논문 21-46-01-04 The Journal of Korean Institute of Communications and Information Sciences '21-01 Vol.46 No.01
https://doi.org/10.7840/kics.2021.46.1.32

OFDM 시스템의 물리계층 보안을 위한 랜덤 라틴방진 기반 고속주파수 도약 기법

현 석 준•, 백 호 기*, 임 재 성°

Random Latin Square Based Fast Frequency Hopping Scheme for Physical Layer Security in OFDM Systems

Seokjun Hyeon•, Hoki Baek*, Jaesung Lim°

요 약

최근 UAV, 지능형무기체계와 같은 새로운 군용 플랫폼의 원격운용은 물론 고용량의 지휘정찰 전술정보를 전송할 수 있는 고효율 OFDM(Orthogonal Frequency Division Multiplexing) 웨이브폼 기반의 전술데이터링크 도입 필요성이 대두되고 있다. Link-16과 같은 종래의 전술데이터링크 시스템에는 FHSS (Frequency Hopping Spread Spectrum) 기술을 적용하여 높은 저피탐 성능을 보장해왔다. 하지만 OFDM 시스템은 넓은 주파수 대역을 이용하는 특성으로 인해 FHSS 기법을 그대로 적용하는 것에는 많은 제약이 존재한다. 따라서 본 논문에서는 이를 해결할 수 있는 방식으로서 FFH(Fast Frequency Hopping) OFDM에 라틴 방진(Latin Square)을 적용한 고속 주파수 도약 기법(SecFFH/OFDM)을 제안한다. 이는 OFDM 심볼 시간 내에서 하나의 심볼이 시스템의 모든 부반송파를 랜덤 도약하는 방식으로, 도약 패턴을 알고 있는 송/수신단만이 정상적인 송/수신을 가능하게 하는 비화통신을 제공한다. 이에 대한 검증을 MATLAB으로 수행하였으며, 제안하는 기법의 암호화 성능 분석 또한 보인다.

Key Words : Tactical Datalink, Frequency Hopping, OFDM(Orthogonal Frequency Division Multiplexing), Secure Communication, Physical Layer Security

ABSTRACT

Recently, there is a need to introduce a tactical data link using a high-efficiency OFDM (Orthogonal Frequency Division Multiplexing) waveform capable of transmitting high-capacity command and reconnaissance tactical information as well as remote operation of new military platforms such as intelligent weapon systems such as UAVs. In the conventional tactical data link system such as Link-16, FHSS (Frequency Hopping Spread Spectrum) technology has been applied to ensure a high level of low detectability. However, since the OFDM system uses a wide frequency bandwidth, there are many limitations to applying the FHSS technique as it is. Therefore, in this paper, we propose a fast frequency hopping technique (SecFFH/OFDM) that applies Latin Square to FFH (Fast Frequency Hopping) OFDM as a solution to this problem. This is a method in which one symbol randomly hops all subcarriers of the system within the OFDM symbol time, and provides

※ "본 연구는 방위사업청과 국방과학연구소가 지원하는 미래전투체계 네트워크기술 특화연구센터 사업의 일환으로 수행되었음.(UD190033ED)"
• First Author : Republic of Korea Air Force, sjheun1117@ajou.ac.kr, 정회원
° Corresponding Author : Department of Military Digital Convergence, Ajou University, jaslim@ajou.ac.kr, 종신회원
* Department of Military Digital Convergence, Ajou University, neloyou@ajou.ac.kr, 종신회원
논문번호 : 202009-232-A-RN, Received September 21, 2020; Revised October 10, 2020; Accepted October 13, 2020

secret communication in which only the transmitting end and the receiving end knowing the hopping pattern can communicate normally. In order to verify this, it was performed in MATLAB, and it was verified that the proposed technique can be used as a physical layer encryption technique requiring low detectability.

Ⅰ. 서 론

전술데이터링크는 표적정보, 피아식별정보, 작전식별정보 등의 다양한 전술 데이터를 각종 무기체계 및 지휘통제체계와 같은 전략자산에 공유하여 네트워크 기반 효과중심작전을 수행할 수 있도록 하는 통신 체계이다.

전술정보의 공유는 군사작전 체계의 특성상 전술데이터링크를 통해 공유되는 모든 정보는 암호화를 통해 적에게 그 내용이 노출되지 않아야 한다. 이러한 목적으로 Link-16[1]에서는 암호화를 MSEC(Message Security), TSEC(Transmission Security)의 두 가지 방식을 통해 수행한다. MSEC의 경우 암호화 알고리즘을 통해 메시지 레벨의 암호화를 지원하며, TSEC의 경우 지터, 의사 잡음 부호, 주파수 도약 기법을 통해 신호 레벨의 암호화를 지원한다. 이 중에 주파수 도약 기법은 초당 77000회의 매우 빠른 주파수 도약을 통해 도약 패턴을 모르는 적으로부터의 도청을 방지할 수 있다.[2]

최근 각종 무기체계들의 지능화 및 네트워크화에 따라 공유해야 할 전술정보 데이터의 양이 점점 방대해지고 있으며, 특히 사진 및 영상과 같은 고용량 전술정보의 실시간 전송을 위해 OFDM 웨이브폼 기반 전술데이터링크의 설계가 필요하다. OFDM 기술은 최근 수년 동안 IEEE 802.11, LTE, 5G NR과 같은 상용 무선네트워크 물리계층 표준에 적용되어 비약적인 전송속도 향상을 가져왔다. 하지만 주파수 도약 기법을 OFDM 시스템에 그대로 적용하는 것은 현실적으로 많은 제약이 있다.

OFDM 시스템에서 데이터 전송에 앞서 송/수신단 간의 채널 상태 정보의 획득 및 공유는 매우 중요한 과정이다. 채널 상태 정보는 채널의 주파수 응답 특성이므로, 시스템에서 사용하는 전체 대역폭에 걸쳐서 획득되어야 하지만, 반송파를 도약하는 주파수 도약 OFDM 기법에서 넓어진 대역폭에 대한 채널 추정을 위한 프리앰블(Preamble) 전송은 통신시스템의 지나친 오버헤드(Overhead)로서 작용한다. 이러한 문제를 해결하기 위하여 임베디드(Embedded) 형태의 프리앰블 동기화 기법[3]을 고려해볼 수 있으나, 이 경우에도 시스템이 점유하는 주파수 폭이 지나치게 비대해지는 근본적인 문제를 해결할 수 없다. 이를 해결하기 위해서 Fast- Frequency-Hopping OFDM(FFH/OFDM)에 대한 연구[4,5]가 제안되어 반송파의 도약이 아닌 데이터 심볼간의 OFDM 부반송파 순환 도약을 통해 대역폭의 비대화 없이 주파수 선택적 페이딩(Frequency Selective Fading) 환경에서 효과적인 다이버시티(Diversity) 이득을 얻을 수 있음을 보여주었다.

본 논문에서는 FFH/OFDM 시스템에 랜덤 라틴 방진 기반의 고속 주파수 도약기법(SecFFH/OFDM)을 제안한다. 이는 기존의 반송파 도약 OFDM 기법들이 갖는 근본적인 문제점인 대역폭 비대화를 극복하면서 OFDM신호의 물리계층 암호화를 제공할 수 있다. 또한, 기존 FFH/OFDM의 순시주파수 행렬의 라틴 방진 특성을 유지하며 랜덤화하는 과정을 통해 FFH/OFDM 기법이 갖는 주파수 다이버시티 이득을 유지할 수 있다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 제안하는 기법의 원형인 FFH/OFDM 기법을 소개한다. 3장에서는 제안하는 라틴 방진 기반 고속 주파수 도약 OFDM을 기술한다. 그리고 4장에서는 MATLAB을 이용한 모의실험을 통해 제안한 기법의 효과성을 입증하고, 마지막으로 5장에서는 결론을 통해 연구의 핵심을 요약하며 끝맺는다.

Ⅱ. 기존 FFH/OFDM 기법

서론에서 언급했듯 FFH/OFDM[3]은 OFDM 시스템에서 중심주파수의 도약에 의한 시스템 대역폭 비대화를 방지할 수 있는 기법이다. 이는 송신단에서의 신호 생성 시 필요한 IDFT(이산 푸리에 역변환) 행렬을 행단위 순환 치환하여 새로운 IDFT 행렬을 생성하고, 이를 이용하여 OFDM 신호를 생성함으로써 하나의 심볼이 심볼 시간 안에 모든 부반송파를 순환 도약하도록 한다. 이를 통해 주파수 선택적 페이딩 환경에서 다이버시티 이득을 얻을 수 있다.

IDFT를 이용한 OFDM 신호 생성은 식 (1)과 같이 표현할 수 있다.

$$b = Dd \tag{1}$$

위 식에서 b는 OFDM 신호의 시간 영역 표본화 벡터, d는 부반송파에 할당될 심볼들을 원소로 갖는 벡터를 의미한다. D는 이산 푸리에 역변환 행렬을 나타내며, N개의 부반송파를 갖는 OFDM 시스템의 경우 D는 N차 정사각행렬이며, 벡터 b와 d는 $N\times 1$의 크기를 갖는 열벡터이다. 행렬 D의 성분은 식 (2)와 같다.

$$D(u,v)=e^{j2\pi(u-1)(v-1)/N}/\sqrt{N}\quad 1\le u,v\le N \tag{2}$$

식 (2)에서 u는 시간 영역 인덱스를, v는 부반송파 인덱스를 의미한다.

한편, FFH/OFDM 기법에서는 심볼의 부반송파 순환 도약을 위해 다음과 같은 N차 정사각행렬 Φ를 정의한다.

$$\Phi(u,v)=\mathrm{mod}(u+v-2,N)\quad 1\le u,v\le N \tag{3}$$

위 식에서 Φ는 주파수 도약을 위한 순시주파수를 나타내는 행렬이며, u는 시간 영역 인덱스, v는 OFDM 전송 전 병렬화된 심볼의 인덱스이다. 위와 같은 순시주파수 행렬에 의하여 하나의 심볼이 심볼 시간 안에 모든 주파수를 순환하며 도약하게 되며, 행렬 Φ를 이용하여 새롭게 정의된 고속 주파수 도약 OFDM 신호 생성을 위한 IDFT 행렬 D_{FFH}는 다음과 같이 정의된다.

$$D_{FFH}(u,v)=e^{j2\pi\Phi(u,v)(u-1)/N}/\sqrt{N}\quad 1\le u,v\le N \tag{4}$$

식 (4)에서 u는 시간 영역 인덱스를, v는 병렬화된 심볼 인덱스를 의미한다.

한편, 식 (4)에서 정의한 D_{FFH}를 이용한 FFH/OFDM 신호의 생성은 식 (1)과 유사하게 다음과 같이 정의할 수 있다.

$$b_{FFH}=D_{FFH}d \tag{5}$$

식 (5)의 b_{FFH}는 FFH/OFDM 신호에 대한 시간 영역에서의 표본화 벡터를 의미한다.

FFH/OFDM에 대한 디지털 신호 시스템에서의 실제적 구현을 위하여, 선형 선행부호화(Linear Pre-coding) 행렬 U을 통한 심볼벡터의 코딩을 먼저 수행한 후, 그 결과를 IDFT 행렬 D를 이용해 FFH/OFDM 심볼의 시간 영역 표본 벡터를 생성한다.

$$D_{FFH}d=DUd \tag{6}$$

식 (6)에 의하여 선행부호화 행렬 U는 다음과 같이 정의된다.

$$U=D^{-1}D_{FFH} \tag{7}$$

따라서 b_{FFH}는 식 (8)과 같이 표현된다.

$$b_{FFH}=DUd \tag{8}$$

한편, 심볼간 간섭(Inter Symbol Interference, ISI)을 방지하기 위해 신호 벡터 b_{FFH}의 성분 중 일부를 복사하여 순환 접두를 만들 수도 있으며, 이 경우 수신단에서 이에 대한 제거 또한 고려해야 한다.

선형 선행부호화 행렬 U에 의해 처리된 심볼 벡터 d_{FFH}를 다음과 같이 표현할 수 있다.

$$d_{FFH}=Ud \tag{9}$$

따라서 FFH/OFDM 기법은 행렬 U를 통해 전처리된 심볼 벡터 d_{FFH}를 IDFT 연산을 통해 전송하는 것과 동일하다고 볼 수 있다. 이렇게 생성된 신호는 무선 채널을 통해 전송된다.

Ⅲ. 제안하는 SecFFH/OFDM 기법

본 장에서는 FFH/OFDM 기법에 내재되어 있는 라틴 방진 성질을 소개하고, 이를 바탕으로 라틴 방진의 성질을 이용하여 물리계층 암호화를 수행하는 SecFFH/OFDM 기법을 소개한다.

라틴 방진이란 각 행과 열이 각각 주어진 값을 중복되지 않도록 포함하는 정사각행렬을 의미한다.

라틴방진의 크기를 $n\in N$이라 하고, n개의 원소를 갖는 유한집합을 Σ라고 하자(N은 자연수의 집합을 의미한다.). 이때 Σ의 원소를 라틴 방진의 '알파벳(Alphabet)'라고 정의한다. 집합 Σ에 대한 임의의 라틴 방진 행렬을 L이라고 하고, L의 i번째 행, j번째 열에 해당하는 원소를 L_{ij}라고 나타낸다면 L의 행벡터와 열벡터는 다음과 같은 성질을 갖는다.

$$\begin{aligned}\{L_{i1},L_{i2},\cdots,L_{in}\}&=\Sigma\ \ (i\in\{x\mid 1\le x\le n, x\in N\})\\ \{L_{1j},L_{2j},\cdots,L_{nj}\}&=\Sigma\ \ (j\in\{x\mid 1\le x\le n, x\in N\})\end{aligned} \tag{10}$$

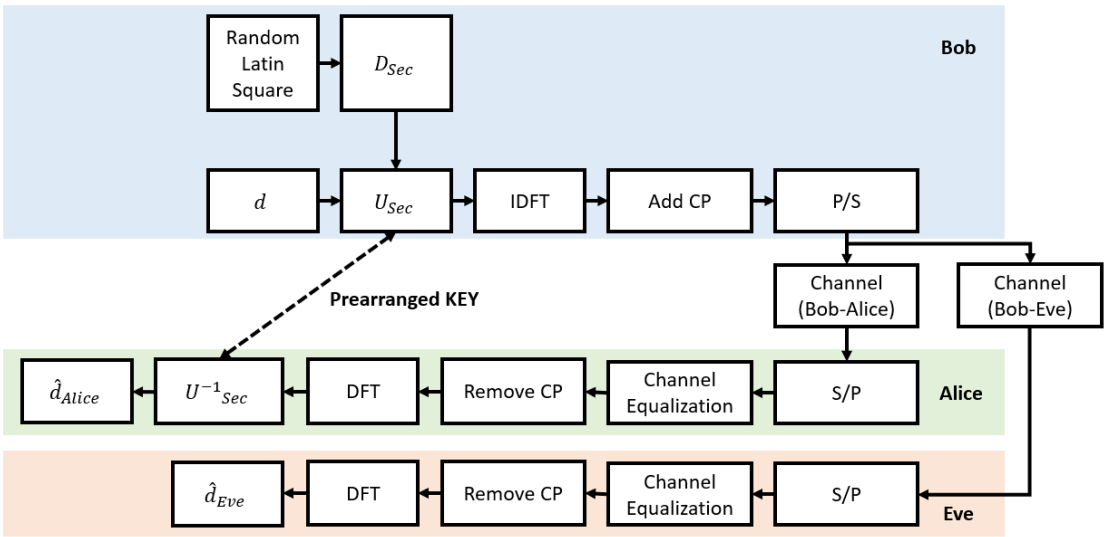


그림 1. SecFFH/OFDM 송수신단 블록선도
Fig. 1. Block diagram of SecFFH/OFDM transceiver

즉, L의 모든 행벡터와 열벡터는 Σ의 모든 알파벳을 중복 없이 포함한다.

앞서 살펴본 라틴 방진의 성질을 이용하면 FFH/OFDM 기법에 대한 물리계층 암호화를 수행할 수 있다. FFH/OFDM 기법에서, 식 (3)의 순시주파수 행렬의 열벡터는 심볼 시간 내에서 변화하는, 심볼 하나가 전송될 부반송파 주파수의 인덱스를 나타낸다. 즉, 부반송파 하나의 도약 패턴을 의미한다. 이때의 식 (3)의 순시주파수 행렬 Φ은 부반송파의 개수 N에 대하여, 0부터 $N-1$까지의 정수들을 알파벳으로 갖는 라틴 방진이다. 이를 통해 부반송파 하나의 도약패턴에 해당하는 Φ의 열벡터는 모든 부반송파 인덱스를 중복 없이 포함하여, 심볼 시간 동안 전체 시스템 대역에 대한 주파수 다이버시티 이득을 얻는다.

하나의 심볼이 특정 시간에 점유하고 있는 부반송파를 의미하는 Φ의 행벡터(이를테면, k번째 행벡터는 k번째 시간 영역 표본에서 각 심볼들이 점유하고 있는 부반송파 인덱스를 나타낸다.)는 중복 없는 성분을 가져야만 심볼 간의 충돌 없는 전송을 보장한다. 이를 도식으로 표현한 것이 그림 2이다.

따라서 FFH/OFDM의 주파수 다이버시티 이득을 보존하면서 물리계층 암호화를 위한 키 공간(Key Space)의 확보를 위한 방법으로, 집합 Σ의 원소들을 알파벳으로 갖는 다양한 형태의 라틴 방진을 순시주파수 행렬 Φ_{Sec}로 사용하여 이를 공유하는 송/수신단 간의 비화 통신의 구현이 가능하다. 본 논문에서는 Φ_{Sec}를 랜덤 라틴 방진 순시주파수 행렬이라고 명명하며, 다음과 같이 랜덤 라틴 방진 순시주파수 행렬을 생성한다.

우선, 순환형태의 라틴 방진 행렬을 앞서 살펴본 식 (3)과 동일하게 정의한다.

다음으로 1부터 N까지의 자연수들의 순열(Permutation)로 구성된 두 개의 벡터 p_1, p_2를 생성한다. 이를테면, $N=4$인 경우, $p_1=(1,4,3,2)$와 $p_2=(3,1,2,4)$의 벡터쌍이 하나의 예시가 될 수 있다. 기존에 잘 알려진 랜덤 순열 생성 알고리즘인 Fisher-Yates 셔플 알고리즘을 사용하여 이와 같은 벡

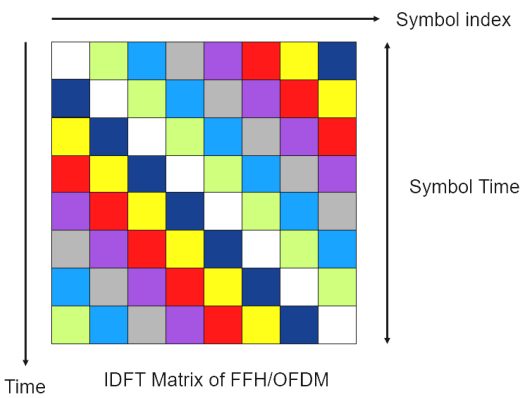


그림 2. N=8인 경우의 FFH/OFDM 주파수 도약 패턴
Fig. 2. Frequency Hopping Pattern of FFH/OFDM (N=8)

터를 생성할 수 있다. Fisher-Yates 셔플 알고리즘은 중복없는 원소들로 구성된 시퀀스를 임의로 섞는 알고리즘으로서, 시퀀스의 임의의 원소를 뽑아 새로운 리스트에 삽입하고, 뽑은 원소를 원래의 시퀀스에서 삭제하고 다시 임의의 원소를 뽑는 과정을 반복하여 시퀀스에 남은 원소가 없을 때 까지 이를 반복하여 완성된 리스트를 랜덤 순열의 결과로 이용하는 알고리즘이다. 본 논문에서는 N개의 부반송파를 갖는 SecFFH/OFDM 변조를 위하여 N차원 벡터인 p_1, p_2를 $p_0 = 1, 2, 3, \ldots, N$에 Fisher-Yates 알고리즘을 적용하여 생성한다.

마지막으로, 새로운 랜덤 라틴 방진 순시주파수 행렬을 다음과 같이 정의한다.

$$\Phi_{Sec}(u,v) = \Phi(p_1(u), p_2(v)) \tag{11}$$

식 (11)에서 $p_1(u), p_2(v)$는 각각 벡터 p_1, p_2의 u번째, v번째 성분을 의미한다. 식 (11)은 앞서 생성한 순환형태의 라틴방진 행렬 Φ을 p_1, p_2를 이용한 행간 섞음(Shuffle), 열간 섞음을 의미한다. Φ의 행벡터, 열벡터가 중복된 성분을 갖지 않으므로 이들의 행간 섞음, 열간 섞음을 통해 생성된 Φ_{Sec}의 행벡터, 열벡터가 중복된 성분을 갖지 않다는 것은 자명하며, 이에 따라 Φ_{Sec}은 모든 행벡터, 열벡터가 직교하는 라틴방진 특성을 만족하고, 이를 통해 주파수 다이버시티 이득을 달성할 수 있다. 다음은 $N=8$, $p_1 = (3, 7, 5, 1, 2, 8, 4, 6)$, $p_2 = (4, 6, 2, 3, 1, 5, 8, 7)$ 인 경우 생성된 Φ_{Sec}의 예시이다.

$$\Phi_{Sec} = \begin{pmatrix} 5\ 7\ 3\ 4\ 2\ 6\ 1\ 0 \\ 1\ 3\ 7\ 0\ 6\ 2\ 5\ 4 \\ 7\ 1\ 5\ 6\ 4\ 0\ 3\ 2 \\ 3\ 5\ 1\ 2\ 0\ 4\ 7\ 6 \\ 4\ 6\ 2\ 3\ 1\ 5\ 0\ 7 \\ 2\ 4\ 0\ 1\ 7\ 3\ 6\ 5 \\ 6\ 0\ 4\ 5\ 3\ 7\ 2\ 1 \\ 0\ 2\ 6\ 7\ 5\ 1\ 4\ 3 \end{pmatrix} \tag{12}$$

N개의 부반송파를 갖는 SecFFH/OFDM 시스템에서, Φ_{Sec}은 크기가 N이며 알파벳 집합 $\Sigma = \{0,1,\cdots N-1\}$에 대한 랜덤 라틴 방진이 된다. 한편, 일반적으로 크기가 N인 라틴 방진의 종류는 $N!*(N-1)!$가지로 알려져 있으며, 이에 따라 비화통신에 사용되는 키 영역(Key Space)의 크기가 결정된다.

이렇게 생성된 순시주파수 행렬 Φ_{Sec}을 바탕으로 SecFFH/OFDM 시스템의 이산 푸리에 역변환 행렬 D_{Sec}을 다음과 같이 정의할 수 있다.

$$D_{Sec}(u,v) = e^{j2\pi\Phi_{Sec}(u,v)(u-1)/N}/\sqrt{N}\ 1 \le u,v \le N \tag{13}$$

식 (13)에서 u는 시간 인덱스, v는 부반송파에 실릴 심볼의 인덱스이다. 앞서 살펴본 FFH/OFDM 기법과 같이 다음과 같은 연산을 통해 선형 전처리행렬 U_{Sec}을 계산한다.

$$U_{Sec} = D^{-1}D_{Sec} \tag{14}$$

송신단과 수신단은 비화통신을 위하여 U_{Sec}행렬을 암호(Key)로서 반드시 사전에 공유하고 있어야만 한다.

전송해야 할 데이터 심볼 벡터를 d라고 하면, 시간 영역에서 표본화 된 SecFFH/OFDM 신호 벡터 b_{Sec}은 다음과 같이 표현된다.

$$b_{Sec} = DU_{\mathrm{sec}}d \tag{15}$$

페이딩 채널을 통해 수신단에게 전송된 시간 영역 표본화 신호에는 수신단에서의 가우시안 열잡음이 포함되고, 수신단은 이에 대한 DFT 연산을 통하여 SecFFH/OFDM 심볼을 복조한다.

$$\hat{d}_{Sec} = H_f^{-1}e_f = D^{-1}b_{Sec} + H_f^{-1}n_f \tag{!6}$$

식 (16)에서 e_f는 수신단이 수신한 심볼의 주파수 영역 표현으로, 식 (17)와 같이 표현된다.

$$e_f = H_f D^{-1}b + n_f \tag{17}$$

마지막으로 수신단은 송신단과 사전에 공유한 암호화 행렬 U_{Sec}의 역행렬을 $\hat{d}_{Sec}$에 곱하여 원본 심볼 벡터 $\hat{d}$를 얻어낸다.

$$\hat{d} = U_{Sec}^{-1}\hat{d}_{Sec} \tag{18}$$

그림 1.은 SecFFH/OFDM 시스템의 도식이다. 송신자 Bob이 인가(legal)된 수신자 Alice에게 데이터를 전송할 때, 도청자 Eve가 신호를 탈취하여 원본 신호

에 대한 복조를 시도한다. 그러나 Eve는 사전에 정의된 암호인 을 공유하지 않으므로 정상적인 복조가 불가능하다.

SecFFH/OFDM 기법은 기존 주파수 도약 시스템과 달리 국부발진기의 주파수를 직접 조작하는 것이 아닌, 전송할 심볼 벡터에 선형 선행부호화 행렬을 곱하여 부반송파를 도약하는 것과 같은 효과를 얻을 수 있어 실제 시스템 적용에 용이하다는 장점이 있다.

Ⅳ. 모의 실험

4.1 모의실험 환경

본 논문에서 제안하는 SecFFH/OFDM 시스템의 모의실험 구성은 다음과 같다. 128개의 부반송파를 사용하는 OFDM 시스템에 대하여 100회의 심볼 타임 동안 총 12,800개의 심볼을 전송하였으며, 심볼 변조 방식으로는 16-QAM을 사용하였다. FFT를 수행하는 행렬연산의 특성으로 인해 심볼은 하나의 심볼타임 안에서 128회의 주파수 도약을 실시한다. 하나의 심볼은 144개의 시간 영역 표본으로 구성되며, 이는 순환 전치 영역의 표본 16개와 IDFT로 생성된 128개의 표본으로 구성된다.

표 1. 시뮬레이션 파라미터
Table 1. Simulation parameters

파라미터	값
부반송파 개수	128 개
심볼 전송 횟수	100 회
심볼 변조 방식	16-QAM
심볼 길이	144 (128+16) 표본
총 비트 개수	51200 개

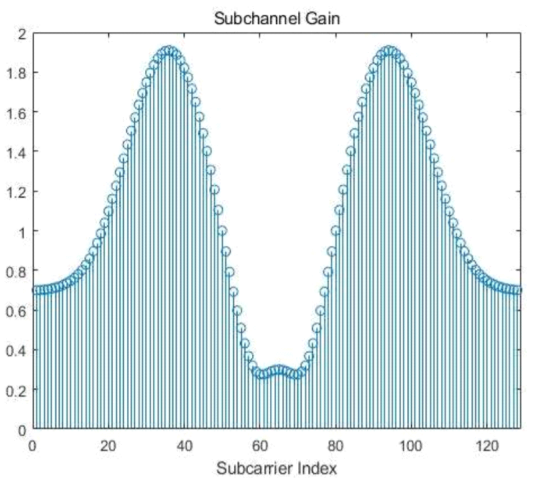


그림 3. 주파수 선택적 페이딩을 겪는 Bob-Eve간 무선 채널의 임펄스 응답
Fig. 3. Impulse Response of Frequency Selective Fading Channel between Bob and Eve

송신자 Bob이 전송한 신호는 주파수 선택적 페이딩 채널을 통해 전달되고, Alice또는 Eve는 주파수 선택적 페이딩 채널을 통과한 신호와 각자의 수신기에서 발생하는 AWGN가 섞인 신호를 수신하게 된다. 그림 3은 Bob-Eve간의 주파수 선택적 페이딩 채널의 채널 임펄스 응답을 표현한다.

4.2 모의실험 결과

이번 절에서는 제안하는 SecFFH/OFDM 기법의 성능 평가를 위하여 진행한 MATLAB을 활용한 모의실험 결과를 확인하고 분석한다. 주파수 선택적 페이딩 환경에서 AWGN의 영향을 받아 수신단의 신호 세기에 따라 SNR의 값이 달라지는 환경에서의 비트 에러율(BER)을 확인하였다.

그림 4를 통해 알 수 있듯, SecFFH/OFDM 기법이 기존 FFH/OFDM 기법과 같은 수준의 주파수 다이버시티 이득을 얻어낸다는 것을 알 수 있다. 또한 올바른 복호화 키 U_{Sec}를 갖지 못한 Eve는 정상적인 수신이 불가능하다는 것을 알 수 있다.

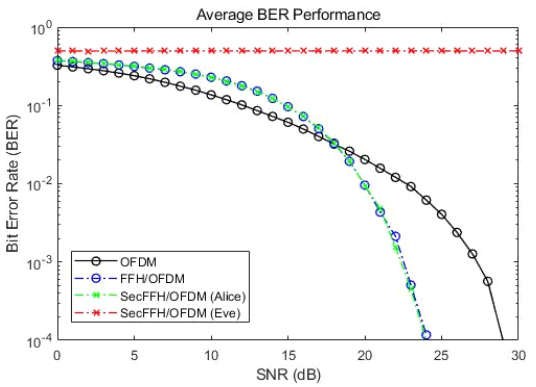


그림 4. SNR값에 따른 BER 비교
Fig. 4. Comparison of BER according to SNR

4.3 SecFFH/OFDM 물리계층 보안 성능 분석

본 논문에서 제안하는 SecFFH/OFDM의 암호화 성능은 암호화키로서 생성 가능한 U_{Sec}의 가짓수에 따라 그 키 공간(Key Space)의 크기가 결정된다고 볼 수 있다. 크기가 N인 라틴 방진에 대하여 그 종류가 $N!*(N-1)!$인 것으로 알려져 있으므로[6] N개의 부반송파를 갖는 OFDM 시스템은

표 2. 표준 무선네트워크 규격에서의 키 공간
Table 2. Key Space Size in Standard Wireless Network Specification

데이터 부반송파 개수 (N)	암호화 수준 ($f(N)$)
48 (802.11a)	3.21×10^{120}
52 (802.11n/20MHz)	1.25×10^{134}
108 (802.11n/40MHz)	1.62×10^{346}
162 (LTE/3MHz)	9.33×10^{575}
560 (LTE/10MHz)	2.29×10^{2592}
1080 (LTE/20MHz)	8.27×10^{5614}

$f(N) = N!*(N-1)!$의 키 공간을 갖는다고 할 수 있다. 표 2는 여러 가지 표준 무선네트워크 규격에서 SecFFH/OFDM를 적용하였을 때의 키 공간 크기를 나타낸다.

한편, SecFFH/OFDM의 선형 전처리행렬 U_{Sec}에 의한 심볼 은닉으로 인해 동기수신이 가능한 수신단에서의 성상도(Constellation Map)는 그림 5과 같이 나타난다.

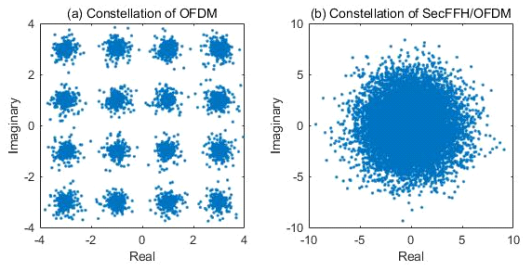


그림 5. OFDM과 SecFFH/OFDM의 16-QAM 성상도 비교
Fig. 5. 16-QAM constellation of SecFFH/OFDM

V. 결 론

본 논문에서는 라틴 방진의 다양성을 이용하여 OFDM의 물리계층 암호화를 수행할 수 있는 SecFFH/ OFDM 기법을 제안하였다. 모의실험을 통해 SecFFH/OFDM 기법을 적용하였을 때 기존 FFH/OFDM의 주파수 도약을 통해 얻을 수 있는 주파수 다이버시티 이득을 그대로 가져가면서, 라틴 방진의 특성으로 얻어지는 키 공간의 확보를 통해 비화 통신이 가능함을 보였다.

References

[1] H. Baek, S. Jung, and J. Lim, "Survey of tactical data link technology for network centric operations," *Commun. Korean Inst. Inf. Sci. and Eng.*, vol. 28, no. 7, pp. 56-69, 2010.

[2] J. Yu, H. Noh, H. Baek, and J. Lim, "Multinet performance evaluation of tactical data link according to the number of channels and frequency hopping rate in UHF," in *KICS Summer Conf.*, pp. 43-44, 2014.

[3] L. Mailaender, "Anti-jam communications using frequency-hopped OFDM and LDPC with erasure decoding ("Minotaur")," *2013 IEEE MILCOM 2013*, San Diego, CA, USA, Nov. 2013.

[4] T. Scholand, T. Faber, A. Seebens, J. Lee, J. Cho, H. W. Lee, and P. Jung, "Fast frequency hopping OFDM concept," *IEEE Electron. Lett.*, vol. 41, no. 13, Jun. 2005.

[5] Y. Liu, X. Li, and X. Xu, "A broadband transmission technology based on FFH-OFDM," *2018 8th LISS*, pp. 1-5, Toronto, ON, Canada, Aug. 2018.

[6] A. D. Keedwell and J. Denes, "*Latin squares and applications*," 2nd Ed., North-Holland, 2015.

현 석 준 (Seokjun Hyeon)

2020년 2월 : 아주대학교 국방디지털융합학과 학사
2020년 6월~현재 : 대한민국 공군
<관심분야> OFDM 기반 전술 데이터링크, 무선네트워크, 인공지능 통신시스템, 국방전술통신

백 호 기 (Hoki Baek)

2006년 2월 : 아주대학교 정보 및 컴퓨터공학 학사

2008년 2월 : 아주대학교 정보통신공학 석사

2014년 2월 : 아주대학교 컴퓨터공학 박사

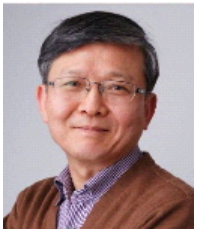
2014년 3월~2015년 2월 : 아주대학교 장위국방연구소 전임연구원

2015년 3월~현재 : 아주대학교 국방디지털융합학과 강의교수

<관심분야> 5G/6G 통신네트워크, UAV 통신네트워크, IoT, 국방전술통신, 시간동기, 위치인식

[ORCID:0000-0001-9213-7845]

임 재 성 (Jaesung Lim)



1983년 2월 : 아주대학교 전자공학 학사

1985년 2월 : KAIST 영상통신 석사

1994년 2월 : KAIST 디지털통신 박사

1998년 3월~현재 : 아주대학교 국방디지털융합학과 교수

2004년 3월~현재 : 아주대학교 국방전술네트워크 연구센터장

<관심분야> 이동 및 위성통신, 무선네트워크, 국방전술통신

[ORCID:0000-0003-0080-9398]