Secrecy Performance Analysis of Alamouti-STBC With Decision Feedback Detection in Time-Selective Fading Channels

Dongjin Kim†, Yujae Song‡, and Seong Ho Chae†‡
† Department of IT Semiconductor Convergence Engineering, Tech University of Korea
‡ Department of Computer Software Engineering, Kumoh National Institute of Technology
†‡ Department of Electronics Engineering, Tech University of Korea
Email: kdj95061@tukorea.ac.kr, songyj@kumoh.ac.kr, shchae@tukorea.ac.kr

***Abstract*—This paper analyzes the achievable secrecy transmission rates (STRs) of Alamouti space–time block coding (STBC) with the decision feedback (DF) detection in wiretap time-selective fading channels and studies how to optimally design the Wyner's codebook to maximize it. Specifically, we derive the STR with both connection outage probability and secrecy outage probability for an arbitrary temporal correlation and find the optimal codeword rate and the secrecy rate to maximize it.**

***Index Terms*—Alamouti space–time block coding, decision feedback detection, time-selective fading channel**

I. Introduction

As one of key techniques to exploit the spatial and temporal diversity of multiple-input multiple-output (MIMO) systems, the space-time block coding (STBC) has drawn much attention. As an initial work for STBC, Alamouti [1] proposed the orthogonal STBC for two transmit and one receive antenna system and showed that full diversity and data rate can be obtained via linear maximum-likelihood (LML) detection for static channels. Thereafter, various orthogonal and quasi-orthogonal STBCs were proposed in multi-antenna systems [2], [3].

Recently, there have been also growing efforts to use Almouti STBC for enhancing the physical layer security (PLS) [4]–[6]. However, these works were conducted for the static fading channels, so they might not be directly implemented in the time-selective fading channels. Motivated by it, this paper proposes the decision feedback (DF) detection which can successively eliminate the interference in time-selective fading channel and investigates how much secrecy performance can be achieved via DF detection and how to design the Wyner's codebook to maximize the security performance. Specifically, we derive the secrecy transmission rate with both connection and secrecy outage probabilities for an arbitrary temporal correlation and then find the optimal codeword and secrecy rates to maximize it.

II. System model

Let us consider a time-selective Rayleigh fading wiretap channel in which a legitimate transmitter (Alice) transmits the Alamouti space-time block coded message to its designated receiver (Bob) and an eavesdropper (Eve) tries to eavesdrop it. We assume that Alice is equipped with two antennas and both Bob and Eve are equipped with one antenna. Both Bob and Eve have the full channel state information (CSI), while Alice does not have it. The channels vary for every symbol times with a temporal correlation. Due to the lack of full CSI, for transmitting a secret message of rate R_{S}, Alice constructs a nested structured Wyner's codebook with arbitrarily chosen two constant rates $R_{\mathrm{T}}(> R_{\mathrm{E}})$ and R_{E}, where $R_{\mathrm{S}} = R_{\mathrm{T}} - R_{\mathrm{E}}$ holds [7]. Alice sends the secret message to Bob via Alamouti STBC by preventing Eve's eavesdropping. That is, Alice transmits two consecutive symbols via Alamouti encoding matrix [1] given by $\mathbf{S}_n = \begin{bmatrix} s_1 & s_2 \\ -s_2^* & s_1^* \end{bmatrix}$, where $\mathbb{E}[s_i^2] = E_s$ for $i \in \{1, 2\}$ and (t, m)-th element of the matrix indicates the transmitted symbol of m-th antenna at t-th symbol time. The received signal of the receiver $k \in \{\mathrm{Bob}, \mathrm{Eve}\}$ over two symbol times can be represented as

$$\begin{bmatrix} r_{k,1} \\ r_{k,2}^* \end{bmatrix} = \begin{bmatrix} h_{k,1,1} & h_{k,2,1} \\ h_{k,2,2}^* & -h_{k,1,2}^* \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} + \begin{bmatrix} z_{k,1} \\ z_{k,2}^* \end{bmatrix}, \quad (1)$$

where $z_{k,t}$ is the additive complex white Gaussian noise with zero mean and variance σ_k^2 at the receiver k at the t-th symbol time. $h_{k,m,t}$ indicates the Rayleigh fading channel between Alice's m-th antenna and the antenna of receiver k at the t-th symbol time. The channels are assumed to be temporally correlated and their correlation degree is $\mathbb{E}[h_{k,i,1} h_{k,i,2}^*] = \rho_k$, where $\rho_k \in [0, 1]$. Note that $\rho_k = 0$ means the completely independent time-varying for every symbol times, while $\rho_k = 1$ means that the channels are static.

When the decision feedback detection is used at the receiver $k \in \{\mathrm{Bob}, \mathrm{Eve}\}$, its decision metric can be expressed as [3]

$$\hat{s}_{k,1} = \arg\min_{s \in S} \left\| r_{k,1} - \left(\zeta_k / \sqrt{\omega_k}\right) s \right\|^2, \quad (2)$$

$$\hat{s}_{k,2} = \arg\min_{s \in S} \left\| r_{k,2} - \sqrt{\omega_k} s - \left(\varepsilon_k^* / \sqrt{\omega_k}\right) \hat{s}_{k,1} \right\|^2, \quad (3)$$

where $\varepsilon_k = h_{k,1,1}^* h_{k,2,1} - h_{k,1,2}^* h_{k,2,2}$, $\zeta_k = |h_{k,1,1} h_{k,1,2}^* + h_{k,2,1} h_{k,2,2}^*|$, $\omega_k = |h_{k,1,2}|^2 + |h_{k,2,1}|^2$. Note that directly deriving the exact form of the received signal-to-noise ratio (SNR) is not easy. Instead, we approximate the received SNR of the receiver k with the DF detection for the transmit antenna $i = 1, 2$ as [3]

$$\gamma_{k,1} = (\zeta_k^2 / 2\omega_k) \bar{\gamma}_k, \quad \gamma_{k,2} \approx (\omega_k / 2) \bar{\gamma}_k, \quad (4)$$

where $\bar{\gamma}_k = 2E_s/\sigma_k^2$ represents the average SNR.

III. Achievable Secrecy Transmission Rates

In this section, we analyze the achievable secrecy transmission rate (STR) of Alamouti STBC with the DF detection in the time-selective fading channels. When the receiver $k \in \{\mathrm{Bob}, \mathrm{Eve}\}$ performs the DF detection, its achievable rate can be expressed as $R_k = \frac{1}{2}\sum_{i=1}^{2} \log_2\left(1+\gamma_{k,i}\right)$. According to Wyner's encoding scheme, transmission of message of rate R_{S} can be succeed when the achievable rate of Alice-Bob link is higher than R_{T} (i.e., connection outage) as well as that of Alice-Eve link is smaller than R_{E} (i.e., secrecy outage). Therefore, the STR for the secrecy message of rate R_{S} can be defined as the following [7].

$$T = R_{\mathrm{S}}\left(1-\mathbb{P}\left[\mathrm{E}_{\mathrm{co}}\right]\right)\left(1-\mathbb{P}\left[\mathrm{E}_{\mathrm{so}}\right]\right), \tag{5}$$

where $\mathbb{P}\left[\mathrm{E}_{\mathrm{co}}\right] = \mathbb{P}\left(R_{\mathrm{Bob}} \leq R_{\mathrm{T}}\right)$ and $\mathbb{P}\left[\mathrm{E}_{\mathrm{so}}\right] = \mathbb{P}\left(R_{\mathrm{Eve}} > R_{\mathrm{E}}\right)$.

The connection outage probability of Bob with the DF detection can be represented as

$$\mathbb{P}\left[\mathrm{E}_{\mathrm{co}}\right] = 1-\left(1+\left(1+|\rho_{\mathrm{Bob}}|^2\right)\frac{\bar{R}_{\mathrm{T}}}{\bar{\gamma}_{\mathrm{Bob}}}\right)e^{-\frac{2\bar{R}_{\mathrm{T}}}{\bar{\gamma}_{\mathrm{Bob}}}}, \tag{6}$$

where $\bar{R}_{\mathrm{T}} = 2^{R_{\mathrm{T}}}-1$. Similarly, the secrecy outage probability of Eve with the DF detection can be represented as

$$\mathbb{P}\left[\mathrm{E}_{\mathrm{so}}\right] = \left(1+\left(1+|\rho_{\mathrm{Eve}}|^2\right)\frac{\bar{R}_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{Eve}}}\right)e^{-\frac{2\bar{R}_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{Eve}}}}, \tag{7}$$

where $\bar{R}_{\mathrm{E}} = 2^{R_{\mathrm{E}}}-1$. Finally, by using (5), (6), and (7), the STR can be expressed as

$$\begin{aligned} T =& R_{\mathrm{S}}\left(1+\left(1+|\rho_{\mathrm{Bob}}|^2\right)\frac{\bar{R}_{\mathrm{T}}}{\bar{\gamma}_{\mathrm{Bob}}}\right)e^{-\frac{2\bar{R}_{\mathrm{T}}}{\bar{\gamma}_{\mathrm{Bob}}}} \\ &\times\left[1-\left(1+\left(1+|\rho_{\mathrm{Eve}}|^2\right)\frac{\bar{R}_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{Eve}}}\right)e^{-\frac{2\bar{R}_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{Eve}}}}\right]. \end{aligned} \tag{8}$$

As R_{T} increases and R_{E} decreases, R_{S} increases but both $\mathbb{P}\left[\mathrm{E}_{\mathrm{co}}\right]$ and $\mathbb{P}\left[\mathrm{E}_{\mathrm{so}}\right]$ increase. This motivates us to find optimal $R_{\mathrm{T}}^{\star}$ and $R_{\mathrm{E}}^{\star}$ to maximize the STR and they can be obtained by solving the following optimization problem.

$$\left(R_{\mathrm{T}}^{\star}, R_{\mathrm{E}}^{\star}\right) = \arg\max_{R_{\mathrm{T}}, R_{\mathrm{E}}} R_s^{p,q}, \text{ s.t. } R_{\mathrm{T}} \geq R_{\mathrm{E}} > 0. \tag{9}$$

Unfortunately, the above optimization problem is non-convex, so we can find the optimal solution by exhaustive searching.

IV. Numerical Results

We evaluate the STRs to verify our obtained insights that optimally choosing R_{T} and R_{E} can maximize the STR. Fig. 1 plots the contour maps of STRs and their maximum points versus R_{T} and R_{E} when two different detection methods (the proposed DF detection and the conventional LML detection) are adopted at Bob and Eve, where $E_s = 40$ (dBm) and $\rho_{\mathrm{Bob}} = \rho_{\mathrm{Eve}} = 0.9$. This figure shows that the STRs are superior in the order of DF-LML, DF-DF, LML-LML, LML-DF. This is because the DF detector can effectively eliminate the interference by temporal correlation and thus the decoding capability of DF detection is superior to that of LML detection.

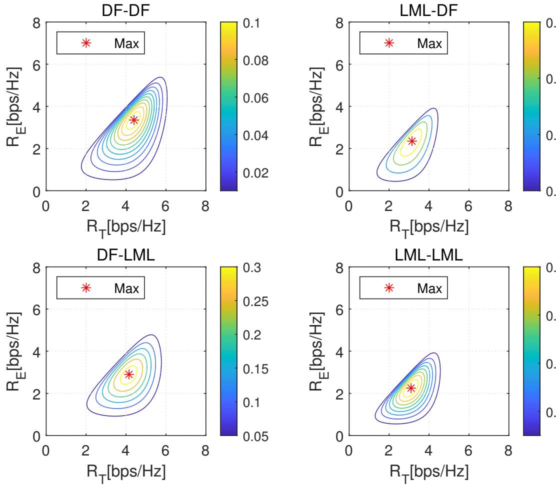

Fig. 1. Comparison of STRs versus R_{T} and R_{E}.

V. Conclusions

This paper has analyzed the secrecy performance of Alamouti STBC with decision feedback detection in wiretap time-selective fading channels. We have derived the achievable STRs with both connection and secrecy outage probabilities for an arbitrary temporal correlation and showed that optimally controlling codeword rate and secrecy rate can maximize the STRs.

Acknowledgments

This work was supported in part by the MSIT(Ministry of Science and ICT), Korea, under the ICAN(ICT Challenge and Advanced Network of HRD) program (IITP-2022-RS-2022-00156326) supervised by the IITP(Institute of Information & Communications Technology Planning & Evaluation) and in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2021R1F1A1050633).

References

[1] S. Alamouti, "A Simple Transmitter diversity technique for wireless communications" *IEEE J. Sel. Areas of Commun.*, vol. 16, no. 8, pp. 1451-1458, Oct. 1998.

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

[3] H. Lee, R. W. Heath, and E. J. Powers, "Information outage probability and diversity order of Alamouti transmit diversity in time-selective fading channels," *IEEE Trans. Vehi. Tech.*, vol. 16, no. 6, pp. 3890–3895, Nov. 2008.

[4] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1656–1667, Mar. 2014.

[5] T. Allen, A. Tajer, and N. AL-Dhahir, "Secure Alamouti multiple access channel transmissions: Multiuser transmission and multi-Antenna eavesdroppers," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1510-1513, Oct. 2019.

[6] S. H. Chae, I. Bang, and H. Lee, "Physical layer security of QSTBC with power scaling in MIMO wiretap channels," *IEEE Trans. Vehi. Tech.*, vol. 69, no. 5, pp. 5647-5651, May 2020.

[7] S. H. Chae, W. Choi, J. H. Lee, and T. Q. S. Quek, "Enhanced secrecy in stochastic wireless networks: artificial noise with secrecy protected zone," *IEEE Trans. Inform. Forensics and Security*, vol. 9, no. 10, pp. 1617-1628, Oct. 2014.