Master's Thesis

석사 학위논문

Performance Improvement of the Uplink WCDMA Scrambling Code Identification Using Multiple Antennas Combining

Chankeun Park (박 찬 근 朴 贊 根)

Department of Information and Communication Engineering

정보통신융학공학전공

DGIST

2017

Master's Thesis

석사 학위논문

Performance Improvement of the Uplink WCDMA Scrambling Code Identification Using Multiple Antennas Combining

Chankeun Park (박 찬 근 朴 贊 根)

Department of Information and Communication Engineering

정보통신융학공학전공

DGIST

2017

Performance Improvement of the Uplink WCDMA Scrambling Code Identification Using Multiple Antennas Combining

Advisor: Professor Ji-Woong Choi

Co-Advisor: Professor Hongsoo Choi

By

Chankeun Park

Department of Information and Communication Engineering

DGIST

A thesis submitted to the faculty of DGIST in partial fulfillment of the requirements for the degree of Master of Science in the Department of Information and Communication Engineering. The study was conducted in accordance with Code of Research Ethics[1)].

July. 03. 2017

Approved by

Professor Ji-Woong Choi (Signature)

(Advisor)

Professor Hongsoo Choi (Signature)

(Co-Advisor)

1) Declaration of Ethical Conduct in Research**:** I, as a graduate student of DGIST, hereby declare that I have not committed any acts that may damage the credibility of my research. These include, but are not limited to: falsification, thesis written by someone else, distortion of research findings or plagiarism. I affirm that my thesis contains honest conclusions based on my own careful research under the guidance of my thesis advisor.

Performance Improvement of the Uplink WCDMA Scrambling Code Identification Using Multiple Antennas Combining

Chankeun Park

Accepted in partial fulfillment of the requirements for the degree of
Master of Science

July. 03. 2017

Head of Committee_____(인)

Prof. Ji-Woong Choi

Committee Member_____(인)

Prof. Jihwan Choi

Committee Member_____(인)

Prof. Hongsoo Choi

MS/IC

201522030

박찬근.Chankeun Park.Performance Improvement of the Uplink WCDMA Scrambling Code Identification Using Multiple Antennas Combining. Department of Information and communication Engineering. 2017. 39p. Adviosr Prof. Ji-Woong Choi, Co-Advisor Prof. Jihwan Choi, Prof. Hongsoo Choi.

Contents

List of Figures

Abstract

In this thesis, I develop an eavesdropping method for uplink wideband code division multiple access (WCDMA) system. In order to achieve effective eavesdropping of uplink WCDMA message, one of the most demanding systematic characteristics is the scrambling code information. While the previous works of identifying the scrambling code use only one antenna and cannot operate well in practical environments having low signal to noise power ratio (SNR), I propose an improved method for robust identification performance in more practical scenarios by using multiple antennas. The proposed method exploits not only multiple antennas but also non-coherent combining (NCC) which enables combining the received signals of each antenna without any channel state information (CSI). Through numerical simulation, I demonstrate that the proposed method is effective for both slow and fast fading environments and evaluate the performance using various system parameters.

In the second Chapter, I explain the conventional scrambling code identification method. This method consists of chip-level processing, min-sum algorithm, and scrambling code identification. Chip-level processing makes the received signal to the shifted m-sequence from upper shift register sequence (SRS) of the scrambling code generator. Min-sum algorithm is used to reliably detect the shifted m-sequence in the presence of interference. Finally, scrambling code identification determine the uplink scrambling code by using shifted m-sequence and transition matrices. In the third Chapter, I described the proposed NCC in order to obtain better performance, discuss how the proposed method differs from the conventional method, and analyze how the performance gain in performance is achieved.

I. INTRODUCTION

Although 3G communication becomes less used, it is still being provided in many countries [1]. Especially, North Korea is recently providing WCDMA system to senior officials. Therefore, the research for eavesdropping the WCDMA messages is still receiving much attention, e.g., identifying the messages between enemies for military purposes.

Since constructing the uplink WCDMA message contains the scrambling operation, it is necessary to obtain the scrambling code information to achieve effective eavesdropping. While some of the previous works provide blind identification method of the scrambling code, practical issues in real-world implementations have not been widely considered. For example, one of the recent works related to this thesis for identifying the scrambling code of the WCDMA message is provided in [2]. However, since [2] assumes relatively simple and impractical communication environment, the algorithm works properly only in relatively high SNR. We may improve the detecting performance over [2] by increasing the size of the parity check matrix or the length of the input bit sequence for min-sum algorithm [2]. However, such increment does not provide satisfactory improvement in performance and even might result in prohibitive computational complexity.

For an alternative choice, I focus on exploiting non-coherent combining (NCC) using multiple antennas. Since NCC can combine the signals of each antenna, NCC-based blind scrambling code identification might be a wise solution for practical implementation without any channel estimation procedure. By jointly employing the NCC with multiple antennas, I pursue the scrambling code identification to operate in practical SNR without noticeable computational complexity increment.

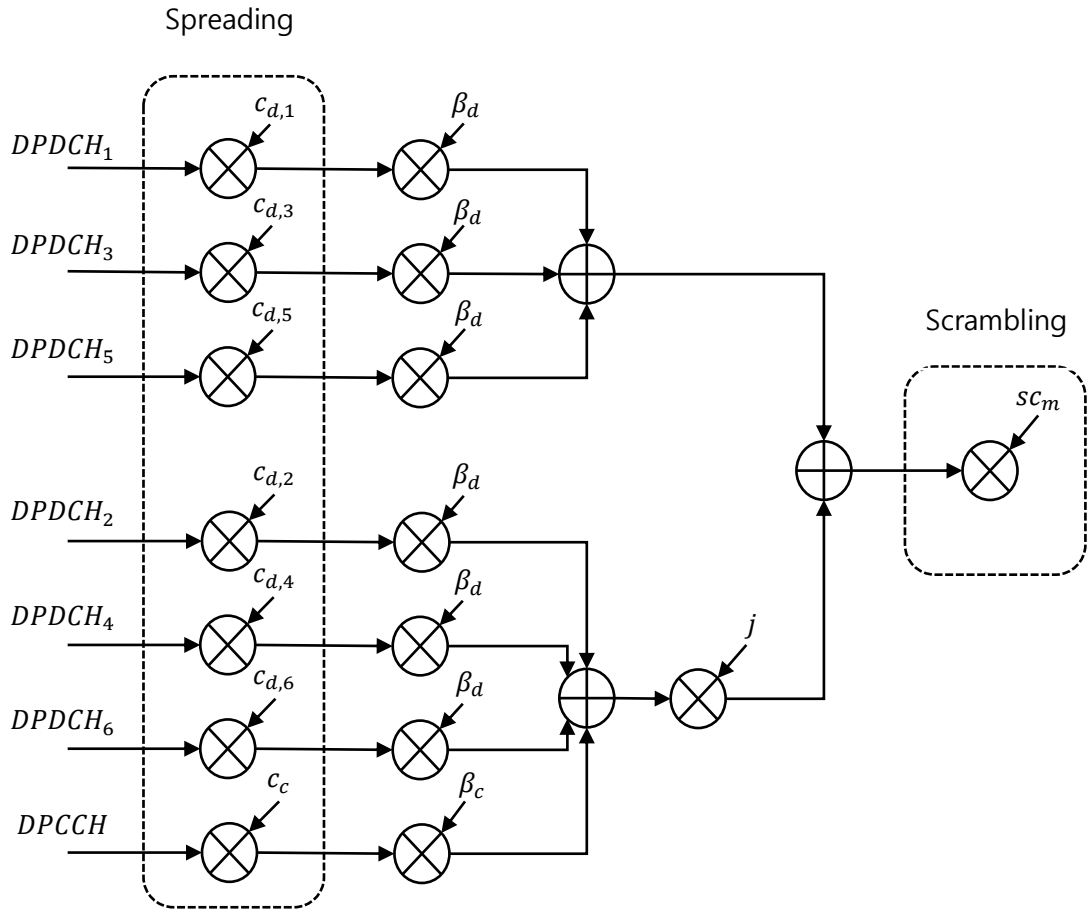

Figure 1.1 Overall process of generating a WCDMA message

Furthermore, this thesis provides NCC-based scrambling code identification algorithm is along with numerical performance evaluation in various practical scenarios. To be specific, the performance for different sizes of the parity check matrices and numbers of antennas in various channels are discussed. In addition, the performance of NCC is compared with maximal ratio combining (MRC), which is the optimum combiner that provides the lower bound of possible error rate with perfect CSI.

Next, the generation process of the uplink WCDMA message is provided, which consists of constructing the channelization and the scrambling codes. The channelization codes and scrambling code are selected according to 3rd generation partnership project (3GPP) standard [3]. Figure 1.1 is the overall process of generating a WCDMA message

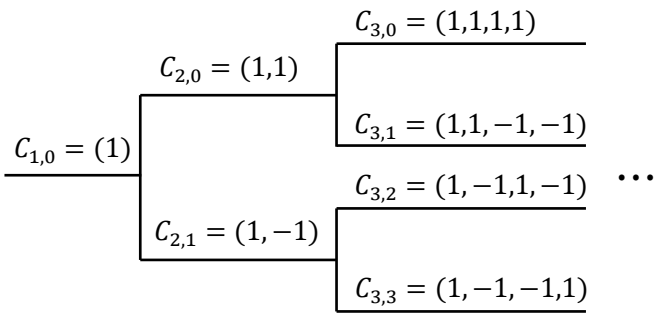

Figure 1.2 Code tree for channelization code

consisting of spreading operation and scrambling operation, where $c_{d,k}$ and c_c are the channelization codes for dedicated physical data channel (DPDCH) and dedicated physical control channel (DPCCH) which convey the data and control data, respectively, k is the index of DPDCH, and β_d and β_c are gain values that are signaled by higher layers.

The rest of this thesis is organized as follows. Detailed procedure of uplink WCDMA signaling is explained in the remaining part of chapter II. Also, conventional uplink scrambling code identification method is explained in chapter III. Uplink scrambling code identification algorithm using NCC is developed in chapter IV. After that, chapter V presents simulation results and performance analysis, and I conclude our paper in chapter VI.

1.1 Channelization code

Channelization codes are generated by following the structure of the orthogonal variable spreading factor (OVSF) codes construction. These codes maintain orthogonality with other physical channels and can be defined using code tree of Figure

1.2. The channelization code is denoted as $C_{SF,t}$ where SF denotes the spreading factor and t is

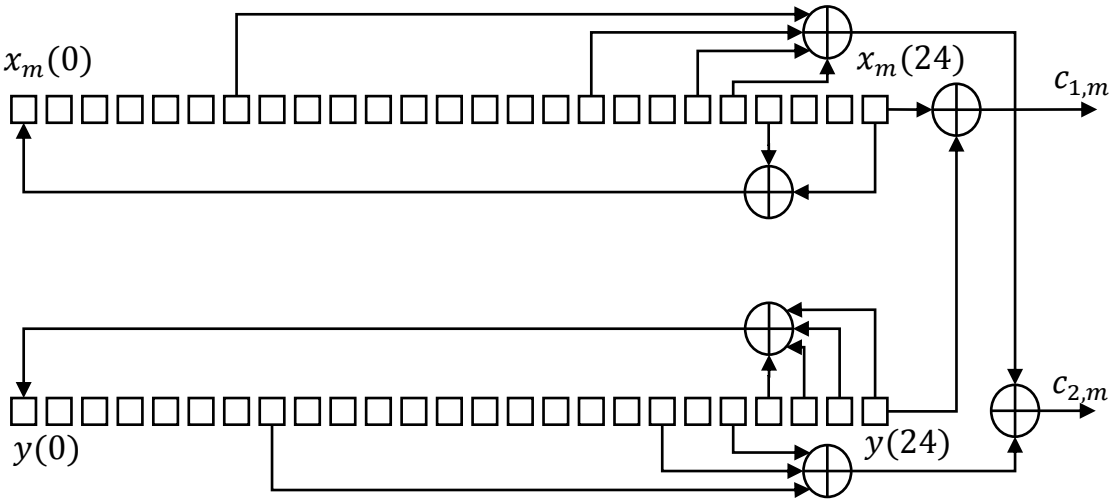

Figure 1.3 Scrambling code generator

the code index. DPCCH is always spread by as $c_c = C_{256,0}$. When only one DPDCH is transmitted, the code of DPDCH is decided as $c_{d,1} = C_{SF,SF/4}$. And if more than one DPDCHs are to be transmitted, the codes of all DPDCHs are $c_{d,k} = C_{4,t}$ where $t = 1$ if $k \in \{1,2\}$, $t = 3$ if $k \in \{3,4\}$, and $t = 2$ if $k \in \{5,6\}$.

1.2 Scrambling code

Scrambling code is constructed from the scrambling code generator which has two shift register sequences (see Figure 1.3). Let $x_m(k)$ and $y(k)$ be m-sequence from the upper and the lower SRS with the primitive polynomials of $X^{25} + X^3 + 1$ and $X^{25} + X^3 + X^2 + X + 1$, respectively, where the initial conditions are

$$x_m(0) = m_0, \dots, x_m(23) = m_{23}, x_m(24) = 1, m_i \in \{0,1\} \quad (1)$$

and

$$\mathrm{y}(0) = \mathrm{y}(1) = \cdots = \mathrm{y}(24) = 1. \quad (2)$$

Then, two real-valued sequences $c_{1,m}(k)$ and $c_{2,m}(k)$ are represented by

$$c_{1,m}(k) = Z_m(k) \tag{3}$$

and

$$c_{2,m}(k) = Z_m((k + 16777232) mod (2^{25} - 1)) \tag{4}$$

where $Z_m(k) = 1 - 2(x_m(k) \oplus y(k))$ and $k = 0, \dots, 2^{25} - 2$. Finally, the scrambling code $sc_m(k)$ is obtained from (3) and (4) as

$$sc_m(k) = c_{1,m}(k)\left(1 + j(-1)^k c_{2,m}\left(2\left\lfloor\frac{k}{2}\right\rfloor\right)\right). \tag{5}$$

1.3 Generation of the WCDMA message

The process for the generation of the WCDMA message consists of spreading and scrambling operation. The spreading operation is used to control data rate in uplink. After that, the scrambling is performed for dividing users in uplink.

1.3.1 Spreading operation

An uplink WCDMA message consists of DPDCHs and a DPCCH. Each of the physical channels undergoes spreading process to increase the bandwidth of the signal defined by a channelization code. In this thesis, for brevity, only one DPDCH transmission scenario is considered, and the spread signals for DPDCH and DPCCH are

$$DPDCH_S(k) = DPDCH_1(k/SF)\mathrm{Ch}_{dpdch}(k) \tag{6}$$

and

$$DPCCH_S(k) = DPCCH(k/256)\mathrm{Ch}_{dpcch}(k),\ k = 0, \dots, 38399, \tag{7}$$

respectively, where $\mathrm{Ch}_{dpdch}(k) = [C_{SF,SF/4}, C_{SF,SF/4} \dots, C_{SF,SF/4}]_{1\times 38400}$ and $\mathrm{Ch}_{dpcch}(k) = [C_{256,0}, C_{256,0} \dots, C_{256,0}]_{1\times 38400}$. After the spreading operation, the spread

DPDCHs and DPCCH are weighted by β_d and β_c, respectively. Next, the weighted signals are multiplexed into I-path and Q-path.

1.3.2 Scrambling operation

After spreading operation, the multiplexed signal is scrambled by a predefined scrambling code (see Figure 1.3). Then, the transmitted signal is represented by

$$T(k) = sc_m(k)\big(\beta_d DPDCH_S(k) + j\beta_c DPCCH_S(k)\big). \quad (8)$$

where $k = 0,1,\dots,38399$. The scrambling operation does not change the bandwidth of signal, but divide users in uplink.

1.4 Lemmas

Before discussion the following lemmas are introduced for further explanation.

Lemma 1.1. (*Property of m-sequence*) [4]

$$m(k+\tau_1) = m(k+\tau_2) \oplus m(k+\tau_3) \quad (6)$$

and

$$m(2k) = m(k+\tau_4) \quad (7)$$

where $\oplus$ is the exclusive or, $m(k)$ is the m-sequence, and τ_1, τ_2, τ_3, and τ_4 are the unique delays. In other words, the decimated m-sequence and the m-sequence adding differently shifted versions are also the m-sequence with different time offset.

Lemma 1.2. (*Property of channelization and scrambling code*) [2]

Note that $DPDCH_S(k)$, $DPCCH_S(k)$, and $sc_m(k)$ satisfy the following properties as

$$DPDCH_S(2k+1)DPDCH_S(2k) = 1, \quad (8)$$

$$DPCCH_S(2k+1)DPCCH_S(2k) = 1, \quad (9)$$

$$DPCCH_S(2k+1)DPDCH_S(2k) = DPDCH_S(2k+1)DPCCH_S(2k), \quad (10)$$

and

$$sc_m(2k+1)sc_m^*(2k) = -2j\tilde{X}(k)\tilde{Y}(k) \quad (11)$$

where $\tilde{X}(k) = 1 - 2\tilde{x}(k)$ and $\tilde{Y}(k) = 1 - 2(y(2k) \oplus y(2k+1) \oplus y(2k+4) \oplus y(2k+6) \oplus y(2k+17))$.

II. CONVENTIONAL UPLINK SCRAMBLING CODE IDENTIFICATION METHOD

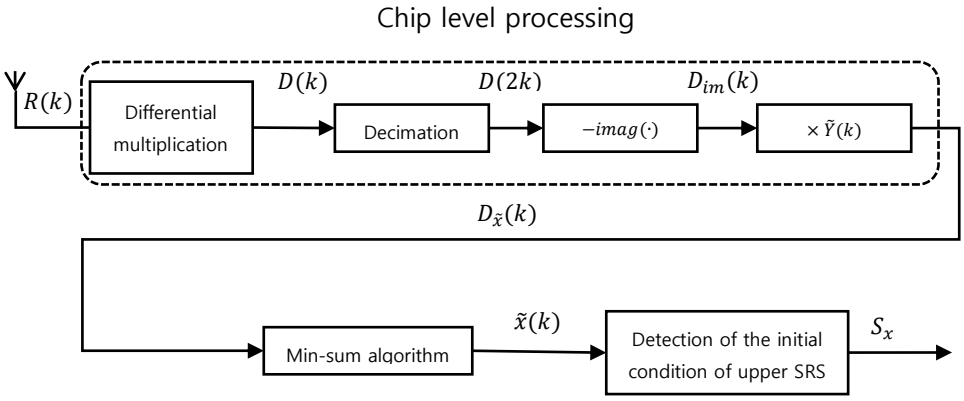

Figure 2.1 Overall process of scrambling code identification

In this chapter, the conventional uplink scrambling code identification process with a single antenna is discussed, where the overall process is illustrated in Figure 2.1. The received signal is represented as

$$R(k) = sc_m(k)\left(\beta_d DPDCH_S(k) + j\beta_c DPCCH_S(k)\right) + n(k) \quad (12)$$

where $n(k)$ is the circular symmetric complex random noise that follows the complex Gaussian distribution $\mathcal{CN}(0, \sigma_n^2)$.

2.1 Chip level processing

The purpose of chip level processing is to obtain expression for $\tilde{x}(k)$ where

$$\tilde{x}(k) = x_m(2k) \oplus x_m(2k+1) \oplus x_m(2k+4) \oplus x_m(2k+7) \oplus x_m(2k+18). \quad (13)$$

From Lemma 1.1, it is clear that $\tilde{x}(k)$ is the shifted version of the m-sequence from the upper SRS. After the antenna receives the signal, the differential multiplication is performed as

$$D(k) = R^*(k)R(k+1) = P(k) + I(k) \tag{14}$$

where

$$P(k) = sc_m(k+1)sc_m^*(k)$$
$$\times \{\beta_d^2 DPDCH_S(k+1)DPDCH_S(k) + \beta_c^2 DPCCH_S(k+1)DPCCH_S(k) + j\beta_c\beta_d$$
$$\times \big(DPCCH_S(k+1)DPDCH_S(k) - DPDCH_S(k+1)DPCCH_S(k)\big)\} \tag{15}$$

is the signal term and

$$I(k) = sc_m(k+1)\big(\beta_d DPDCH_S(k+1) + j\beta_c DPCCH_S(k+1)\big) \times n^*(k)$$
$$+sc_m^*(k)\big(\beta_d DPDCH_S(k) - j\beta_c DPCCH_S(k)\big) \times n(k+1) \tag{16}$$

is the interference term. Then $D(k)$ is decimated as

$$D(2k) = P(2k) + I(2k)$$
$$= sc_m(2k+1)sc_m^*(2k)\{\beta_d^2 DPDCH_S(2k+1)DPDCH_S(2k)$$
$$+\beta_c^2 DPCCH_S(2k+1)DPCCH_S(2k)$$
$$+j\beta_c\beta_d\big(DPCCH_S(2k+1)DPDCH_S(2k) - DPDCH_S(2k+1)DPCCH_S(2k)\big)\}. \tag{17}$$

From Lemma 2, (17) can be rewritten as

$$D(2k) = -2j(\beta_d^2 + \beta_c^2)\tilde{X}(k)\tilde{Y}(k) + I(2k) \tag{18}$$

where $\tilde{X}(k) = 1 - 2\tilde{x}(k)$ and $\tilde{Y}(k) = 1 - 2(y(2k) \oplus y(2k+1) \oplus y(2k+4) \oplus y(2k+6) \oplus y(2k+17))$. After that, the output $D_{\tilde{X}}(k)$ of the chip level processing is obtained by exploiting the imaginary part of $D(2k)$, that is, the negative value of the imaginary part of $D(2k)$ is

$$D_{im}(k) = -imag\big(D(2k)\big) = 2(\beta_d^2 + \beta_c^2)\tilde{X}(k)\tilde{Y}(k) - imag\big(I(2k)\big). \tag{19}$$

Then, since $\tilde{Y}(k) \times \tilde{Y}(k) = 1$, the input vector of min-sum algorithm $D_{\tilde{X}}(k)$ is computed by using $D_{im}(k)$ and $\tilde{Y}(k)$ as

$$D_{\tilde{X}}(k) = D_{im}(k)\tilde{Y}(k) = 2(\beta_d^2 + \beta_c^2)\tilde{X}(k) - imag(I(2k))\tilde{Y}(k) \tag{20}$$

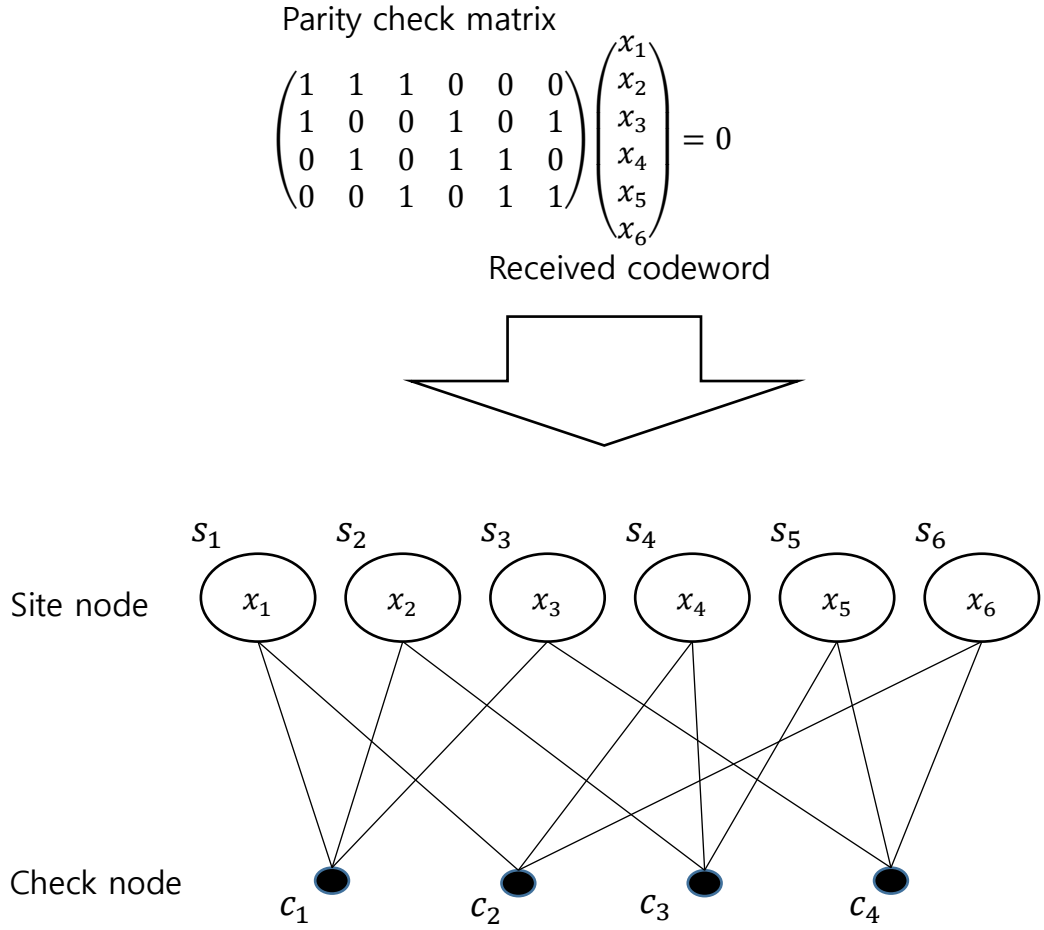

Figure 2.2 One example of Tanner graph generation

where $k = 0,1, \dots, M-1$ and M is the length of the input vector of the min-sum algorithm.

Since the detection performance is degraded due to the interference term $imag(I(2k))\tilde{Y}(k)$ in (20), once $D_{\tilde{X}}(k)$ is obtained, the min-sum scheme is employed for reliable identification. To this end, the detailed discussion of detecting $\tilde{X}(k)$ will be provided in the following.

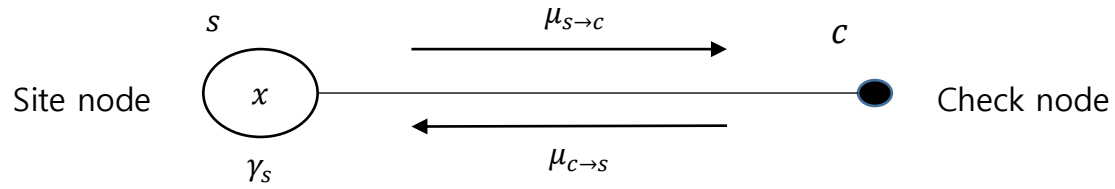

Figure 2.3 Local and intermediate cost functions

2.2 Min-sum algorithm

In this subchapter, min-sum algorithm is discussed which is the generalization of well-known decoding algorithms such as the Viterbi algorithm and consists of initialization, iteration, and termination [5]. First, the Tanner graph corresponding to the parity check matrix for $\tilde{x}(k)$ has to be decided. Since $\tilde{x}(k)$ is the shifted version of x_m, the parity check matrix can be decided by the primitive polynomial of the upper SRS in Figure 1.3 as

$$g_{x_m}(D) = X^{25} + X^3 + 1. \tag{21}$$

Then, the parity check matrix can be easily determined by using (21) as

$$H_0 = \begin{pmatrix} H_{temp} & 0 & \cdots & 0 \\ 0 & H_{temp} & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & H_{temp} \end{pmatrix}_{(M-25)\times M} . \tag{22}$$

where $H_{temp} = (1\ 0\ 0\ 1\ 0\ 0\ \cdots 0\ 0\ 1)_{1\times 25}$ is the binary representation of $g_{x_m}(D)$. The Tanner graph can be also determined corresponding to (22) (see Figure 2.2). The parameter terms used in Tanner graph are defined as follows (see Figure 2.3): 1) there is one local cost function for each site denoted by $\gamma_{s_k}(X)$, and 2) for each pair for site and check nodes, there is one site-to-check intermediate cost function $\mu_{s\to c}$ and check-to-site intermediate cost function $\mu_{c\to s}$. In this algorithm, $\gamma_{s_k}(X)$ is used to compute final cost function μ_{s_k} on which the final decisions are based.

2.2.1 Initialization

In the initialization step, I have to define the local cost functions $\gamma_{s_k}(X)$ to each side node as

$$-\log P\left(D_{\tilde{X}}(k)\middle|\tilde{X}\right), k = 0,1,\dots,M-1 \tag{23}$$

where $\tilde{X} = \pm 1$. Furthermore, every intermediate cost function $\mu_{s\to c}$ and $\mu_{c\to s}$ are initially set to zero.

2.2.2 Iteration

After the initialization of $\gamma_{s_k}(\tilde{X})$, $\mu_{s\to c}$, and $\mu_{c\to s}$, the iteration process is performed. Note that $\mu_{s\to c}$ is updated as the sum of the site's local cost and all contributions coming into s except the one from c, that is,

$$\mu_{s\to c}(\tilde{X}) = \gamma_s(\tilde{X}) + \sum_{s\in c':c'\neq c}\mu_{c'\to s}(\tilde{X}) \; where \; \tilde{X} = 1 \; or \; -1. \tag{24}$$

And $\mu_{c\to s}$ is also obtained by examining all locally valid configurations on s' that match $\tilde{X} = \prod_{s'\in c:s'\neq s}(x_{s'})$ on the site s, by summing all contributions coming into c except the one from s. Then $\mu_{c\to s}$ is obtained by minimizing the summation of $\mu_{s'\to c}$ as

$$\mu_{c\to s}(\tilde{X}) = \min_{\tilde{X}=\prod_{s'\in c:s'\neq s}(x_{s'})}\left(\sum_{s'\in c:s'\neq s}\mu_{s'\to c}(x_{s'})\right). \tag{25}$$

2.2.3 Termination

After sufficient number of iterations, the final cost functions $\mu_{s_k}(\tilde{X})$ are updated as

$$\mu_{s_k}(\tilde{X}) = \gamma_{s_k}(\tilde{X}) + \sum_{s_k\in c'}\mu_{c'\to s_k}(\tilde{X}). \tag{26}$$

By comparing $\mu_{s_k}(\tilde{X}=1)$ with $\mu_{s_k}(\tilde{X}=-1)$, the *k*-th codeword for each site can be determined as

$$D_{\tilde{X}}(k) = \begin{cases} -1, & \mu_{s_k}(1) > \mu_{s_k}(-1) \\ 1, & \mu_{s_k}(1) \leq \mu_{s_k}(-1) \end{cases}. \tag{27}$$

Then, the parity check is performed using the modified codeword and parity check matrix. If the parity check is successful, it is directly delivered to the following detection stage. Otherwise, the iteration stage is repeated until the parity check is successfully performed with the updated local cost functions

$$\gamma_{s_k}(\tilde{X}) = \mu_{s_k}(\tilde{X}) \tag{28}$$

or it meets the maximum number of iterations.

Using (21), one can employ the redundancy model to improve the performance of the min-sum algorithm [6]. That is, different primitive polynomials can be used to generate the same sequence.

$$(g_{x_m}(D))^{2^j} = X^{25\cdot 2^j} + X^{3\cdot 2^j} + 1 \tag{29}$$

where j is a nonnegative integer. In this regard, H_n is defined as the parity check matrix generated from $(g_{x_m}(D))^{2^n}$ with n redundancies as

$$H_{redun} = \begin{pmatrix} H_0 \\ H_1 \\ \vdots \\ H_n \end{pmatrix}. \tag{30}$$

Using (30) as parity check matrix in min-sum algorithm, the performance of min-sum algorithm can be improved.

2.3 Scrambling code identification

In this stage, I determine the initial condition of $x_m(k)$ by using $\tilde{x}(k)$ extracted by min-sum algorithm. First, $\tilde{x}_{decim}(2k)$ is defined as

$$\tilde{x}(k) = \tilde{x}_{decim}(2k) \tag{31}$$

where

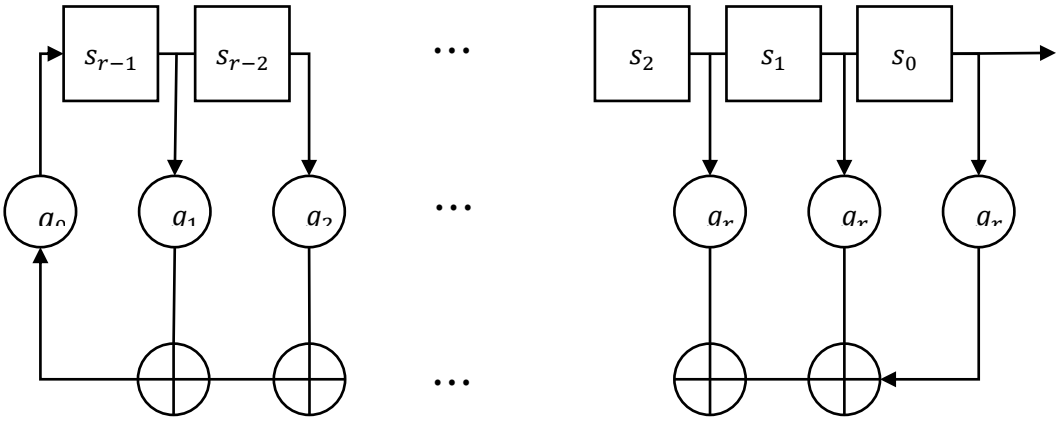

Figure 2.4 Fibonacci feedback generator

$$\tilde{x}_{decim}(k) = x_m(k) \oplus x_m(k+1) \oplus x_m(k+4) \oplus x_m(k+7) \oplus x_m(k+18). \quad (32)$$

Next, $S_{\tilde{x}}$ and $S_{\tilde{x}_{decim}}$ are defined as

$$S_{\tilde{x}} = [\tilde{x}(0), \tilde{x}(1), \dots, \tilde{x}(24)]^T, \quad (33)$$

and

$$S_{\tilde{x}_{decim}} = [\tilde{x}_{decim}(0), \tilde{x}_{decim}(1), \tilde{x}_{decim}(2) \dots, \tilde{x}_{decim}(24)]^T, \quad (34)$$

respectively, which satisfy

$$S_{\tilde{x}_{decim}} = TS_{\tilde{x}} \quad (35)$$

where T is the transition matrix [7]. The process for obtaining T is as follows. Let A be an m-sequence and A_o by the sampled m-sequence by sampling every o-th chip of A. In addition, denote A_p and $A_{o,p}$ by pth chip of and A and A_o, respectively. Then the below equation is established.

$$A_0 = A_{o,0},$$

$$A_1 = A_{o,p},$$

$$A_2 = A_{o,2p},$$

$$\vdots$$

$$A_n = A_{o,vp} \tag{36}$$

where $op = 1\ (mod\ 2^r - 1)$ and r is the number of shift register. Let α be root of the generator polynomial $g(X)$, then α^{-p} is

$$\alpha^{-p} = \sum_{u=0}^{r-1} g_{p,u}\, \alpha^{-u} \tag{37}$$

where $g_{p,u} \in \{0,1\}$, and $A_{o,p}$ is

$$A_{o,p} = \sum_{u=0}^{r-1} g_{p,u} A_{o,u}. \tag{38}$$

Finally, by defining T_{tmp} as an $r \times r$ matrix of where the u-th row of the matrix consists of the coefficients of α^{-up} $(0 \le u \le r-1)$, the relationship between A^r and A_k^r can be expressed as

$$A^r = T_{tmp} A_k^r. \tag{39}$$

By setting $p = 2$ and $k = 2^{r-1}$, T is represented by

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}_{25\times 25} \tag{40}$$

Using (32) to obtain $x_m(k)$, I can define the transition matrix P as [8]. That is, Fibonacci feedback generator (see Figure 2.4) is considered with the parameter S_n

$$S_e = \begin{pmatrix} s_{0,e} \\ s_{1,e} \\ s_{2,e} \\ \vdots \\ s_{r-2,e} \\ s_{r-1,e} \end{pmatrix}_{r\times 1}, \tag{41}$$

where $s_{r-1,e}$ is the $(r-1)$th content in shift register sequence at time index e. Then, the contents at time $e+1$ are

$$s_{0,e+1} = (0 \quad 1 \quad 0 \quad 0 \quad \cdots \quad 0)\begin{pmatrix} s_{0,e} \\ s_{1,e} \\ s_{2,e} \\ \vdots \\ s_{r-2,e} \\ s_{r-1,e} \end{pmatrix} = s_{1,e},$$

$$s_{1,e+1} = (0 \quad 0 \quad 1 \quad 0 \quad \cdots \quad 0)\begin{pmatrix} s_{0,e} \\ s_{1,e} \\ s_{2,e} \\ \vdots \\ s_{r-2,e} \\ s_{r-1,e} \end{pmatrix} = s_{2,e},$$

$$s_{2,e+1} = (0 \quad 0 \quad 0 \quad 1 \quad \cdots \quad 0)\begin{pmatrix} s_{0,e} \\ s_{1,e} \\ s_{2,e} \\ \vdots \\ s_{r-2,e} \\ s_{r-1,e} \end{pmatrix} = s_{3,e},$$

$$s_{2,e+1} = (g_r \quad g_{r-1} \quad g_{r-2} \quad g_{r-4} \quad \cdots \quad g_1)\begin{pmatrix} s_{0,e} \\ s_{1,e} \\ s_{2,e} \\ \vdots \\ s_{r-2,e} \\ s_{r-1,e} \end{pmatrix}$$

$$= g_r s_{0,e} + g_{r-1} s_{1,e} + g_{r-1} s_{1,e} +, \dots, + g_1 s_{r-1,e}. \tag{42}$$

Using (32) and (42), P is then obtained as

$$P = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & 0 & \vdots & \dots & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & \dots & 0 \end{pmatrix}_{25\times 25}. \tag{43}$$

Finally, I can obtain the initial condition S_x of upper SRS as

$$S_x = (I + P + P^4 + P^7 + P^{18})^{-1} S_{\tilde{x}_{decim}}. \tag{44}$$

III.UPLINK SCRAMBLING CODE IDENTIFICATION USING NCC

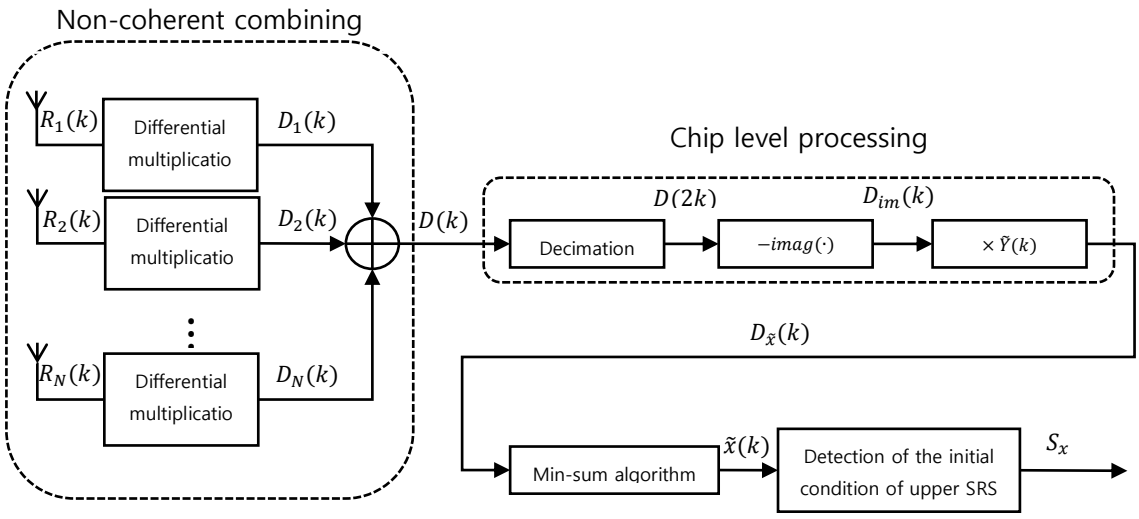

Figure 3.1 Overall process of scrambling code identification using non-coherent combining

In this chapter, I provide the uplink scrambling code identification process, where the overall process is illustrated in Figure 3.1. Since the chip-level processing and scrambling code identification are identical to the procedures in the previous chapter, we only discuss NCC and min-sum algorithm in this chapter.

3.1 Non-coherent combining

The received signal in each antenna is represented as

$$R_i(k) = h_i sc_m(k)\left(\beta_d DPDCH_S(k) + j\beta_c DPCCH_S(k)\right) + n_i(k) \quad (45)$$

where $1 \le i \le N$, N is the number of antennas, and h_i and $n_i(k)$ are the Rayleigh slow fading channel and the circular symmetric complex random noise with $\mathcal{CN}(0, \sigma_n^2)$ for i-th antenna, respectively. After each antenna receives the signal, the differential multiplication is performed as

$$D_i(k) = R_i^*(k)R_i(k+1) = |h_i|^2 P(k) + I_i(k) \tag{46}$$

where $P(k)$ is the signal term and $I_i(k)$ is the interference term. Then, it can be combined as

$$D_{NCC}(k) = \sum_{i=1}^{N} D_i(k) = (|h_1|^2 + \cdots + |h_N|^2)P(k) + I_1(k) + I_2(k) + \cdots + I_1(k)$$

$$= (|h_1|^2 + \cdots + |h_N|^2)P(k) + I_{NCC}(k) \tag{47}$$

where $I_{NCC}(k) = \sum_{i=1}^{N} I_i(k)$. Note that from (47), one can notice that the signal combining does not require any channel estimation procedure since $D_i(k)$'s are directly accumulated.

3.2 Chip-level processing

Similar to the chip-level processing with single antenna scenario, the input vector $D_{\tilde{X}}(k)$ of min-sum algorithm of chip level processing is represented by

$$D_{\tilde{X}}(k) = 2(|h_1|^2 + \cdots + |h_N|^2)(\beta_d^2 + \beta_c^2)\tilde{X}(k) - imag(I_{NCC}(2k))\tilde{Y}(k) \tag{48}$$

where $k = 0,1,\ldots,M-1$ and M is the length of the input vector of the min-sum algorithm. When comparing (48) to (20), the desired term $2(\beta_d^2 + \beta_c^2)\tilde{X}(k)$ is multiplied by gain $(|h_1|^2 + \cdots + |h_N|^2)$.

3.3 Min-sum algorithm

In this subchapter, I explain the method for obtaining the initial values of each site node. After the chip-level processing with NCC, the min-sum algorithm is similarly applied as in the single antenna scenario. However, from (23) and (48), one can notice that identifying $P(D_{\tilde{X}}(k)|\tilde{X})$ is quite difficult since the channel information $(|h_1|^2 +$

$\cdots + |h_N|^2)$ is not given. Therefore, I numerically observed its distribution by histogram and

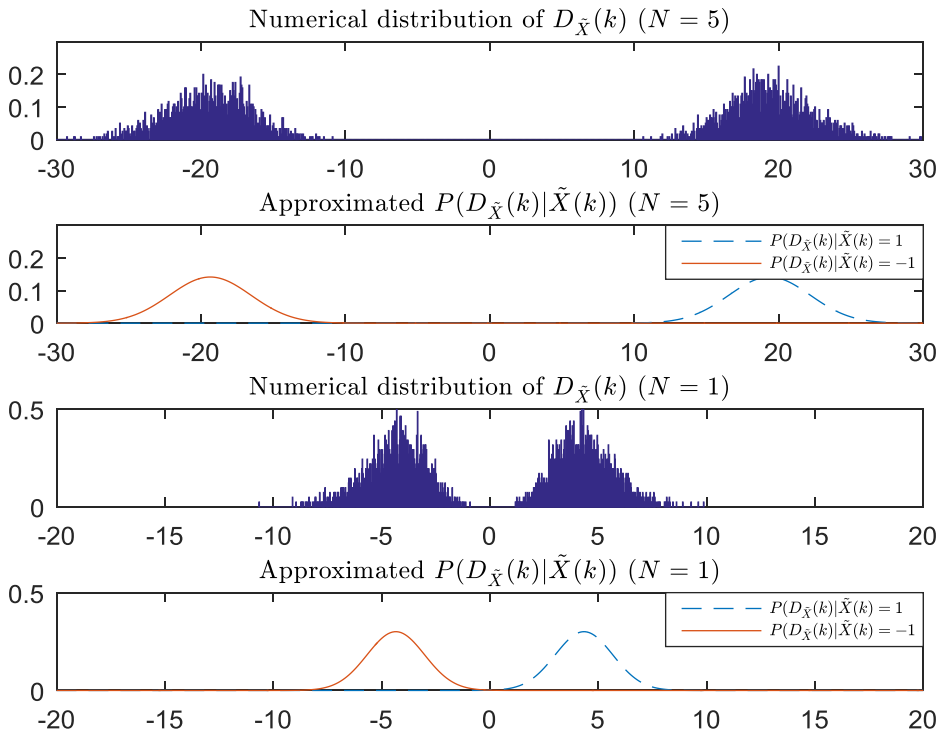

Figure 3.2 Examples of the histogram and its approximated distributions of $D_{\tilde{X}}(k)$ $(N = 1, 5)$

could notice that $P(D_{\tilde{X}}(k)|\tilde{X})$ can be approximated to Gaussian distribution (see Figure 3.2). To this end, I extracted the samples of positive side of histogram of $D_{\tilde{X}}(k)$ to compute the unbiased estimated sample mean and the variance as

$$\hat{\mu}_{ms} = \frac{1}{q}\sum_{k=1}^{q} D_k$$

and

$$\hat{\sigma}_{ms} = \frac{1}{q-1}\sum_{k=1}^{q} (D_k - \hat{\mu}_{ms})^2,$$

respectively, where D_k are samples of the positive side of $D_{\tilde{X}}(k)$ and q is the number of samples in the positive side. Then, (23) can be roughly approximated as

$$\gamma_{s_k}(\tilde{X}) = -\log\left(\frac{1}{\hat{\sigma}_{ms}\sqrt{2\pi}}\exp\left(\frac{(D_{\tilde{X}}(k)-\hat{\mu}_{ms}(\tilde{X}))^2}{2\hat{\sigma}_{ms}}\right)\right) \quad (49)$$

where $k = 0,1,\ldots,M-1$, $\hat{\mu}_{ms}(1) = \hat{\mu}_{ms}$, and $\hat{\mu}_{ms}(-1) = -\hat{\mu}_{ms}$. With such approximation, the min-sum algorithm is performed identically to that of the conventional scrambling code identification method.

IV. Eavesdropping the WCDMA messages

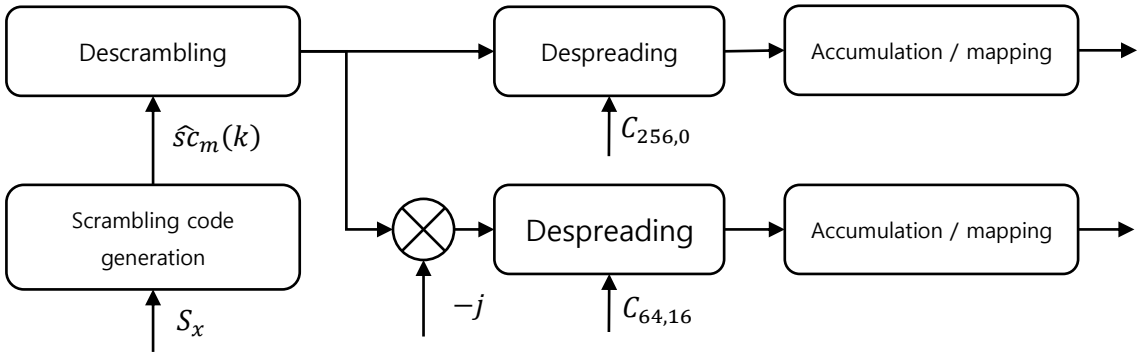

Figure 4.1 Process for eavesdropping WCDMA messages

Using the scrambling code identified by the procedures in the previous chapters, one can achieve WCDMA message eavesdropping by following the structure shown in Figure 4.1. To be specific, this process consists of scrambling code generation, descrambling, despreading, accumulation, and bit detection.

Using obtained scrambling code $\widehat{sc}_m(k)$, descrambling operation is represented by

$$R_{dsc}(k) = \frac{1}{2}\widehat{sc}_m^*(k)R(k) = \frac{1}{2}\widehat{sc}_m^*(k)sc_m(k)\left(\beta_d DPDCH_S(k) + j\beta_c DPCCH_S(k)\right) \quad (50)$$

where $R(k)$ is the received signal[1]. If $\widehat{sc}_m(k) = sc_m(k)$, $R_{dsc}(k)$ can be rewritten as

$$R_{dsc}(k) = \beta_d DPDCH_S(k) + j\beta_c DPCCH_S(k). \quad (51)$$

After that, using the channelization codes $C_{64,16}$ and $C_{256,0}$ for DPDCH and DPCCH respectively, despreading operation is performed as

$$R_{dsp\_dpdch}(k) = R_{dsc}(k)Ch_{dpdch}(k) \quad (52)$$

and

$$R_{dsp\_dpcch}(k) = -jR_{dsc}(k)Ch_{dpcch}(k) \quad (53)$$

[1] For brevity, the channel information and AWGN terms are omitted.

where $R_{dsp\_dpdch}(k)$ and $R_{dsp\_dpcch}(k)$ are the despread DPDCH and DPCCH, respectively, $Ch_{dpdch}(k) = [C_{64,16}, C_{64,16} \dots, C_{64,16}]_{1\times 38400}$, and $Ch_{dpcch}(k) = [C_{256,0}, C_{256,0} \dots, C_{256,0}]_{1\times 38400}$.

Next, the accumulation stage converts the chip-unit signal into the bit-unit signal. Because SF for DPDCH is 64, the accumulation term is

$$\mathrm{DPDCH}_{tmp}(n) = \sum_{i=0}^{63} R_{dsp\_dpdch}(64n + k), n = 0, \dots, 599. \quad (54)$$

Similarly, since SF for DPCCH is 256, the accumulation term is

$$\mathrm{DPCCH}_{tmp}(n) = \sum_{i=0}^{255} R_{dsp\_dpcch}(256n + k), n = 0, \dots, 149. \quad (55)$$

Finally, the bit detection stage detects the positive values to $+1$ and the negative values to -1. That is, the mapping operation for DPDCH and DPCCH are

$$\widehat{\mathrm{DPDCH}}_1(n) = sign(\mathrm{DPDCH}_{tmp}(n))$$

and

$$\widehat{\mathrm{DPCCH}}_1(n) = sign\left(\mathrm{DPCCH}_{tmp}(n)\right), \quad (56)$$

respectively, where $sign(\cdot)$ is the signum function [11].

V. SIMULATION RESULTS & PERFORMANCE ANALYSIS

In this chapter, numerical simulation results are provided for different parameters such as the number w of redundancies and the number of antennas N, and the appropriate parameters for proper operation in practical SNR ranges. In the simulation, the SNR is defined as E_c/N_0 where E_c is the energy associated with each chip and N_0 is the noise spectral density. In addition, the performance of NCC is compared with the optimal MRC assuming perfect CSI at the receiver, since such MRC provides the optimal performance. I use the detecting failure probability P_E as a performance metric, that is,

$$P_E = P(\tilde{S}_x \neq S_x). \tag{49}$$

The communication system is assumed as the speech service of 12.2 kbps with $SF = 64$, $\beta_d = 11/15$, $\beta_c = 1$, and $M = 4{,}000$ [9]. And the maximum number of iterations for the min-sum algorithm is 20.

5.1 Error rate evaluation for slow and fast fading channels

I assume the Rayleigh slow fading channel as a quasi-static channel during 10ms per frame, and the Rayleigh fast fading channel as dynamic time varying channel during 10ms are assumed. To be specific, the Rayleigh fading channel is characterized by

$$h(k+1) = \alpha h(k) + \sqrt{1-\alpha^2}w(k) \tag{50}$$

where $w(k) = \left(1/\sqrt{2}\right)\left(X(k) + jY(k)\right), X(k), Y(k) \sim N(0,1)$ and $k = 0, \ldots, 38399$. Note that since the smaller the value of α is, the faster the channel variation is, and thus the slow and fast fading channels are assumed by h with $\alpha = 1$ and $\alpha = 0.9$, respectively.

As shown in Figure 5.1 and Figure 5.2, one can observe that as the number of antennas increases, the performance becomes better. For example, when using two antennas rather

than using only one antenna, around 5dB gain in E_c/N_0 can be achieved at error rate of $P_E = 10^{-1}$ (see Figure 5.1 and 5.2). On the other hand, when $N = 15$, one can notice that around 1.5dB gain is obtained compared to $N = 10$ scenario. In addition, as provided in Figure 5.3, one can also find that when $n = 6$, very small gain in E_c/N_0 is achieved over that of $n = 4$. Therefore, in order to achieve near-optimal performance, $N = 15$ and $n = 6$ might be a wise choice for $E_c/N_0 = -12dB$ at $P_E = 10^{-1}$. It is worthwhile noting that WCDMA 12.2kbps speech messages should be successfully decodable at E_c/N_0 of -17dB at the lowest at the base station (BS) in AWGN channels [9] and some margins are necessary for fading channels. Simulation results show that the proposed method can operate around E_c/N_0 of -12dB in Rayleigh fading channels. Therefore, one can expect that the proposed method is suitable for the practical environments.

5.2 Comparison of NCC and MRC

Next, the performance of NCC is compared to MRC, which provides the optimal detection performance due to the genie-aided setup. MRC method provides weight vectors defined as $h_i/||\mathbf{h}||_2$ to receive antennas and combine them for further process [10], where the rest of the detection procedure is identical to NCC.

As observed in Figure 5.4, NCC and MRC perform similarly in single antenna scenario. On the other hand, the performance gap between NCC and MRC increases with the number of antennas. This is because after the differential multiplication, the signal term $P(k)$ of NCC and MRC is the same but the interference terms $I_{NCC}(k)$ and $I_{MRC}(k)$ are different. To be specific, the average power of $I_{NCC}(k)$ and $I_{MRC}(k)$ are represented by

$$\mathrm{E}[|I_{NCC}(\mathrm{k})|^2] = 4(\beta_d^2 + \beta_c^2)(|h_1|^2 + \cdots + |h_N|^2)\sigma_n^2 + N\sigma_n^4 \quad (51)$$

and

$$\mathrm{E}[|I_{MRC}(\mathrm{k})|^2] = 4(\beta_d^2 + \beta_c^2)(|h_1|^2 + \cdots + |h_N|^2)\sigma_n^2 + \sigma_n^4. \quad (52)$$

From (51) and (52), one can notice that the average power of $I_{MRC}(k)$ does not depend on N while the average power of $I_{NCC}(k)$ increases with N. Thus, the performance gap between NCC and MRC increases as N increases. However, there is still significant gain even for large N with the proposed NCC scheme. Nevertheless, the performance gap when exploiting a small number of antennas is quite marginal. Thus, MRC performance is considered as a benchmark lower bound.

In spite of the performance difference between MRC and NCC, NCC is suitable for eavesdropping scenarios due to unknown CSI. Therefore, NCC is more practical method than MRC in eavesdropping scenarios.

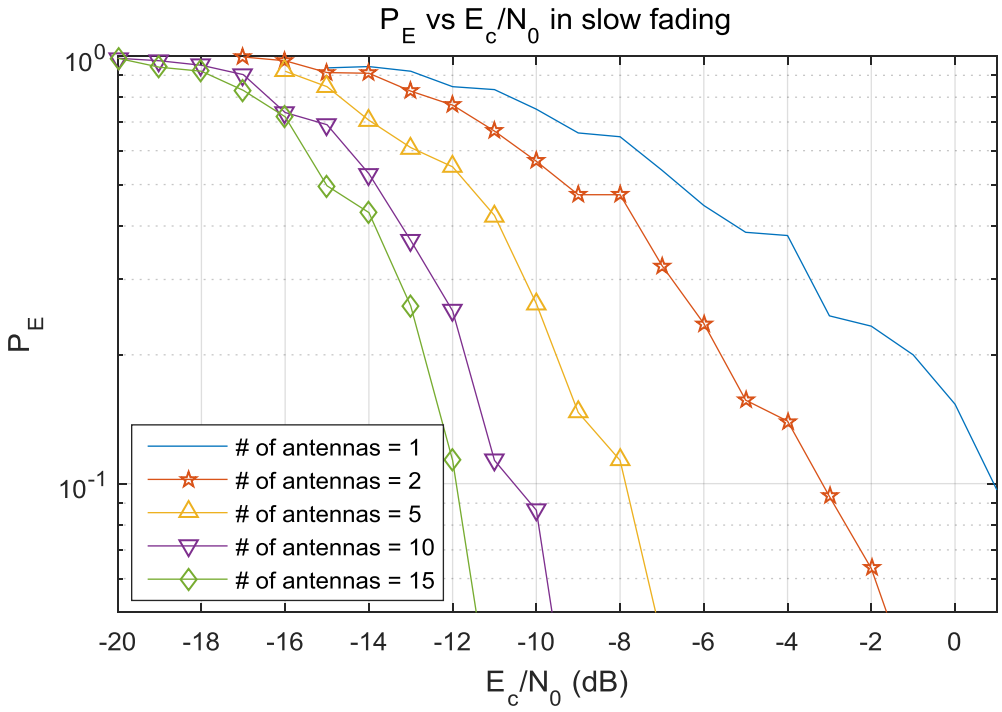

Figure 5.1 Performance of NCC in slow fading channel $(\alpha = 1,\ n = 6)$

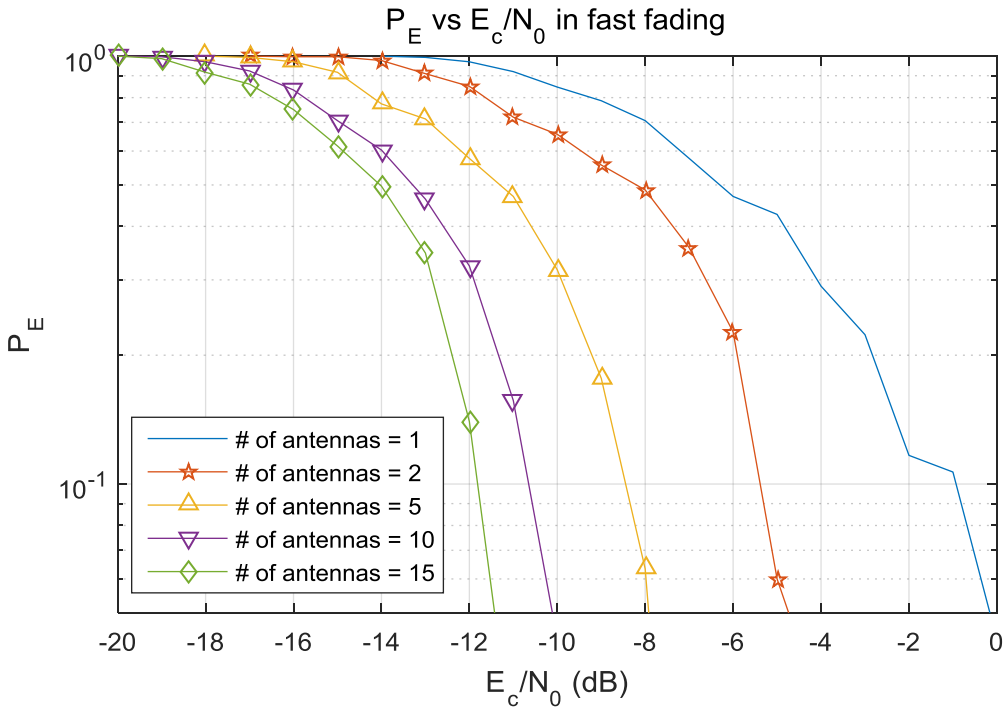

Figure 5.2 Performance of NCC in fast fading channel $(\alpha = 0.9,\ n = 6)$

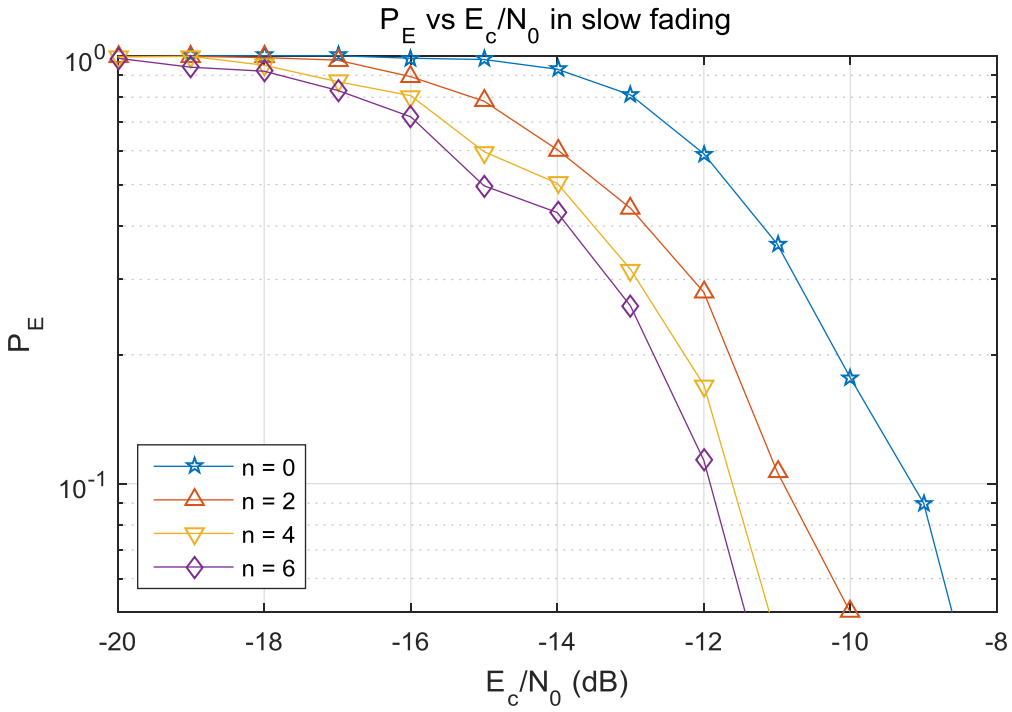

Figure 5.3 Performance for different n ($\alpha = 1,\ N = 15$)

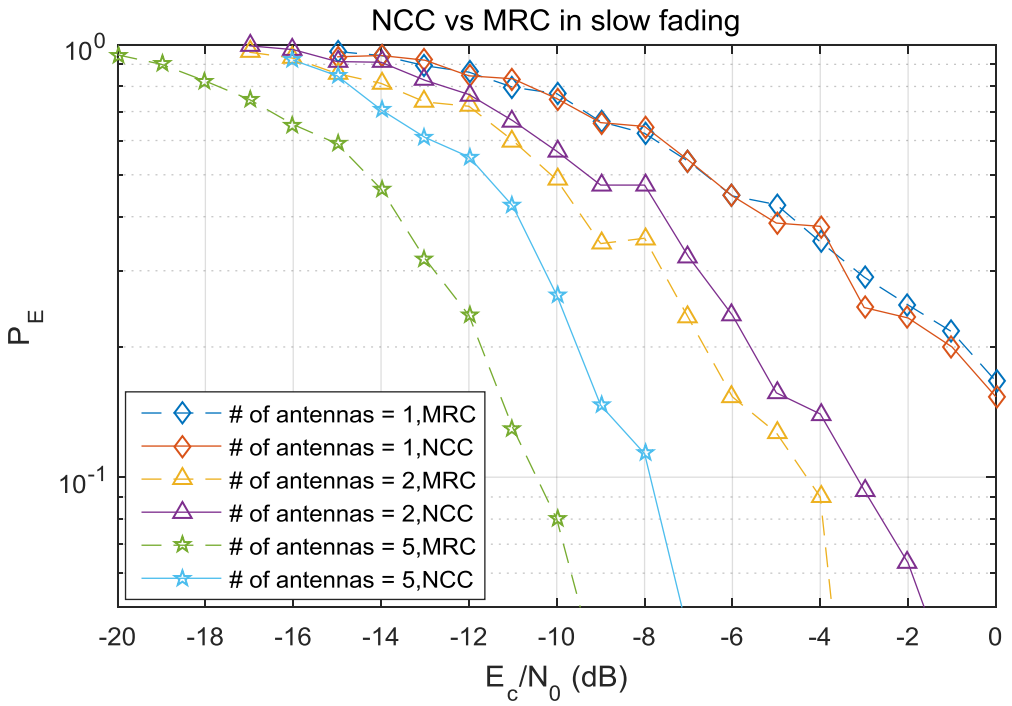

Figure 5.4 Performance comparison of MRC and NCC ($\alpha = 1,\ n = 6$)

VI. CONCLUSION

In this thesis, I improved the performance of identifying the scrambling code in uplink WCDMA systems by using multiple antennas based on NCC. In addition, the numerical simulation results showed that the proposed method achieves substantial gain in SNR than conventional schemes. Furthermore, I also provided a proper parameter selected for achieving effective scrambling code identification in practical environments.

In the second chapter, I have explained the conventional scrambling code identification method. Also, if only one antenna is used, the larger size of parity check matrix is required for obtaining the better detecting performance, which is highly likely to substantially increase the computational burden. In order to prevent such scenario while improving the performance, in the third chapter, the proposed scrambling code identification method named by NCC is proposed in order to obtain significant gain with negligible increment of the computational complexity. Since NCC does not require the channel estimation, it is also suitable for practical eavesdropping scenarios.

In forth chapter, the simulation results for the proposed method have been shown. Also, the system parameters have been provided for obtaining near-optimal performance. When compared with case of only one antenna, near-optimal case of NCC has around 11dB gain. And the proposed method can well operate in extremely fast fading channel.

REFERENCE

[1] Ericsson mobility report, Ercsson, 2016.

[2] M. des Noes, V. Savin, Ros L., and Brossier J.M., "Blind identification of the uplink scrambling code index of a WCDMA transmission and application to femtocell networks," in IEEE International Conference on Communications, Budapest, Hungary, 2013.

[3] TS25.213 v.4.4.0 Spreading and modulation (FDD), 3GPP, 2004.

[4] R.J. McEliece, Finite fields for computer scientists and engineers, Springer, 1987.

[5] N.Wiberg, Codes and decoding on general graphs, Ph.D. dissertation, Linkoping University, Sweden, 1996.

[6] O.W. Yeung and K.M. Chugg, "An iterative algorithm and low complexity hardware architecture for fast acquisition of long PN codes in UWB systems," The Journal of VLSI Signal Processing, vol. 43, no. 1, pp. 2542, 2006.

[7] B. Arazi, "Decimation of m-sequences leading to nay desired phase shift," Electronics Letters, vol. 13, no. 7, pp. 213215, 1977.

[8] R.L. Peterson, R.E. Ziemer, and D.E. Borth, Introduction to spreading spectrum communications, Prentice Hall, 1995.

[9] TS25.104 v.4.9.0 BS Radio Transmission and Reception (FDD), 3GPP, 2007.

[10] Tse, D., and Viswanath, P. Fundamentals of Wireless Communication, Cambridge University Press, 2005.

[11] Sign function. (n.d.). Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Sign_function. Accessed May. 08, 2017.

요 약 문

비동기 다중안테나 결합을 이용한 WCDMA 스크램블링 코드 판별 성능 향상

WCDMA 통신 표준은 과거의 서비스임에도 불구하고 다양한 국가에서 사용중이다. 특히 북한에서는 최근 고위 간부들에게 WCDMA 시스템을 제공하고 있다. 그러므로 WCDMA 메시지를 도청하기 위한 연구가 진행되었다.

상향 링크 WCDMA 메시지를 생성하는 과정은 스프레딩과 스크렘블링 연산을 포함한다. 스프레딩과 스크렘블링 연산은 각각 채널라이제이션 코드와 스크램블링 코드를 사용한다. 상향 링크에서는 유저를 구분하기 위해 유저마다 다른 스크램블링 코드를 사용한다. 그러므로 어떤 특정 유저의 WCDMA 메시지를 도청하기 위해서는 그 유저의 스크램블링 코드를 얻어내는 것이 필수적이다. 그러므로 상향 링크 WCDMA 메시지의 도청을 위해서는 그 메시지의 스크램블링 코드를 추출하는 것이 필수적이다.

기존의 단일 안테나를 사용하여 스크램블링 코드를 추출하는 방식이 있지만, 이는 실제 WCDMA 통신 환경의 신호대잡음비 (signal to noise ratio, SNR)보다 높은 SNR 에서만 동작이 가능하다. 본 논문은 다중 안테나를 사용하여 동작 가능한 SNR 을 낮추는 NCC 기법을 제안한다. NCC 기법은 어떤 채널 추정 없이도 신호들을 결합할 수 있다. 시뮬레이션 결과는 제안된 기법이 약 -12dB 의 잡음전력밀도에 대한 칩에너지 (E_c/N_0)에서 동작하는 것과 슬로우 페이딩 채널뿐만 아니라 페스트 페이딩 채널에서도 잘 동작하는 것을 보여준다.

Acronyms

WCDMA - Wideband code division multiple access

NCC - Non-coherent combining

SNR - Signal-to-noise ratio

DPDCH - Dedicated physical data channel

DPCCH - Dedicated physical control channel

OVSF - Orthogonal variable spreading factor

SF - Spreading factor

MRC - Maximal ratio combining

3GPP - 3 generation partnership project

SRS - Shift register sequence

CSI - Channel state information

AWGN - Additive white Gaussian noise

BS - Base station