논문 20-45-12-06 The Journal of Korean Institute of Communications and Information Sciences '20-12 Vol.45 No.12
https://doi.org/10.7840/kics.2020.45.12.2072

랜덤 위상 회전을 갖는 오픈 루프 시공간 블록 부호의 해킹 안전성

김 영 주°

Hacking Evaluation of Open-Loop Space-Time Block Codes Having Random Phase Rotation

Young-ju Kim°

요 약

랜덤 위상 회전을 갖는 오픈 루프 시공간 블록 부호에서 최대 우도 추정으로 물리 계층 해킹을 시도하는 경우의 성능을 분석한다. 2-PSK 성운으로 랜덤 위상 회전을 한다는 것을 해커가 알고 있는 경우, 기존 연구에서 다루지 않은 일반적인 동작 범위가 넘는 높은 신호 대 잡음비에서 해킹이 가능하다.

Key Words : communication system security, physical layer, transmit diversity, space-time codes

ABSTRACT

The performance of physical layer hacking with maximum likelihood estimation, is described over secure open-loop space-time block codes having random phase rotation. Whenever the hacker knows the fact that the sender uses 2-PSK randomly rotated phases, The hacker can decipher the transmitted information at a relative high signal-to-noise ratio, which did not investigated in the literature[6].

Ⅰ. 서 론

무선 통신 신호는 주변의 공간으로 전송되므로 도청의 위협성을 항상 가지고 있다. 통신 시스템의 보안은 반드시 필요하며, 일반적으로 물리계층보다 상위의 레벨에서 다양한 암호화 프로토콜을 사용하여 구현하고 있다. 최근에는 단일 혹은 다중 송수신 안테나의 채널 정보를 비밀 키로 활용하여 물리계층에서 보안 기능을 수행하는 연구가 이루어지고 있다[1,2]. 무선 채널 행렬의 널 (null) 공간에 인공적인 잡음을 발생시키거나, 수신기 쪽으로 빔성형 또는 선부호화를 하여 물리계층 보안을 하는 기법도 있다[3-5]. 이와 같은 기법의 경우에는 송신기에서 무선 채널 정보를 알고 있어야 하므로 수신기로부터 무선 채널 정보를 피드백 받아야 한다[1-5]. 한편 수신기로부터 채널 정보를 받지 않는 오픈 루프 방식을 채택한 연구도 있다. 다중 송수신 안테나 시스템에서 송신기 안테나 별로 랜덤 위상을 발생시켜 해킹에 대한 안전성을 강화하는 오픈 루프 시공간 부호로 송신 신호를 안전하게 전송할 수 있다[6]. 본 레터에서는 랜덤 위상을 갖는 오픈 루프 시공간 블록 부호에서 기존 연구에서 다루지 않은 신호 대 잡음비가 일반적인 동작범위보다 매우 높은 영역에서는 해킹이 될 수 있음을 컴퓨터 시뮬레이션으로 보인다.

Ⅱ. 시스템 모델

송신자 앨리스는 수신자 밥에게 알라무티 코딩을 이용하여 신호를 전송한다. 밥 외의 수신자 이브는 앨리스의 송신 신호의 수신을 못하도록 그림 1에 보이듯이 송신 안테나별로 랜덤하게 위상을 발생시켜 신호 성운을 회전시킨다.

k번째 송신 신호 $s_{1,k}$과 $s_{2,k}$를 두 개의 안테나에서 서로 독립적인 위상 회전을 하여 알라무티 코딩을 한다. k번째 시간슬롯 1에서 $s_{1,k}e^{j\theta_{1,k}}$ 심벌과 $s_{2,k}e^{j\theta_{2,k}}$ 심벌을 첫 번째 안테나와 두 번째 안테나에서 송신하고 k번째 시간슬롯 2에서 $-s_{2,k}^{*}e^{j\theta_{1,k}}$ 심벌과 $s_{1,k}^{*}e^{j\theta_{2,k}}$ 심벌을 첫 번째 안테나와 두 번째 안테나에서 송신한다. 아래와 같이 알라무티 코드워드를 행렬로 표시할 수 있다.

$$C(s_{1,k},s_{2,k},\theta_{1,k},\theta_{2,k})=\begin{pmatrix} s_{1,k}e^{j\theta_{1,k}} & s_{2,k}e^{j\theta_{2,k}} \\ -s_{2,k}^{*}e^{j\theta_{1,k}} & s_{1,k}^{*}e^{j\theta_{2,k}} \end{pmatrix} \quad (1)$$

°First and Corresponding Author : (ORCID:0000-0002-5844-8612)Chungbuk National University Department of Information and Communication Engineering, Research Institute for Computer and Information Communication, yjkim@cbnu.ac.kr, 정교수, 종신회원
논문번호 : 202008-211-A-LU, Received August 27, 2020; Revised September 21, 2020; Accepted September 25, 2020

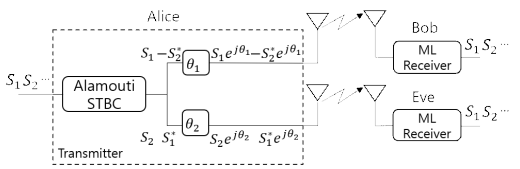

그림 1. 시스템 블록도.
Fig. 1. System block diagram.

식 (1)은 알라무티 행렬의 유니터리 변환으로 직교성이 유지된다. 랜덤 위상이 더해져 그 위상을 정확히 알지 못하면 해킹이 어려워진다. 앨리스와 밥은 비밀키를 공유하고 유사 랜덤 위상을 발생시켜 알라무티 코딩을 한다. 밥은 무선 채널 정보뿐만 아니라 랜덤 위상 값도 알고 있으므로 완전히 알라무티 디코딩을 할 수 있다. 이브는 앨리스의 신호를 해킹하려고 하는 사용자로 앨리스의 입장에서 최악의 조건을 가정한다.

(i) 이브는 앨리스가 송신하는 신호의 무선 채널 정보를 완벽히 안다.

(ii) 이브는 앨리스의 성운에 대한 정보를 가지고 있다. 즉, L-PSK에서 L값을 알고 있다.

(iii) 앨리스가 랜덤 위상을 갖는 알라무티 코딩을 사용하고 있으며, 코드워드 마다 다른 랜덤 위상을 적용하는 것을 안다.

그러나 이브는 랜덤 위상 값을 모르며 밥의 수신 안테나와 충분히 떨어져 있어서 밥의 무선 채널 수신 정보를 알지 못한다. 본 레터에서 벡터는 밑줄이 있는 영문 소문자로 표시하고, 행렬은 대문자로 표기한다. 공액 복소수 (허미션, hermitian)는 영문자의 위 첨자에 (*)와 같이 애스터리스크로 표기한다.

Ⅲ. 랜덤 위상 회전을 갖는 알라무티 코드의 해킹

앨리스는 L-PSK 심벌 $S=\{e^{j2\pi(m-1)/L}/\sqrt{E_s}|m=1,\cdots,L\}$를 가지고 식 (1)과 같이 알라무티 코딩을 한다. 이때, $\theta_{1,k}$와 $\theta_{2,k}$는 랜덤하게 발생되며 밥은 랜덤 위상을 알고 있으나 이브는 알지 못한다. 이브가 랜덤 위상을 알아내는 과정이 본 레터의 해킹 과정이다.

3.1 알라무티 인코딩에서 위상 회전

회전 위상 $\theta_{1,k}$와 $\theta_{2,k}$는 신호의 L-PSK 성운 중에서 랜덤하게 선택된다. 예를 들면 L-PSK 성운이 $e^{j2\pi l/L}$, $l=1,\cdots,L-1$이라고 할 때, i번째 안테나의 랜덤 위상은 $\theta_{i,k}=2\pi l'/L$, $l'=1,\cdots,L-1$이다. 따라서 위상 회전된 송신 심벌들이 L-PSK가 되어 첨두값 대 평균값의 비율 (peak to average ratio, PAR)은 증가하지 않는다. 이외에도 앨리스는 밥의 무선 채널 정보를 필요로 하지 않는 오픈 루프 구조이므로 밥의 채널 정보를 피드백을 받을 필요가 없다.

3.2 밥의 ML 디코더

밥의 k번째 알라무티 코드워드 수신 신호 두 개 샘플은 다음과 같다.

$$\begin{pmatrix} r_{1,k} \\ r_{2,k} \end{pmatrix} = \begin{pmatrix} s_{1,k}e^{j\theta_{1,k}} & s_{2,k}e^{j\theta_{2,k}} \\ -s_{2,k}^{*}e^{j\theta_{1,k}} & s_{1,k}^{*}e^{j\theta_{2,k}} \end{pmatrix} \begin{pmatrix} h_1 \\ h_2 \end{pmatrix} + \begin{pmatrix} n_{1,k} \\ n_{2,k} \end{pmatrix} \tag{2}$$

h_i는 i번째 송신 안테나에서 수신되는 무선 페이딩으로 원 대칭이고 독립이면서 일정한 분포를 갖는 복소수 가우시안 랜덤 값들로 평균은 0이고 실수 및 허수축의 분산은 각각 1/2이다. $\{s_{t,k},\ t=1,2\}$는 알라무티 코드워드의 두 개 심벌이다. $\{n_{t,k}\}$는 가산성 잡음 샘플이다. 무선 페이딩은 알라무티 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. 식 (2)는 다음과 같이 표현될 수 있다.

$$\begin{pmatrix} r_{1,k} \\ -r_{2,k}^{*} \end{pmatrix} = \begin{pmatrix} h_1 e^{j\theta_{1,k}} & h_2 e^{j\theta_{2,k}} \\ -h_2^{*}e^{-j\theta_{1,k}} & h_1^{*}e^{-j\theta_{2,k}} \end{pmatrix} \begin{pmatrix} s_{1,k} \\ s_{2,k} \end{pmatrix} + \begin{pmatrix} n_{1,k} \\ -n_{2,k}^{*} \end{pmatrix} \tag{3}$$
$$\underline{r_k} = H(\underline{\theta})\,\underline{s_k} + \underline{n_k}$$

이때 $H^{*}(\underline{\theta})H(\underline{\theta}) = \left(|h_1|^2 + |h_2|^2\right)I_2 = \|\underline{h}\|^2 I_2$이므로 위상 회전 시킨 채널 $H(\underline{\theta})$는 직교 행렬이다. $H(\underline{\theta})$가 직교 행렬이므로 밥의 최대 가능도 (ML, maximum likelihood) 수신기에서 추정된 송신 심벌은 다음과 같으며, 알라무티 코딩과 동일하게 송수신기 복잡도는 증가하지 않으면서 다이버시티 성능을 온전히 가진다.

$$\hat{\underline{s_k}} = \frac{1}{\|\underline{h}\|^2} H^{*}(\underline{\theta})\underline{r_k} \tag{4}$$

3.3 이브의 ML 디코더

이브의 수신 신호 $\underline{x_k}$는 밥의 수신 신호와 유사하게 모델링 될 수 있다. 독립적인 채널 페이딩 계수는

$\{g_i\}$이고, 잡음 샘플은 $\{w_{i,k}\}$이다. 이브가 수신하는 신호는 다음과 같이 표현된다.

$$\underline{x_k} = G(\underline{\theta})\underline{s_k} + \underline{w_k} \tag{5}$$

이브가 무선 채널 정보를 완전히 안다고 해도 랜덤 위상 $\{\theta_{i,k}\}$는 알지 못한다. 그러나 $\{\theta_{i,k}\}$가 L^2 개 조합 중에 하나이고 $\{s_{i,k}\}$도 L^2개 조합 중에 하나임을 알고 있다. 따라서 $O(L^4)$의 탐색 복잡도를 갖는 ML 추정을 아래 식으로 수행해야 한다.

$$\{\hat{\underline{s}}_k, \hat{\underline{\theta}}\} = \arg\max_{\underline{\tilde{s}_k}} \| \underline{x_k} - G(\underline{\tilde{\theta}})\underline{\tilde{s}_k} \|^2 \tag{6}$$

L이 증가함에 따라 $O(L^4)$가 지수 승으로 증가한다. ML 수신기의 계산 속도를 증가시키기 위해 $G(\underline{\tilde{\theta}})$ 행렬이 직교임을 이용하고 L^2개의 $\underline{\tilde{\theta}}$ 조합에 대한 병렬 구조를 갖는 다음과 같은 조건부 ML 수신기를 구현할 수 있다[6].

$$\begin{aligned}\left(\underline{\tilde{s}_k}|\underline{\tilde{\theta}}\right)_{ML} &= \left(G^*(\underline{\tilde{\theta}}) \cdot G(\underline{\tilde{\theta}})\right)^{-1} G^*(\underline{\tilde{\theta}}) \cdot \underline{x_k} \\ &= \left(G^*(\underline{\tilde{\theta}}) / \| \underline{g} \|^2\right) \cdot \underline{x_k}\end{aligned} \tag{7}$$

식 (7)의 값들 중에서 $\hat{\underline{s}_k}$와 가장 유클리드 거리가 가까운 심벌을 선택한다.

Ⅳ. 컴퓨터 시뮬레이션 및 결론

위상회전 알라무티 코드의 비트에러율을 컴퓨터 시뮬레이션하여 신호 대 잡음비에 대해 그림 2와 같이 플롯한다. 대쉬 선은 위상 회전을 완전히 아는 밥의 성능 곡선이고, 점이 찍힌 선은 이브가 1개의 위상 회전을 아는 경우이고, 가위표가 찍힌 선은 이브가 2개 위상을 ML 추정한다. 그림 2의 왼쪽은 BER을 선형으로 오른쪽은 데시벨로 플롯한다. L개 위상일 경우는 도 성능 곡선이 평행이동 하게 된다. 이브는 무선 채널 정보를 완전히 안다고 해도 랜덤 위상 회전의 정보를 모르기 때문에 철저한 탐색을 하는 과정에서 ML 수신기의 성능이 매우 저하된다. 신호 대 잡음비가 10dB 내외의 일반적인 동작 범위에서는 비트오율이 0.5가 유지될 정도로 해킹이 불가능하다. 그러나 2-PSK 성운의 알라무티 코딩의 경우 신호 대 잡음비가 90dB 이상일 경우에는 해킹이 충분히 가능해진다.

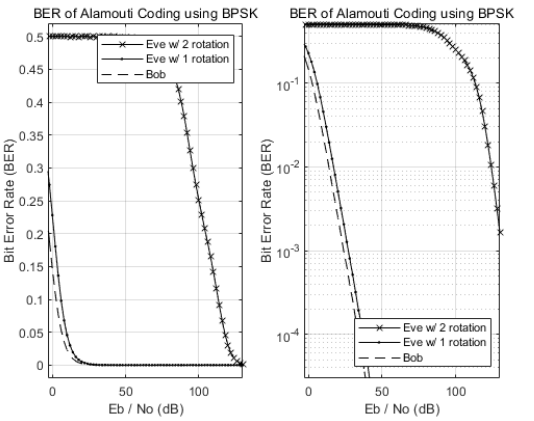

그림 2. 이브와 밥의 ML 수신기 비트에러율
Fig. 2. ML Detector BER for Eve and Bob

References

[1] H. Koorapaty, A. A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Commun. Lett.*, vol. 4, no. 2, pp. 52-55, Feb. 2000.

[2] A. E. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, pp. 3235-3249, Dec. 2003.

[3] R. Negi and S. Goel, "Secret communication using artificial noise," *IEEE Veh. Technol. Conf.*, vol. 3, pp. 1906-1910, 2005.

[4] Y. J. Kim and C. W. Seo, "An adaptive equal gain differential transmission using M-PSK constellations," *J. IEIE*, vol. 53, no. 3, pp. 332-339, Mar. 2016.

[5] S. A. A. Fakoorian, H. Jafarkhani, and A. L. Swindlehurst, "Secure space-time block coding via artificial noise alignment," in *Proc. Conf. Rec. 45th ASILOMAR*, pp. 651-655, Nov. 2011.

[6] T. Allen, J. Cheng, and N. Al-Dhahir, "Secure space-time block coding without Transmit CSI," *IEEE Wireless Commun. Lett.*, vol. 3, no. 6, pp. 573-576, Dec. 2014.