Journal of the Korea Industrial Information Systems Research Vol.27 No.5, Oct. 2022 :25-36
http://dx.doi.org/10.9723/jksiis.2022.27.5.025 ISSN:1229-3741

단일 반송파 변조를 위한 공간 주파수 블록 코드의 난수 부호 반전 기법

(Random Sign Reversal Technique in Space Frequency Block Code for Single Carrier Modulation)

정 혁 구[1)*]
(Hyeok-Koo Jung)

요 약 본 논문은 단일 반송파 변조를 위한 공간 주파수 블록 코드에서의 랜덤 부호 반전 기술을 제안한다. 종래의 시공간 그리고 공간 주파수 블록 코드는 전파 환경이 공개되어 있으므로 심각한 전파 탈취 문제를 극복해야 한다. 이러한 전파 공개 문제를 피하기 위해, 시공간 블록 코드를 위한 랜덤 코드 데이터 보호 방법이 제안되어 있지만, 이 알고리즘은 직교 주파수 분할 다중화 블록별로 채널 결합을 바꿀 수 있는데, 이와 같은 종류의 느린 스위칭은 근처의 수신기들이 전송된 데이터를 검출할 확률을 증가시킨다. 이 논문은 데이터 심볼 기반의 빠른 스위칭 알고리즘 즉, 단일 반송파 변조를 위한 공간 주파수 블록 코드에서의 랜덤 부호 반전 기술을 제안한다. 모의실험 결과는 제안하는 알고리즘이 랜덤 부호 반전 타이밍 시퀀스를 모르는 수신기의 성능과 비교하여 우수한 성능을 보유하고 있다는 것을 나타내었다.

핵심주제어: 랜덤 코드, 데이터 보호, 부호 반전, 타이밍 시퀀스, 공간 주파수 블록 코드

Abstract This paper proposes a random sign reversal technique in space frequency block code for single carrier modulation. The traditional space time and frequency block coding technique may be confronted with radio environments openly, severe radio hijacking problems are to be overcome. In order to avoid such an open radio issue, random coded data protection technique for space-time block code was proposed, but this algorithm can change channel combination per an Orthogonal Frequency Division Multiplexing block. This kind of slow switching increases the probability that nearby receivers will detect the transmitted data. This paper proposes a fast switching algorithm per data symbols' basis which is a random sign reversal technique in space frequency block code for Single Carrier Modulation. It is shown in simulation that the proposed one has a superior performance in comparison with the performance of the receiver which do not know the random timing sequence of sign reversal.

Keywords: Random Code, Data Protection, Sign Reversal, Timing Sequence, Space Frequency Block Code

* Corresponding Author: junghk@hanbat.ac.kr
Manuscript received August 19, 2022 / revised October 17, 2022 / accepted October 23, 2022
1) 한밭대학교 모바일융합공학과, 제1저자

1. 서 론

실내 무선 환경에서 다중 송신기 그리고 다중 수신기 구조를 사용하는 다중 반송파 방식 즉, 직교 주파수 분할 다중화 방식이 다중 경로 페이딩 왜곡에 효과적으로 대응하는 것으로 알려져 있다 (IEEE SA 802.11 WG, 2009; Jin 2015, 2017; Huh and Kim, 2015). 이와 같이 전파가 무작위적으로 산란하여 퍼지는 전파 환경에서 최적의 효율을 나타내는 최대 율 수신 결합은 다중 송신기 그리고 수신기의 경우에 특히 효과적인 것으로 알려져 있으며, 시공간 블록 코드로서 다중 송신 안테나의 경우에도 수신기에서 결합 이득을 얻으려고 하는 방법들이 제안되었다 (Alamouti, 1988; Al-Dhahir, 2001; Jeon and Jung, 2006). 이와 같은 직교 주파수 분할 다중화 알고리즘을 단일 반송파에 적용하고자 하는 것은 송신기에 있는 푸리에 역 변환기를 수신기에서 사용하는 것으로 수신기에서는 시간 영역 신호로부터 주파수 영역 신호를 만들고 채널 보상 그리고 채널 결합을 수행한 후 푸리에 역 변환기를 사용하는 구조를 가지고 있다 (Al-Dhahir, 2001).

그런데 실내 무선 랜 전파 환경은 공개되어 있으므로 거리적으로 가깝게 위치한 다른 수신기들에 의해서 전파를 수신한 후 무선 데이터가 탈취당하는 기술들이 공유되어 있는 것으로 보여진다 (Bombal, 2020). 따라서 이와 같이 전파가 공개되어 사용하고 있는 다중 송수신 안테나 환경에서는 종래의 암호화 기법과 더불어 사용자 데이터를 쉽게 검출할 수 없게 하는 방법들이 중요하게 되었다.

이러한 알고리즘으로는 송신기들의 소스 데이터 블록들을 교환하여 채널 스위칭을 발생시키는 알고리즘(Jung, 2018)이 제안되었고, 이러한 직접적인 소스 데이터 블록들의 교환 방법이 복잡함으로 그 복잡도를 낮추려고 시도한 알고리즘이 부호 반전 채널 스위칭 알고리즘(Jung, 2020)이며 이 방법은 시공간 블록 코드에 작용한 것이었으며, 이 방법을 공간 주파수 블록 코드 알고리즘으로 확장 적용한 알고리즘(Jung, 2020)이 제안되었다.

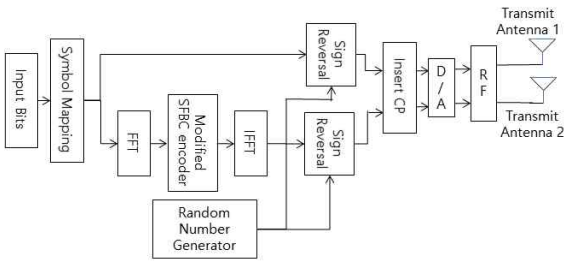
한편 부호 반전 알고리즘은 데이터 전송 중 어느 시점에 부호 반전이 발생하는가가 데이터를 보호하는데 중요한 문제가 되었고, 이 시점을 난수를 활용하여 시점을 알아내기 힘들게 하고자 하는 알고리즘(Jung, 2021)이 시공간 블록 코드에 적용할 수 있도록 제안되었다. 하지만 이 방법은 채널 스위칭 시점이 직교 주파수 분할 다중화 데이터 블록 별로 이루어지므로 느린 스위칭이 이루어지고 있고 스위칭하는 방법의 종류가 작아서 더 다양한 스위칭 방법이 필요하게 되었다.

본 논문에서는 난수 특히 월시 코드를 활용하고 좀 더 빠른 스위칭을 발생시키기 위하여 블록별이 아닌 데이터 심볼별로 스위칭을 발생시킬 수 있도록 공간 주파수 블록 코드에 적용하여 부호 반전을 무작위적으로 실행하여 데이터 보호를 수행하는 알고리즘을 제안하고 HiperLAN/2 A 채널 환경에서 모의실험하고 그 실험 결과를 보여준다. 모의 실험결과는 종래의 알고리즘과 비교하였으며, 결과는 비트오류율로 제시하였다. 논문의 구성은 2장에서는 이 논문에서 제안하고 있는 단일 반송파 시스템 응용분야에서 난수 코드를 활용하여 공간 주파수 블록 코드에 적용하는 데이터 보호방법을 제안하며, 시간 영역과 주파수 영역에서 신호를 기술한다. 3장에서는 모의실험 환경과 성능 비교에 관하여 기술하였으며, 4장에서 결론을 제시하였다.

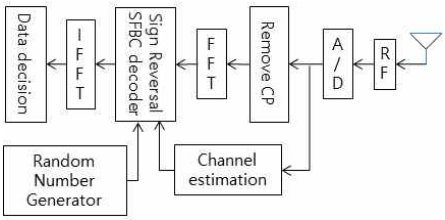
2. 난수 코드를 활용하여 공간 주파수 블록 코드에 적용하는 데이터 보호 방법

제안하는 난수 코드를 활용하는 데이터 보호 방법을 사용하는 단일 반송파 변조의 공간 주파수 블록 코드의 송신기 그리고 수신기 블록도는 Fig. 1에 제시하며, 종래의 직교 주파수 분할 다중화 블록도는 Fig. 2와 같다. 본 논문에서 제안하는 알고리즘을 구현하기 위해서는 난수 코드를 제공하는 난수 발생기라는 블록이 추가되어 있으며 이 블록의 입력 3비트 신호에 따라 여덟 종류의 공간 주파수 블록 코드 알고리즘이 동작하는데 부호 반전, 즉 +부호면 -부호로, -부호면 +부호로 바꿈, 은 모두 사용하며, 첫 번째 방법은 전통적인 공간 주파수 블록 코드의 전송 데이터를 안테나 별로 배열하느냐 아니면 주파

수 축으로 배열하느냐에 따라서 A, B 방법으로 나뉘며, 두 번째는 송신 안테나들 중에서 단 하나의 송신 안테나 신호의 부호를 반전하는 방법을 사용하며, 세 번째는 주파수 영역에서 하나의 직교 주파수 분할 다중화 블록을 구성하는 부반송파들의 부호를 반전시키는 방법을 사용하

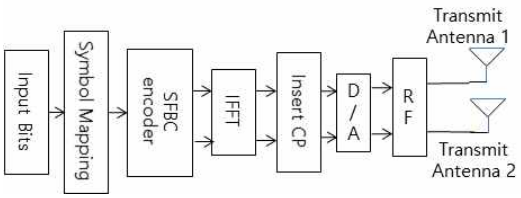


(a) Transmitter

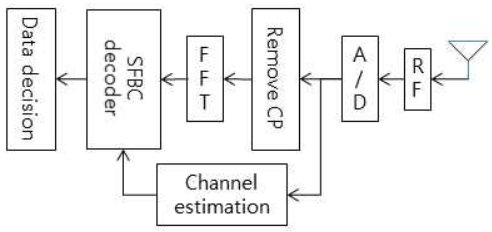


(b) Receiver

Fig. 1 Block diagrams of the proposed Random Number Coded data protection for Space Frequency Block code for Single Carrier Modulation



(a) Transmitter



(b) Receiver

Fig. 2 Block diagrams of the traditional Space Frequency Block code for Orthogonal Frequency Division Multiplexing System

고자 한다. 이와 같은 공간 주파수 블록 코드 8가지 방법을 공간 주파수 블록 코드의 하나의 그룹에 월시 코드의 3비트를 이용하여 8가지 방법중의 하나를 선택하여 부호 반전하는 방법을 사용하여 수신기에서 실행하는 결합 방법을 다양하게 함으로써 다른 수신기의 신호 검출을 어렵게 하는 방법을 제시한다. 월시 코드를 확장하는 것은 하다마드 행렬을 이용하여 다음과 같은 확장 방법을 사용하여 실행한다.

$$H(n) = H_{2n} = \begin{bmatrix} H_n & H_n \\ H_n & \overline{H_n} \end{bmatrix} \quad (1)$$

$$H_0 = [0]$$

여기서 ($\bar{}$)는 반전을 의미한다. 본 논문에서는 소스 블록 신호 하나의 크기가 512를 사용하고 또한 월시 코드는 $H(1024) = H_{2048}$를 사용하게 되는데, 하나의 소스 블록 신호 2개 당 3비트의 월시코드를 할당하여 사용하게 된다.

여기서 H(1024) 는 1024x1024 행렬이므로, 1024종류의 1024bit 들이 있게 되고, 송수신기는 1024종류 중 어떤 한 종류의 값을 난수 코드로 사용할 것을 고른 후 송수신기가 모두 그 값을 나우어 가진 후 그 난수 코드를 발행하게 된다. 해당 난수 코드는 768종류만이 필요하며 1024개 중에서 768개를 선택하여 실행하도록 한다. 난수 월시 코드에 관해서는 테이블 방식의 ROM 형식으로 전체 데이터를 저장하는 경우에는 1024x1024 비트 중에서 실제 사용하는 768x768 비트의 테이블이 필요하지만, 실제로 사용할 때에는 768 종류 중의 하나인 768 비트가 필요하게 된다. 하지만 테이블 방식으로 난수표 전체를 공유하지 않고 전송 모드에 따라서 결정되는 768 비트의 데이터를 송신기와 수신기가 공유하는 방법을 사용한다면 실제 전송이 개시되기 이전의 준비 단계에서 미리 난수 데이터 768 비트를 공유하는 방법을 사용하면 된다. 하나의 공간 주파수 블록 코드 그룹이 2개의 주파수 부반송파 별로 3비트의 코드를 가지고 2개의 주파수 부반송파 즉 공간 주파수 블록 코드 그룹 당 난수화를 실행한다. 먼저 3비트를 가지고 구성할 수 있는 동작 모드는 8개이며 Table 1과 같이

구성한다. 이와 같은 구성을 따른 월시코드 3비트에 따라 수신기에서는 8종류의 수신 결합 방법 중 결정된 하나의 방법으로 수신하게 되고, 이 3bit로 해당 월시코드를 결정하고 또 이것은 난수이므로 그 공간 주파수 블록 코드의 결합 방법을 결정하는 해당 월시코드를 알 수 없는 수신기의 경우에는 데이터 복호가 어렵게 된다.

2.1 전통적인 공간 주파수 블록코드 종류 A

제안하는 난수 부호 반전 방법의 첫 번째 안테나로 전송될 사용자 데이터를 $\mathbf{s}_1$이라 하면,

$$\mathbf{s}_1 = [s_1(0)\, s_1(1) \cdots s_1(N-1)]^T \qquad (2)$$
$$\mathbf{Q}\mathbf{s}_1 = \mathbf{S}_1$$

여기서 $\mathbf{Q}$는 정규 직교 이산 푸리에 변환 행렬을 의미하며, 이 때 두 번째 안테나로 전송될 $\mathbf{s}_2$ 데이터 블록은 $\mathbf{S}_1$ 데이터 블록을 변형하여 구성하며, 구성하는 방법은 수신기에서 최대 율결합 수신이 가능하도록 공간 주파수 블록 코드의 데이터 구성을 따른다. $\mathbf{S}_1$과 $\mathbf{S}_2$ 데이터 블록은 N/2 개의 공간 주파수 블록으로 나뉘어지며 그 중 m번째 블록의 경우의 데이터 구성은 다음과 같고, 여기서 $\mathbf{S}_2$ 의 m번째 블록은 다음과 같이 기술된다.

$$\begin{bmatrix} S_1(2m) & S_1(2m+1) \\ -S_1^*(2m+1) & S_1^*(2m) \end{bmatrix} \qquad (3)$$

$$S_2(2m) = -S_1^*(2m+1)$$
$$S_2(2m+1) = S_1^*(2m)$$

$$\mathbf{S}_2 = [-S_1^*(1)\; S_1^*(0) \ldots S_1^*(N-2)]^T$$

여기서 $m = 0, 1, \ldots, N/2-1$ 그리고 $(\;)^*$은 공액 복소수를 말한다. 송신기의 푸리에 역변환 블록에서는 이 $\mathbf{S}_2$를 푸리에 역변환하게 되고 그 결과로 만들어지는 신호 $\mathbf{s}_2$ 가 두 번째 안테나에서 전송되는 신호이다.

$$\mathbf{Q}^{-1}\mathbf{S}_2 = \mathbf{s}_2 \qquad (4)$$

여기서 $\mathbf{s}_1$과 $\mathbf{s}_2$는 시간 영역 신호를 의미하며, 아래 첨자의 숫자는 송신기 안테나 번호를 말한다. 이 시간 영역 신호는 각각 사이클릭 프레픽스를 추가한 후 각각 송신 안테나를 통하여 전송하게 된다.

이러한 신호를 수신기에서 표현하면 다음과 같게 된다.

$$\mathbf{y} = \mathbf{s}_1 \otimes \mathbf{h}_1 + \mathbf{s}_2 \otimes \mathbf{h}_2 + \mathbf{n} \qquad (5)$$

여기에서 $\otimes$ 는 컨벌루션을 의미하고, $\mathbf{h}_n$ 는 시간 축에서 n 번째 송신 안테나에서 수신기로의 채널, $\mathbf{n}$ 은 백색 잡음을 의미한다. 각 블록은 길이 ν의 사이클릭 프레픽스를 추가함으로 블록 간 간섭을 제거한다. 수신된 데이터 중에서 사이클릭 프레픽스의 역할로 직교 주파수 분할 다중화 블록에 해당하는 데이터만 시간 영역에서 발췌하여 푸리에 변환하여도 환형컨벌루션이 동작하게 된다.

여기에서 부반송파 채널 값은 두 개의 연이은 부반송파 데이터 간에 일정하다고 가정한다. 특히 채널 $\mathbf{h}_n^m$ 은 $N \times N$ 환형 행렬이며 첫 번째 열은 채널의 임펄스 응답에 $(N-\nu-1)$ 개의 영이 첨부되어 있으며, $\mathbf{h} = \mathbf{Q}^H\mathbf{H}\mathbf{Q}$와 같이 아이겐-분해가 된다 (Strang, 1988). $\mathbf{H}$ 는 대각 행렬들이며 (k,k) 원소는 채널 임펄스 응답의 k 번째 DFT 상수를 의미한다 (Oppenheim, 1989). 이와 같은 시간 영역 신호는 다음과 같이 주파수 영역 신호로 변환된다.

$$\mathbf{Y} = \mathbf{S}_1\mathbf{H}_1 + \mathbf{S}_2\mathbf{H}_2 + \mathbf{N} \qquad (6)$$

가 성립하게 된다.

여기에서 $\mathbf{Q}\mathbf{y} = \mathbf{Y}, \mathbf{Q}\mathbf{s}_1 = \mathbf{S}_1, \mathbf{Q}\mathbf{s}_2 = \mathbf{S}_2$ 을 말하며, $\mathbf{N}$ 은 주파수 영역에서의 백색 잡음을 의미한다. 이 신호에서 m번째 블록의 신호만을 구분하여 표현하면 다음과 같다.

$$Y(2m) = S_1(2m)H_1(2m) - S_1^*(2m+1)H_2(2m) + N(2m) \quad (7)$$
$$Y(2m+1) = S_1(2m+1)H_1(2m+1) + S_1^*(2m)H_2(2m+1) + N(2m+1)$$

위 식과 같은 수신기 신호를 주파수 영역에서 구하면 주파수 영역 추정 신호 S_1 과 S_2 는 다음 식을 통하여 계산할 수 있게 된다.

$$S_1(2m) = \frac{H_1^*(2m)Y(2m) + H_2(2m)Y^*(2m+1)}{|H_1(2m)|^2 + |H_2(2m)|^2} \quad (8)$$
$$S_1(2m+1) = \frac{-H_2(2m)Y^*(2m) + H_1^*(2m)Y(2m+1)}{|H_1(2m)|^2 + |H_2(2m)|^2}$$

여기서 다음과 같이 가정한다.

$$H_1(2m) = H_1(2m+1)$$
$$H_2(2m) = H_2(2m+1)$$
$$m = 0, 1, \ldots, N/2-1$$

최종적으로 N 개의 블록 신호들을 모두 모아서 하나의 블록으로 구성하여 푸리에 역변환함으로써 송신 데이터를 추정할 수 있게 된다. 이 방법은 다음에 기술하는 안테나 축으로 그리고 부반송파 측면에서 부호 반전하는 신호 변형 방법과 구분하기 위하여 전통적인 공간 주파수 블록 코드 A 라고 부른다.

Table 1 Eight kinds of methods for using Walsh code in the transmitter

Walsh code 3bit value	Sign Reversal type	Traditional SFBC types	Signal Reversal configuration
000	a	A	First Ant.
001	b		Second Ant.
010	c		2m-*th* subcarrier
011	d		(2m+1)-*th* subcarrier
100	e	B	First Ant.
101	f		Second Ant.
110	g		2m-*th* subcarrier
111	h		(2m+1)-*th* subcarrier

2.2 공간 주파수 블록 코드 방법 a

한편 전통적인 공간 주파수 블록 코드 방법 A와 다르게 별도로 첫 번째 안테나로 전송되는 데이터의 주파수 영역 신호의 부호를 반전하게 되면, 주파수 영역에서

$$\begin{bmatrix} -S_1(2m) & -S_1(2m+1) \\ -S_1^*(2m+1) & S_1^*(2m) \end{bmatrix} \quad (9)$$

와 같은 구성이 된다. 이 신호의 시간 영역 신호 s_1과 s_2에 사이클릭 프레픽스를 추가하여 송신하게 되는데 그 신호를 수신기에서 푸리에 변환하여 주파수 영역신호로 표현하면 다음과 같다.

$$Y(2m) = -S_1(2m)H_1(2m) - S_1^*(2m+1)H_2(2m) + N(2m) \quad (10)$$
$$Y(2m+1) = -S_1(2m+1)H_1(2m+1) + S_1^*(2m)H_2(2m+1) + N(2m+1)$$

위 식과 같은 수신기 신호를 주파수 영역에서 구하면 주파수 영역 추정 신호 $S_1(2m)$ 과 $S_1(2m+1)$는 다음 식을 통하여 계산할 수 있게 된다.

$$S_1(2m) = \frac{-H_1^*(2m)Y(2m) + H_2(2m)Y^*(2m+1)}{|H_1(2m)|^2 + |H_2(2m)|^2}$$
$$S_1(2m+1) = \frac{-H_2(2m)Y^*(2m) - H_1^*(2m)Y(2m+1)}{|H_1(2m)|^2 + |H_2(2m)|^2} \quad (11)$$

최종적으로 N 개의 블록 신호들을 모두 모아서 하나의 블록으로 구성하여 푸리에 역변환함으로써 송신 데이터를 추정할 수 있게 된다. 이와 같은 신호 구성은 채널이 $H_1(2m)$ 이 $-H_1(2m)$로 바뀌었음을 의미한다. 이 방법을 아래의 다른 결합 방법과 구별하기 위하여 공간 주파수 블록 코드 방법 a 라 한다.

2.3 공간 주파수 블록 코드 방법 b

한편 전통적인 공간 주파수 블록 코드 방법 A와 다르게 별도로 두 번째 안테나로 전송되는 데이터의 주파수 영역 신호의 부호를 반전하게 되면, 주파수 영역에서와 같은 구성이 된다.

$$\begin{bmatrix} S_1(2m) & S_1(2m+1) \\ S_1^*(2m+1) & -S_1^*(2m) \end{bmatrix} \tag{12}$$

이 신호의 시간 영역 신호 s_1과 s_2에 사이클릭 프레픽스를 추가하여 송신하게 되는데 그 신호를 수신기에서 푸리에 변환하여 주파수 영역 신호로 표현하면 다음과 같다.

$$\begin{aligned} Y(2m) &= S_1(2m)H_1(2m) \\ &\quad + S_1^*(2m+1)H_2(2m) + N(2m) \\ Y(2m+1) &= S_1(2m+1)H_1(2m+1) \\ &\quad - S_1^*(2m)H_2(2m+1) + N(2m+1) \end{aligned} \tag{13}$$

위 식과 같은 수신기 신호를 주파수 영역에서 구하면 주파수 영역 추정 신호 $S_1(2m)$ 과 $S_1(2m+1)$는 다음 식을 통하여 계산할 수 있게 된다.

$$\begin{aligned} S_1(2m) &= \frac{H_1{}^*(2m)Y(2m) - H_2(2m)Y^*(2m+1)}{|H_1(2m)|^2 + |H_2(2m)|^2} \\ S_1(2m+1) &= \frac{H_2(2m)Y^*(2m) + H_1^*(2m)Y(2m+1)}{|H_1(2m)|^2 + |H_2(2m)|^2} \end{aligned} \tag{14}$$

최종적으로 N 개의 블록 신호들을 모두 모아서 하나의 블록으로 구성하여 푸리에 역변환함으로써 송신 데이터를 추정할 수 있게 된다. 이와 같은 신호 구성은 채널이 $H_2(2m)$ 이 $-H_2(2m)$로 바뀌었음을 의미한다. 이 방법을 아래의 다른 결합 방법과 구별하기 위하여 공간 주파수 블록 코드 방법 b 라 한다.

2.4 공간 주파수 블록 코드 방법 c

한편 전통적인 공간 주파수 블록 코드 방법 A와 다르게 별도로 $2m$번째 부반송파 데이터의 주파수 영역 신호의 부호를 반전하게 되면, 주파수 영역에서

$$\begin{bmatrix} -S_1(2m) & S_1(2m+1) \\ S_1^*(2m+1) & S_1^*(2m) \end{bmatrix} \tag{15}$$

와 같은 구성이 된다. 이 신호의 시간 영역 신호 s_1과 s_2에 사이클릭 프레픽스를 추가하여 송신하게 되는데 그 신호를 수신기에서 푸리에 변환하여 주파수 영역신호로 표현하면 다음과 같다.

$$\begin{aligned} Y(2m) &= -S_1(2m)H_1(2m) \\ &\quad + S_1^*(2m+1)H_2(2m) + N(2m) \\ Y(2m+1) &= S_1(2m+1)H_1(2m+1) \\ &\quad + S_1^*(2m)H_2(2m+1) + N(2m+1) \end{aligned} \tag{16}$$

위 식과 같은 수신기 신호를 주파수 영역에서 구하면 주파수 영역 추정 신호 $S_1(2m)$ 과 $S_1(2m+1)$는 다음 식을 통하여 계산할 수 있게 된다.

$$\begin{aligned} S_1(2m) &= \frac{-H_1^*(2m)Y(2m) + H_2(2m)Y^*(2m+1)}{|H_1(2m)|^2 + |H_2(2m)|^2} \\ S_1(2m+1) &= \frac{H_2(2m)Y^*(2m) + H_1^*(2m)Y(2m+1)}{|H_1(2m)|^2 + |H_2(2m)|^2} \end{aligned} \tag{17}$$

최종적으로 N 개의 블록 신호들을 모두 모아서 하나의 블록으로 구성하여 푸리에 역변환함으로써 송신 데이터를 추정할 수 있게 된다 이와 같은 신호 구성은 채널 $H_1(2m)$이 $H_2(2m)$와 서로 바뀌었음을 의미하며 또한 송신신호 $S_1(2m)$은 $S_1^*(2m+1)$로 그리고 $S_1(2m+1)$은 $S_1^*(2m)$으로 바뀐 것과 같다는 것을 알 수 있다. 이 방법을 아래의 다른 결합 방법과 구별하기 위하여 공간 주파수 블록 코드 방법 c 라 한다.

2.5 공간 주파수 블록 코드 방법 d

한편 전통적인 공간 주파수 블록 코드 방법 A와 다르게 별도로 $2m+1$번째 부반송파 데이터의 주파수 영역 신호의 부호를 반전하게 되면 데이터의 부호를 반전하게 되면, 주파수 영역에서

$$\begin{bmatrix} S_1(2m) & -S_1(2m+1) \\ -S_1^*(2m+1) & -S_1^*(2m) \end{bmatrix} \tag{18}$$

와 같은 구성이 된다. 이 신호의 시간 영역 신호 $\mathbf{s_1}$과 $\mathbf{s_2}$에 사이클릭 프레픽스를 추가하여 송신하게 되는데 그 신호를 수신기에서 푸리에 변환하여 주파수 영역신호로 표현하면 다음과 같다.

$$\begin{aligned} Y(2m) &= S_1(2m)H_1(2m) \\ &\quad - S_1^*(2m+1)H_2(2m) + N(2m) \\ Y(2m+1) &= -S_1(2m+1)H_1(2m+1) \\ &\quad - S_1^*(2m)H_2(2m+1) + N(2m+1) \end{aligned} \tag{19}$$

위 식과 같은 수신기 신호를 주파수 영역에서 구하면 주파수 영역 추정 신호 $S_1(2m)$ 과 $S_1(2m+1)$는 다음 식을 통하여 계산할 수 있게 된다.

$$\begin{aligned} S_1(2m) &= \frac{H_1^*(2m)Y(2m) - H_2(2m)Y^*(2m+1)}{|H_1(2m)|^2 + |H_2(2m)|^2} \\ S_1(2m+1) &= \frac{-H_2(2m)Y^*(2m) - H_1^*(2m)Y(2m+1)}{|H_1(2m)|^2 + |H_2(2m)|^2} \end{aligned} \tag{20}$$

최종적으로 N 개의 블록 신호들을 모두 모아서 하나의 블록으로 구성하여 푸리에 역변환함으로써 송신 데이터를 추정할 수 있게 된다. 이와 같은 신호 구성은 채널 $H_1(2m)$이 $H_2(2m)$와 서로 바뀌었음을 의미하며 또한 송신신호 $S_1(2m)$은 $-S_2^*(2m+1)$로 그리고 $S_1(2m+1)$은 $-S_1^*(2m)$으로 바뀐 것과 같다는 것을 알 수 있다. 이 방법을 아래의 다른 결합 방법과 구별하기 위하여 공간 주파수 블록 코드 방법 d 라 한다.

2.6 전통적인 공간 주파수 블록코드 종류 B

한편 전통적인 공간 주파수 블록 코드 방법에서 가공하지 않은 데이터를 보내는 것을 하나의 송신안테나가 아니고 하나의 주파수 영역으로 보내는 것으로 변경하면, 주파수 영역에서

$$\begin{bmatrix} S_1(2m) & -S_1^*(2m+1) \\ S_1(2m+1) & S_1^*(2m) \end{bmatrix} \tag{21}$$

와 같은 구성이 된다. 이 신호의 시간 영역 신호 $\mathbf{s_1}$과 $\mathbf{s_2}$에 사이클릭 프레픽스를 추가하여 송신하게 되는데 그 신호를 수신기에서 푸리에 변환하여 주파수 영역신호로 표현하면 다음과 같다.

$$\begin{aligned} Y(2m) &= S_1(2m)H_1(2m) \\ &\quad + S_1(2m+1)H_2(2m) + N(2m) \\ Y(2m+1) &= -S_1^*(2m+1)H_1(2m+1) \\ &\quad + S_1^*(2m)H_2(2m+1) + N(2m+1) \end{aligned} \tag{22}$$

위 식과 같은 수신기 신호를 주파수 영역에서 구하면 주파수 영역 추정 신호 $S_1(2m)$ 과 $S_1(2m+1)$는 다음 식을 통하여 계산할 수 있게 된다.

$$\begin{aligned} S_1(2m) &= \frac{H_1^*(2m)Y(2m) + H_2(2m)Y^*(2m+1)}{|H_1(2m)|^2 + |H_2(2m)|^2} \\ S_1(2m+1) &= \frac{H_2^*(2m)Y(2m) - H_1(2m)Y^*(2m+1)}{|H_1(2m)|^2 + |H_2(2m)|^2} \end{aligned} \tag{23}$$

최종적으로 N 개의 블록 신호들을 모두 모아서 하나의 블록으로 구성하여 푸리에 역변환함으로써 송신 데이터를 추정할 수 있게 된다. 이 방법은 다음에 기술하는 안테나 축으로 그리

고 부반송파 측면에서 부호 반전하는 신호 변형 방법과 구분하기 위하여 전통적인 공간 주파수 블록 코드 B 라고 부른다.

2.7 공간 주파수 블록 코드 방법 e

한편 전통적인 공간 주파수 블록 코드 방법 B와 다르게 별도로 첫 번째 안테나로 전송되는 데이터의 주파수 영역 신호의 부호를 반전하게 되면, 주파수 영역에서

$$\begin{bmatrix} -S_1(2m) & S_1^*(2m+1) \\ S_1(2m+1) & S_1^*(2m) \end{bmatrix} \tag{24}$$

와 같은 구성이 된다. 이 신호의 시간 영역 신호 s_1과 s_2에 사이클릭 프레픽스를 추가하여 송신하게 되는데 그 신호를 수신기에서 푸리에 변환하여 주파수 영역신호로 표현하면 다음과 같다.

$$\begin{aligned} Y(2m) &= -S_1(2m)H_1(2m) \\ &\quad + S_1(2m+1)H_2(2m) + N(2m) \\ Y(2m+1) &= S_1^*(2m+1)H_1(2m+1) \\ &\quad + S_1^*(2m)H_2(2m+1) + N(2m+1) \end{aligned} \tag{25}$$

위 식과 같은 수신기 신호를 주파수 영역에서 구하면 주파수 영역 추정 신호 $S_1(2m)$ 과 $S_1(2m+1)$는 다음 식을 통하여 계산할 수 있게 된다.

$$\begin{aligned} S_1(2m) &= \frac{-H_1^*(2m)Y(2m) + H_2(2m)Y^*(2m+1)}{|H_1(2m)|^2 + |H_2(2m)|^2} \\ S_1(2m+1) &= \frac{H_2^*(2m)Y(2m) + H_1(2m)Y^*(2m+1)}{|H_1(2m)|^2 + |H_2(2m)|^2} \end{aligned} \tag{26}$$

최종적으로 N 개의 블록 신호들을 모두 모아서 하나의 블록으로 구성하여 푸리에 역변환함으로써 송신 데이터를 추정할 수 있게 된다. 이와 같은 신호 구성은 채널 $H_1(2m)$이 $H_2(2m)$와 서로 바뀌었음을 의미하며 또한 송신신호 $S_1(2m)$은 $S_1(2m+1)$로 그리고 $S_1(2m+1)$은 $-S_1(2m)$으로 바뀐 것과 같다는 것을 알 수 있다. 이 방법을 다른 결합 방법과 구별하기 위하여 공간 주파수 블록 코드 방법 e 라 한다.

2.8 공간 주파수 블록 코드 방법 f

한편 전통적인 공간 주파수 블록 코드 방법 B와 다르게 별도로 두 번째 안테나로 전송되는 데이터의 주파수 영역 신호의 부호를 반전하게 되면, 주파수 영역에서

$$\begin{bmatrix} S_1(2m) & -S_1^*(2m+1) \\ -S_1(2m+1) & -S_1^*(2m) \end{bmatrix} \tag{27}$$

와 같은 구성이 된다. 이 신호의 시간 영역 신호 s_1과 s_2에 사이클릭 프레픽스를 추가하여 송신하게 되는데 그 신호를 수신기에서 푸리에 변환하여 주파수 영역신호로 표현하면 다음과 같다.

$$\begin{aligned} Y(2m) &= S_1(2m)H_1(2m) \\ &\quad - S_1(2m+1)H_2(2m) + N(2m) \\ Y(2m+1) &= -S_1^*(2m+1)H_1(2m+1) \\ &\quad - S_1^*(2m)H_2(2m+1) + N(2m+1) \end{aligned} \tag{28}$$

위 식과 같은 수신기 신호를 주파수 영역에서 구하면 주파수 영역 추정 신호 $S_1(2m)$ 과 $S_1(2m+1)$는 다음 식을 통하여 계산할 수 있게 된다.

$$\begin{aligned} S_1(2m) &= \frac{H_1{}^*(2m)Y(2m) - H_2(2m)Y^*(2m+1)}{|H_1(2m)|^2 + |H_2(2m)|^2} \\ S_1(2m+1) &= \frac{-H_2^*(2m)Y(2m) - H_1(2m)Y^*(2m+1)}{|H_1(2m)|^2 + |H_2(2m)|^2} \end{aligned} \tag{29}$$

최종적으로 N 개의 블록 신호들을 모두 모아서 하나의 블록으로 구성하여 푸리에 역변환함

으로써 송신 데이터를 추정할 수 있게 된다. 이와 같은 신호 구성은 채널 $H_1(2m)$이 $H_2(2m)$와 서로 바뀌었음을 의미하며 또한 송신신호 $S_1(2m)$은 $-S_1(2m+1)$로 그리고 $S_1(2m+1)$은 $S_1(2m)$으로 바뀐 것과 같다는 것을 알 수 있다. 이 방법을 아래의 다른 결합 방법과 구별하기 위하여 공간 주파수 블록 코드 방법 f 라 한다.

2.9 공간 주파수 블록 코드 방법 g

한편 전통적인 공간 주파수 블록 코드 방법 B와 다르게 별도로 $2m$번째 부반송파 데이터의 부호를 주파수 영역 신호의 반전하게 되면, 주파수 영역에서

$$\begin{bmatrix} -S_1(2m) & -S_1^*(2m+1) \\ -S_1(2m+1) & S_1^*(2m) \end{bmatrix} \tag{30}$$

와 같은 구성이 된다. 이 신호의 시간 영역 신호 s_1과 s_2에 사이클릭 프레픽스를 추가하여 송신하게 되는데 그 신호를 수신기에서 푸리에 변환하여 주파수 영역신호로 표현하면 다음과 같다.

$$\begin{aligned} Y(2m) &= -S_1(2m)H_1(2m) \\ &\quad -S_1(2m+1)H_2(2m)+N(2m) \\ Y(2m+1) &= -S_1^*(2m+1)H_1(2m+1) \\ &\quad +S_1^*(2m)H_2(2m+1)+N(2m+1) \end{aligned} \tag{31}$$

위 식과 같은 수신기 신호를 주파수 영역에서 구하면 주파수 영역 추정 신호 $S_1(2m)$ 과 $S_1(2m+1)$는 다음 식을 통하여 계산할 수 있게 된다.

$$\begin{aligned} S_1(2m) &= \frac{-H_1^*(2m)\,Y(2m)+H_2(2m)\,Y^*(2m+1)}{|H_1(2m)|^2+|H_2(2m)|^2} \\ S_1(2m+1) &= \frac{-H_2^*(2m)\,Y(2m)-H_1(2m)\,Y^*(2m+1)+}{|H_1(2m)|^2+|H_2(2m)|^2} \end{aligned} \tag{32}$$

최종적으로 N 개의 블록 신호들을 모두 모아서 하나의 블록으로 구성하여 푸리에 역변환함으로써 송신 데이터를 추정할 수 있게 된다. 이와 같은 신호 구성은 채널 $H_1(2m)$이 $H_2(2m)$와 서로 바뀌었음을 의미하며 또한 송신신호 $S_1(2m)$은 $-S_1(2m+1)$로 그리고 $S_1(2m+1)$은 $-S_1(2m)$으로 바뀐 것과 같다는 것을 알 수 있다. 이 방법을 아래의 다른 결합 방법과 구별하기 위하여 공간 주파수 블록 코드 방법 g 라 한다.

2.10 공간 주파수 블록 코드 방법 h

한편 전통적인 공간 주파수 블록 코드 방법 B 와 다르게 별도로 $2m+1$번째 부반송파 데이터의 주파수 영역 신호의 부호를 반전하게 되면 데이터의 부호를 반전하게 되면, 주파수 영역에서

$$\begin{bmatrix} S_1(2m) & S_1^*(2m+1) \\ S_1(2m+1) & -S_1^*(2m) \end{bmatrix} \tag{33}$$

와 같은 구성이 된다. 이 신호의 시간 영역 신호 s_1과 s_2에 사이클릭 프레픽스를 추가하여 송신하게 되는데 그 신호를 수신기에서 푸리에 변환하여 주파수 영역신호로 표현하면 다음과 같다.

$$\begin{aligned} Y(2m) &= S_1(2m)H_1(2m) \\ &\quad +S_1(2m+1)H_2(2m)+N(2m) \\ Y(2m+1) &= S_1^*(2m+1)H_1(2m+1) \\ &\quad -S_1^*(2m)H_2(2m+1)+N(2m+1) \end{aligned} \tag{34}$$

Table 2 Eight kinds of methods for using Walsh code in the receiver

Walsh code 3bit value	000	001	010	011
SFBC method	a	b	c	d
Rx signals	$H_1(2m)$ $\Leftarrow -H_1(2m)$	$H_2(2m)$ $\Leftarrow -H_2(2m)$	$H_1(2m)$ $\Leftrightarrow H_2(2m)$ $S_1(2m)$ $\Leftarrow S_1^*(2m+1)$ $S_1(2m+1)$ $\Leftarrow S_1^*(2m)$	$H_1(2m)$ $\Leftrightarrow H_2(2m)$ $S_1(2m)$ $\Leftarrow -S_1^*(2m+1)$ $S_1(2m+1)$ $\Leftarrow -S_1^*(2m)$
Walsh code 3bit value	100	101	110	111
SFBC method	e	f	g	h
Rx signals	$H_1(2m)$ $\Leftrightarrow H_2(2m)$ $S_1(2m)$ $\Leftarrow S_1(2m+1)$ $S_1(2m+1)$ $\Leftarrow -S_1(2m)$	$H_1(2m)$ $\Leftrightarrow H_2(2m)$ $S_1(2m)$ $\Leftarrow -S_1(2m+1)$ $S_1(2m+1)$ $\Leftarrow S_1(2m)$	$H_1(2m)$ $\Leftrightarrow H_2(2m)$ $S_1(2m)$ $\Leftarrow -S_1(2m+1)$ $S_1(2m+1)$ $\Leftarrow -S_1(2m)$	$H_1(2m)$ $\Leftrightarrow H_2(2m)$ $S_1(2m)$ $\Leftarrow S_1(2m+1)$ $S_1(2m+1)$ $\Leftarrow S_1(2m)$

위 식과 같은 수신기 신호를 주파수 영역에서 구하면 주파수 영역 추정 신호 $S_1(2m)$ 과 $S_1(2m+1)$는 다음 식을 통하여 계산할 수 있게 된다.

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

$$S_1(2m+1) = \frac{H_2^*(2m)Y(2m) + H_1(2m)Y^*(2m+1)}{|H_1(2m)|^2 + |H_2(2m)|^2} \quad (35)$$

최종적으로 N 개의 블록 신호들을 모두 모아서 하나의 블록으로 구성하여 푸리에 역변환함으로써 송신 데이터를 추정할 수 있게 된다. 이와 같은 신호 구성은 채널 $H_1(2m)$이 $H_2(2m)$와 서로 바뀌었음을 의미하며 또한 송신신호 $S_1(2m)$은 $S_1(2m+1)$로 그리고 $S_1(2m+1)$은 $S_1(2m)$으로 바뀐 것과 같다는 것을 알 수 있다. 이 방법을 아래의 다른 결합 방법과 구별하기 위하여 공간 주파수 블록 코드 방법 h 라 한다. 이상과 같은 월시코드와 8 가지 공간 주파수 블록코드 방법들과 최종적인 수신 신호 결합 방법들 간의 관계를 Table 2와 같이 제시한다. 이것을 구현하는 경우의 추가적인 블록은 칩 설계에서 부동 소숫점 데이터 교환기가 될 것으로 보이며, 4 개의 부동 소숫점 데이터 교환기가 필요하다. 수신기에서의 결합 방법은 난수인 3 비트의 월시코드로 8가지 공간 주파수 블록 코드 방법 중 하나로 결정되며 해당 공간 주파수 블록 코드의 결합 방법은 외부 수신기의 경우에는 알아내기 어려워 공개된 전파라 하더라도 정확한 데이터 검출은 어렵게 된다. 3장에서는 모의실험 및 성능 비교에 관하여 기술하였으며 월시 코드를 사용하여 공간 주파수 블록 코드 8가지 모드 중 하나를 활용하는 데이터 보호 알고리즘의 성능과 난수 월시 코드를 전혀 알지 못하는 또는 부분적으로 알아낸 외부 침입 수신기들에서의 성능과 비교하였다.

3. 모의실험 및 성능 비교

3.1 실험환경

단일 반송파 시스템인 모의실험 환경에서 실험 변수들은 다음과 같다. 전체 주파수 대역은 20MHz 대역이며 데이터 블록들은 N=512 개로 구성된다. 하나의 데이터 심볼 주기는 26.4μs이며, 유효 심볼 주기는 25.6μs 그리고 보호 구간은 0.8μs이다. 송신기에서의 데이터 페이로드는 512개, 보호구간은 16개인 데이터 심볼 528 개를 하나의 공간 주파수 블록 코드 그룹으로 묶어서 전송한다. 모의실험 환경의 채널로는 HiperLAN/2 채널 A를 사용하였으며 수신기에서 채널 상태 정보는 알고 있는 것으로 가정하였으며, 각 채널은 독립적인 레일리 페이딩을 겪고 각각 50 Hz의 도플러 주파수인 다중 채널 모델을 사용하였다. 또한 모의실험에 사용한 소스 데이터 심볼들은 채널 코덱을 거치지 않고

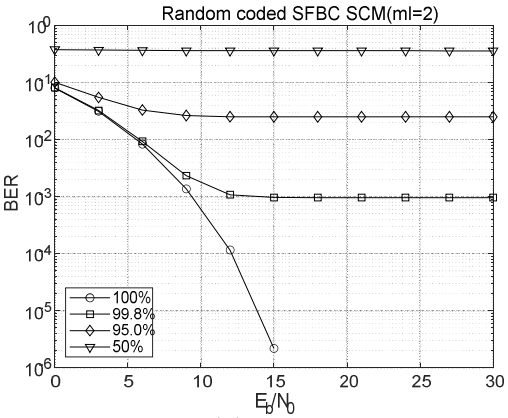
사용하였으며, 월시코드는 1024x1024를 사용하였고 이중 768 비트의 신호를 골라서 3 비트씩 256개의 그룹으로 묶여서 256개 그룹의 공간 주파수 블록 코드에 a, b, c, d, e, f, g, h와 같은 8가지 방법으로 수신 결합이 가능한 코드를 사용한다. 이월시코드를 100%, 99.8%, 95%, 50% 알고 있는 경우를 각각 100%, 99.8%, 95%, 50% 이렇게 4가지의 모의실험 환경에서 실험하였다. 난수코드를 알고 있는 비율의 선정은 오류 비율이 선형인 구간으로 선정하였다. 변조 수준은 무선 랜의 변조 방식인 2비트(QPSK), 4비트(16 QAM), 6비트(64 QAM)을 가정하여 실험하였다.

3.2 실험결과

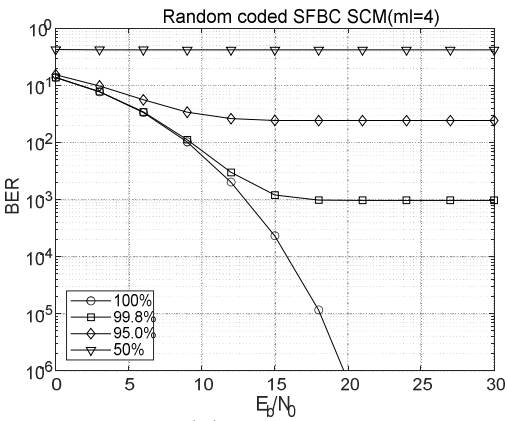
Fig. 3은 각 실험 결과를 보이는데, 50%의 코드를 알고 있는 경우는 수신 데이터의 오류율이 0.5에 가깝고, 95%, 99.8% 의 순서로 오류율이 줄어드는 것을 볼 수 있었다. 제안하는 난수 코드 방식(100%)은 정상적인 수신 성능을 보이고 있음을 알 수 있으며, 이와 같은 수신 성능은 변조 수준에 관계없이, QPSK, 16 QAM, 64 QAM 의 경우 모두 동일하게 나타났다. 이러한 수신 성능 결과로 보면, 코드를 전혀 모르는 외부 수신기의 경우에는 데이터의 검출이 통신에서 이론적 오류율의 최대치인 0.5에 가깝게 오류가 발생함을 알 수 있고, 코드를 우연히 알게 되는 경우 중 50%, 95%, 99.8% 확률로 난수 코드와 결합 방법 두 가지를 알고 있는 외부 수신기라 하더라도 데이터의 정상적인 송수신이 불가능하다고 볼 수 있다.

4. 결 론

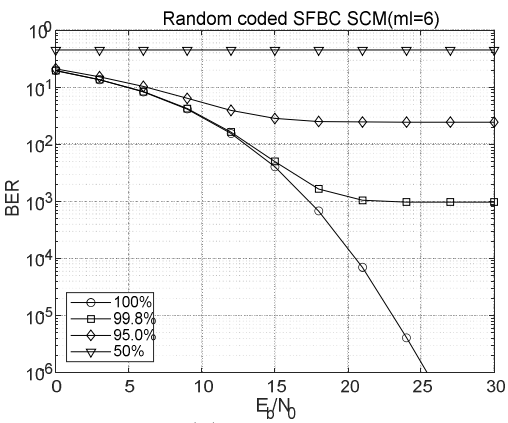
이 논문은 난수 코드를 활용하여 공간 주파수 블록 코드의 데이터를 보호하는 방법을 제안한다. 제안하는 알고리즘은 송신단에서는 주파수 축 방향으로 그리고 송신 안테나 축 방향으로 간단한 부호 반전을 적용하는 방법을 제안하였으며 난수 코드를 활용하는 이러한 방법들은 종



(a) QPSK



(b) 16 QAM



(c) 64 QAM

Fig. 3 Performance of the random coded Space-Frequency Block Code for Single Carrier Modulation

래의 방법보다 외부 수신기가 검출하기 어려운 방법을 제안하였다. 따라서 다중 송수신 안테나 규격 특히 공간 주파수 블록 코드를 사용하는 통신 시스템들에서 송수신기의 복잡도가 크게 증가하지 않는 간단한 데이터 보호방법을 제시하였다.

References

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), pp. 304-306, July

Alamouti S. (1988), "A simple transmit diversity technique for wireless communications," IEEE J. Select. Areas Commun., 16(8), pp. 1451-1458, Oct.

Bombal David (2020), https://www.youtube.com/watch?v=J8A8rKFZW-M, *Brute force WiFi WPA2*, Dec. 19.

Huh N. C., and KimS. (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), pp. 1003-1006, March

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 Codeing," *Journal of the Korea Industrial Information Systems*, 23(5), pp. 1-8, Oct.

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), pp. 567-570. Feb.

Jung H. K. (2020), "Sign Reversal Channel Switching Method for Space-Frequency Block Code in Orthogonal Frequency Division Multiplexing System," *Journal of the Korea Industrial Information Systems Research*, 25(5), pp. 13-21. Oct.

Jung H. K. (2021), "Random Coded Data Protection Technique in Space-Time Block Code," *The Trans. of the Korea Institute of Electrical Engineers*, 70P(4), pp. 270-276. Dec.

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

Strang G. (1988), *Linear algebra and its applications*, 3rd ed., Harcourt Brace & company

정 혁 구 (Hyeok-Koo Jung)

- 정회원
- 연세대 전기공학과 공학학사
- 연세대 전기공학과 공학석사
- 중앙대 전자공학과 공학박사
- (현재) 한밭대학교 정보기술대학 모바일융합공학과 교수
- 관심분야: 무선통신, 딥러닝 신호처리