\mathbf{Z}}_{\mathrm{LLL\_MMSE}} = \left(\mathbf{H}'^{H}\mathbf{H}' + \sigma^2\mathbf{P}^{H}\mathbf{P}\right)^{-1}\mathbf{H}'^{H}\mathbf{Y}$$

5: The modified quantization in improved lattice space is taken:

$$\widehat{\mathbf{Z}} = a\left(\left\lceil \frac{1}{a}\widetilde{\mathbf{Z}} - \frac{1}{2}\mathbf{P}^{-1}\mathbf{I}\right\rfloor + \frac{1}{2}\mathbf{P}^{-1}\mathbf{I}\right).$$

a is the power normalization parameter, and $\lceil\ \rfloor$ is the roundness of real value.
6: Final detection result $\widehat{\mathbf{X}}$ is calculated.

$$\widehat{\mathbf{X}} = \mathbf{P}\widehat{\mathbf{Z}}$$

Algorithm 2: Algorithm LR-MUD.

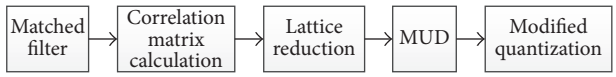

Figure 2: Process of the LR-MUD algorithm.

4.3. Lattice Reduction Aided Multiple User Detection (LR-MUD). With lattice reduction, the correlation matrix $\mathbf{H}$ can be transformed to matrix $\mathbf{H}'$, which has better orthogonality. The analysis of the MUD method in Section 2 shows that with a correlation matrix with better orthogonality the influence of noise can be better suppressed.

The process of lattice reduction aided multiple user detection algorithm is shown in Algorithm 2

The basic process of the algorithm is shown in Figure 2. The signal power and signal delay estimation accuracy is important to the performance of the algorithm. To estimate the signal power in the MAI scene, a synchronization-head can be used to improve the estimation accuracy. The signal delay and carrier phase information can be given by the signal tracking loop. The measurement accuracy can be improved by extending integration time and by using a large correlator design. Related research shows that week spread spectrum signals like GPS can be tracked stably when SNR is lower than −4 dB.

The complexity of ML is $O({N_s}^M)$, where N_s is the modulation order and M is the signal number. The complexity of ML increases with N_s exponentially. The complexity of ZF and MMSE is relatively low, given as $O(M^3)$. The main computation of the MUD method is in the inversion of the correlation matrix. The lattice reduction process is added based on the MUD in the LR-MUD method. The increased computation includes QR decomposition and inversion of matrix $\mathbf{P}$. The increase in complexity is linear, and thus the complexity is still $O(M^3)$. Compared with ML, LR-MUD has superior performance in regard to complexity.

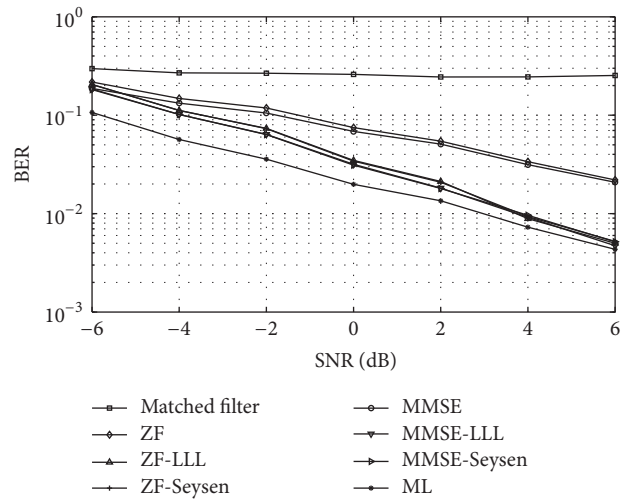

Figure 3: BER of LR-MUD with different SNR scenarios.

5. Simulation and Analysis

In this section, simulations of the LR-MUD method of SS communication are presented. The signal modulation is QPSK, and the spread code sequence is a group of gold codes.

Figure 3 shows a demodulation BER in different SNR scenarios. The signal number is 6, and the spread ratio is 16. Signal power is distributed randomly in the range of 0–6 dB, and the BER of all signals is counted. MAI can be cancelled effectively by the ZF or MMSE method. The BER of the two algorithms is lower than the BER of the basic matched filter method, but the performance is much weaker than that of the ML method. In the figure, ZF-LLL and ZF-Seysen are the tested LR-MUD methods based on a combination of the ZF method using a lattice reduction by LLL and Seysen. Likewise, MMSE-LLL and MMSE-Seysen are the tested LR-MUD methods based on the MMSE method using a lattice reduction by LLL and Seysen. The BER of LR-MUD is

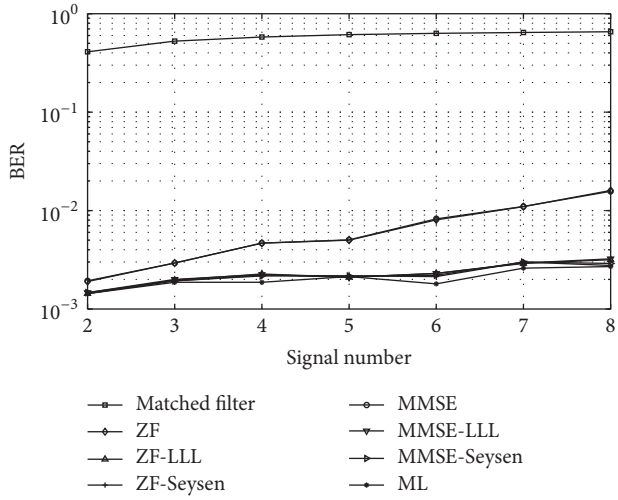

Figure 4: BER of desired signal with different signal numbers.

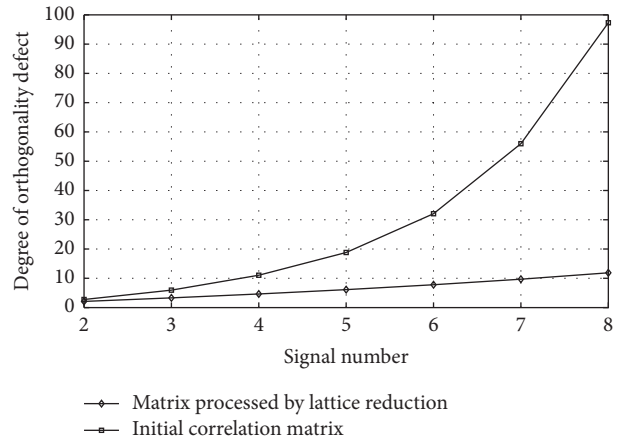

Figure 5: Degree of orthogonality defect of a correlation matrix with different signal numbers.

reduced significantly compared with the MUD methods, and its performance approaches ML with an increase of SNR. The algorithm gain compared to MUD is more than 4 dB.

Figure 4 shows the demodulation BER of a desired signal with different numbers of interference signals. Here, the spread ratio is 16 and the SNR of the covert signal is 0 dB. The power of the other signals is randomly distributed in the 0–20 dB range compared to the desired signal. The BER of the traditional MUD method increases with an increase in signal number. Performance near ML is achieved by LR-MUD and remains steady even with an increase in signal number. LR-MUD shows superiority when subjected to a greater number of interference signals. With the same BER requirements, the number of interfering high-power signals is 7 for LR-MUD, compared to 2 for the traditional MUD method.

Figure 5 shows the variation in the orthogonality of the correlation matrix. Along with the increase of signal number, the degree of orthogonality defect for the initial correlation matrix increases, which results in the demodulation deterioration in the traditional MUD method. In contrast, the degree of orthogonality defect of the matrix processed by LR increases only slightly. Furthermore, this is the explanation for why LR-MUD performs better than the traditional MUD method.

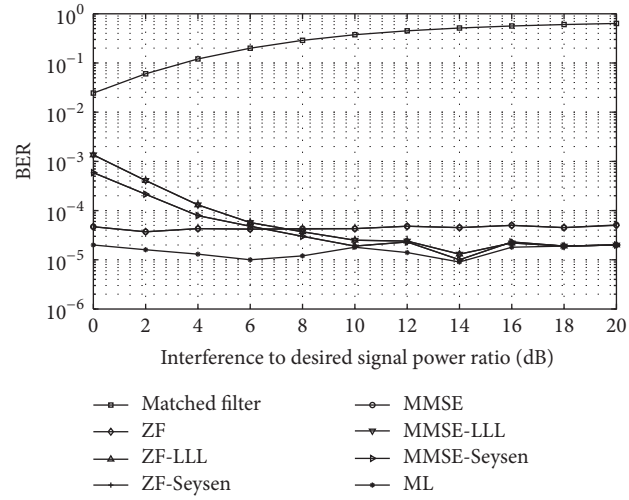

Figure 6: BER of a desired signal with different interference to signal power ratios.

Figure 6 shows the simulation result with different signal power ratios. The spread ratio is 32 and the signal number is 6. SNR of covert signal is 0 dB. The power of the covert signal and noise remain stable, while the power of 5 interference signals increases gradually. The BER of the desired signal is counted. The BER of the MUD method does not change with the increase in power; a fixed gap remains between ML and MUD method. The BER of LR-MUD decreases with the power increase of interference signals, and finally near ML performance is achieved when the interference to signal power ratio is larger than 10 dB. This shows the effect of lattice reduction. When the correlation between signals is good, the algorithm gain of the LR is relatively limited. When the correlation between signals is poor, the algorithm gain of LR will increase. Therefore, LR-MUD is suitable to use in intense near-far scenarios.

Figure 7 shows the variation of the degree of orthogonality defect for a correlation matrix with an increase of interference to signal power ratio. The orthogonality defect of the correlation matrix does not change. With a lattice reduction, the orthogonality of the correlation matrix is improved, and the effect improves further with an increase in interference power.

Figure 8 shows the variation of demodulation error coefficient for a desired signal with an increase of interference to signal power ratio. The change of the demodulation error coefficient is consistent with the BER change shown in Figure 6. With additional increase of interference to signal power ratio, the amplification of noise decreases with the LR-MUD method. This is the main reason why LR-MUD performs better than traditional the MUD method.

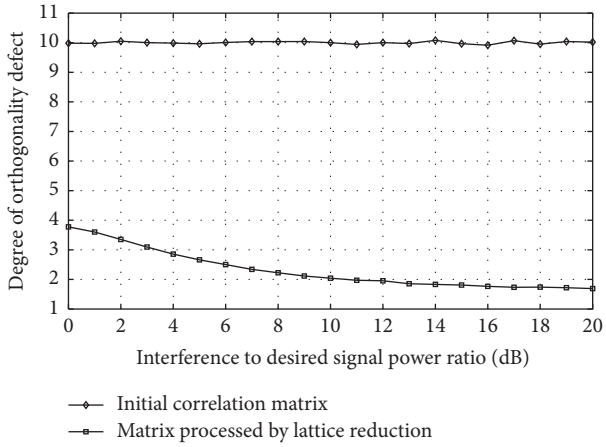

Figure 7: The degree of orthogonality defect for a correlation matrix with different interference to signal power ratios.

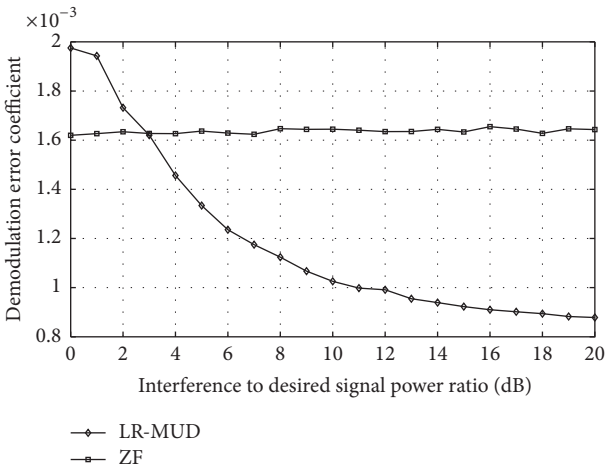

Figure 8: Demodulation error coefficient with different interference to signal power ratios.

6. Design of a Covert Communications System Based on LR-MUD

Because of the excellent performance gain in intense near-far scenarios, LR-MUD is appropriate for implementation in covert communication systems based on SS principles. A block diagram for a covert communications system design is given in Figure 9.

The system includes a covert signal transmitter, covert signal receiver, and common signal transmitter. High-power signals can be transmitted by the covert transmitter as well as a number of common signal transmitters. The covert signal and at least one high-power signal should be transmitted by a covert transmitter synchronously. At the receiver, the capture and tracking of covert signals should be performed using the synchronous high-power signal. All signals will be demodulated with the LR-MUD method.

Figure 10 is the simulation result of the covert transmission performance with different spread ratios. SNR of covert signal is 0 dB and coverage signal number is 5. With

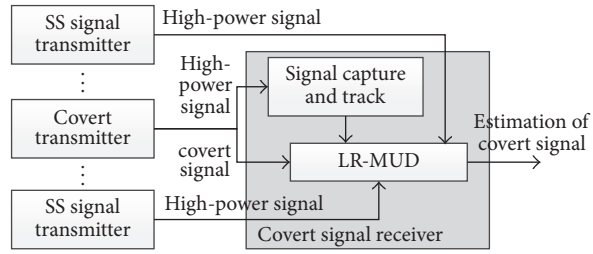

Figure 9: System diagram of a covert communications system based on LR-MUD.

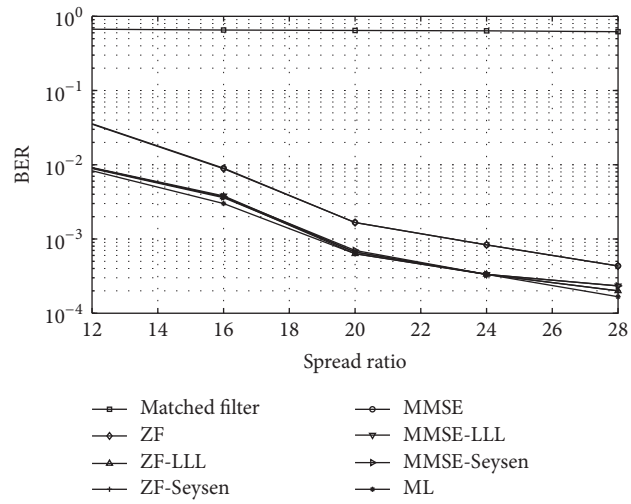

Figure 10: BER of a covert signal with different spread ratios.

the increase of spread ratio, BER decreases with the cost of information rate. The same BER can be achieved by LR-MUD with a lower spread ratio compared to the common MUD method. Higher information rates can be realized by LR-MUD with the same wireless link resource and concealment requirements.

7. Summary and Conclusions

In this paper, lattice reduction theory and related algorithms are applied to the MUD of a spread spectrum communications system, and an algorithm called LR-MUD is presented. Theoretical analyses and simulation results on the LR-MUD method are carried out, showing excellent near-far effect suppression performance. Based on the LR-MUD method, a design of a covert communications system can be feasibly realized. The covert signal can be transmitted at a higher information rate with the coverage of more high-power cochannel signals. Thus, higher transmission rates and concealment performance are achieved using the same link resources.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors acknowledge the National Natural Science Foundation of China (Grant 91638203) and the National Key Research and Development Program of China (Grant 2016YFB0502102).

References

[1] Y. Cao, H. Zhang, X. Zhao, and H. Yu, "Covert communication by compressed videos exploiting the uncertainty of motion estimation," *IEEE Communications Letters*, vol. 19, no. 2, pp. 203–206, 2015.

[2] M. Cunche, M.-A. Kaafar, and R. Boreli, "Asynchronous covert communication using bittorrent trackers," in *Proceedings of the 16th IEEE International Conference on High Performance Computing and Communications, HPCC 2014, 11th IEEE International Conference on Embedded Software and Systems, ICESS 2014 and 6th International Symposium on Cyberspace Safety and Security, CSS 2014*, pp. 827–830, fra, August 2014.

[3] H. Shi and A. Tennant, "Covert communication using a directly modulated array transmitter," in *Proceedings of the 8th European Conference on Antennas and Propagation, EuCAP 2014*, pp. 352–354, nld, April 2014.

[4] L. Li, J. Zheng, and L. Zheng, "The Chaotic Code-hopping Spread Spectrum Communication System[J]," *Science Technology and Engineering*, vol. 13, no. 30, pp. 176–180, 2014.

[5] X. Zhao, X. Ma, and W. Qu, "Analysis of the parasitic small signal coupling with RDSS RF signal [J]," *Telecommunication Engineering*, vol. 49, no. 8, pp. 40–44, 2009.

[6] Y. Hou, M. Li, X. Yuan, Y. T. Hou, and W. Lou, "Cooperative Interference Mitigation for Heterogeneous Multi-Hop Wireless Networks Coexistence," *IEEE Transactions on Wireless Communications*, vol. 15, no. 8, pp. 5328–5340, 2016.

[7] Q. Zhou and X. Ma, "Receiver designs for differential UWB systems with multiple access interference," *IEEE Transactions on Communications*, vol. 62, no. 1, pp. 126–134, 2014.

[8] G. I. Kechriotis and E. S. Manolakos, "Hopfield neural network implementation of the optimal CDMA multiuser detector," *IEEE Transactions on Neural Networks*, vol. 7, no. 1, pp. 131–141, 1996.

[9] S.-N. Shi, Y. Shang, and Q.-L. Liang, "A novel linear multi-user detector," *Acta Electronica Sinica*, vol. 35, no. 3, pp. 426–429, 2007.

[10] Y. Yu, J. Li, Z. Wang, S. Wang, and H. Zhang, "Blind multiuser detection in MC-CDMA: Schmidt-orthogonalization and subspace tracking Kalman filtering," in *Proceedings of the 2011 3rd International Conference on Communications and Mobile Computing, CMC 2011*, pp. 375–380, chn, April 2011.

[11] Z. Xie, R. T. Short, and C. K. Rushforth, "A Family of Suboptimum Detectors for Coherent Multiuser Communications," *IEEE Journal on Selected Areas in Communications*, vol. 8, no. 4, pp. 683–690, 1990.

[12] W. Zheng, J. Li, Y. Luo, J. Chen, and J. Wu, "Multi-user interference pre-cancellation for downlink signals of multi-beam satellite system," in *Proceedings of the 2013 3rd International Conference on Consumer Electronics, Communications and Networks, CECNet 2013*, pp. 415–418, chn, November 2013.

[13] Y. Bao and B. Yu, "A MAI cancellation algorithm with near ML performance," in *Proceedings of the IEEE International Conference on Communication Software and Networks, ICCSN 2015*, pp. 196–200, chn, June 2015.

[14] M. R. Bremner, *Lattice Basis Reduction: An introduction to the LLL algorithm and its applications*, vol. 300, CRC Press, Inc., Boca Raton, FL, USA, 2012.

[15] S. M. Dias and N. J. Vieira, "Concept lattices reduction: Definition, analysis and classification," *Expert Systems with Applications*, vol. 42, no. 20, pp. 7084–7097, 2015.

[16] B. A. Lamacchia, *Basis reduction algorithms and subset sum problems [D]. [Master's dissertation]*, Massachusetts Inst Technol, 1991.

[17] A. K. Lenstra, J. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, no. 4, pp. 515–534, 1982.

[18] P. Q. Nguyen and J. Stern, "Lattice reduction in cryptology: an update," in *Algorithmic number theory (Leiden, 2000)*, vol. 1838 of *Lecture Notes in Comput. Sci.*, pp. 85–112, Springer, Berlin, 2000.

[19] C.-P. Schnorr and M. Euchner, "Lattice basis reduction: improved practical algorithms and solving subset sum problems," *Mathematical Programming*, vol. 66, no. 2, Ser. A, pp. 181–199, 1994.

[20] P. Q. Nguyen and J. Stern, "Lattice Reduction in Cryptology: An Update [C]," *Lecture Notes in Computer Science*, no. 4, pp. 85–112, 1838.

[21] X. Ma and W. Zhang, "Performance analysis for MIMO systems with lattice-reduction aided linear equalization," *IEEE Transactions on Communications*, vol. 56, no. 2, pp. 309–318, 2008.

[22] L. G. Barbero, T. Ratnarajah, and C. Cowan, "A comparison of complex lattice reduction algorithms for MIMO detection," in *Proceedings of the 2008 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP*, pp. 2705–2708, usa, April 2008.