상관관계를 갖는 MIMO 채널에서 하나의 피드백 비트를 이용한 OSTBC의 물리계층 보안 성능 평가

이상준* · 이인호*

*국립한경대학교

Secrecy Performance Evaluation of OSTBC using One-Bit Feedback in Correlated MIMO Channels

Sangjun Lee* · In-Ho Lee*

*Hankyong National University

E-mail : ihlee@hknu.ac.kr

요 약

본 논문에서는 통신 신호를 도청하는 도청자가 존재하는 환경인 와이어탭(wiretap) 채널을 가정하여 하나의 피드백 비트를 이용한 직교 시공간 블록 코드(orthogonal space-time block code, OSTBC)의 물리계층 보안 성능을 평가한다. 여기서, 공간적 상관관계를 갖는 MIMO(multiple-input multiple-output) 채널을 가정한다. 본 논문에서는 하나의 피드백 비트를 이용한 OSTBC(one-bit feedback based OSTBC, F-OSTBC) 기술을 제시하고, 각 노드에서의 공간 채널 상관계수를 다양하게 가정하여 F-OSTBC와 기존의 OSTBC, 그리고 송신 안테나 선택 기술에 대한 보안 아웃티지 성능을 비교한다.

ABSTRACT

In this paper, we evaluate a physical layer security performance of orthogonal space-time block code(OSTBC) using one-bit feedback in the presence of an eavesdropper in wiretap channels, where we assume spatially correlated MIMO(multiple-input multiple-output) channels. In this paper, we present the one-bit feedback based OSTBC(F-OSTBC) scheme and compare security outage performances of F-OSTBC, conventional OSTBC, and transmission antenna selection schemes for various spatial correlation conditions at each node.

키워드

MIMO, 직교 시공간 블록 코드, 보안, 공간적 상관관계, 아웃티지 확률

Ⅰ. 서 론

기존의 통신 보안은 주로 암호학(cryptography)의 관점에서 연구되어졌으나, 현재는 무선 통신의 물리계층에서 활발히 연구되어지고 있다[1]. [2]에서는 채널상태정보의 피드백을 줄이기 위하여 MIMO 직교 시공간 블록 코드(orthogonal space-time block code, OSTBC)를 이용한 물리계층 보안 성능이 분석되었다. 또한, 실질적인 채널 환경을 고려하기 위하여 안테나 간 상관계수를 갖는 채널을 가정하여 보안 아웃티지 성능을 분석하였다. [3,4]에서는, 물리계층 보안 성능을 증

가시키기 위하여 원천 노드에서 가장 좋은 채널을 갖는 안테나를 선택하는 방식인 송신 안테나 선택 기술(transmit antenna selection, TAS)을 이용하였다. TAS 기술은 OSTBC와 달리 송신 안테나 선택을 위한 피드백을 요구한다.

아웃티지 성능 측면에서 TAS는 OSTBC 보다 우수하지만, 피드백 오버헤드 측면에서 피드백을 요구하지 않는 OSTBC가 TAS 보다 우수하다. 본 논문에서는, TAS보다 낮은 피드백 오버헤드를 요구하면서 성능 열하는 최소화하기 위한 하나의 피드백 비트를 이용한 OSTBC(one-bit feedback based OSTBC, F-OSTBC)기술을 제시한다.

II. 시스템 모델

시스템 모델은 원천 노드(source node, *S*), 목적지 노드(destination node, *D*), 그리고 도청 노드(eavesdropper node, *E*)로 구성된 MIMO 와이어탭 채널을 고려한다. 본 논문에서는 원천 노드가 목적지 노드와 도청 노드의 채널상태정보(channel state information, CSI)를 모른다고 가정한다. 원천 노드, 목적지 노드, 그리고 도청 노드의 안테나 개수는 $n_s = n_d = n_e = 4$로 가정한다. 또한, 코드 율(code rate, R_C)은 $R_C = s_n / T$로 정의된다. 이 때, s_n와 T는 각각 원천 노드에서 전송되는 심볼의 개수와 주기를 의미한다. 목적지 노드와 도청 노드에서의 수신 신호는 다음과 같이 표현된다.

$$\begin{aligned} Y_D &= H_{SD}X + N_D, \quad at\ destination\ node \\ Y_E &= H_{SE}X + N_E. \quad at\ eavesdropper\ node \end{aligned} \tag{1}$$

식 (1)에서, Y_D와 Y_E는 각각 $n_d \times T$행렬, $n_e \times T$행렬이다. 또한, X는 OSTBC 송신 신호를 의미하는 $n_s \times T$행렬이다. N_D와 N_E는 각각 목적지 노드와 도청 노드에서의 평균 0과 분산 σ^2을 갖는 백색 가우시안 잡음 행렬 $n_d \times T$와 $n_e \times T$를 의미한다. H_{SD}와 H_{SE}는 각각 원천 노드-목적지 노드와 원천 노드-도청 노드의 공간적 상관관계를 갖는 MIMO 채널을 의미하며 다음과 같이 표현된다[5].

$$\begin{aligned} H_{SD} &= (R_D)^{1/2} H_w^{SD} (R_S)^{1/2}, \\ H_{SE} &= (R_E)^{1/2} H_w^{SE} (R_S)^{1/2}. \end{aligned} \tag{2}$$

식 (2)에서, 원천 노드와 목적지 노드, 그리고 도청 노드에서의 안테나 간 상관관계 행렬을 의미하는 R_S, R_D, 그리고 R_E는 각각 $n_s \times n_s$, $n_d \times n_d$, 그리고 $n_e \times n_e$행렬이다. 또한, $(\bullet)^{1/2}$는 행렬의 hermitian square root를 의미한다. H_w^{SD}와 H_w^{SE}는 각각 원천 노드-목적지 노드와 원천 노드-도청 노드의 독립적이고 균일분포를 갖는 복소 가우시안 랜덤 변수들의 행렬을 의미한다. 본 논문에서 모든 노드들에 대한 평균 송신 신호 대 잡음비(signal-to-noise ratio, SNR)는 $\rho = P/\sigma^2$로서 표현된다. 이 때, P는 모든 노드에서의 송신전력을 의미한다.

OSTBC에서 MIMO 채널은 심볼 당 순시 수신 SNR을 갖는 독립적인 SISO(single-input single-output) 채널로 표현될 수 있다. 원천 노드-목적지 노드와 원천 노드-도청 노드의 순시 수신 SNR γ_{SD}와 γ_{SE}는 각각 다음과 같이 표현된다.

$$\begin{aligned} \gamma_{SD} &= (\rho / R_C n_s) \| H_{SD} \|^2, \\ \gamma_{SE} &= (\rho / R_C n_s) \| H_{SE} \|^2. \end{aligned} \tag{3}$$

식 (3)에서, $\| H_{SD} \|^2$와 $\| H_{SE} \|^2$는 각각 H_{SD}와 H_{SE}의 제곱 연산된 Frobenius norm을 의미한다[5].

III. 보안 채널 용량과 아웃티지 확률

3. 1. 보안 채널 용량

1) 기존의 OSTBC(conventional OSTBC, C-OSTBC)

원천 노드의 모든 안테나를 이용하여 신호를 전송한다. C-OSTBC에서의 원천 노드-목적지 노드와 원천 노드-도청 노드의 채널 용량 C_{SD}와 C_{SE}는 다음과 같이 표현된다.

$$\begin{aligned} C_{SD} &= R_C \log(1 + \gamma_{SD}), \\ C_{SE} &= R_C \log(1 + \gamma_{SE}). \end{aligned} \tag{4}$$

C-OSTBC에서의 와이어탭 채널에 대한 보안 채널 용량 C_S는 다음과 같이 표현된다.

$$C_S = \begin{cases} C_{SD} - C_{SE}, & \gamma_{SD} > \gamma_{SE} \\ 0. & \gamma_{SD} \le \gamma_{SE} \end{cases} \tag{5}$$

2) 1 비트 피드백 선택 기반 OSTBC(one-bit feedback based OSTBC, F-OSTBC)

원천 노드에서 인접한 안테나를 묶어 두 개의 그룹을 구성하여 그 중에서 좋은 성능을 제공하는 그룹의 인덱스만을 피드백하는 방식이다. 따라서 피드백을 위하여 하나의 비트를 요구한다. F-OSTBC에서의 원천 노드-목적지 노드의 채널 용량 C_{SD}^*는 다음과 같이 표현된다.

$$C_{SD}^* = R_C \log(1 + \gamma_{SD,i^*}). \tag{6}$$

식 (6)에서, i^*는 다음과 같이 표현된다.

$$i^* = \arg\max_{i=1,2}\{R_C \log(1+\gamma_{SD,i})\}. \quad (7)$$

식 (7)에서, i에 대한 안테나 그룹은 다음과 같다.

$$G_{ant} = \begin{cases} \{1,2\} & \text{for } i=1 \\ \{3,4\} & \text{for } i=2, \end{cases} \quad (8)$$

여기서, 안테나 그룹 G_{ant}의 원소들은 안테나의 인덱스들을 의미한다. 원천 노드-도청 노드의 채널 용량은 C-OSTBC의 것과 동일하다. F-OSTBC에서의 와이어탭 채널에 대한 보안 채널 용량 C_S는 다음과 같이 표현된다.

$$C_S = \begin{cases} C_{SD}^* - C_{SE}, & \gamma_{SD,i^*} > \gamma_{SE} \\ 0. & \gamma_{SD,i^*} \le \gamma_{SE} \end{cases} \quad (9)$$

3. 2. 보안 아웃티지 확률

와이어탭 채널 환경에서 보안 아웃티지 확률 $P_O(R)$는 C_S가 목표 보안 데이터 율(target secrecy data rate, R)보다 작을 확률로 정의되고, 다음과 같이 표현된다.

$$P_O(R) = \Pr(C_S < R). \quad (10)$$

Ⅳ. 시뮬레이션 결과

본 장에서는 몬테 카를로(Monte-Carlo) 시뮬레이션 방식을 이용하여 결과를 분석한다. 그림 1은 높은 상관관계(high correlation, HC)와 낮은 상관관계(low correlation, LC)를 가정하여 C-OSTBC, F-OSTBC, 그리고 TAS에 대한 보안 아웃티지 확률을 분석한다. 이 때, 목표 보안 데이터 율은 1bps/Hz로 가정한다. 더욱 가시적인 시뮬레이션 분석을 위하여 도청 노드의 평균 SNR은 -5dB로 가정한다.

OSTBC에서 송신 안테나가 두 개일 경우와 그 이상일 경우, 코드 율은 각각 최대 1과 3/4이다[6]. 따라서 그림 1에서는 F-OSTBC와 C-OSTBC에 대한 코드 율을 각각 1과 3/4으로 가정한다.

HC에서는 원천 노드, 목적지 노드, 그리고 도청 노드가 갖는 안테나 간 상관관계를 결정하는 변수인 Λ와 d를 각각 0.1, 0.5로 가정한다. LC에서는 원천 노드, 목적지 노드, 그리고 도청 노드가 갖는 안테나 간 상관관계를 결정하는 변수인 Λ와 d를 각각 1, 5로 가정한다. 이 때, Λ와 d는 각각 확산 각도와 두 안테나 간 파장의 거리를 의미한다.

$$\beta(d) \approx \exp(-23\Lambda^2 d^2). \quad (11)$$

식 (11)는 안테나 간 상관관계 행렬을 구성하는 상관계수 $\beta(d)$을 나타낸다[7].

시뮬레이션 결과를 통해, HC와 LC에서 보안 아웃티지 성능이 TAS>F-OSTBC>C-OSTBC임을 확인할 수 있다. 특히, HC와 LC에서 F-OSTBC가 C-OSTBC보다 TAS에 근접하는 것을 볼 수 있다. 또한, C-OSTBC, F-OSTBC, 그리고 TAS에서 각각

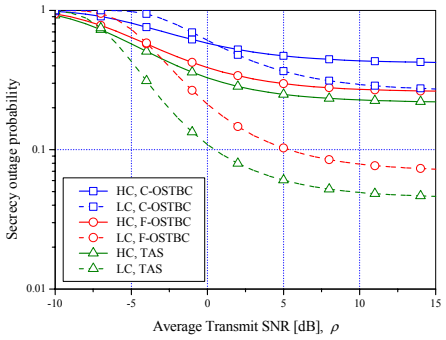

그림 1. 안테나 간 HC, LC에 따른 C-OSTBC, F-OSTBC, 그리고 TAS에 대한 보안 아웃티지 확률

ρ=1dB, -4dB, 그리고 -7dB를 기준으로 낮은 ρ에서는 HC, 높은 ρ에서는 LC가 더 좋은 보안 아웃티지 성능을 나타냄을 확인할 수 있다. 이것은, 낮은 ρ에서는 수신 전력 이득의 비중이 증가하는 반면에, 높은 ρ에서는 다이버시티 이득의 비중이 증가하기 때문이다[8].

Ⅴ. 결 론

본 논문에서는 도청자가 존재하는 MIMO 와이어탭 채널에서 F-OSTBC 기술을 제시하였고, F-OSTBC와 C-OSTBC, 그리고 TAS 기술의 보안 아웃티지 확률 성능을 비교하였다. 시뮬레이션 결과를 통해, HC와 LC에서 보안 아웃티지 성능이 TAS>F-OSTBC>C-OSTBC임을 확인하였다. 또한, HC와 LC에서 F-OSTBC가 C-OSTBC보다 TAS에 근접하는 것을 확인함으로써 F-OSTBC가 보안 아웃티지 성능 측면에서 큰 이득을 얻을 수 있음을 알 수 있다.

감사의 글

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발 사업의 일환으로 수행하였음. [14-000-04-001, 초연결 스마트 모바일 서비스를 위한 5G 이동통신 핵심기술 개발]

참고문헌

[1] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory,* vol. 54, no. 6, pp. 2515-2534, June 2008.

[2] Nuwan S. Ferdinand, Daniel Benevides da Costa, and Matti Latva-aho, "Physical layer security in MIMO OSTBC line-of-sight wiretap channels with arbitrary transmit/receive antenna correlation," *IEEE Commun, Lett.,* vol. 2, no. 5, pp. 467-470, Oct. 2013.

[3] N. Yang, P. L. Yoeh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channel," *IEEE Trans. Commun.,* vol. 61, no. 1, pp. 144-154, Jan. 2013.

[4] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Rorens. Security,* vol. 8, no. 1, pp. 254-259, Jan. 2013.

[5] E. G. Larsson and P. Stoica, *Space-Time Block Coding for Wireless Communications.* Cambridge, U.K.: Cambridge Univ. Press, 2003.

[6] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Inform. Theory,* vol. 45, no. 5, pp. 1456-1467, July 1999.

[7] G. D. Durgin and T. S. Rappaport, "Effects of multipath angular spread on the spatial cross-correlation of received voltage envelopes," in *Proceedings of the IEEE VTS 50th Vehicular Technology Conference (VTC '99)*, pp. 996-1000, Sep. 1999.

[8] Z. Wang and G. B. Giannakis, "A simple and general parameterization quantifying performance in fading channels," *IEEE Trans. Commun.,* vol. 51, no. 8, pp. 1389-1398, Aug. 2003.