

레터논문 (Letter Paper)

방송공학회논문지 제28권 제1호, 2023년 1월 (JBE Vol.28, No.1, January 2023)

<https://doi.org/10.5909/JBE.2023.28.1.145>

ISSN 2287-9137 (Online) ISSN 1226-7953 (Print)

# MIMO 시스템에서 옥토니언 시공간 부호를 이용한 물리계층 보안에 대한 성능 분석

김영주<sup>a)†</sup>, 곽범근<sup>a)</sup>, 임슬민<sup>a)</sup>, 진천덕<sup>b)</sup>

## Performance Evaluation of Octonion Space-Time Coded Physical Layer Security in MIMO Systems

Young Ju Kim<sup>a)†</sup>, BeomGeun Kwak<sup>a)</sup>, Seulmin Lim<sup>a)</sup>, and Cheon Deok Jin<sup>b)</sup>

### 요약

송신 안테나 수가 4개인 다중 송수신 안테나 시스템에서 랜덤 위상을 갖는 오픈 루프 옥토니언 시공간 블록 부호를 적용했을 때, 불법적인 수신자가 최대 유사도 추정으로 물리계층을 해킹하는 경우의 성능을 분석한다. 합법적 수신자만 알 수 있는 무작위 위상을 불법적 수신자인 해커가 전혀 모르거나 일부를 알아냈을 때 신호 대 잡음비에 따른 비트 에러율을 분석한다. 또한 기존 논문의 옥토니언 부호가 직교성이 충분하지 않음을 보이고 완전한 직교성을 갖는 옥토니언 부호를 적용한다. 컴퓨터 시뮬레이션에서 랜덤위상은 2-PSK 성운으로 하고 있다는 것을 해커가 알고 있고 4개 송신 안테나의 랜덤 위상을 모두 해커가 추정할 경우에는 신호 대 잡음비가 100dB까지 해킹이 불가능하다. 그러나 랜덤 위상의 일부를 알게 되면 신호 대 잡음비가 20dB 이상에서 비트에러율이  $10^{-3}$  정도로 유지되므로 해킹이 가능해진다.

### Abstract

Open-loop Octonion space-time block code for 4 transmit antenna system is considered and random phases are applied to 4 transmit antennas for physical layer security. When an illegal hacker estimates the random phases of 1 through 4 transmit antennas with maximum likelihood (ML), this letter analyzes the bit error rate (BER) performances versus signal-to-noise ratio (SNR). And the Octonion code in the literature<sup>[1]</sup> does not have full orthogonality so, this letter employs the perfect orthogonal Octonion code. When the hacker knows that the random phases are 2-PSK constellations and he should estimate all the 4 random phases, the hacking is impossible until 100dB. When the hacker possibly know that some of the random phases, bit error rate goes down to  $10^{-3}$  so, the transmit message could be hacked.

Keyword : physical layer security, MIMO, diversity, space-time codes, hacking

a) 충북대학교 전자정보대학 정보통신공학부(College of Electrical and Computer Eng., School of Information and Communication, Research Institute for Computer and Information Communication, Chungbuk National University)

b) (우)휴로 (Huro)

† Corresponding Author : 김영주(Young-Ju Kim)

E-mail: yjkim@cbnu.ac.kr

Tel: +82-43-261-3375

ORCID: <https://orcid.org/0000-0002-5844-8612>

※ This work was supported by the International Science & Business Belt support program, through the Korean Innovation Foundation funded by the Ministry of Science and ICT.

· Manuscript November 20, 2022; Revised December 20, 2022; Accepted December 20, 2022.

Copyright © 2023 Korean Institute of Broadcast and Media Engineers. All rights reserved.

“This is an Open-Access article distributed under the terms of the Creative Commons BY-NC-ND (<http://creativecommons.org/licenses/by-nc-nd/3.0>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited and not altered.”

## 1. 서론

무선 통신은 근본적으로 송신 신호를 다수에게 전송하게 되어 항상 보안의 문제를 가지고 있다. 5세대 이동통신이 상용화 되면서 다양한 무선 모듈을 탑재한 기기들의 수가 급격히 증가하면서 더욱 해킹의 위험성도 증가한다. 본 논문은 물리계층 보안에 관한 것으로 무선 채널 정보를 송신기가 필요로 하지 않는 개회로(開回路) 방식의 시공간 블록 부호를 적용한 물리 계층의 보안에 관한 연구이다<sup>[1-4]</sup>. 기존의 연구에서는<sup>[2]</sup> 송신 안테나가 2개일 경우 랜덤 위상을 갖는 알라무티 부호를 적용한 시스템에서 신호 대 잡음비에 따른 비트 에러율을 분석하여 높은 신호 대 잡음비에서 도청의 위험이 있음을 보였다. 본 논문은 송신 안테나가 4개인 MIMO 시스템에 옥토니언 부호를 적용하고 송신 안테나에 합법적 수신자와 공유하는 랜덤 위상을 적용한다. 만약 불법적 수신자가 랜덤 위상의 일부를 알게 되는 경우의 성능을 분석한다. 신호 대 잡음비가 증가함에 따라 옥토니언 부호의 경우도 해킹이 될 수 있음을 보인다. 또한 기존 논문에서<sup>[1]</sup> 제시된 옥토니언 시공간 블록 부호의 식이 완전한 직교성을 보이지 않음을 밝힌다. 본 논문에서는 완전한 직교성을 가지는 옥토니언 시공간 블록 부호를<sup>[3]</sup> 이용한다.

## II. 시스템 모델

송신자는 합법 수신자에게 옥토니언 시공간 블록부호를

이용하여 신호를 전송한다. 합법 수신자 외의 불법 도청자는 송신 신호의 수신을 못 하도록 그림 1에 보이듯이 위상  $\theta_1, \theta_2, \theta_3, \theta_4$ 을 송신 안테나별로 랜덤하게 발생시켜 신호 성운을 회전시킨다. 세 개의 송신 신호  $S_1, S_2, S_3$ 를 옥토니언 시공간 블록 부호화를 하여 네 개의 안테나에 서로 독립적인 위상 회전을 하여 네 개의 시간 슬롯으로 전송한다. 식 (1)과 같이 옥토니언 부호를 행렬로 표현할 수 있다.

$$C(s_1, s_2, s_3, \theta_1, \theta_2, \theta_3, \theta_4) = \begin{pmatrix} s_1 e^{j\theta_1} & s_2 e^{j\theta_2} & s_3 e^{j\theta_3} & 0 \\ -s_2^* e^{j\theta_1} & s_1^* e^{j\theta_2} & 0 & -s_3 e^{j\theta_4} \\ -s_3^* e^{j\theta_1} & 0 & s_1^* e^{j\theta_3} & s_2 e^{j\theta_4} \\ 0 & s_3^* e^{j\theta_2} & -s_2^* e^{j\theta_3} & s_1 e^{j\theta_4} \end{pmatrix} \quad (1)$$

옥토니언 부호는 완전한 직교성이 유지되므로  $CC^H = (|s_1|^2 + |s_2|^2 + |s_3|^2)I_4$ 이다. 이때,  $I_4$ 는 4차 단위행렬이다. 한편 기존 논문에서 사용된 옥토니언 부호의 식은 완전한 직교성을 보이지 않는다<sup>[1]</sup>. 기존 논문의 성능 시뮬레이션에서는 직교성을 갖는 옥토니언 부호를 이용했을 것으로 보이는데, 부호의 표기에서 오류가 발생한 것으로 보인다. 기존 논문에 표기된  $CC^H$ 의 행렬을 구해보면 수식 (2)와 같다<sup>[1]</sup>.

16개 원소 중에서 대각 원소를 제외하고 12개 원소가 0이 되어야 하는데, 8개 원소만 0이 된다. 따라서 직교성이 유지되지 못하므로 비트에러율이  $10^{-3}$  이하로 내려가지 않는 문제가 발생한다.

송신자와 합법 수신자는 비밀 키를 공유하고 유사 랜덤

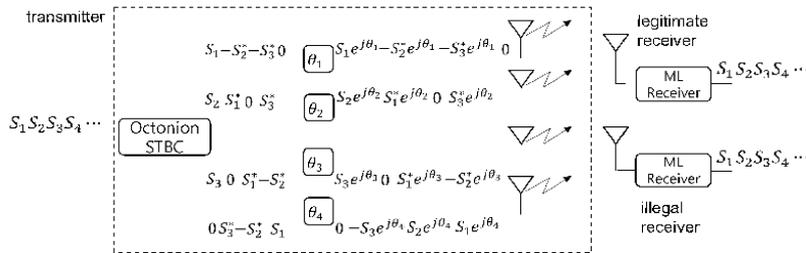


그림 1. 시스템 블록도  
Fig. 1. System block diagram

$$CC^H = \begin{pmatrix} |s_1|^2 + |s_2|^2 + |s_3|^2 & 0 & 0 & 2s_2 s_3 \\ 0 & |s_1|^2 + |s_2|^2 + |s_3|^2 & 0 & 0 \\ 0 & 0 & |s_1|^2 + |s_2|^2 + |s_3|^2 & -2s_1^* s_2 \\ 2s_2^* s_3 & 0 & -2s_1^* s_2 e^{j\theta_3} & |s_1|^2 + |s_2|^2 + |s_3|^2 \end{pmatrix} \quad (2)$$

위상을 발생시켜 옥토니언 부호화를 한다. 합법 수신자는 무선 채널 정보뿐만 아니라 랜덤 위상 값도 알고 있으므로 최대 유사도 (maximum likelihood, ML) 복호를 할 수 있다. 불법 도청자는 송신자의 신호를 해킹하려고 하는 사용자로 송신자의 입장에서 최악의 조건을 아래와 같이 가정한다.

- 불법 도청자는 합법 수신자가 송신하는 신호의 무선 채널 정보와 송신 신호의 정보를 완벽히 안다. 즉,  $L$ -PSK에서  $L$ 값을 안다.
- 랜덤 위상도  $L$ -PSK에서 발생시킨다.
- 송신 심벌마다 다른 랜덤 위상이 적용되는 것을 안다.
- 송신 안테나에 적용되는 랜덤 위상의 일부를 불법 도청자가 알 수 있다.

본 논문에서 벡터는 밑줄이 있는 영문 소문자로 표시하고, 행렬은 대문자로 표기한다. 공액 복소수는 영문자의 위첨자에 에스터리스크로 표시한다.

### III. 랜덤 위상 회전을 갖는 옥토니언 부호의 해킹

송신자는  $L$ -PSK 심벌  $S = \{e^{j2\pi(m-1)/L} / \sqrt{E_s} | m=1, \dots, L\}$ 를 가지고 식 (1)과 같이 옥토니언 부호화를 한다. 이때,  $\theta_i$ ,  $i=1, \dots, 4$ 는 랜덤하게 발생되며 합법 수신자는 랜덤 위상을 알고 있으나 불법 도청자는 랜덤 위상을 모두 모르거나 일부만 알고 있다. 불법 도청자가 송신 심벌뿐만 아니라 랜덤 위상도 함께 최대 유사도 추정을 하는 과정이 본 논문의 해킹 과정이다.

#### 1. 옥토니언 부호에서 위상 회전

회전 위상  $\theta_i$ 는 신호의  $L$ -PSK 성운 중에서 랜덤하게 선택된다. 예를 들면  $L$ -PSK 성운이  $e^{j2\pi l/L}$ ,  $l=1, \dots, L-1$ 이라고 할 때,  $i$ 번째 안테나의 랜덤 위상은  $\theta_i = 2\pi l'/L$ ,  $l'=1, \dots, L-1$ 이다. 따라서 위상 회전된 송신 심벌들이  $L$ -PSK가 되어 첨두값 대 평균값의 비율 (peak to average ratio, PAR)은 증가하지 않는다. 이외에도 송신자는 합법 수신자의 무선 채널 정보를 필요로 하지 않는 개회로 방식이므로 합법 수신자의 채널 정보를 피드백 받을 필요가 없다.

#### 2. 합법 수신자의 최대 유사도 복호기

합법 수신자의 수신 신호  $r = [r_1 r_2 r_3 r_4]^T$ 는 다음과 같다.

$$r = C \underline{h} + n \quad (3)$$

$\underline{h} = [h_1 h_2 h_3 h_4]^T$ 의 각 원소는  $i=1, \dots, 4$ 번째 송신 안테나에서 수신되는 무선 페이딩으로 원 대칭이고 독립이면서 일정한 분포를 갖는 복소수 가우시안 랜덤 값들로 평균은 0이고 실수 및 허수축의 분산은 각각  $1/2$ 이다.  $C$ 는 식 (1)의 위상 회전을 포함한 옥토니언 부호이다.  $\underline{n} = [n_1 n_2 n_3 n_4]^T$ 의 각 원소는 가산성 잡음 샘플이다. 무선 페이딩은 옥토니언 부호의 코드워드 전송 기간에는 변하지 않고, 잡음 샘플은 원 대칭이고 독립이면서 일정한 분포를 갖는 복소수 가우시안 랜덤 값들로 평균은 0이고 실수 및 허수축의 분산은 각각  $N_0/2$ 이다.

합법 수신자는 위상 회전 정보를 모두 알고 있으므로, 세 개의 송신 신호는  $L^3$ 개 조합 중의 하나이다. 따라서  $O(L^3)$ 의 탐색 복잡도를 갖는 최대 유사도 추정을 아래 식으로 수행한다.

$$\hat{\underline{s}} = \arg \max_{\underline{s}} \|r - C\underline{h}\|^2 \quad (4)$$

이때  $\hat{\underline{s}}$ 는 식 (1)의 송신 신호의 모든 조합이다.

#### 3. 불법 도청자의 최대 유사도 복호기

불법 도청자의 수신 신호  $\underline{x}$ 는 합법 수신자의 수신 신호와 유사하게 모델링 될 수 있다. 독립적인 채널 페이딩 계수는  $\underline{g} = [g_1 g_2 g_3 g_4]^T$ 이고, 잡음 벡터는  $\underline{w} = [w_1 w_2 w_3 w_4]^T$ 이다. 불법 도청자가 수신하는 신호는 다음과 같이 표현된다.

$$\underline{x} = C \underline{g} + \underline{w} \quad (5)$$

도청자가 무선 채널 정보를 완전히 알아도 랜덤 위상은 알지 못한다. 그러나 랜덤 위상이  $L^4$ 개 조합 중에 하나이고 신호는  $L^3$ 개 조합 중에 하나임을 알고 있다. 따라서  $O(L^7)$ 의 탐색 복잡도를 갖는 최대 유사도 추정을 아래 식으로 수행해야 한다.

$$\hat{s} = \arg \max_{\tilde{s}} \| \underline{x} - C\tilde{q} \|^2 \quad (6)$$

이때  $\tilde{s}$ 는 식 (1)의 송신 신호의 모든 조합이다.

#### IV. 컴퓨터 시뮬레이션 및 결론

송신 안테나의 수는 4개이고 수신 안테나의 수는 1개로 한다. 2-PSK로 변조된 심볼을 전송하고 물리계층 보안을 위해 4개의 송신 안테나에 2-PSK 성운과 같이 0도와 180도 위상을 랜덤하게 발생시킨다. 불법 도청자가 4개의 랜덤 위상 모듈을 최대 유사도 추정을 하는 경우의 비트 에러율 성능 곡선은 그림 2의 점선으로 (ML with 4 rotations) 표시한다. 불법 도청자가 랜덤 위상의 일부를 탐지하여 3개, 2개, 1개의 위상을 최대 유사도 추정을 하는 경우의 성능 곡선도 보인다. 그림 2에서 보이듯이 불법 도청자가 4개 위상을 모두 추정해야 하는 경우에는 신호 대 잡음비가 100dB 까지는 도청이 불가능하다. 그러나 기존 연구에서<sup>[1]</sup> 보이지 않은 120dB에서 비트 에러율이  $8 \times 10^{-3}$  정도로 부분적인 해킹이 가능해진다. 송신 안테나 수가 2개인 시스템과는<sup>[2]</sup> 달리 에러 언덕 (floor)이 발생한다. 불법 도청자가 3개 혹은 2개 위상을 추정해야 하는 경우에는 신호 대 잡음비가 25dB 이상에서  $2 \times 10^{-3}$  및  $10^{-3}$ 의 비트 에러율로 에러 언덕을 보이므로 충분히 도청이 가능하다. 불법 도청자가 4개

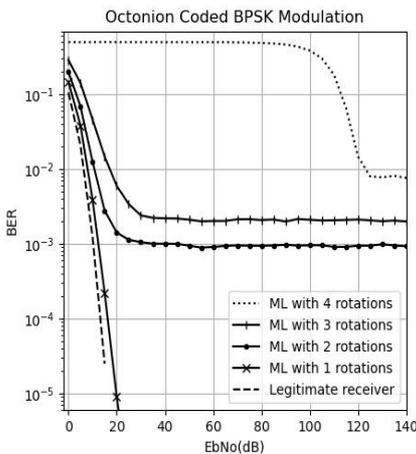


그림 2. 합법 및 불법 도청자의 최대 유사도 비트 에러율  
Fig. 2. ML bit error rate of legitimate and illegal receivers

의 랜덤 위상 중에 3개를 이미 알고 있고 랜덤 위상이 2-PSK의 두 개 성운 중 한 개의 성운만 추정하면 되는 경우에는 에러 언덕도 없고 비트 에러율  $10^{-4}$ 에서 합법적 수신자보다 약 4dB의 성능 저하를 보인다. 기존 연구에서도 1개 위상만 추정하는 경우에는 합법 수신자 성능과 3dB 내외의 성능 감소가 있다<sup>[2]</sup>. 그림 3에는 직교성을 갖지 않는 식 (2)를 이용한 시스템의 비트 에러율을 보인다. 합법적 수신자의 비트 에러율도  $10^{-2}$  보다 개선되지 않는다. 이때 SISO는 송수신 안테나가 각각 1개일 경우의 성능이며, 완전한 직교성을 갖는 식 (1)의 옥토니언 부호를 적용한 경우의 성능도 보인다.

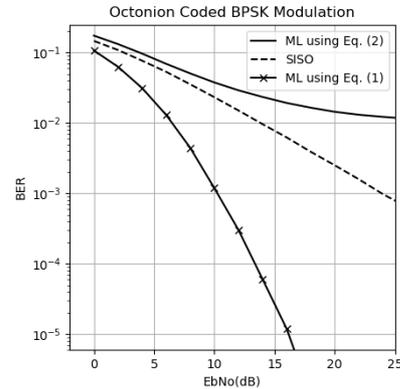


그림 3. 식 (2)를 이용한 합법 수신자의 최대 유사도 비트 에러율  
Fig. 3. ML bit error rate of the legitimate receiver employing Eq. (2)

#### 참고 문헌 (References)

- [1] T. Allen, J. Cheng, and N. Al-Dhahir, "Secure space-time block coding without Transmit CSI," *IEEE Wireless Commun. Letters*, vol. 3, no. 6, pp. 573-576, Dec. 2014.  
doi: 10.1109/LWC.2014.2344666
- [2] Y. J. Kim, "Hacking evaluation of open-loop space-time block codes having random phase rotation," *Journal of KICS*, vol. 45, no. 12, pp. 2072-2074, Dec., 2020.  
doi: 10.7840./kics.2020.45.12.2072
- [3] S. Diggavi, N. Al-Dhahir, A. Stamoulis, and A. R. Calderbank, "Great expectations: The value of spatial diversity in wireless networks," *Proc. IEEE J.*, vol. 92, no. 2, pp. 219-270, Feb., 2004.  
doi: 10.1109/JPROC.2003.821914
- [4] J. Choi, J. Joung, and Y. Cho, "Artificial-noise - aided space-time line code for enhancing physical layer security of multiuser MIMO downlink transmission," *IEEE Systems Journal*, vol. 16, no. 1, pp. 1289-1300, Mar., 2022.  
doi: 10.1109/JSYST.2021.3075721