On the achievable secrecy transmission rates by Alamouti space-time block coding in time-selective fading channels

Dongjin Kim,[1] Girim Kwon,[2,✉] Hoojin Lee,[3] and Seong Ho Chae[4,✉]

[1] *Department of IT Semiconductor Convergence Engineering, Tech University of Korea, Siheung, South Korea*

[2] *Laboratory for Information and Decision Systems, Massachusetts Institute of Technology, Cambridge, Massachusetts, USA*

[3] *Division of IT Convergence Engineering, Hansung University, Seoul, South Korea*

[4] *Department of Electronics Engineering, Tech University of Korea, Siheung, South Korea*

✉ Email: shchae@tukorea.ac.kr; girimk@mit.edu

In this letter, the authors study the security performance of Alamouti space-time block coding (STBC) with two different linear detection strategies, linear maximum likelihood (LML) and zero-forcing (ZF), over time-selective Rayleigh fading channels. Specifically, the connection and secrecy outage probabilities for general temporal correlation when the legitimate receiver and eavesdropper adopt the LML and ZF detectors are first derived. Then the secrecy transmission rates for various combinations of LML and ZF detectors at the legitimate receiver and eavesdropper are derived. The authors also found that the optimal control of the codeword rate and secrecy rate can maximize the secrecy transmission rates.

Introduction: Physical layer security (PLS) has recently received a great deal of attention as a promising solution to improve the security of wireless communication. Unlike the traditional complexity-based cryptographic solutions, PLS can protect wireless communications against eavesdropping attacks by exploiting the intrinsic randomness of wireless channels, for example, fading, noise, interference. The space-time block coding (STBC) has been deemed as a key technique to exploit the spatial and temporal diversity for multiple-input multiple-output (MIMO) systems. The first orthogonal STBC was proposed by Alamouti [1] for two transmit antennas and it was shown that full diversity and full data rate can be achieved via linear maximum likelihood (LML) detection in the quasi-static channels. There have been continuous efforts to utilize Alamouti STBC for PLS [2–6]. The optimal power allocation with two best transmit antenna selection for Alamouti STBC was proposed, and its secrecy outage probability (SOP) was investigated in MIMO wiretap channels [2]. The Alamouti STBC with random phase rotations for secure communication was proposed in [3]. The SOP and the asymptotic secrecy diversity order of Alamouti STBC with the modified transmit antenna selection were analysed for MIMO wiretap channels having the feedback errors [4]. Li et al. analysed the exact and asymptotic SOPs for perfect and imperfect successive interference cancellations in Alamouti STBC non-orthogonal multiple access [5]. The closed-form approximated SOP of the quasi-orthogonal STBC that linearly combines two Alamouti STBC was derived in [6]. However, these works were built up on the quasi-static fading channels, so they cannot be directly applicable to the time-selective fading channels.

When the channels experience the time-selective fading, the orthogonal property of Alamouti STBC does not hold, and the maximum performance of Alamouti STBC cannot be achieved due to the interference caused by time correlation. Motivated by this, here, we study how much security performance can be achieved by Alamouti STBC with two different linear detection strategies, LML and zero-forcing (ZF), over time-selective Rayleigh fading channels. To this end, we first derive the connection and SOPs of a legitimate receiver and an eavesdropper with LML and ZF detectors for a general temporal correlation. We then derive the secrecy transmission rates for various combinations of LML and ZF detectors at the legitimate receiver and eavesdropper and investigate how to optimally construct the nested structured Wyner's codebook, that is, how to optimally choose the codeword rate and secrecy rate, to maximize the secrecy transmission rate. We also discover that the secrecy transmission rates are higher in the order of ZF-LML, ZF-ZF, LML-LML, LML-ZF and they are mainly influenced by the detection method of legitimate receiver rather than that of eavesdropper.

System model: We consider a multiple-input single-output (MISO) wiretap channel where a transmitter (Alice) sends a secret message to a receiver (Bob) via Alamouti STBC and a passive eavesdropper (Eve) overhears it. Alice has two transmit antennas and both Bob and Eve have a single receive antenna. Bob and Eve have the full channel state information (CSI) of their own channels, while Alice does not have any CSI. Alice has the total transmit energy $2E_s$ and allocates equal energy E_s to each antenna per each symbol duration due to the lack of CSI. The channels are assumed to experience the time-selective Rayleigh fading which varies for every symbol intervals with a certain degree of correlation. For notational simplicity, we denote Bob and Eve as B and E, respectively, throughout the letter.

Due to the lack of CSI, Alice sets a constant secrecy rate R_S and constructs Wyner's codebook with a nested structure by arbitrarily choosing two rates $R_T (> R_E)$ and R_E such that $R_S = R_T - R_E$ [7, 8]. Alice transmits the codeword to Bob against Eve's eavesdropping by using Alamouti STBC. Specifically, Alice transmits two consecutive symbols s_1 and s_2 by constructing Alamouti encoding matrix [1] given by $\mathbf{S}_n = \begin{bmatrix} s_1 & s_2 \\ -s_2^* & s_1^* \end{bmatrix}$, where $\mathbb{E}[s_1^2] = \mathbb{E}[s_2^2] = E_s$ and (t, m)-th element represents the symbol transmitted from m-th antenna at t-th symbol duration.

Then, the received signal of the receiver $k \in \{B, E\}$ over two time instants can be written as

$$\underbrace{\begin{bmatrix} r_{k,1} \\ r_{k,2}^* \end{bmatrix}}_{\mathbf{r}_k} = \underbrace{\begin{bmatrix} h_{k,1,1} & h_{k,2,1} \\ h_{k,2,2}^* & -h_{k,1,2}^* \end{bmatrix}}_{\mathbf{H}_k} \underbrace{\begin{bmatrix} s_1 \\ s_2 \end{bmatrix}}_{\mathbf{s}} + \underbrace{\begin{bmatrix} z_{k,1} \\ z_{k,2}^* \end{bmatrix}}_{\mathbf{z}_k}, \tag{1}$$

where $z_{k,t}$ represents the additive complex white Gaussian noise with zero mean and variance σ_k^2 at the receiver k at t-th symbol period. $h_{k,m,t}$ represents the channel between the m-th transmit antenna of Alice and the receive antenna of the receiver k at t-th symbol period. It is modelled as an identically distributed complex Gaussian random variable with zero mean and unit variance. The channels are spatially uncorrelated, but temporally correlated with a correlation $\mathbb{E}[h_{k,i,1} h_{k,i,2}^*] = \rho_k$, where $\rho_k \in [0, 1]$. Note that $\rho_k = 0$ implies the independently time-varying channels for every symbol periods, while $\rho_k = 1$ implies the static channel.

The successful transmission of secrecy rate R_S can occur when the channel capacity of Alice–Bob link is higher than R_T as well as that of Alice–Eve link is smaller than R_E. Therefore, let us define two outage events as follows:

- $\mathrm{E}_{\mathrm{co}}^p$(connection outage): When Bob adopts the detection method $p \in \{\mathrm{LML}, \mathrm{ZF}\}$, the channel capacity of Alice–Bob link is smaller than the transmitted codeword rate R_T, so the transmitted codeword cannot be decoded.
- $\mathrm{E}_{\mathrm{so}}^q$(secrecy outage): When Eve adopts the detection method $q \in \{\mathrm{LML}, \mathrm{ZF}\}$, the channel capacity of Alice–Eve link is higher than R_E, so the perfect secrecy cannot be guaranteed.

Then, the secrecy transmission rate for the secrecy rate R_S can be defined as follows [7, 8]:

$$R_s^{p,q} = R_S\big(1 - \Pr[\mathrm{E}_{\mathrm{co}}^p]\big)\big(1 - \Pr[\mathrm{E}_{\mathrm{so}}^q]\big), \tag{2}$$

where $\Pr[\mathrm{E}_{\mathrm{co}}^p] = \Pr(C_{\mathrm{B}}^p \le R_T)$ and $\Pr[\mathrm{E}_{\mathrm{so}}^q] = \Pr(C_{\mathrm{E}}^q > R_E)$, where C_{B}^p and C_{E}^q represent the achievable rates of Alice–Bob link with a detection method p and Alice–Eve link with a detection method q, respectively.

Two linear detection strategies: The decision statistic vector can be obtained by multiplying the matched filter matrix $\mathbf{H}_k^H$ to the received vector in (1) as

$$\tilde{\mathbf{r}}_k = \mathbf{H}_k^H \mathbf{H}_k + \mathbf{H}_k^H \mathbf{z}_k = \mathbf{G}_k \mathbf{s} + \tilde{\mathbf{z}}_k, \tag{3}$$

where $\mathbf{G}_k = \begin{bmatrix} \omega_{k,1} & \varepsilon_k \\ \varepsilon_k^* & \omega_{k,2} \end{bmatrix}$, where $\varepsilon_k = h_{k,1,1}^* h_{k,2,1} - h_{k,1,2}^* h_{k,2,2}$, $\omega_{k,1} = |h_{k,1,1}|^2 + |h_{k,2,2}|^2$, $\omega_{k,2} = |h_{k,1,2}|^2 + |h_{k,2,1}|^2$. If the channel is static, $\mathbf{H}$ becomes orthogonal and $\omega_{k,1} = \omega_{k,2}$ and $\varepsilon_k = 0$ hold. However, when

the channel is time-selective, $\mathbf{H}$ becomes no longer orthogonal and non-zero off-diagonal component ε_k survives in $\mathbf{G}_k$, which causes the interference in decoding of the symbols.

We consider two linear detection strategies, LML and ZF, for decoding of Bob and Eve. The LML detector is the conventional decoding scheme for Alamouti code in quasi-static channels. When the conventional LML detector is adopted at the receiver $k \in \{\mathrm{B}, \mathrm{E}\}$, its decision rule can be represented by

$$\hat{s}_{k,i}^{\mathrm{LML}} = \arg\min_{s_i \in S} \|r_{k,i}^{\mathrm{LML}} - \omega_{k,i}^{1/2} s_i\|^2, \quad \text{for } i = 1, 2, \tag{4}$$

where $\mathbf{r}_k^{\mathrm{LML}} = \mathbf{\Theta}_k \mathbf{H}_k^H \mathbf{r}_k$, where $\mathbf{\Theta}_k = \begin{bmatrix} \omega_{k,1}^{-1/2} & 0 \\ 0 & \omega_{k,2}^{-1/2} \end{bmatrix}$. The received signal-to-noise ratio (SNR) of the receiver k with LML detector for the transmit symbol index $i = 1, 2$ can be represented by

$$\gamma_{k,i}^{\mathrm{LML}} = \frac{E_s}{E_s\left(1 - |\rho_k|^2\right) + \sigma_k^2} \omega_{k,i} = \frac{\bar{\gamma}_k}{\left(1 - |\rho_k|^2\right)\bar{\gamma}_k + 2} \omega_{k,i}, \tag{5}$$

where $\bar{\gamma}_k = 2E_s/\sigma_k^2$ is the average SNR at the receive antenna.

The ZF detector can eliminate the off-diagonal terms ε_k in $\mathbf{G}_k$. When the ZF detector is adopted at the receiver $k \in \{\mathrm{B}, \mathrm{E}\}$, its decision rule can be represented by

$$\hat{s}_{k,i}^{\mathrm{ZF}} = \arg\min_{s_i \in S} \|r_{k,i}^{\mathrm{ZF}} - \zeta_k \omega_{k,3-i}^{-1/2} s_i\|^2, \quad \text{for } i = 1, 2, \tag{6}$$

where $\mathbf{r}_k^{\mathrm{ZF}} = \mathbf{\Phi}_k \mathbf{G}_k^{-1} \mathbf{H}_k^H \mathbf{r}_k$, where $\mathbf{\Phi}_k = \begin{bmatrix} \zeta_k \omega_{k,2}^{-1/2} & 0 \\ 0 & \zeta_k \omega_{k,2}^{-1/2} \end{bmatrix}$ and $\zeta_k = |h_{k,1,1} h_{k,1,2}^* + h_{k,2,1} h_{k,2,2}^*|$. The received SNR of the receiver $k \in \{\mathrm{B}, \mathrm{E}\}$ with ZF detector for the transmit symbol index $i = 1,\ 2$ can be represented by

$$\gamma_{k,i}^{\mathrm{ZF}} = \frac{\zeta_k^2 E_s}{\omega_{k,3-i}\sigma_k^2} = \frac{\zeta_k^2}{2\omega_{k,3-i}} \bar{\gamma}_k. \tag{7}$$

Secrecy transmission rates: We analyse the secrecy transmission rate of Alamouti STBC with two linear detection strategies, LML and ZF, over the time-selective fading channels.

When Bob adopts the detection method $p \in \{\mathrm{LML}, \mathrm{ZF}\}$, the achievable rate between Alice and Bob in bits per second per hertz over a time-selective fading channel is given by [9]

$$\mathrm{C}_{\mathrm{B}}^p = \frac{1}{2} \sum_{i=1}^{2} \log_2\left(1 + \gamma_{\mathrm{B},i}^p\right). \tag{8}$$

Similarly, when Eve adopts the detection strategy $q \in \{\mathrm{LML}, \mathrm{ZF}\}$, the achievable rate between Alice and Eve in bits per second per hertz over a time-selective fading channel is given by

$$\mathrm{C}_{\mathrm{E}}^q = \frac{1}{2} \sum_{i=1}^{2} \log_2\left(1 + \gamma_{\mathrm{E},i}^q\right). \tag{9}$$

The connection outage probability of Bob with LML detector can be approximated as the first output of LML detector [10], so it can be expressed as

$$\Pr\left[\mathrm{E}_{\mathrm{co}}^{\mathrm{LML}}\right] = \Pr\left[C_{\mathrm{B}}^{\mathrm{LML}} \le R_{\mathrm{T}}\right] \backsimeq \Pr\left[\gamma_{\mathrm{B},1}^{\mathrm{LML}} \le \bar{R}_{\mathrm{T}}\right] \tag{10}$$

$$= \Pr\left[\omega_{k,1} < 2\left(1 - |\rho_{\mathrm{B}}|^2 + \frac{2}{\gamma_{\mathrm{B}}}\right)\bar{R}_{\mathrm{T}}\right] \tag{11}$$

$$= 1 - \left(1 + \left(1 - |\rho_{\mathrm{B}}|^2 + \frac{2}{\bar{\gamma}_{\mathrm{B}}}\right)\bar{R}_{\mathrm{T}}\right) e^{-\left(1 - |\rho_{\mathrm{B}}|^2 + \frac{2}{\bar{\gamma}_{\mathrm{B}}}\right)\bar{R}_{\mathrm{T}}}, \tag{12}$$

where $\bar{R}_{\mathrm{T}} = 2^{R_{\mathrm{T}}} - 1$ and $\omega_{k,1}$ follows the central chi-square distribution with 4 degrees of freedom.

For the ZF detector, $\gamma_{\mathrm{B},1}^{\mathrm{ZF}}$ and $\gamma_{\mathrm{B},2}^{\mathrm{ZF}}$ have the same distribution given by $p_{\gamma_{\mathrm{B},1}}^{\mathrm{ZF}}(x) = p_{\gamma_{\mathrm{B},2}}^{\mathrm{ZF}}(x) = \vartheta_{\mathrm{B}}(1 + \eta_{\mathrm{B}} x) e^{-(\nu_{\mathrm{B}} - \eta_{\mathrm{B}})x}$ with $\vartheta_{\mathrm{B}} = 2(1 - |\rho_{\mathrm{B}}|^2)/\bar{\gamma}_{\mathrm{B}}$, $\eta_{\mathrm{B}} = 2|\rho_{\mathrm{B}}|^2/(1 - |\rho_{\mathrm{B}}|^2)\bar{\gamma}_{\mathrm{B}}$, and $\nu_{\mathrm{B}} = 2/(1 - |\rho_{\mathrm{B}}|^2)\bar{\gamma}_{\mathrm{B}}$ [11]. Accordingly, the connection outage probability of Bob with ZF detector can be expressed as

$$\Pr\left[\mathrm{E}_{\mathrm{co}}^{\mathrm{ZF}}\right] = \Pr\left[C_{\mathrm{B}}^{\mathrm{ZF}} \le R_{\mathrm{T}}\right] \backsimeq \Pr\left[\gamma_{\mathrm{B},1}^{\mathrm{ZF}} \le \bar{R}_{\mathrm{T}}\right] \tag{13}$$

$$= \int_0^{\bar{R}_{\mathrm{T}}} \vartheta_{\mathrm{B}}(1 + \eta_{\mathrm{B}} x) e^{-(\nu_{\mathrm{B}} - \eta_{\mathrm{B}})x} dx \tag{14}$$

$$= 1 - \left(1 + 2|\rho_{\mathrm{B}}|^2 \frac{\bar{R}_{\mathrm{T}}}{\bar{\gamma}_{\mathrm{B}}}\right) e^{-\frac{2\bar{R}_{\mathrm{T}}}{\bar{\gamma}_{\mathrm{B}}}}. \tag{15}$$

Similarly, the SOPs of Eve with $q \in \{\mathrm{LML}, \mathrm{ZF}\}$ detection can be written by

$$\Pr\left[\mathrm{E}_{\mathrm{so}}^{\mathrm{LML}}\right] = \Pr\left[C_{\mathrm{E}}^{\mathrm{LML}} > R_{\mathrm{E}}\right] \tag{16}$$

$$= \left(1 + \left(1 - |\rho_{\mathrm{E}}|^2 + \frac{2}{\bar{\gamma}_{\mathrm{E}}}\right)\bar{R}_{\mathrm{E}}\right) e^{-\left(1 - |\rho_{\mathrm{E}}|^2 + \frac{2}{\bar{\gamma}_{\mathrm{E}}}\right)\bar{R}_{\mathrm{E}}}, \tag{17}$$

$$\Pr\left[\mathrm{E}_{\mathrm{so}}^{\mathrm{ZF}}\right] = \Pr\left[C_{\mathrm{E}}^{\mathrm{ZF}} > R_{\mathrm{E}}\right] = \left(1 + 2|\rho_{\mathrm{E}}|^2 \frac{\bar{R}_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{E}}}\right) e^{-\frac{2\bar{R}_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{E}}}}, \tag{18}$$

where $\bar{R}_{\mathrm{E}} = 2^{R_{\mathrm{E}}} - 1$.

Consequently, by plugging (12), (15), (17) and (18) into (2), the secrecy transmission rates for all possible combinations can be written by (19), (20), (21) and (22), respectively.

$$R_s^{\mathrm{LML,LML}} = R_{\mathrm{S}}\left(1 + \left(1 - |\rho_{\mathrm{B}}|^2 + \frac{2}{\bar{\gamma}_{\mathrm{B}}}\right)\bar{R}_{\mathrm{T}}\right) e^{-\left(1 - |\rho_{\mathrm{B}}|^2 + \frac{2}{\bar{\gamma}_{\mathrm{B}}}\right)\bar{R}_{\mathrm{T}}} \left[1 - \left(1 + \left(1 - |\rho_{\mathrm{E}}|^2 + \frac{2}{\bar{\gamma}_{\mathrm{E}}}\right)\bar{R}_{\mathrm{E}}\right) e^{-\left(1 - |\rho_{\mathrm{E}}|^2 + \frac{2}{\bar{\gamma}_{\mathrm{E}}}\right)\bar{R}_{\mathrm{E}}}\right]. \tag{19}$$

$$R_s^{\mathrm{LML,ZF}} = R_{\mathrm{S}}\left(1 + \left(1 - |\rho_{\mathrm{B}}|^2 + \frac{2}{\bar{\gamma}_{\mathrm{B}}}\right)\bar{R}_{\mathrm{T}}\right) e^{-\left(1 - |\rho_{\mathrm{B}}|^2 + \frac{2}{\bar{\gamma}_{\mathrm{B}}}\right)\bar{R}_{\mathrm{T}}} \left(1 - \left(1 + 2|\rho_{\mathrm{E}}|^2 \frac{\bar{R}_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{E}}}\right) e^{-\frac{2\bar{R}_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{E}}}}\right). \tag{20}$$

$$R_s^{\mathrm{ZF,LML}} = R_{\mathrm{S}}\left(1 + 2|\rho_{\mathrm{B}}|^2 \frac{\bar{R}_{\mathrm{T}}}{\bar{\gamma}_{\mathrm{B}}}\right) e^{-\frac{2\bar{R}_{\mathrm{T}}}{\bar{\gamma}_{\mathrm{B}}}} \left[1 - \left(1 + \left(1 - |\rho_{\mathrm{E}}|^2 + \frac{2}{\bar{\gamma}_{\mathrm{E}}}\right)\bar{R}_{\mathrm{E}}\right) e^{-\left(1 - |\rho_{\mathrm{E}}|^2 + \frac{2}{\bar{\gamma}_{\mathrm{E}}}\right)\bar{R}_{\mathrm{E}}}\right]. \tag{21}$$

$$R_s^{\mathrm{ZF,ZF}} = R_{\mathrm{S}}\left(1 + 2|\rho_{\mathrm{B}}|^2 \frac{\bar{R}_{\mathrm{T}}}{\bar{\gamma}_{\mathrm{B}}}\right) e^{-\frac{2\bar{R}_{\mathrm{T}}}{\bar{\gamma}_{\mathrm{B}}}} \left(1 - \left(1 + 2|\rho_{\mathrm{E}}|^2 \frac{\bar{R}_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{E}}}\right) e^{-\frac{2\bar{R}_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{E}}}}\right). \tag{22}$$

For given R_{E}, as R_{T} increases, the secrecy rate R_{S} increases, but the connection outage probability increases. Similarly, for given R_{T}, as R_{E} decreases, the secrecy rate R_{S} increases, but the SOP increases. These relationships motivate us to find the optimal $R_{\mathrm{T}}^\star$ and $R_{\mathrm{E}}^\star$ to maximize the secrecy transmission rate. Therefore, for given detection strategy combinations $p \in \{\mathrm{LML}, \mathrm{ZF}\}$ of Bob and $q \in \{\mathrm{LML}, \mathrm{ZF}\}$ of Eve, the optimal $R_{\mathrm{T}}^\star$ and $R_{\mathrm{E}}^\star$ can be found by solving the following optimization problem.

$$(R_{\mathrm{T}}^\star, R_{\mathrm{E}}^\star) = \arg\max_{R_{\mathrm{T}}, R_{\mathrm{E}}} R_s^{p,q} \tag{23}$$

$$\text{subject to } R_{\mathrm{T}} \ge R_{\mathrm{E}} \ge 0. \tag{24}$$

However, unfortunately, the optimization problem is non-convex optimization problem, so the optimal solution can be found by relying on the brute-force searching. Specifically, we choose the sufficiently large value of $R_{\mathrm{T}}^{\mathrm{up}}$ which makes $R_s^{p,q} \approx 0$ and set $R_{\mathrm{E}}^{\mathrm{up}} = R_{\mathrm{T}}^{\mathrm{up}}$. Then, we quantize the ranges of $0 \le R_{\mathrm{E}} \le R_{\mathrm{E}}^{\mathrm{up}}$ and $0 \le R_{\mathrm{T}} \le R_{\mathrm{T}}^{\mathrm{up}}$ with L equi-spaced values and examine the secrecy transmission rates for all quantized values to find the optimal $R_{\mathrm{T}}^\star$ and $R_{\mathrm{E}}^\star$ which maximize the secrecy transmission rate.

Numerical results: In this section, we evaluate the secrecy transmission rates of Alamouti STBC with the combination of two detectors, LML and ZF, over MISO wiretap time-selective Rayleigh fading channels, to verify our analytical results in previous sections and understand how various system parameters affect the secrecy transmission rates. We consider the first-order autoregression model AR(1) for the time-selective channel fading [12]. Unless otherwise stated, the baseline simulation parameters are as follows: $E_s = 45$ (dBm), $R_{\mathrm{T}} = 3$ (bps/Hz), $R_{\mathrm{E}} = 2$ (bps/Hz), $\rho_{\mathrm{B}} = \rho_{\mathrm{E}} = 0.95$, $\sigma_{\mathrm{B}}^2 = \sigma_{\mathrm{E}}^2 = 1$.

Figure 1 plots the Monte Carlo simulated connection and SOPs of LML and ZF (marks) and their analysis (lines) versus the average symbol energy E_s(dBm) for various ρ_{B} and ρ_{E}. This figure verifies that our

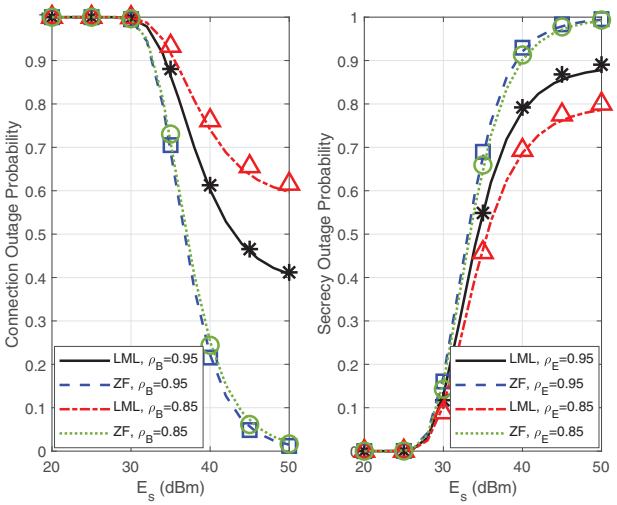

Fig. 1 *Comparison of the Monte Carlo simulated connection and secrecy outage probabilities (marks) and their analysis (line) versus E_s for various ρ_B and ρ_E*

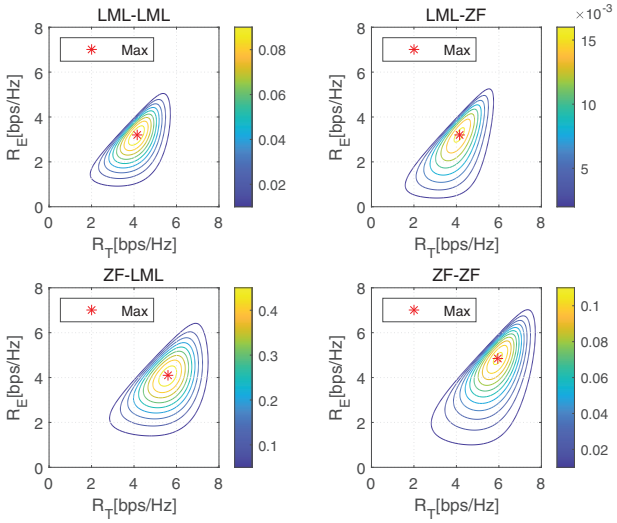

Fig. 2 *Contour maps of secrecy transmission rates for LML–LML, LML–ZF, ZF–LML, ZF–ZF versus R_T and R_E*

analytical results (12), (15), (17) and (18) match well with the Monte Carlo simulation results for general value of ρ_B and ρ_E. As E_s increases, the connection outage probability decreases, while the SOP increases. This is because the received SNRs of Bob and Eve simultaneously increase. This figure also shows that the connection outage probabilities of LML and ZF detectors increase as ρ_B decreases and the SOPs of LML and ZF detectors decrease as ρ_E decreases. This implies that the low temporal correlation (i.e. independently time-varying channels) disturbs the decoding of Bob and Eve, which can be beneficial from the perspective of security. This figure shows that the ZF detector is superior to the LML detector because the ZF detector can effectively cancel the off-diagonal interference terms caused by low temporal correlation.

Figure 2 plots the contour maps of secrecy transmission rates and their maximum points versus R_T and R_E for the combinations of LML–LML, LML–ZF, ZF–LML, ZF–ZF. Interestingly, the secrecy transmission rates are higher in the order of ZF–LML, ZF–ZF, LML–LML, LML–ZF. This implies that the decoding capability of ZF detector is superior to that of LML detector and the detection strategy of Bob is more dominant than that of Eve in terms of secrecy transmission rate. This figure validates that the optimal control of R_T and R_E can maximize the secrecy transmission rate.

Conclusions: We have studied the PLS of Alamouti STBC with two linear detection methods, LML and ZF, over MISO wiretap time-selective Rayleigh fading channels. For arbitrary temporal correlation, we have derived the connection and SOPs of legitimate receiver and eavesdropper for LML and ZF detectors and then derived the secrecy transmission rates for four different combinations of detection strategies, LML–LML, LML–ZF, ZF–LML, ZF–ZF. We have found that the secrecy transmission rates are higher in the order of ZF–LML, ZF–ZF, LML–LML, LML–ZF and they are mainly influenced by the detection method of legitimate receiver rather than that of eavesdropper. We have discovered that the optimal control of transmit codeword rate and secrecy rate can maximize the secrecy transmission rate. Our analytical results can be applied to any secured mobile networks such as vehicular networks.

Acknowledgements: This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the Grand Information Technology Research Center support program (IITP-2020-0-101741) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation). The work of Hoojin Lee was financially supported by Hansung University

Conflict of interest: The authors have declared no conflict of interest.

Data availability statement: Data sharing is not applicable to this article as no new data were created or analysed in this study.

Received: *27 May 2022* Accepted: *12 June 2022*
doi: 10.1049/ell2.12563

References

1 Alamouti, S.M.: A Simple transmitter diversity technique for wireless communications. *IEEE J. Sel. Areas Commun.* **16**(8), 1451–1458 (1998)
2 Yan, S., Yang, N., Malaney, R., Yuan, J.: Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels. *IEEE Trans. Wireless Commun.* **13**(3), 1656–1667 (2014)
3 Allen, T., Cheng, J., Al-Dhahir, N.: Secure space-time block coding without transmitter CSI. *IEEE Wireless Commun. Lett.* **3**(6), 573–576 (2014)
4 Coşkun, A.F., Kucur, O.: Secrecy outage probability of conventional and modified TAS/Alamouti-STBC schemes with power allocation in the presence of feedback errors. *IEEE Trans. Veh. Technol.* **68**(3), 2609–2623 (2019)
5 Li, M., Yuan, H., Yue, X., Mudaidat, S., Maple, C., and Diannati, M.: Secrecy outage analysis for Alamouti space–time block coded non-orthogonal multiple access. *IEEE Commun. Lett.* **24**(7), 1405–1409 (2020)
6 Chae, S.H., Bang, I., Lee, H.: Physical layer security of QSTBC with power scaling in MIMO wiretap channels. *IEEE Trans. Veh. Technol.* **69**(5), 5647–5651 (2020)
7 Chae, S.H., Choi, W., Lee, J.H., Quek, T.Q.S.: Enhanced secrecy in stochastic wireless networks: artificial noise with secrecy protected zone. *IEEE Trans. Inf. Forensics Security* **9**(10), 1617–1628 (2014)
8 Chae, S.H., Choi, W.: Optimal power allocation for artificial noise in a poisson interference field. *IEEE Commun. Lett.* **20**(8), 1671–1674 (2016)
9 Lee, H., Heath, R.W., Powers, E.J.: Information outage probability and diversity order of Alamouti transmit diversity in time-selective fading channels. *IEEE Trans. Veh. Technol.* **16**(6), 3890–3895 (2008)
10 Vielmon, A., Li, Y., Barry, J.R.: Performance of Alamouti transmit diversity over time-varying Rayleigh-fading channels. *IEEE Trans. Wireless Commun.* **3**(5), 1369–1373 (2004)
11 Lin, D.-B., Chiang, P.-H., Li, H.-J.: Performance analysis of two-branch transmit diversity block-coded OFDM systems in time-varying multipath Rayleigh-fading channels. *IEEE Trans. Veh. Technol.* **54**(1), 136–148 (2005)
12 Tran, T.A., Sesay, A.B.: A generalized linear quasi-ML decoder of OSTBCs for wireless communications over time-selective fading channels. *IEEE Trans. Wireless Commun.* **3**(3), 855–864 (2004)