

# 직교 주파수 분할 다중화 시스템의 공간 주파수 블록 코딩에서의 부호 반전 채널 스위칭 기법

(Sign Reversal Channel Switching Method for Space-Frequency Block Code in Orthogonal Frequency Division Multiplexing System)

정혁구<sup>1)\*</sup>  
(Hyeok-Koo Jung)

**요약** 이 논문은 직교 주파수 분할 다중화 시스템에 사용하는 공간 주파수 블록 코딩에서의 부호 반전 채널 스위칭 알고리즘을 제안한다. 소스 데이터를 다른 안테나로 보내는 경우에는 수신기는 바뀐 그 채널에 적합하도록 결합 방법을 바꾸어야 한다. 만일 미리 정의된 채널 스위칭 시퀀스를 모르는 수신기라면, 수신한 데이터를 정확하게 복호할 수 없게 된다. 채널 스위칭을 위한 송신 데이터를 바꾸는 경우에는 데이터 심볼들을 공간 주파수 블록 코딩 형식에 맞추어서 바꾸어야 한다. 이 논문에서는 송신 안테나 간의 데이터 심볼들을 바꾸는 것이 아닌 단지 부호 반전 방법을 제안한다. 이 방법을 사용하면 다른 결합 방법을 발생시킴으로써 수신기에서 간단한 암호화로 동작함을 보였다.

**핵심주제어:** 결합, 공간 주파수 블록 코드, 부호 반전, 직교 주파수 분할 다중화, 채널 스위칭

**Abstract** This paper proposes a sign reversal channel switching method in space-frequency block code for orthogonal frequency division multiplexing system. In case of sending source data on other antenna, it is necessary for the receiver to change combining method according to the channel variation. If one does not know the predefined channel switching sequence, it is not possible to decode the received data precisely. In transmit data symbols' exchanges for a channel switching, data symbols are exchanged according to a format of space-frequency block code. In this paper, we proposes a simple sign reversal method except exchanging data symbols between transmit antennas. It is shown that this method occurs another combining method for a simple encryption in the receiver.

**Keywords:** Combining, Space frequency block code, Sign reversal, Orthogonal frequency division multiplexing, Channel switching

---

\* Corresponding Author : junghk@hanbat.ac.kr  
Manuscript received July 27, 2020 / revised September 15,  
2020 / accepted October 05, 2020

1) 한밭대학교 정보통신공학과, 제1저자, 교신저자

## 1. 서론

직교 주파수 분할 다중화 (Orthogonal frequency division multiplexing: OFDM) 시스템은 송수신

안테나 개수가 하나인 환경인 IEEE802.11a 및 다중 송수신 안테나 환경인 IEEE802.11n (Jin 2015, 2017; Huh and Kim, 2015; IEEE SA 802.11 WG, 2009)를 포함하는 실내 무선 랜 응용의 경우에 쓰이고 있고, 직교 주파수 분할 다중화 시스템에 선택적 결합 그리고 최대율 수신 결합 (Maximum ratio combining: MRC)을 하이브리드하게 조합한 기술 (Jeon and Jung, 2006) 등이 송수신 안테나가 하나인 환경에 적용할 수 있도록 개발되어 왔다. 또한 송신기의 송신 블록이 많아지고 있는 환경에서도 수신기 안테나가 증가하면서 발생하는 다이버시티 결합 이득을 목적으로 하는 기술로서 Alamouti의 시공간 블록 코드 (Space-time block code: STBC)이 제안 (Alamouti, 1998) 되었으며, 이러한 방법을 데이터 심볼이 아니라 일정한 개수의 블록으로 묶어서 다루는 직교 주파수 분할 다중화 시스템에 응용하는 연구가 있었으며, 이것을 Al-Dhahir는 송수신 안테나가 하나인 반송파 시스템에서 주파수 영역 등화기를 사용하는 활용 연구결과 (Al-Dhahir, 2001)를 제시하였다.

한편 무선 통신 채널이 전파가 도달하는 거리 내의 모든 기기들에 도달하므로 간단한 무선 수신기만 사용하여도 와이파이 비밀번호를 비롯하여 통신 신호를 획득하고 해독하는 일 (TECHroid INDIA, 2020)이 가능해 짐에 따라, 최근에는 간단한 암호화 알고리즘이 송신기와 수신기가 미리 공유한 시간에 따라 두 개의 직교 주파수 분할 다중화 심볼동안 송신기 신호를 교환하는 방법 (Jung, 2018)이 제안되었다. 그러나 이 방법은 송신기 신호들을 모두 교환해야 하는 단점때문에 보다 간단한 방법으로 특히 부호만을 바꿈으로 채널 스위칭 효과를 볼 수 있는 알고리즘 (Jung, 2020)이 제안되었다. 그런데 이러한 방법은 시간과 공간 2차원에서의 부호 반전 알고리즘을 적용한 것으로서 다른 차원에서의 분할 알고리즘 특히 공간 주파수 블록 코드에서의 실행 방법 및 성능 분석이 연구될 필요가 있다.

본 논문은 공간 및 주파수 환경에서 통신하는 송신 안테나들의 전송 데이터들 간의 채널 스위칭을 함으로써 발생하는 암호화 효과로 일반 수

신기에서는 정상적으로 데이터를 복호하지 못하고 난독화를 일으키는 부호 반전 채널 스위칭 알고리즘을 제안하고자 한다. 보통 공간 주파수 블록 코딩 방법은 두 송신 안테나에 데이터를 송신하는데, 공간 주파수 축상에서 두 개의 안테나에 각각 수신기에서 결합이 가능하여 수신기 이득을 얻을 수 있는 최대율 결합이 가능하도록 설계되어 있는 송신용 데이터를 송신하게 된다. 그런데 송신기에서의 암호화 효과는 송신 안테나 간의 데이터 교환 없이도 단지 송신 안테나의 데이터 부호만 바꾸어도 공간 주파수 블록 코딩에서의 채널 스위칭 효과가 발생한다. 이와 같은 부호 반전 공간 주파수 블록 코딩 알고리즘을 모의 실험하여 그 채널 스위칭 시간 정보를 아는 경우와 모르는 경우를 가정하여 수신기 데이터의 부호 반전된 경우와 부호 반전이 적용되지 않은 경우의 수신기 성능 비교를 모의 실험을 통해 제시하였다.

이 논문의 구성은 2장에서는 종래의 공간 주파수 블록 코딩을 직교 주파수 분할 다중화 시스템에 적용하는 방법에 대하여 설명하고, 3장에서는 제안하는 부호 반전 채널 스위칭 방법을 적용하는 직교 주파수 분할 다중화 시스템에 관하여 설명하고, 4장은 모의 실험결과와 고찰 그리고 5장에서 결론을 제시하였다.

## 2. 공간 주파수 블록 코딩을 적용하는 직교 주파수 분할 다중화 시스템

종래의 방법인 직교 주파수 분할 다중화 시스템에 적용하는 공간 주파수 블록 코딩 알고리즘의 블록도는 Fig. 1에 기술하였다. 공간 주파수 블록 코드는 송신기 다이버시티를 확장시키는 방법으로서 기존의 수신기 다이버시티를 증가시키는 최대율 결합 방법을 적용한 것이다. 이 장에서 설명하는 공간 주파수 블록 코딩 알고리즘은 원래의 송신 데이터와 아울러 원래의 송신 데이터를 공간 주파수 축으로 변형하여 두 개의 송신 안테나에서 송신하는 것이다. 만일 송신기에서 구성하는 두 개의 크기가  $N/2$  인  $S_1$ 과  $S_2$ 는 식

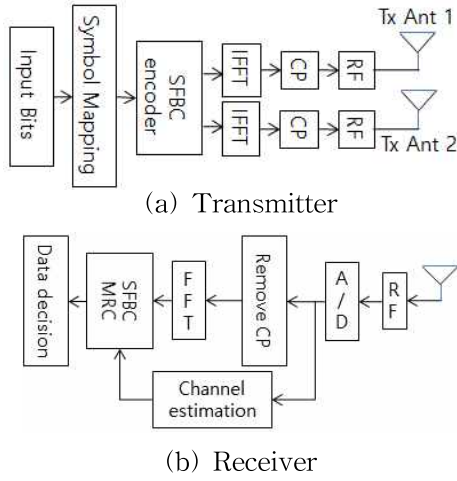


Fig. 1 SFBC OFDM Block Diagram

(1)과 같다고 가정한다,

$$\begin{aligned} \mathbf{S}_1 &= [S_1(0) S_1(1) \dots S_1(N/2-1)]^T \\ \mathbf{S}_2 &= [S_2(0) S_2(1) \dots S_2(N/2-1)]^T \end{aligned} \quad (1)$$

여기서,  $(\cdot)^T$ 는 전치행렬을 의미하며,  $(\cdot)^*$ 는 공액복소수를 의미한다.

공간 주파수 블록 코딩의 데이터 구성에 필요한  $\mathbf{S}_1^*$ 과  $-\mathbf{S}_2^*$ 는 식 (1)을 이용하여 식 (2)와 같이 구성한다.

$$\begin{aligned} \mathbf{S}_1^* &= [S_1^*(0) S_1^*(1) \dots S_1^*(N/2-1)]^T \\ -\mathbf{S}_2^* &= [-S_2^*(0) -S_2^*(1) \dots -S_2^*(N/2-1)]^T \end{aligned} \quad (2)$$

이와 같이 구성한  $\mathbf{S}_1, \mathbf{S}_2, \mathbf{S}_1^*, -\mathbf{S}_2^*$ 들을 이용하여 공간 주파수 블록 코딩 방법에 따라 두 개의 송신 안테나에서 전송할 신호를 구성하면 식 (3)과 같다.

$$\begin{aligned} \mathbf{X}_1 &= [S_1(0) - S_2^*(0) \ S_1(1) - S_2^*(1) \ \dots \\ &\quad S_1(N-2) - S_2^*(N-1)]^T \\ \mathbf{X}_2 &= [S_2(0) \ S_1^*(0) \ S_2(1) \ S_1^*(1) \ \dots \\ &\quad S_2(N-2) \ S_1^*(N-1)]^T \end{aligned} \quad (3)$$

여기서,  $\mathbf{S}_1$ 과  $\mathbf{S}_2$ 의 각 원소는  $\mathbf{X}_1$ 과  $\mathbf{X}_2$ 의 짝

수 인덱스 위치에 있으며,  $\mathbf{X}_1$ 과  $\mathbf{X}_2$ 의 홀수 인덱스 위치의 데이터는 주파수 영역에서 공간 주파수 블록 코딩 알고리즘에서 정한 방법에 의하여 짝수 인덱스 위치의 데이터를 변형하여 만든다.

이와 같이 구성한 공간 주파수 블록 코딩 알고리즘의 하나의 직교 주파수 분할 다중화 블록 안의 하나의 공간 주파수 블록 코딩 그룹의 신호 구성은 식 (4)와 같다.

$$\begin{pmatrix} S_1(n) - S_2^*(n) \\ S_2(n) \ S_1^*(n) \end{pmatrix} \quad (4)$$

여기서, 세로축은 송신 안테나를 의미하며,  $n = 0, 1, \dots, N/2-1$  이다.

이렇게 구성된 공간 주파수 블록 코딩 알고리즘의 송신 신호를 받아서 수신기에서 수신한 신호를 주파수 영역에서 보면 식 (5), (6)과 같다.

$$Y(2m) = S_1(2m)H_1(2m) + \dots + S_2(2m)H_2(2m) + N_1(2m) \quad (5)$$

$$Y(2m+1) = -S_2^*(2m)H_1(2m+1) + \dots + S_1^*(2m)H_2(2m+1) + N_2(2m+1) \quad (6)$$

여기서,  $m = 0, 1, \dots, N/2-1$ 이다.

송신신호는 안테나에서 수신된 신호를 이용하여 식 (7), (8)과 같은 최대율 결합방법을 이용하면 다이버시티 이득이 2배인 송신신호를 얻을 수 있게 된다.

$$S_1(2m) \cong \frac{Y(2m)H_1^*(2m) + Y^*(2m+1)H_2(2m)}{|H_1(2m)|^2 + |H_2(2m)|^2} \quad (7)$$

$$S_2(2m) \cong \frac{Y(2m)H_2^*(2m) - Y^*(2m+1)H_1(2m)}{|H_1(2m)|^2 + |H_2(2m)|^2} \quad (8)$$

여기서,  $m = 0, 1, \dots, N/2-1$ ,

$$H_1(2m) \cong H_1(2m+1), H_2(2m) \cong H_2(2m+1)$$

라고 가정한다.

### 3. 공간 주파수 블록 코딩 시스템을 위한 부호 반전 채널 스위칭 알고리즘

Fig. 2는 제안하는 방법인 직교 주파수 분할 다중화 시스템에 사용할 수 있는 부호 반전 채널 스위칭을 적용하는 공간 주파수 블록 코딩 알고리즘 블록도이다. 제안하는 알고리즘에는 종래의 공간 주파수 블록 코딩 알고리즘과 부호 반전 알고리즘이 병렬로 존재하며, 두 방법 간의 스위칭을 조절하는 시간 제어 블록이 있는 것이 특징이다. 이 논문에서 제안하고자 하는 부호 반전 채널 스위칭 알고리즘을 설명하고자 한다. 먼저 송신기에서 구성하는 두 개의 크기가  $N/2$  인  $\mathbf{S}_1$ 과  $\mathbf{S}_2$ 는 식 (1)과 같다고 가정한다. 종래의 공간 주파수 분할 다중화 방법의  $\mathbf{S}_1$ 과  $\mathbf{S}_2$ 의 각 원소는  $\mathbf{X}_1$ 과  $\mathbf{X}_2$ 의 짝수 인덱스 위치에 있으며,  $\mathbf{X}_1$ 과  $\mathbf{X}_2$ 의 홀수 인덱스 위치의 데이터는 짝수 인덱스 위치의 데이터를 변형하여 식 (2)와 같이 만든다. Fig. 2의 공간 주파수 블록 코딩 부호기에서는 식 (1)의 신호를 입력받아 두 개의 송신 안테나로 전송하기 위한  $\mathbf{X}_1$ 과  $\mathbf{X}_2$ 를 식 (3)과 같이 구

성하게 된다.

Fig. 3에서 부호 반전 채널 스위칭 알고리즘이 동작하는 경우는 시간 제어 블록에서 부호 반전 블록으로 사용자 데이터인 두 개의 크기가  $N/2$  인  $\mathbf{S}_1$ 과  $\mathbf{S}_2$ 를 입력하게 되고 부호 반전이 홀수 인덱스 시간에서 발생한다고 하면, 부호 반전 공간 주파수 블록 코딩 알고리즘의 신호들은 식 (9)와 같이 구성된다.

$$\begin{pmatrix} S_1(n) & S_2^*(n) \\ S_2(n) & -S_1^*(n) \end{pmatrix} \quad (9)$$

따라서 부호 반전으로 구성된 송신 안테나에서의 신호는 식 (10)과 같이 구성된다.

$$\begin{aligned} \mathbf{X}_1 &= [S_1(0) \quad S_2^*(0) \quad S_1(1) \quad S_2^*(1) \cdots \\ &\quad S_1(N-1) \quad S_2^*(N-1)]^T \\ \mathbf{X}_2 &= [S_2(0) - S_1^*(0) \quad S_2(1) - S_1^*(1) \cdots \\ &\quad S_2(N-1) - S_1^*(N-1)]^T \end{aligned} \quad (10)$$

또한 신호의 구성은 홀수 인덱스에서의 부호 반전에 따라 식(9)와 같이 구성되는 것도 있지만, 사용자 데이터  $\mathbf{S}_1$ 과  $\mathbf{S}_2$ 를 같은 안테나로 송신하고 다른 안테나의 신호는  $\mathbf{S}_1$ 과  $\mathbf{S}_2$  데이터를 변형하여 사용한다고 가정하면 식 (11)과 같이 신호 구성을 사용할 수 있다.

[공간 주파수 블록 코드 구성의 다른 예]

$$\begin{pmatrix} S_1(n) & S_2(n) \\ -S_2^*(n) & S_1^*(n) \end{pmatrix} \quad (11)$$

따라서 송신 안테나에서의 신호는 식 (12)와 같이 구성된다.

$$\begin{aligned} \mathbf{X}_1 &= [S_1(0) \quad S_2(0) \quad S_1(1) \quad S_2(1) \cdots \\ &\quad S_1(N-1) \quad S_2(N-1)]^T \\ \mathbf{X}_2 &= [-S_2^*(0) \quad S_1^*(0) - S_2^*(1) \quad S_1^*(1) \cdots \\ &\quad -S_2^*(N-1) - S_1^*(N-1)]^T \end{aligned} \quad (12)$$

이렇게 변형된 공간 주파수 블록 코드의 부호 반전 알고리즘은 두 개의 안테나에서의 홀수 인

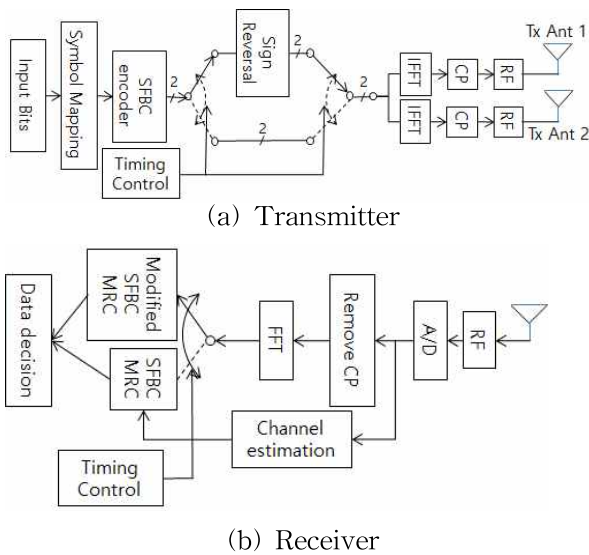


Fig. 2 Sign Reversal Channel Switching SFBC OFDM Block Diagram

텍스에서의 부호 반전이 아니고 식 (13)과 같이 두 번째 안테나의 하나의 데이터 그룹 내에서 인접 주파수 데이터간에 부호 반전을 사용한다.

$$[부호반전 구성] \quad \begin{pmatrix} S_1(n) & S_2(n) \\ S_2^*(n) & -S_1^*(n) \end{pmatrix} \quad (13)$$

따라서 송신 안테나에서의 신호는 식 (14)와 같이 구성된다.

$$\begin{aligned} \mathbf{X}_1 &= [S_1(0) \ S_2(0) S_1(1) \ S_2(1) \dots S_1(N-1) \ S_2(N-1)]^T \\ \mathbf{X}_2 &= [S_2^*(0) - S_1^*(0) S_2^*(1) - S_1^*(1) \dots S_2^*(N-1) - S_1^*(N-1)]^T \end{aligned} \quad (14)$$

한편 공간 주파수 블록 코딩 알고리즘과 부호 반전 알고리즘을 하이브리드하게 스위칭하기 위한 시간 정보를 조정하는 시간 제어 블록의 동작을 설명하면 다음과 같다. 먼저 시간 제어 시퀀스의 동작으로 시간 제어 블록의 신호가 Low 인 경우에는 종래의 공간 주파수 블록 코딩 방법을 사용하고, High 인 경우에는 부호 반전 알고리즘을 사용한다고 가정한다.

$$\begin{array}{l} tx1: \overbrace{S_1(n) - S_2^*(n)} \quad \overbrace{S_1(n) \ S_2^*(n)} \quad \overbrace{S_1(n) - S_2^*(n)} \\ tx2: \overbrace{S_2(n) \ S_1^*(n)} \quad \overbrace{S_2(n) - S_1^*(n)} \quad \overbrace{S_2(n) \ S_1^*(n)} \end{array}$$

- Low : 종래의 공간 주파수 블록 코딩
- High : 부호 반전 공간 주파수 블록 코딩

이러한 시간 제어 시퀀스는 송신기와 수신기가 동시에 적용해야 암호화 효과를 얻을 수 있는데, 직교 주파수 분할 다중화 블록 내에서 각 공간 주파수 블록 코드의 그룹 별로 홀수 그룹은 종래의 공간 주파수 블록 코드로 짝수 그룹은 부호 반전하여 송수신 하는 것으로 가정하는 것도 간단한 시간 제어 시퀀스로 동작할 수 있다. 다소 복잡한 시간 제어 시퀀스로 제안할 수 있는 것으로는 난수 발생기를 사용하여 각 시드 (Seed) 별로 난수를 이용한 시간 제어 시퀀스를 구성하고

시드별 시간 제어 시퀀스를 직교 주파수 분할 다중화 블록내의 공간 주파수 블록 코드의 32 개의 그룹별 동작 (0 또는 1)을 구성할 수 있다. 즉 32 비트의 데이터를 미리 송수신기의 초기 셋업 과정에서 공유하면 일반적인 수신기가 알기 어려운 통신방법으로 구성될 수 있다. 4장 모의실험 및 고찰에서 제안하는 32그룹 중의 하나(또는 다섯 개)에서 오류가 발생한다는 가정은 위의 32 비트 중의 하나(또는 다섯 개)를 몰랐다고 가정하는 경우의 오류이다.

송신기에서 이와 같이 구성되어 전송된 신호들은 푸리에 역변환기를 거쳐서  $\mathbf{x}_1$  과  $\mathbf{x}_2$ 가 되며, 이 신호들에 길이  $L$  인 사이클릭 프리픽스 (Cyclic prefix: CP)를 삽입한 후 두 개의 송신 안테나를 통하여 각각 전송된다. 이때, 인접한 두 개의 주파수에서의 채널은 일정하다고 가정한다. 수신기 안테나에서 수신된 신호는 식 (15)와 같다.

$$\mathbf{y} = \mathbf{x}_1 \otimes \mathbf{h}_1 + \mathbf{x}_2 \otimes \mathbf{h}_2 + \mathbf{n} \quad (15)$$

여기서  $\mathbf{y}$ ,  $\mathbf{x}_1$ ,  $\mathbf{x}_2$ ,  $\mathbf{n}$ 는 길이  $(N+L)$ 의 벡터 신호이며,  $\mathbf{y}$ 는 수신기 안테나에서의 신호이고,  $\mathbf{n}$ 은 백색잡음이며,  $\otimes$ 은 컨벌루션을 의미한다. 또한  $\mathbf{h}_1$ 과  $\mathbf{h}_2$ 는  $(N+L) \times (N+L)$ 순환 행렬이며 첫 번째 칼럼이 채널 임펄스 응답에 '영'이 추가되며, 송신기 1과 2에서 수신기까지의 채널을 말하며, 고유치 분해를 통해  $\mathbf{h}_1 = \mathbf{Q}^H \mathbf{H}_1 \mathbf{Q}$ ,  $\mathbf{h}_2 = \mathbf{Q}^H \mathbf{H}_2 \mathbf{Q}$  (Strang, 1988; Oppenheim and Schaffer, 1989). 여기서  $\mathbf{H}_1$ 과  $\mathbf{H}_2$ 는 대각행렬이며,  $(k, k)$  원소는 각각 채널 임펄스 응답의  $k$ 번째 DFT 계수에 해당한다. 수신기에서는 사이클릭 프리픽스를 제거한 후, 식 (15)의  $\mathbf{y}$ 는 푸리에 변환기를 통해 식 (16)과 같이 주파수 영역 신호  $\mathbf{Y}$ 로 변환된다.

$$\mathbf{Y} = \mathbf{H}_1 \mathbf{X}_1 + \mathbf{H}_2 \mathbf{X}_2 + \mathbf{N} \quad (16)$$

여기서,  $\mathbf{N}$ 은 시간영역 백색잡음  $\mathbf{n}$ 의 주파수 영역 신호를 말한다.

수신기에서의 주파수 영역 신호는 식 (17), (18)과 같다.

$$Y(2m) = S_1(2m)H_1(2m) + S_2(2m)H_2(2m) + N_1(2m) \quad (17)$$

$$Y(2m+1) = S_2^*(2m)H_1(2m+1) - S_1^*(2m)H_2(2m+1) + N_2(2m+1) \quad (18)$$

여기서,  $m = 0, 1, \dots, N/2 - 1$ 이다.

따라서 송신신호는 안테나에서 수신된 신호를 이용하여 식 (17), (18)와 같이 최대율 결합방법을 이용하면 다이버시티 이득이 2배인 송신신호  $S_1(2m)$ ,  $S_2(2m)$ 를 얻을 수 있게 된다.

$$S_1(2m) \cong \frac{Y(2m)H_1^*(2m) - Y^*(2m+1)H_2(2m)}{|H_1(2m)|^2 + |H_2(2m)|^2} \quad (19)$$

$$S_2(2m) \cong \frac{Y(2m)H_2^*(2m) + Y^*(2m+1)H_1(2m)}{|H_1(2m)|^2 + |H_2(2m)|^2} \quad (20)$$

여기서,  $m = 0, 1, \dots, N/2 - 1$ ,

$$H_1(2m) \cong H_1(2m+1), H_2(2m) \cong H_2(2m+1)$$

라고 가정한다.

따라서 종래의 공간 주파수 블록코딩을 사용할 때의 데이터 복호 방법은 식 (7), (8)이며, 부호 반전이 있을 경우의 데이터 복호방법은 식 (19)과 (20)과 같게 된다. 종래의 공간 주파수 블록 코딩과 비교하면, 부호 반전 결합 방법은 채널  $H_1(2m)$ 과  $H_2(2m)$ 가 바뀌었으면서 동시에  $S_1(2m)$ 과  $S_2(2m)$ 가 바뀐 것과 같은 결과가 된다. 한편 종래의 공간 주파수 블록 코드 구성이 식 (11)과 같은 경우에는 주파수 영역 신호 구성과 추정된 송신 신호는 식 (21), (22)와 같이 구성된다.

$$Y(2m) = S_1(2m)H_1(2m) + S_2^*(2m)H_2(2m) + N_1(2m) \quad (21)$$

$$Y(2m+1) = S_2(2m)H_1(2m+1) + S_1^*(2m)H_2(2m+1) + N_2(2m+1) \quad (22)$$

여기서,  $m = 0, 1, \dots, N/2 - 1$ 이다.

따라서 송신신호는 안테나에서 수신된 신호를 이용하여 식 (23), (24)를 얻을 수 있게 된다.

$$S_1(2m) \cong \frac{Y(2m)H_1^*(2m) + Y^*(2m+1)H_2(2m)}{|H_1(2m)|^2 + |H_2(2m)|^2} \quad (23)$$

$$S_2(2m) \cong \frac{Y(2m+1)H_1^*(2m) - Y^*(2m)H_2(2m)}{|H_1(2m)|^2 + |H_2(2m)|^2} \quad (24)$$

여기서,  $m = 0, 1, \dots, N/2 - 1$ ,

$$H_1(2m) \cong H_1(2m+1), H_2(2m) \cong H_2(2m+1)$$

라고 가정한다.

식 (11)의 공간 주파수 블록 코드의 부호 반전 알고리즘의 수신신호는 식 (25), (26)과 같다.

$$Y(2m) = S_1(2m)H_1(2m) + S_2^*(2m)H_2(2m) + N_1(2m) \quad (25)$$

$$Y(2m+1) = S_2(2m)H_1(2m+1) - S_1^*(2m)H_2(2m+1) + N_2(2m+1) \quad (26)$$

여기서,  $m = 0, 1, \dots, N/2 - 1$ 이다.

이 때 송신신호는 최대율 결합방법을 이용하여 식 (27), (28)을 얻을 수 있게 된다.

$$S_1(2m) \cong \frac{Y(2m)H_1^*(2m) - Y^*(2m+1)H_2(2m)}{|H_1(2m)|^2 + |H_2(2m)|^2} \quad (27)$$

$$S_2(2m) \cong \frac{Y(2m+1)H_1^*(2m) + Y^*(2m)H_2(2m)}{|H_1(2m)|^2 + |H_2(2m)|^2} \quad (28)$$

여기서,  $m = 0, 1, \dots, N/2 - 1$ ,

$$H_1(2m) \cong H_1(2m+1), H_2(2m) \cong H_2(2m+1)$$

라고 가정한다.

4장 모의실험에서는 부호 반전 시간 시퀀스에 따라 미리 규정한 송신 순서를 공유하여 알고 있는 수신기와 그렇지 못한 수신기에서의 데이터 오류율을 모의실험을 통하여 보이고자 한다.

#### 4. 모의 실험 및 고찰

직교 주파수 분할 다중화 시스템의 모의 실험에 사용한 환경변수는 다음과 같다. 직교 주파수 분할 다중화 시스템이 사용하는 20 [MHz] 대역은 푸리에 변환 블록의 개수  $N=512$ 의 데이터 블록들로 분할해서 처리한다. 유효 심볼 주기는 25.6 [ $\mu$ s], 그리고 보호 구간은 0.8 [ $\mu$ s]이며, 둘을 포함하는 하나의 직교 주파수 분할 다중화 심볼 주기는 26.4 [ $\mu$ s]이다. 송신기에서는 528 개의 심볼들마다 그룹으로 묶어서 전송하며, 이 때 데이터 페이로드는 512이며, 보호구간은 16 데이터 심볼이다. 송수신기내의 푸리에변환 (FFT) 그리고 푸리에역변환 (IFFT) 블록의 크기는 512로 하며 도플러 주파수  $f_d=50$  [Hz]로 가정한다. 또한 모의 실험 채널 환경으로는 HiperLAN/2 채널 A를 사용하였으며, 채널 상태 정보를 수신기가 알고 있으며, 인접하여 위치한 두 개의 직교 주파수 분할 다중화 데이터 심볼들의 채널 계수는 동일하다고 가정하였다.

Fig. 3과 4는 부호 반전 공간 주파수 블록 코딩을 적용하여 송수신하는 일반적인 수신기가 일정한 비율로 부호반전 시퀀스를 놓친 경우의 성능을 보여준다. 여기에서는 하나의 직교 부파수 분할 다중화 심볼 내에서 32 그룹 중의 하나 (1/32) 또는 다섯 번 (5/32) 부호 반전하는 것을 놓쳤다고 가정하는 두 가지 경우의 성능을 보여준다. 오류마루에서의 비트오류확률로 두 경우의 성능을 비교하면  $1.65 \times 10^{-3}$  와  $8.20 \times 10^{-3}$  로써 32 그룹 중의 다섯 번 (5/32) 부호 반전을 놓친 경우가 한번 놓친 경우보다 오류 성능이 안 좋은

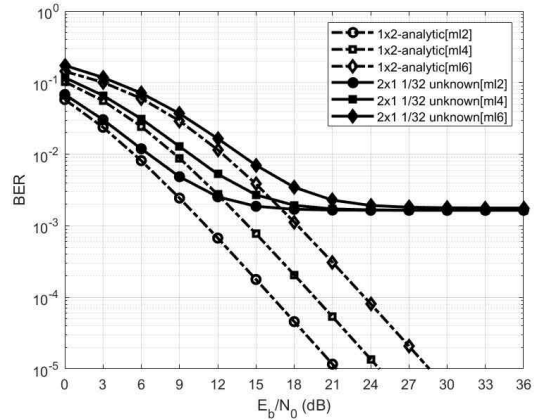


Fig. 3 Performance in Case of 1/32 Missing Rate of Channel Switching in Sign Reversal SFBC OFDM

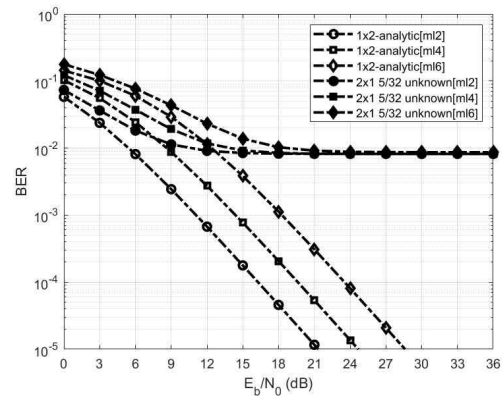


Fig. 4 Performance in Case of 5/32 Missing Rate of Channel Switching in Sign Reversal SFBC OFDM

것을 알 수 있다.

또한 모의 실험은 변조 수준이 QPSK (ml=2), 16QAM (ml=4), 64QAM (ml=6) 3가지의 경우에 대해서 모의실험을 수행하였으며, 32 그룹 중의 하나를 잘못 추정하였을 때의 비트오류확률의 시작점과 포화점에서의 비트오류확률과  $E_b/N_0$ 를 Table. 1-3에 정리하였다. 오류마루현상은 QPSK, 16QAM, 64QAM 각각 15, 18, 21[dB]에서 시작하며, 포화된 곳에서의 비트오류확률은 각각  $1.65 \times 10^{-3}$ ,  $1.65 \times 10^{-3}$ ,  $1.82 \times 10^{-3}$  임을 보여준다.

Table 1 BER Comparison (ml=2, Error 1/32)

$E_b/N_0$ [dB]	Error floor	Simulation model	BER
15	start	SR	$2.25 \times 10^{-4}$
		Error 1/32	$1.87 \times 10^{-3}$
27	saturation	SR	$7.81 \times 10^{-7}$
		Error 1/32	$1.65 \times 10^{-3}$

Table 2 BER Comparison (ml=4, Error 1/32)

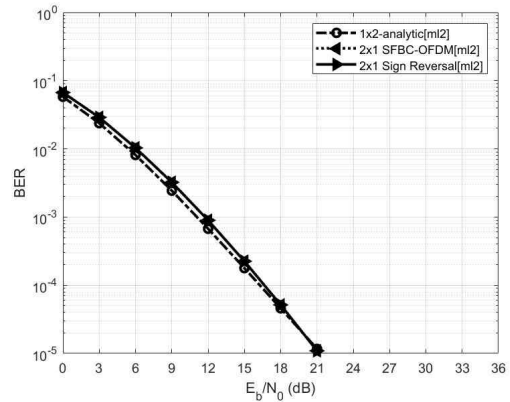
$E_b/N_0$ [dB]	Error floor	Simulation model	BER
18	start	SR	$2.90 \times 10^{-4}$
		Error 1/32	$1.93 \times 10^{-3}$
27	saturation	SR	$8.98 \times 10^{-6}$
		Error 1/32	$1.65 \times 10^{-3}$

Table 3 BER Comparison (ml=6, Error 1/32)

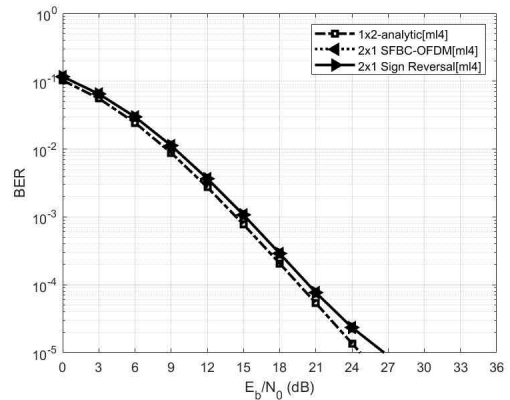
$E_b/N_0$ [dB]	Error floor	Simulation model	BER
21	start	SR	$5.49 \times 10^{-4}$
		Error 1/32	$2.28 \times 10^{-3}$
27	saturation	SR	$7.86 \times 10^{-5}$
		Error 1/32	$1.82 \times 10^{-3}$

Fig. 5는 본 논문에서 제안하는 부호 반전 방법을 사용한 공간 주파수 블록 코딩 방법을 사용한 경우의 성능 곡선이다. 종래의 방법인 공간 주파수 블록 코딩 알고리즘의 경우에는 32그룹 전체의 채널 결합 방법을 안다고 가정하였으며, 그 경우에는 부호 반전 알고리즘과 성능이 같았다. 이것은 일반적인 수신기로 수신하는 경우 종래의 공간 주파수 블록 코딩 알고리즘이 전파 환경이 공개되어 데이터 복호가 가능하지만, 부호 반전 알고리즘의 경우에는 데이터 복호가 어렵다는 사실을 보여주고 있다. 따라서 제안하는 부호 반전 알고리즘에서는 시간 제어 시퀀스를 송수신기 간에 미리 공유하여 알게 되면 그것을 모르고 있는 일반 수신기들에게 암호화 효과로 동작됨을 알 수 있다.

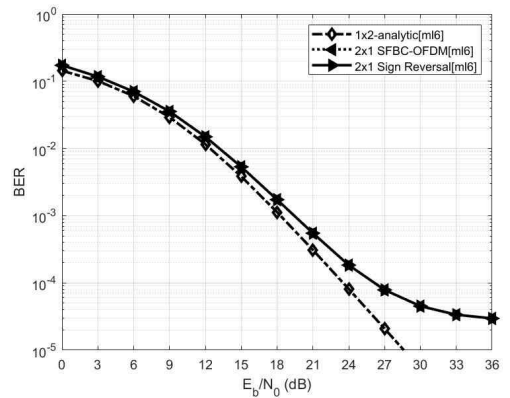
또한 공간 주파수 블록 코딩 알고리즘의 전송 데이터 구성 방법은 공간 축으로 또는 주파수 축



(a) QPSK(ml=2)



(b) 16 QAM(ml=4)



(c) 64 QAM(ml=6)

Fig. 5 Performance of Sign Reversal SFBC OFDM



으로 변형될 수 있으므로 이와 같은 다양한 암호화 구성 방법은 시간 시퀀스 정보와 함께 수신 데이터 복조를 힘들게 하는 구성요소로 동작 가능하게 된다.

## 5. 결론

이 논문은 종래의 부호 반전 시공간 블록 코딩에 적용되는 채널 스위칭으로 발생하는 암호화 효과를 공간 주파수 블록 코딩 방법에 적용하였다. 또한 종래의 방법과 부호 반전 방법간의 스위칭에 사용할 수 있는 시간 제어 시퀀스를 제시하였다. 종래의 알고리즘이 직교 주파수 분할 다중화 알고리즘의 블록 단위 신호들에 적용된 것이라면 제안하는 알고리즘은 데이터 심볼 단위에 적용한 것이다. 또한 데이터 전송 전에 부호 반전 시간 정보를 송수신기가 상호간에 알도록 함으로써 간단한 부호 반전 송신만으로 이 시간 정보를 모르는 일반적인 수신기로는 데이터 수신이 어렵다는 것을 제시하였다.

## References

Alamouti, S. (1998). A Simple Transmit Diversity Technique for Wireless Communications, *IEEE J. Select. Areas Commun.*, 16(8), 1451-1458.

Al-Dhahir, N. (2001). Single-Carrier Frequency-Domain Equalization for Space-Time Block-Coded Transmissions Over Frequency-Selective Fading Channels, *IEEE Commun. Letters*, 5(7), 304-306.

Huh N.C., and Kim S. (2015). Incremental Channel Scan Scheme based on Neighbor Channel Information in IEEE 802.11 Wireless LANs, *Journal of KIISR*, 20(5), 25-35.

IEEE SA 802.11 WG (2009). *IEEE P802.11n, Part 11, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.

Jeon, W. G., and Jung, H. K. (2006). Hybrid SC/MRRC Technique for OFDM Systems, *IEICE Trans. Commun.*, E89-B(3), 1003-1006.

Jin S., (2015). A Simulation Study on the Performance of the RAW in IEEE 802.11ah WLANs, *Journal of KIISR*, 20(2), 39-44.

Jin S. (2017). Numerical Analysis of Power Save Multi-poll Operation in IEEE 802.11 WLANs, *Journal of KIISR*, 22(3), 13-18.

Jung, H. K. (2018). A Simple Encryption Technology for Space-Time Block Coding, *Journal of the Korea Industrial Information Systems Research*, 23(5), 1-8. <http://dx.doi.org./10.9723/jksii.2018.23.5.001>

Jung, H. K. (2020). Sign Reversal Channel Switching method in Space-Time Block Code for OFDM Systems, *IEICE Trans. on Fund. of Electronics, Commun. and Computer Science*, E103-A(2), 567-570.

Oppenheim, A. and Schaffer, R. (1989). *Discrete-Time Signal Processing*, Englewood Cliffs, NJ: Prentice-Hall.

Strang, G. (1988). *Linear Algebra and Its Applications*, 3rd Ed., Harcourt Brace & Company.

TECHroid INDIA (2020). *How To Connect WiFi Without Any Password in 2020*, <https://www.youtube.com/watch?v=6quk-Bv5K4M> (Accessed on Oct. 6th, 2020)



**정혁구 (Hyeok-Koo Jung)**

- 정회원
- 연세대학교 공과대학 전기공학과 공학학사
- 연세대학교 일반대학원 전기공학과 공학석사
- 중앙대학교 전자공학과 공학박사
- 한밭대학교 정보기술대학 정보통신공학과 교수
- 관심분야 : 무선통신 모델, OFDM 시스템