KICS The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express 9 (2023) 714–721

www.elsevier.com/locate/icte

Secrecy outage probability and diversity order of Alamouti STBC over time-selective fading channels

Seong Ho Chae[a], Hoojin Lee[b,*]

[a] Department of Electronics Engineering, Tech University of Korea, Siheung, 15073, Republic of Korea
[b] Department of Convergence Security, Hansung University, Seoul, 02876, Republic of Korea

Received 16 March 2022; received in revised form 21 January 2023; accepted 2 February 2023
Available online 8 February 2023

Abstract

This paper studies physical layer security for Alamouti space–time block code (STBC) with joint maximum likelihood (JML) or zero forcing (ZF) detection techniques particularly over multi-input single-output (MISO) wiretap time-selective Rayleigh fading channels. Specifically, we derive the secrecy outage probabilities (SOPs) and their concise but effective approximations for various combinations of JML and ZF at the legitimate receiver and eavesdropper. We also investigate the secrecy diversity gain by applying the high signal-to-noise ratio (SNR) approximation of SOP and prove that the corresponding asymptotic diversity order of two, two, one, and one can be achieved for JML-JML, JML-ZF, ZF-JML, and ZF-ZF, respectively. Our asymptotic analytical results corroborate that the secrecy diversity order is dominantly affected by the detection strategy of the legitimate receiver rather than that of the eavesdropper.

Keywords: Physical layer security; Alamouti space–time block code; Time-selective fading; Secrecy diversity order; Secrecy outage probability

1. Introduction

Multiple-Input Multiple-Output (MIMO) has become a key technology for modern wireless communication systems. Since mid-1990s, the space–time block coding, which is able to exploit the spatial and temporal diversity, has continuously drawn much attention as a key MIMO transmission technology. The first simple orthogonal space–time block code (OSTBC) was proposed for two transmit antennas system by Alamouti [1] and it was shown that full diversity and full data rate can be achieved through a simple symbolwise linear maximum-likelihood (LML) detection over the quasi-static channels. This pioneering work triggered researches on developing various OSTBCs and quasi-orthogonal STBCs (QSTBCs) to achieve either full diversity or full data rate for more than two transmit antenna systems [2]. However, when the channel is time-selective, the LML decoding no longer offers optimum performance because the channel matrix is no longer orthogonal and the transmit antennas interfere with each other. To resolve this issue, various advanced detection techniques for the STBC have been proposed for time-selective fading channels, including joint maximum likelihood (JML), zero forcing (ZF), decision feedback (DF), etc. [3–5].

Security is always an important issue in wireless communication due to the broadcast nature of the radio signals. Physical layer security (PLS), which can ensure secure communications by exploiting the physical characteristics of wireless channel, has received a great deal of attention in the past few years. The average secrecy capacity and secrecy outage probability (SOP) were analyzed over $\alpha-\eta-\kappa-\mu$ fading channel which is a generalized fading model encompassing Rayleigh, Hoyt, Rice, Weibul, $\kappa-\mu$ and $\alpha-\mu$ channels [6]. The average secrecy capacity and SOP when the main channel and eavesdropper channels experience the spatially correlated $\alpha-\mu$ fading channels [7]. However, these papers did not consider the space–time block codes and the temporally correlated time-selective fading channels.

Many studies have been carried out to understand PLS of Alamouti STBC-based secure wireless communication system [8–11]. The SOP of two transmit antenna selection with Alamouti STBC code and power allocation scheme was investigated in MIMO wiretap channels [8]. The modified two transmit antenna selection with Alamouti STBC and power allocation scheme in the presence of feedback errors was

* Corresponding author.
E-mail addresses: shchae@tukorea.ac.kr (S.H. Chae), hjlee@hansung.ac.kr (H. Lee).
Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

https://doi.org/10.1016/j.icte.2023.02.004

proposed in MIMO wiretap channels [9]. The exact and approximated SOPs of QSTBC were investigated in MIMO wiretap channels [10]. The SOP of a STBC non-orthogonal multiple access was analyzed [11]. However, those works were built up on the static fading channels, so they cannot be directly implemented for time-selective fading channels, which is the main focus of this paper.

There have been also a few trials to study PLS for time-selective fading channels [12–14]. However, the works [12, 13] did not consider the Alamouti STBC and [14] failed to discover the secrecy diversity order of SOP. Motivated by this observation, our paper studies PLS of Alamouti STBC with two different detection strategies over MISO wiretap time-selective Rayleigh fading channels. Specifically, we consider JML and ZF as the detection strategies of the legitimate receiver and the eavesdropper, and analyze the SOPs of their all possible combinations, i.e., JML-JML, JML-ZF, ZF-JML, and ZF-ZF. We further investigate the secrecy diversity gain from the high SNR approximation of SOP and prove that the secrecy diversity order of two, two, one, and one can be achieved for JML-JML, JML-ZF, ZF-JML, and ZF-ZF, respectively. Finally, we verify the accuracy of our analytical results with some numerical simulations.

2. System model

We consider MISO wiretap channels, in which a transmitter (Alice) is equipped with two transmit antennas and both a legitimate receiver (Bob) and a passive eavesdropper (Eve) have a single antenna each. The channel state information (CSI) is assumed to be available at Bob and Eve. Alice has total transmit energy $2E_s$ per symbol duration and allocates equal transmit energy E_s to each transmit antenna for data symbol transmission. We assume that all channels experience the *time-selective Rayleigh fading* which varies for every symbol intervals, but is temporally correlated with a certain degree. For notational simplicity, we denote Bob and Eve as B and E, respectively, throughout the paper.

Alice wants to send the message to Bob securely against eavesdropping of Eve by adopting orthogonal Alamouti STBC to achieve the full diversity. Specifically, for nth codeword interval, Alice transmits two consecutive data symbols s_{2n-1} and s_{2n} by constructing the following 2×2 Almouti encoding matrix [1] given by

$$\mathbf{S}_n = \begin{bmatrix} s_{2n-1} & s_{2n} \\ -s_{2n}^* & s_{2n-1}^* \end{bmatrix}, \tag{1}$$

where $\mathbb{E}[s_{2n-1}^2] = \mathbb{E}[s_{2n}^2] = E_s$, $\forall n \in \{1, 2, \ldots\}$, where E_s represents the average symbol energy. The (t, m)-th element of the matrix represents the transmitted symbol from mth antenna at tth symbol period. Note that Alamouti STBC transmits two data symbols via two transmit antennas over two symbol periods. Specifically, Alice simultaneously transmits two data symbols s_{2n-1} and s_{2n} via antenna 1 and 2 in the first symbol period and then transmits two data symbols $-s_{2n}^*$ and s_{2n-1}^* via transmit antennas 1 and 2 in the second symbol period.

Then, the received signal of Bob and Eve (i.e., $k \in \{\mathrm{B}, \mathrm{E}\}$) over two time instants is given in the matrix form as

$$\mathbf{r}_{k,n} = \mathbf{H}_{k,n}\mathbf{s}_n + \mathbf{z}_{k,n}, \tag{2}$$

where $\mathbf{r}_{k,n} = \left[r_{k,2n-1}, r_{k,2n}^*\right]^T$ and $\mathbf{z}_{k,n} = \left[z_{k,2n-1}, z_{k,2n}^*\right]^T$ represent the received signal vector and the additive noise vector of the receiver $k \in \{\mathrm{B}, \mathrm{E}\}$ respectively, $\mathbf{s}_n = [s_{2n-1}, s_{2n}]^T$ represents the transmitted symbol vector, and $\mathbf{H}_{k,n}$ represents the effective channel matrix between Alice and the receiver $k \in \{\mathrm{B}, \mathrm{E}\}$ given by

$$\mathbf{H}_{k,n} = \begin{bmatrix} h_{k,1,2n-1} & h_{k,2,2n-1} \\ h_{k,2,2n}^* & -h_{k,1,2n}^* \end{bmatrix}. \tag{3}$$

$\{z_{k,t}\}$ represents the additive complex white Gaussian noise with zero mean and variance σ_k^2 at the receiver $k \in \{\mathrm{B}, \mathrm{E}\}$ at tth symbol period. $\{h_{k,i,t}\}$ represents the channel impulse responses (CIRs) between the ith transmit antenna of Alice and the receive antenna of the receiver $k \in \{\mathrm{B}, \mathrm{E}\}$ at tth symbol period and is modeled as identically distributed complex Gaussian random variable with zero mean and unit variance. They are spatially uncorrelated, but temporally correlated with a correlation $\mathbb{E}[h_{k,i,2n-1}h_{k,i,2n}^*] = \rho_k$, 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 quasi-static channels. Without loss of generality, we drop the time index n by assuming $n = 1$ for notational simplicity.

3. Detection strategies of Bob and Eve

In this section, we consider two different detection strategies, JML and ZF, for decoding of Bob and Eve. For the linear combining scheme suggested by Alamouti [1], the decision statistic vector of the receiver $k \in \{\mathrm{B}, \mathrm{E}\}$ can be obtained by multiplying the matched filtering matrix $\mathbf{H}_k^H$ to the received vector in (2) as

$$\tilde{\mathbf{r}}_k = \mathbf{H}_k^H\mathbf{H}_k\mathbf{s} + \mathbf{H}_k^H\mathbf{z}_k = \mathbf{G}_k\mathbf{s} + \tilde{\mathbf{z}}_k, \tag{4}$$

where $\mathbf{s} = [s_1, s_2]^T$, $\mathbf{z}_k = [z_{k,1}, z_{k,2}^*]^T$, and

$$\mathbf{H}_k = \begin{bmatrix} h_{k,1,1} & h_{k,2,1} \\ h_{k,2,2}^* & -h_{k,1,2}^* \end{bmatrix}, \tag{5}$$

$$\mathbf{G}_k = \begin{bmatrix} \varphi_{k,1} & \epsilon_k \\ \epsilon_k^* & \varphi_{k,2} \end{bmatrix}, \tag{6}$$

where $\varphi_{k,1} = |h_{k,1,1}|^2 + |h_{k,2,2}|^2$, $\varphi_{k,2} = |h_{k,1,2}|^2 + |h_{k,2,1}|^2$, $\epsilon_k = h_{k,1,1}^* h_{k,2,1} - h_{k,1,2}^* h_{k,2,2}$. Note that when the channel is quasi-static (i.e., $h_{k,1,1} = h_{k,1,2}$ and $h_{k,2,1} = h_{k,2,2}$), $\mathbf{H}_k$ becomes orthogonal and $\varphi_{k,1} = \varphi_{k,2}$ and $\epsilon_k = 0$ hold. On the other hand, when the channel is time-selective, $\mathbf{H}_k$ becomes no longer orthogonal and thus the off-diagonal element ϵ_k becomes non-zero, which causes the interference in the decoding of two symbols.

We consider JML and ZF detectors to eliminate the off-diagonal terms in $\mathbf{G}_k$.

(1) Joint maximum likelihood (JML) detector: Assuming that all the signals in the modulation constellation are equiprobable, a ML detector decides the pair of symbols ($\hat{s}_1$,

$\hat{s}_2$) from the signal constellation $\mathcal{S}$ according to the following metric [5].

$$\hat{\mathbf{s}}_k^{\mathrm{JML}} = \arg\min_{\mathbf{s}\in\mathcal{S}^2} \|\mathbf{r}_k - \mathbf{H}_k\mathbf{s}\|^2. \tag{7}$$

The instantaneous received SNR of the JML detector for transmit antenna $i = 1, 2$ can be represented by $\gamma_{k,i}^{\mathrm{JML}} = \frac{E_s}{\sigma_k^2}\varphi_{k,i} = \frac{\bar{\gamma}_k}{2}\varphi_{k,i}$, where $\bar{\gamma}_k = 2E_s/\sigma_k^2$ is the average SNR at the receive antenna of the receiver $k \in \{\mathrm{B}, \mathrm{E}\}$.

(2) Zero forcing (ZF) detector: The ZF is a linear detection which detects every data stream separately by nulling out the interferences coming from other transmit antennas. The symbol detection metric of the ZF detector is given as [5]

$$\hat{\mathbf{s}}_k^{\mathrm{ZF}} = \arg\min_{\mathbf{s}\in\mathcal{S}^2} \|r_{k,i}^{\mathrm{ZF}} - \zeta_k\varphi_{k,3-i}^{-1/2}s_i\|^2, \text{ for } i = 1, 2, \tag{8}$$

where

$$\mathbf{z}_k^{\mathrm{ZF}} = \mathbf{\Phi}_k\mathbf{G}_k^{-1}\mathbf{H}_k^H\mathbf{r}_k = \left[r_{k,1}^{\mathrm{ZF}}, r_{k,2}^{\mathrm{ZF}}\right]^T \tag{9}$$

with

$$\mathbf{\Phi}_k = \begin{bmatrix} \zeta_k\varphi_{k,2}^{-1/2} & 0 \\ 0 & \zeta_k\varphi_{k,1}^{-1/2} \end{bmatrix}, \tag{10}$$

$$\zeta_k = |h_{k,1,1}h_{k,1,2}^* + h_{k,2,1}h_{k,2,2}^*|. \tag{11}$$

The instantaneous received SNR of the ZF detector for the transmit antenna $i = 1, 2$ is represented by

$$\gamma_{k,i}^{\mathrm{ZF}} = \frac{\zeta_k^2 E_s}{\varphi_{k,3-i}\sigma_k^2} = \frac{\zeta_k^2}{2\varphi_{k,3-i}}\bar{\gamma}_k. \tag{12}$$

4. Analysis of secrecy outage probability

In this section, we analyze the SOP of Alamouti STBC with two different detection methods, JML and ZF, over the time-selective fading channels.

When Bob adopts the detection technique $p \in \{\mathrm{JML}, \mathrm{ZF}\}$, the channel capacity in bits per second per hertz over a fading channel between Alice and Bob is given by

$$C_{\mathrm{B}}^p = \frac{1}{2}\log_2\det\left(\mathbf{I}_2 + \frac{\gamma_{\mathrm{B}}}{2}\mathbf{H}^H\mathbf{H}\right) \tag{13}$$

$$= \frac{1}{2}\sum_{i=1}^{2}\log_2\left(1 + \gamma_{\mathrm{B},i}^p\right). \tag{14}$$

Similarly, when Eve adopts the detection technique $q \in \{\mathrm{JML}, \mathrm{ZF}\}$, the channel capacity between Alice and Eve is given by

$$C_{\mathrm{E}}^q = \frac{1}{2}\sum_{i=1}^{2}\log_2\left(1 + \gamma_{\mathrm{E},i}^q\right). \tag{15}$$

Then, the secrecy capacity which is defined as the maximum achievable rate for the desired receiver while preventing Eve from obtaining any useful information is expressed as

$$C_s^{p,q} = \left[C_{\mathrm{B}}^p - C_{\mathrm{E}}^q\right]^+, \tag{16}$$

where $[x]^+ \triangleq \max(x, 0)$.

We consider the SOP as a performance metric. The SOP is defined as the probability that the secrecy capacity $C_s^{p,q}$ is below a per-defined secrecy rate R_s, which is mathematically expressed as [9,10]

$$P_{\mathrm{so}}^{p,q}(R_s) = \mathbb{P}[C_s^{p,q} < R_s]. \tag{17}$$

It is noteworthy that both JML detector and ZF detector have the same statistics for the received SNRs from all transmit antennas. Hence, we unify the random variables as $\gamma_{\mathrm{B},1}^p = \gamma_{\mathrm{B},2}^p \triangleq \gamma_{\mathrm{B}}^p$ and $\gamma_{\mathrm{E},1}^q = \gamma_{\mathrm{E},2}^q \triangleq \gamma_{\mathrm{E}}^q$ for simple notation. Then, the SOP can be represented by

$$P_{\mathrm{so}}^{p,q}(R_s) = \int_0^\infty f_{\gamma_{\mathrm{E}}^q}(\gamma_{\mathrm{E}})F_{\gamma_{\mathrm{B}}^p}\left(2^{R_s}(1+\gamma_{\mathrm{E}}) - 1\right)d\gamma_{\mathrm{E}}. \tag{18}$$

We next derive the cumulative distribution function (CDF) and the probability density function (PDF) of the received SNR at a receiver $k \in \{\mathrm{B}, \mathrm{E}\}$ for both JML and ZF detection strategies.

4.1. JML detection

For a quasi-static Rayleigh fading channel, all channel coefficients $\{h_{k,i,t}\}$ are modeled as independent identically distributed (i.i.d.) complex circular Gaussian random variable, so $|h_{k,i,t}|^2 \sim \frac{1}{2}\chi^2(2)$ and $\varphi_k \sim \frac{1}{2}\chi^2(4)$ hold, where $x \sim \chi^2(L)$ represents the central chi-square distribution with L degrees of freedom of which PDF is $p_X(x) = \frac{1}{2^{L/2}\Gamma(L/2)}x^{L/2-1}e^{-x/2}$. Since the JML detector has robustness against time selectivity [3], the CDF of received SNR of receiver $k \in \{\mathrm{B}, \mathrm{E}\}$ with JML detection is given by

$$F_{\gamma_k^{\mathrm{JML}}}(\gamma) = \mathbb{P}\left[\gamma_k^{\mathrm{JML}} < \gamma\right] = 1 - \left(1 + \frac{2}{\bar{\gamma}_k}\gamma\right)e^{-\frac{2}{\bar{\gamma}_k}\gamma}, \tag{19}$$

where $\bar{\gamma}_k = 2E_s/\sigma_k^2$ is the average SNR. The PDF of received SNR of receiver $k \in \{\mathrm{B}, \mathrm{E}\}$ for JML detection is given by

$$f_{\gamma_k^{\mathrm{JML}}}(\gamma) = \frac{d}{d\gamma}F_{\gamma_k^{\mathrm{JML}}}(\gamma) = \left(\frac{2}{\bar{\gamma}_k}\right)^2\gamma e^{-\frac{2}{\bar{\gamma}_k}\gamma}. \tag{20}$$

4.2. ZF detection

For $k \in \{\mathrm{B}, \mathrm{E}\}$, $\gamma_{k,1}^{\mathrm{ZF}}$ and $\gamma_{k,2}^{\mathrm{ZF}}$ have the same statistical distribution and their PDFs can be represented by [3]

$$f_{\gamma_{k,1}^{\mathrm{ZF}}}(\gamma) = f_{\gamma_{k,2}^{\mathrm{ZF}}}(\gamma) = \left(\frac{2\left(1 - |\rho_k|^2\right)}{\bar{\gamma}_k} + \left(\frac{2|\rho_k|}{\bar{\gamma}_k}\right)^2\gamma\right)e^{-\frac{2}{\bar{\gamma}_k}\gamma}. \tag{21}$$

Accordingly, if we represent $\gamma_{k,1}^{\mathrm{ZF}}$ and $\gamma_{k,2}^{\mathrm{ZF}}$ as a unified random variable γ_k^{ZF}, then its CDF can be derived as

$$F_{\gamma_k^{\mathrm{ZF}}}(\gamma) = \mathbb{P}(\gamma_{k,1}^{\mathrm{ZF}} < \gamma) = 1 - \left(1 + \frac{2|\rho_k|^2}{\bar{\gamma}_k}\gamma\right)e^{-\frac{2}{\bar{\gamma}_k}\gamma}. \tag{22}$$

Fig. 1 plots the Monte-Carlo simulated CDFs of received SNRs and their analysis for JML and ZF detection versus target received SNR γ for various ρ_k. It is noteworthy that $\rho_k = 0$ and $\rho_k = 1$ correspond to uncorrelated and quasi-static channels, respectively. This figure clearly verifies that the analytical results from (19) and (22) match well with the Monte-Carlo simulation results for general value of ρ_k. As ρ_k

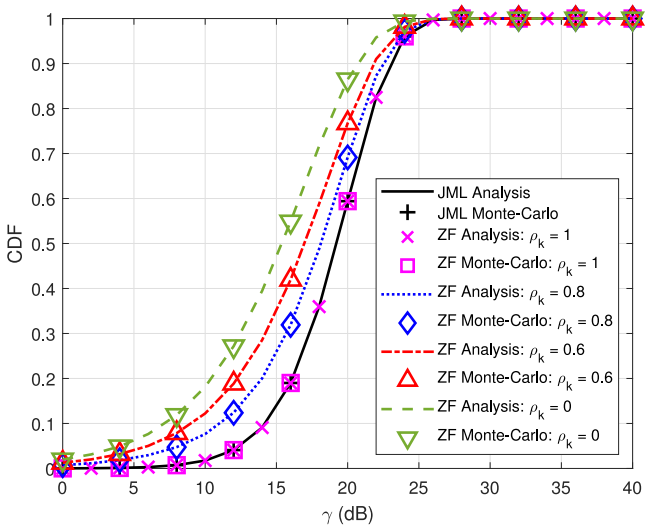

Fig. 1. Monte-Carlo simulated CDFs of received SNRs and their analysis for JML and ZF detection versus target received SNR γ for various ρ_k.

decreases, the CDFs increase more faster to 1, which implies that the smaller ρ_k has the smaller received SNRs. The CDFs of both JML and ZF detection become the same when $\rho_k = 1$.

4.3. Exact secrecy outage probability

By plugging (19)–(22) into (18), we can obtain the exact SOPs for all possible combinations of JML and ZF detections at Bob and Eve as follows:

(1) When $p =$ JML and $q =$ JML,

$$P_{\rm so}^{\rm JML,JML}(R_s) = \int_0^\infty \left(\frac{2}{\bar{\gamma}_{\rm E}}\right)^2 \gamma_{\rm E} e^{-\frac{2}{\bar{\gamma}_{\rm E}}\gamma_{\rm E}} \times \left[1 - \left(1 + \frac{2}{\bar{\gamma}_{\rm B}}\left(2^{R_s}(1+\gamma_{\rm E}) - 1\right)\right) e^{-\frac{2}{\bar{\gamma}_{\rm B}}\left(2^{R_s}(1+\gamma_{\rm E})-1\right)}\right] d\gamma_{\rm E}. \tag{23}$$

(2) When $p =$ JML and $q =$ ZF,

$$P_{\rm so}^{\rm JML,ZF}(R_s) = \int_0^\infty \left(\frac{2\left(1-|\rho_{\rm E}|^2\right)}{\bar{\gamma}_{\rm E}} + \left(\frac{2|\rho_{\rm E}|}{\bar{\gamma}_{\rm E}}\right)^2 \gamma_{\rm E}\right) e^{-\frac{2}{\bar{\gamma}_{\rm E}}\gamma_{\rm E}} \times \left[1 - \left(1 + \frac{2}{\bar{\gamma}_{\rm B}}\left(2^{R_s}(1+\gamma_{\rm E}) - 1\right)\right) e^{-\frac{2}{\bar{\gamma}_{\rm B}}\left(2^{R_s}(1+\gamma_{\rm E})-1\right)}\right] d\gamma_{\rm E}. \tag{24}$$

(3) When $p =$ ZF and $q =$ JML,

$$P_{\rm so}^{\rm ZF,JML}(R_s) = \int_0^\infty \left(\frac{2}{\bar{\gamma}_{\rm E}}\right)^2 \gamma_{\rm E} e^{-\frac{2}{\bar{\gamma}_{\rm E}}\gamma_{\rm E}} \times \left[1 - \left(1 + \frac{2|\rho_{\rm B}|^2}{\bar{\gamma}_{\rm B}}\left(2^{R_s}(1+\gamma_{\rm E}) - 1\right)\right) e^{-\frac{2}{\bar{\gamma}_{\rm B}}\left(2^{R_s}(1+\gamma_{\rm E})-1\right)}\right] d\gamma_{\rm E}. \tag{25}$$

(4) When $p =$ ZF and $q =$ ZF,

$$P_{\rm so}^{\rm ZF,ZF}(R_s) = \int_0^\infty \left(\frac{2\left(1-|\rho_{\rm E}|^2\right)}{\bar{\gamma}_{\rm E}} + \left(\frac{2|\rho_{\rm E}|}{\bar{\gamma}_{\rm E}}\right)^2 \gamma_{\rm E}\right) e^{-\frac{2}{\bar{\gamma}_{\rm E}}\gamma_{\rm E}} \times \left[1 - \left(1 + \frac{2|\rho_{\rm B}|^2}{\bar{\gamma}_{\rm B}}\left(2^{R_s}(1+\gamma_{\rm E}) - 1\right)\right) e^{-\frac{2}{\bar{\gamma}_{\rm B}}\left(2^{R_s}(1+\gamma_{\rm E})-1\right)}\right] d\gamma_{\rm E}. \tag{26}$$

Remark 1. For a quasi-static fading channel, the CDFs of the received SNRs with JML and ZF detection are equivalent as $F_{\gamma_k}^{\rm JML} = F_{\gamma_k}^{\rm ZF} = 1 - \left(1 + \frac{2}{\bar{\gamma}_k}\gamma\right) e^{-\frac{2}{\bar{\gamma}_k}\gamma}$. Thus, when the channels of Bob and Eve are quasi-static, i.e., $\rho_{\rm B} = \rho_{\rm E} = 1$, the exact SOPs of all combinations of JML and ZF detection strategies are equivalent as that of $p = q =$ JML, i.e., (23).

5. Secrecy diversity order

In this section, we derive the approximated SOP and investigate the secrecy diversity order. The secrecy diversity order is defined as the asymptotic ratio of the logarithmic SOP to the logarithmic average SNR of Bob [15,16]:

$$d^{p,q} = -\lim_{\bar{\gamma}_{\rm B}\to\infty} \frac{\log P_{\rm so}^{p,q}(R_s)}{\log \bar{\gamma}_{\rm B}}, \tag{27}$$

which characterizes the reliability of secure wireless communication systems. However, unfortunately, the exact SOPs in (23)–(26) have an intractable integral form, which makes hard to understand its asymptotic behavior with the closed-form expression. To get some useful insights with closed-form expression, we approximate the SOP as follows [17,18]:

$$P_{\rm so}^{p,q}(R_s) \approx \tilde{P}_{\rm so}^{p,q}(R_s) \triangleq \int_0^\infty f_{\gamma_{\rm E}^q}(\gamma_{\rm E}) F_{\gamma_{\rm B}^p}\left(2^{R_s}\gamma_{\rm E}\right) d\gamma_{\rm E}. \tag{28}$$

Note that the approximation becomes more tighter as R_s becomes smaller.

For high $\bar{\gamma}_{\rm B}$, the CDFs for the received SNRs of Bob for JML and ZF detection can be simplified by using Taylor series expansion as

$$F_{\gamma_{\rm B}^{\rm JML}}(\gamma) \approx 2\left(\frac{\gamma}{\bar{\gamma}_{\rm B}}\right)^2, \tag{29}$$

$$F_{\gamma_{\rm B}^{\rm ZF}}(\gamma) \approx \frac{2(1-|\rho_{\rm B}|^2)\gamma}{\bar{\gamma}_{\rm B}}. \tag{30}$$

Applying these relationships to (28), we can obtain the closed-form expression for the approximated SOPs in the high $\bar{\gamma}_{\rm B}$ as the following.

(1) When $p =$ JML and $q =$ JML,

$$\tilde{P}_{{\rm so},\bar{\gamma}_{\rm B}\to\infty}^{\rm JML,JML}(R_s) = \int_0^\infty \left(\frac{2}{\bar{\gamma}_{\rm E}}\right)^2 \gamma_{\rm E} e^{-\frac{2}{\bar{\gamma}_{\rm E}}\gamma_{\rm E}} \cdot 2\left(\frac{2^{R_s}\gamma_{\rm E}}{\bar{\gamma}_{\rm B}}\right)^2 d\gamma_{\rm E} \tag{31}$$

$$= 3 \cdot 2^{2R_s}\left(\frac{\bar{\gamma}_{\rm E}}{\bar{\gamma}_{\rm B}}\right)^2. \tag{32}$$

(2) When $p = \text{JML}$ and $q = \text{ZF}$,

$$\tilde{P}_{\text{so},\bar{\gamma}_\text{B}\to\infty}^{\text{JML,ZF}}(R_s) = \int_0^\infty \left(\frac{2\left(1-|\rho_\text{E}|^2\right)}{\bar{\gamma}_\text{E}} + \left(\frac{2|\rho_\text{E}|}{\bar{\gamma}_\text{E}}\right)^2 \gamma_\text{E} \right) e^{-\frac{2}{\bar{\gamma}_\text{E}}\gamma_\text{E}} \times 2\left(\frac{2^{R_s}\gamma_\text{E}}{\bar{\gamma}_\text{B}}\right)^2 d\gamma_\text{E} \tag{33}$$

$$= 2^{R_s}\left(1+2|\rho_\text{E}|^2\right)\left(\frac{\bar{\gamma}_\text{E}}{\bar{\gamma}_\text{B}}\right)^2. \tag{34}$$

(3) When $p = \text{ZF}$ and $q = \text{JML}$,

$$\tilde{P}_{\text{so},\bar{\gamma}_\text{B}\to\infty}^{\text{ZF,JML}}(R_s) = \int_0^\infty \left(\frac{2}{\bar{\gamma}_\text{E}}\right)^2 \gamma_\text{E} e^{-\frac{2}{\bar{\gamma}_\text{E}}\gamma_\text{E}} \times \frac{2(1-|\rho_\text{B}|^2)2^{R_s}\gamma_\text{E}}{\bar{\gamma}_\text{B}} d\gamma_\text{E} \tag{35}$$

$$= 2\left(1-|\rho_\text{B}|^2\right)2^{R_s}\frac{\bar{\gamma}_\text{E}}{\bar{\gamma}_\text{B}}. \tag{36}$$

(4) When $p = \text{ZF}$ and $q = \text{ZF}$,

$$\tilde{P}_{\text{so},\bar{\gamma}_\text{B}\to\infty}^{\text{ZF,ZF}}(R_s) = \int_0^\infty \left(\frac{2\left(1-|\rho_\text{E}|^2\right)}{\bar{\gamma}_\text{E}} + \left(\frac{2|\rho_\text{E}|}{\bar{\gamma}_\text{E}}\right)^2 \gamma_\text{E} \right) e^{-\frac{2}{\bar{\gamma}_\text{E}}\gamma_\text{E}} \times \frac{2(1-|\rho_\text{B}|^2)2^{R_s}\gamma_\text{E}}{\bar{\gamma}_\text{B}} d\gamma_\text{E} \tag{37}$$

$$= 2^{R_s}\left(1-|\rho_\text{B}|^2\right)\left(1+|\rho_\text{E}|^2\right)\frac{\bar{\gamma}_\text{E}}{\bar{\gamma}_\text{B}}. \tag{38}$$

Note that as target secrecy rate R_s increases, the secrecy outage probability increases. The secrecy outage probability is inversely proportional to the square of the ratio of $\gamma_\text{B}/\gamma_\text{E}$ for JML-JML and JML-ZF and the ratio of $\gamma_\text{B}/\gamma_\text{E}$ for ZF-JML and ZF-ZF. The secrecy outage probability is robust to the time correlation ρ_B and ρ_E for JML-JML. On the other hand, the secrecy outage probability increases as ρ_E increases, but it is robust to ρ_B for JML-ZF. It decreases as ρ_B increases, but is robust to ρ_E for ZF-JML. For ZF-ZF, the secrecy outage probability increases as ρ_E increases and ρ_B decreases.

Using the derived closed-form expressions in (32), (34), (36), and (38), we can further obtain the secrecy diversity order as follows:

(1) When $p = \text{JML}$ and $q = \text{JML}$,

$$d^{\text{JML,JML}} = -\lim_{\bar{\gamma}_\text{B}\to\infty} \frac{\log \tilde{P}_{\text{so}}^{\text{JML,JML}}(R_s)}{\log\bar{\gamma}_\text{B}} \tag{39}$$

$$= -\lim_{\bar{\gamma}_\text{B}\to\infty} \frac{\log\left(3\cdot 2^{2R_s}\left(\bar{\gamma}_\text{E}/\bar{\gamma}_\text{B}\right)^2\right)}{\log\bar{\gamma}_\text{B}} \tag{40}$$

$$= -\lim_{\bar{\gamma}_\text{B}\to\infty} \frac{\log\left(3\cdot 2^{2R_s}\bar{\gamma}_\text{E}^2\right) - 2\log\bar{\gamma}_\text{B}}{\log\bar{\gamma}_\text{B}} \tag{41}$$

$$\doteq 2. \tag{42}$$

(2) When $p = \text{JML}$ and $q = \text{ZF}$,

$$d^{\text{JML,ZF}} = -\lim_{\bar{\gamma}_\text{B}\to\infty} \frac{\log \tilde{P}_{\text{so}}^{\text{JML,ZF}}(R_s)}{\log\bar{\gamma}_\text{B}} \tag{43}$$

$$= -\lim_{\bar{\gamma}_\text{B}\to\infty} \frac{\log\left(2^{R_s}\left(1+2|\rho_\text{E}|^2\right)\left(\frac{\bar{\gamma}_\text{E}}{\bar{\gamma}_\text{B}}\right)^2\right)}{\log\bar{\gamma}_\text{B}} \tag{44}$$

$$= -\lim_{\bar{\gamma}_\text{B}\to\infty} \frac{\log\left(2^{R_s}\left(1+2|\rho_\text{E}|^2\right)\bar{\gamma}_\text{E}^2\right) - 2\log\bar{\gamma}_\text{B}}{\log\bar{\gamma}_\text{B}} \tag{45}$$

$$\doteq 2. \tag{46}$$

(3) When $p = \text{ZF}$ and $q = \text{JML}$,

$$d^{\text{ZF,JML}} = -\lim_{\bar{\gamma}_\text{B}\to\infty} \frac{\log \tilde{P}_{\text{so}}^{\text{ZF,JML}}(R_s)}{\log\bar{\gamma}_\text{B}} \tag{47}$$

$$= -\lim_{\bar{\gamma}_\text{B}\to\infty} \frac{\log\left(2\left(1-|\rho_\text{B}|^2\right)2^{R_s}\frac{\bar{\gamma}_\text{E}}{\bar{\gamma}_\text{B}}\right)}{\log\bar{\gamma}_\text{B}} \tag{48}$$

$$= -\lim_{\bar{\gamma}_\text{B}\to\infty} \frac{\log\left(2\left(1-|\rho_\text{B}|^2\right)2^{R_s}\bar{\gamma}_\text{E}\right) - \log\bar{\gamma}_\text{B}}{\log\bar{\gamma}_\text{B}} \tag{49}$$

$$\doteq 1. \tag{50}$$

(4) When $p = \text{ZF}$ and $q = \text{ZF}$,

$$d^{\text{ZF,ZF}} = -\lim_{\bar{\gamma}_\text{B}\to\infty} \frac{\log \tilde{P}_{\text{so}}^{\text{ZF,ZF}}(R_s)}{\log\bar{\gamma}_\text{B}} \tag{51}$$

$$= -\lim_{\bar{\gamma}_\text{B}\to\infty} \frac{\log\left(2^{R_s}\left(1-|\rho_\text{B}|^2\right)\left(1+|\rho_\text{E}|^2\right)\frac{\bar{\gamma}_\text{E}}{\bar{\gamma}_\text{B}}\right)}{\log\bar{\gamma}_\text{B}} \tag{52}$$

$$= -\lim_{\bar{\gamma}_\text{B}\to\infty} \frac{\log\left(2^{R_s}\left(1-|\rho_\text{B}|^2\right)\left(1+|\rho_\text{E}|^2\right)\bar{\gamma}_\text{E}\right) - \log\bar{\gamma}_\text{B}}{\log\bar{\gamma}_\text{B}} \tag{53}$$

$$\doteq 1. \tag{54}$$

Remark 2. From the analytical results in (42), (46), (50), and (54), we can deduce that the secrecy diversity order over time-selective Rayleigh fading channels is dominantly affected by the detection strategy of the legitimate receiver rather than that of the eavesdropper.

6. Numerical results

In this section, we evaluate the SOPs of Alamouti STBC over MISO wiretap time-selective Rayleigh fading channels and verify our analytical results in the previous sections. We consider the first-order autoregression model AR(1) for the time-selective channel gains [4]. Unless otherwise stated, the baseline simulation parameters are as follows: $E_s = 20$ [dBm], $\sigma_\text{E}^2 = 1$, $\rho_\text{B} = 0.8$.

Fig. 2 compares the exact SOP with its approximation for various R_s [bps] to verify the tightness of our approximation. In Fig. 2, the exact SOP and its approximation are overlapping when $R_s = 0.01$ [bps/Hz], while there exists a slight gap when $R_s = 0.1$ [bps/Hz]. This implies that the tightness of the approximation holds for relatively small R_s [bps], but the gap between the exact SOP and its approximation becomes larger as R_s increases.

Fig. 3 compares the SOPs of JML-JML, JML-ZF, ZF-JML, ZF-ZF versus the ratio of average SNRs between Bob and Eve for various ρ_E. This figure shows that the SOP of ZF-JML is invariant with respect to ρ_E. This is because JML detection has robustness to temporal channel correlation. On the other hand, ρ_E affects the SOPs for both JML-ZF and ZF-ZF cases and their SOPs become higher as ρ_E increases. This is because Eve can decode more information for the secret message with ZF

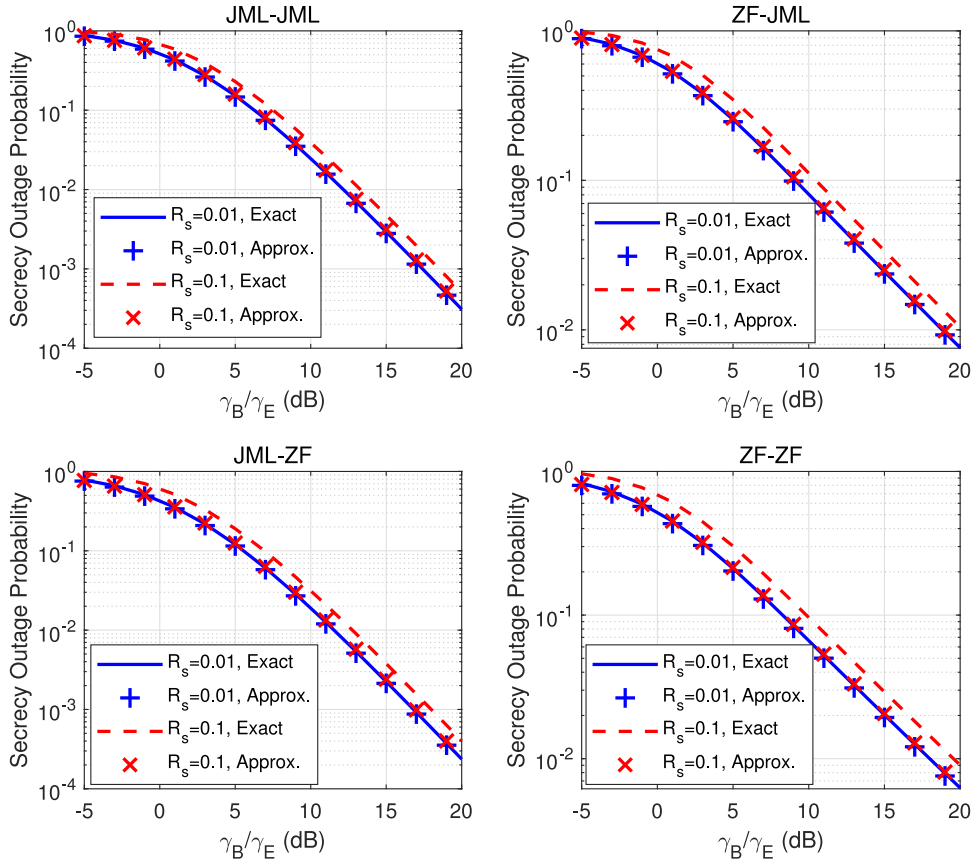

Fig. 2. Comparison between the exact secrecy outage probability and its approximation for various R_s [bps].

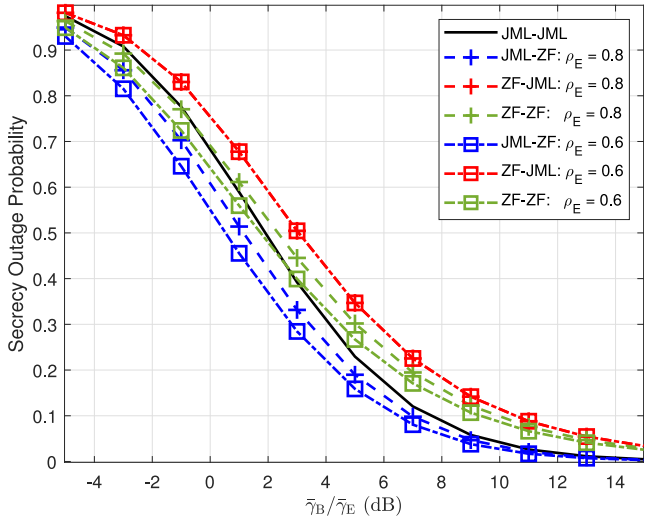

Fig. 3. Comparison of SOPs versus $\bar{\gamma}_B/\bar{\gamma}_E$ (dB) for various ρ_E when $R_s = 0.1$ [bps/Hz].

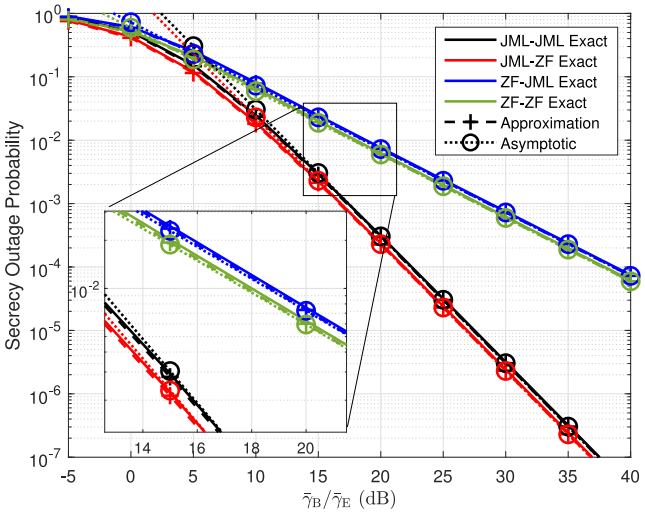

Fig. 4. Comparison of the exact SOPs, their approximations, and asymptotic high SNR approximations versus the ratio γ_B/γ_E (dB) when $R_s = 0.01$ [bps/Hz].

detection as ρ_E increases. This figure also shows that the SOPs are superior in the order of JML-ZF, JML-JML, ZF-ZF, ZF-JML for given ρ_B and ρ_E. This is because the JML detection has higher SNR than ZF detection.

Fig. 4 plots the exact SOPs (23)–(26), their approximations (28), and asymptotic high SNR approximations for JML-JML, JML-ZF, ZF-JML, ZF-ZF (32), (34), (36), (38) versus the ratio of average SNRs between Bob and Eve. This figure clearly shows that the approximation is considerably tight to the exact SOP for relatively low R_s and the secrecy diversity order of two, two, one, and one can be achieved for JML-JML, JML-ZF, ZF-JML, and ZF-ZF, respectively. This figure validates

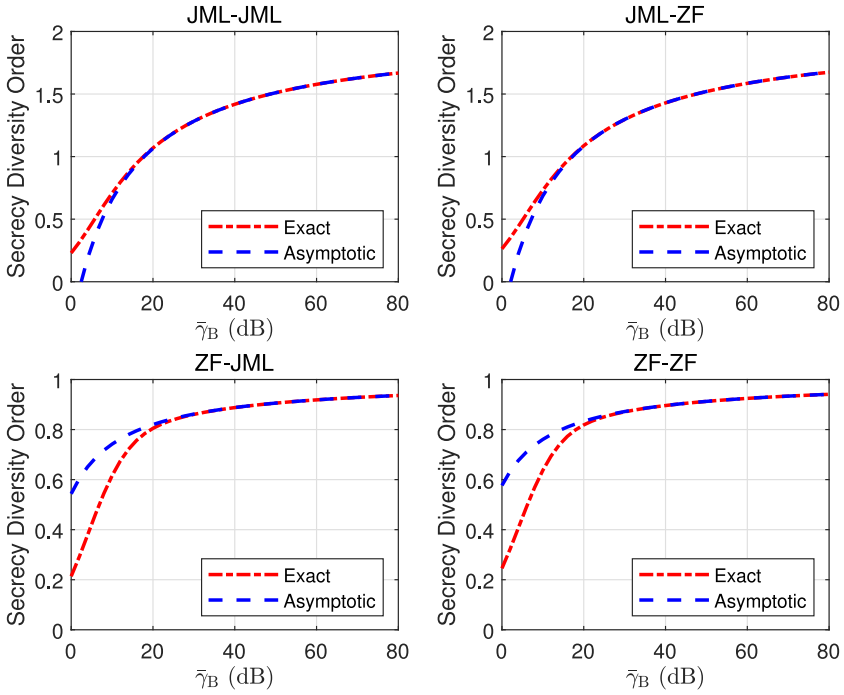

Fig. 5. Comparison of secrecy diversity orders of the exact secrecy outage probability and asymptotic secrecy outage probability when $\rho_B = 0.95$ and $\rho_E = 0.9$.

our observation that the secrecy diversity order is primarily impacted by the detection method of the legitimate receiver.

Fig. 5 plots the secrecy diversity orders of the exact secrecy outage probability and asymptotic secrecy outage probability when $\rho_B = 0.95$ and $\rho_E = 0.9$. As $\bar{\gamma}_B$ increases, the secrecy diversity order of the exact secrecy outage probability converges to that of the asymptotic secrecy outage probability, which validates our asymptotic analytical results. As $\bar{\gamma}_B$ increases, the secrecy diversity order converges to two for JML-JML and JML-ZF, but it converges to one for ZF-JML and ZF-ZF, which is matched to our analysis for asymptotic secrecy diversity order.

7. Conclusions

We have investigated the PLS performance of Almouti STBC with two different detection strategies (i.e., JML and ZF) adopted by the legitimate receiver and eavesdropper, especially over MISO wiretap time-selective fading channels. For arbitrary temporal correlations, we have derived the SOPs and their corresponding approximations for all possible combinations of detectors at Bob and Eve, including JML-JML, JML-ZF, ZF-JML, and ZF-ZF. With the asymptotically high SNR approximated SOPs, we have discovered that the secrecy diversity order of two, two, one, and one can be achieved for JML-JML, JML-ZF, ZF-JML, and ZF-ZF, respectively, and have also found that the achievable secrecy diversity order is mainly influenced by the detection technique employed by the legitimate receiver. Our framework can be extended to general number of transmit antennas with careful design for advanced STBC and detection techniques, which remains as our future work. Incorporation of possible spatial channel correlations between Alice–Bob and Alice–Eve links and more general fading channel models would be other interesting topics of future research.

CRediT authorship contribution statement

Seong Ho Chae: Writing – original draft, Formal analysis, Validation, Investigation, Visualization. **Hoojin Lee:** Conceptualization, Methodology, Supervision, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This research was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2021R1F1A1050633). The work of Hoojin Lee was supported by Hansung University.

References

[1] S.M. Alamouti, A simple transmit diversity technique for wireless communications, IEEE J. Sel. Areas Commun. 16 (8) (1998) 1451–1458.

[2] V. Tarokh, J. Jafarkhani, A.R. Calderbank, Space–time block codes from orthogonal designs, IEEE Trans. Inform. Theory 45 (5) (1999) 1456–1467.

[3] A. Vielmon, Y. Li, J.R. Barry, Performance of Alamouti transmit diversity over time-varying Rayleigh-fading channels, IEEE Trans. Wirel. Commun. 3 (5) (2004) 1369–1373.

[4] T.A. Tran, A.B. Sesay, A generalized linear quasi-ML decoder of OST-BCs for wireless communications over time-selective fading channels, IEEE Trans. Wirel. Commun. 3 (3) (2004) 855–864.
[5] H. Lee, R.W. Heath, E.J. Powers, Information outage probability and diversity order of Alamouti transmit diversity in time-selective fading channels, IEEE Trans. Veh. Tech. 57 (6) (2008) 3890–3895.
[6] A. Mathur, Y. Ai, M.R. Bhatnagar, M. Cheffena, T. Ohtsuki, On physical layer security of $\alpha-\eta-\kappa-\mu$ fading channels, IEEE Commun. Lett. 22 (10) (2018) 2168–2171.
[7] A. Mathur, Y. Ai, M. Cheffena, G. Kaddoum, Secrecy performance of correlated $\alpha-\mu$ fading channels, IEEE Commun. Lett. 23 (8) (2019) 1323–1327.
[8] S. Yan, N. Yang, E. Malaney, J. Yuan, Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels, IEEE Trans. Wirel. Commun. 13 (3) (2014) 1656–1667.
[9] A.F. Coşkun, O. Kucur, Secrecy outage probability of conventional and modified TAS/Alamouti-STBC schemes with power allocation in the presence of feedback errors, IEEE Trans. Veh. Tech. 68 (3) (2019) 2609–2623.
[10] S.H. Chae, I. Bang, H. Lee, Physical layer security of QSTBC with power scaling in MIMO wiretap channels, IEEE Trans. Veh. Tech. 69 (5) (2020) 5647–5651.
[11] M. Li, H. Yuan, X. Yue, S. Muhaidat, C. Maple, M. Dianati, Secrecy outage analysis for Alamouti space–time block coded non-orthogonal multiple access, IEEE Commun. Lett. 24 (7) (2020) 1405–1409.
[12] N.S. Ferdinand, D.B. da Costa, M. Latva-aho, Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection, IEEE Commun. Lett. 17 (5) (2013) 864–867.
[13] S. Kavaiya, D.K. Patel, Z. Ding, Y.L. Guan, S. Sun, Physical layer security in congnitive vehicular networks, IEEE Trans. Commun. 69 (4) (2021) 2557–2569.
[14] D. Kim, G. Kim, H. Lee, S.H. Chae, On the achievable secrecy transmission rates by Alamouti space–time block coding in time-selective fading channels, Electron. Lett. 58 (17) (2022) 672–674.
[15] M. Craiti, A. Gharayeb, C. Assi, M.O. Hasna, On the achievable secrecy diversity of cooperative networks with untrusted relays, IEEE Trans. Commun. 66 (1) (2018) 39–53.
[16] K. Chopra, R. Bose, A. Joshi, Secrecy outage of threshold-based cooperative relay network with and without direct links, EURASIP J. Info. Security 2018 (7) (2018) 1–12.
[17] N. Bhargav, S.L. Cotton, D.E. Simmons, Secrecy capacity analysis over κ - μ fading channels: Theory and applications, IEEE Trans. Commun. 64 (7) (2016) 3011–3024.
[18] J. Moualeu, D. Costa, F. Martinez, W. Hamouda, T. Ngatched, U. Dias, Transmit antenna selection in secure MIMO systems over α - μ fading channels, IEEE Trans. Commun. 67 (9) (2019) 6483–6498.