# Space–Time Line Code for Enhancing Physical Layer Security of Multiuser MIMO Uplink Transmission

Jihoon Choi, *Senior Member, IEEE*, Jingon Joung, *Senior Member, IEEE*,
and Bang Chul Jung, *Senior Member, IEEE*

***Abstract*—In this article, we investigate a secure uplink multiple-input multiple-output communication system, in which the multiple users transmit information to a legitimate access point (AP) when a passive eavesdropper exists. A secure multiple access method is proposed for single-antenna users by employing space–time line codes (STLCs), which enables noncoherent detection at the legitimate AP without channel state information (CSI) and achieves full spatial diversity. While extending the secure STLC scheme from the single-antenna to two-antenna users by combining the STLC with artificial noise (AN) injection, we design a low-complexity AN signals with the optimal power control scheme. The proposed AN is ensured to be eliminated after STLC decoding at the legitimate AP, while sustained in eavesdropper's received signals as interference. Theoretical sum secrecy rates are derived by considering time-varying fading channels with the uncertainty of CSI at the users, and the numerical results verify that the proposed STLC schemes outperform the existing secure transmission schemes in terms of the sum secrecy rate.**

***Index Terms*—Artificial noise, noncoherent detection, secrecy rate, space–time line code.**

## I. Introduction

FOR secure wireless communications, along with cryptographic encryption on an application layer, physical-layer security technologies have been attracting intensive research interest from various fields with numerous successful applications [1], [2]. Recently, secure communication has been emphasized for confidential and privacy data communication in various futuristic and potential fifth-generation (5G) systems, such as wireless power transmission systems [3]–[7], massive multi-input multi-output (MIMO) systems [8]–[11], millimeter-wave systems [12], [13], and unmanned aerial vehicle systems [14]–[16]. The seminal work on information-theoretic security regarding a *wiretap channel* in [18] was extended to a Gaussian channel [19], formally defining secrecy capacity meaning the difference between the capacities of the main (transmitter-to-legitimate receiver) and eavesdropper (transmitter-to-eavesdropper) channels.

The secrecy capacity has been rigorously analyzed for the various types of channels under different conditions regarding the knowledge of the main and eavesdropper channels [20]–[22]. For example, the secrecy capacity of a quasi-static fading channel was analyzed in [20], and the secrecy capacity and achievable secrecy rate regions of a Gaussian multiple access wire-tap channel were analyzed [21], [22]. MIMO systems were employed to improve the secrecy capacity [23]. In [24], the secrecy capacity of a Gaussian MIMO wiretap channel was analyzed, and, under the full channel state information (CSI) condition, in which a transmitter, legitimate receiver, and eavesdropper know both the main and eavesdropper channels, the secrecy capacity of a MIMO wiretap channel was analyzed [25], [26]. As a special case, secure communications for single-input multi-output (SIMO) systems have been investigated [27]–[29]. A secrecy rate was analyzed in SIMO fading channels when multiple eavesdroppers are present [27], a distributed jamming technique was proposed to improve the secrecy rate for a SIMO system [28], and a two-step transmission scheme was considered in which the destination first transmits a random reference symbol to the source and then the source modulates the data symbol by multiplying the received reference symbol [29]. Imperfect CSI has been considered for the secure communications of multiple-input single-output (MISO) [30], MIMO [31], and multiuser MIMO [32] systems.

To mask an information signal and/or improve its strength only at a legitimate receiver, various practical techniques, such as artificial noise (AN) injection/jamming, precoding/beamforming, and cooperation, have also been studied. By adding AN to the intended signal, the secrecy capacity can be significantly improved [33]–[39]. The AN does not affect the intended signal because it is transmitted in the nullspace of the effective main channel, while it affects the eavesdropper's received signal as interference. The power of AN was maximized through a beamformer design under a minimum-mean-square-error constraint at the intended multiple receivers to increase the secrecy rate [40]. On the other hand, the linear precoding and cooperative beamforming methods have been also actively studied in [41]–[43] and [44], respectively, to improve the secrecy capacity.

Various practical secrecy-achieving schemes based on low-density parity check codes, polar codes, and lattice codes have

Manuscript received February 14, 2020; revised May 23, 2020; accepted June 5, 2020. Date of publication June 26, 2020; date of current version August 26, 2021. This work was supported in part by the National Research Foundation of Korea and in part by the Korea government under Grant 2018R1A4A1023826. *(Corresponding author: Jingon Joung.)*

Jihoon Choi is with the School of Electronics and Information Engineering, Korea Aerospace University, Gyeonggi-do 10540, South Korea (e-mail: jihoon@kau.ac.kr).

Jingon Joung is with the School of Electrical and Electronics Engineering, Chung-Ang University, Seoul 06974, South Korea (e-mail: jgjoung@cau.ac.kr).

Bang Chul Jung is with the Department of Electronics Engineering, Chungnam National University, Daejeon 34134, South Korea (e-mail: bcjung@cnu.ac.kr).

Digital Object Identifier 10.1109/JSYST.2020.3001068

been studied for some specific wiretap channels [45]–[47]. Moreover, space-time modulation/coding schemes using multiple antennas have been devised [23], [35], [36]. In [23], it was shown that if the eavesdropper CSI is unavailable at the eavesdropper, the transmitter can enforce a zero information rate to the eavesdropper while delivering positive information rate to the intended receiver through space-time modulation. In [35], AN was designed for a secure space–time block coded (STBC) system with two transmit and receive antennas, i.e., a 2-by-2 MIMO system. In [36], AN signals were designed for a stacked Alamouti STBC and successfully increased the secrecy rate of the multiple access channel.

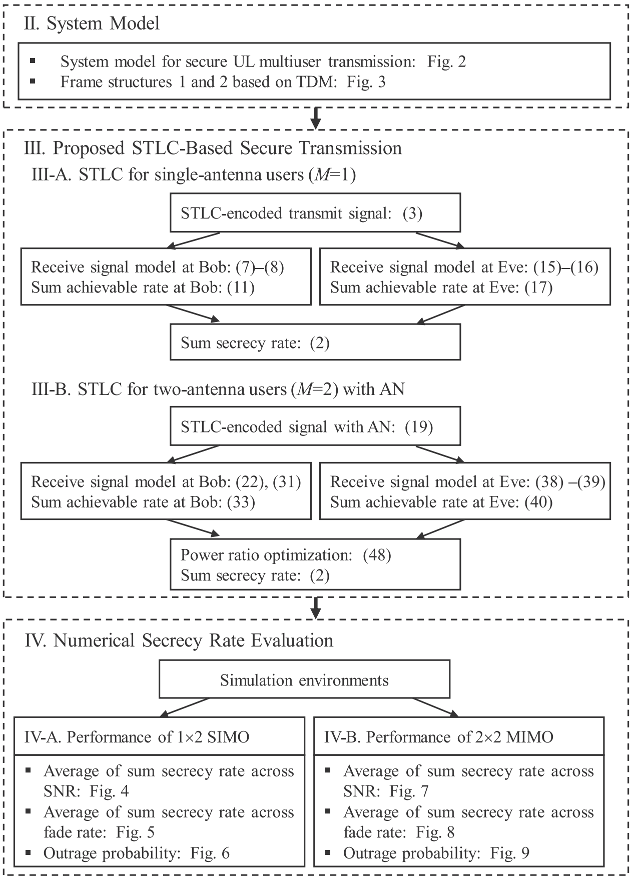

II. System Model
System model for secure UL multiuser transmission: Fig. 2
Frame structures 1 and 2 based on TDM: Fig. 3
III. Proposed STLC-Based Secure Transmission
III-A. STLC for single-antenna users (*M*=1)
STLC-encoded transmit signal: (3)
Receive signal model at Bob: (7)–(8)
Sum achievable rate at Bob: (11)
Receive signal model at Eve: (15)–(16)
Sum achievable rate at Eve: (17)
Sum secrecy rate: (2)
III-B. STLC for two-antenna users (*M*=2) with AN
STLC-encoded signal with AN: (19)
Receive signal model at Bob: (22), (31)
Sum achievable rate at Bob: (33)
Receive signal model at Eve: (38) –(39)
Sum achievable rate at Eve: (40)
Power ratio optimization: (48)
Sum secrecy rate: (2)
IV. Numerical Secrecy Rate Evaluation
Simulation environments
IV-A. Performance of 1×2 SIMO
Average of sum secrecy rate across SNR: Fig. 4
Average of sum secrecy rate across fade rate: Fig. 5
Outrage probability: Fig. 6
IV-B. Performance of 2×2 MIMO
Average of sum secrecy rate across SNR: Fig. 7
Average of sum secrecy rate across fade rate: Fig. 8
Outrage probability: Fig. 9

Fig. 1. Overview of Sections II–IV including the system model, the proposed secure transmission, and numerical evaluation.

Most studies assume that the eavesdropper channel is available at the transmitter; however, this is impractical, especially, if eavesdroppers are purely passive such that they do not actively attack uplink channel training [10], [48]. In this article, we consider a time-division duplex (TDD) communication system composed of multiple users, a legitimate access point (AP), and a passive eavesdropper, in which the uplink (UL) main channel is obtained from channel reciprocity by estimating the downlink (DL) channel; i.e., the main channel is available at users, while it is not available at the eavesdropper. Furthermore, to hinder an eavesdropper from estimating the eavesdropper channel, users do not send any training sequences during UL communications. Since the absence of a training sequence also prevents a receiver from estimating the main channel, noncoherent detection is required at the legitimate AP. Under these CSI conditions, we propose a secure MIMO transmission method using the space–time line code (STLC), which requires full CSI at a transmitter and no CSI at a receiver, where the STLC is initially proposed in [49], applied to multiuser MIMO systems [50], [51], power amplifier shuffling [52], machine learning based blind decoding [53], two-way relays [54]–[56], spatial multiplexing MIMO systems [57], and secure transmission for a point-to-point MIMO channel [58]. For single-antenna users, the sum secrecy rate of UL is derived considering CSI uncertainty at the transmitter. Moreover, the proposed STLC scheme is extended to two-antenna users by employing a new AN structure. In [50], transmit antennas are partitioned into multiple clusters for concurrently conveying multiple STLC data streams, and thus a large number of antennas are required to mitigate the interuser interference. In contrast, by combining the STLC transmission with AN and TDM, the proposed method increases the sum secrecy rate with much less number of transmit antennas while avoiding the interuser interference. The main contributions of this article are summarized as follows.

1) We define two frame structures based on time-division multiplexing (TDM) for multiuser MIMO channels, and propose STLC-based secure transmission methods for the UL multiple access channels in the presence of a passive eavesdropper. When the single-antenna users transmit STLC-encoded information and both the legitimate AP and eavesdropper have two antennas, the sum secrecy rate of UL is derived taking into account CSI uncertainty.
2) To further improve the secrecy of the proposed STLC-based system, two-antenna users with CSI uncertainty are considered that transmits STLC-encoded data in combination with AN. In contrast to [58], in which the AN signals were designed for a single-user STLC system by using singular value decomposition, this article proposes a new AN design method with low computational complexity, especially, for multiple STLC users. By employing the new AN structure, the AN signals from multiple users are eliminated after STLC decoding at the legitimate AP, and the sum secrecy rate is improved by optimizing the power allocation ratio between the desired signal and the AN.
3) Through numerical simulations, the proposed STLC scheme for single-antenna users is compared to a conventional two-step secure transmission [29], and the proposed method with AN for two-antenna users is compared to an existing beamforming scheme with/without AN in [33]. Numerical results reveal that the proposed STLC methods outperform the existing secure transmission techniques in terms of the average secrecy rate and the outage secrecy rate.

As shown in Fig. 1, the rest of this article is organized as follows. Section II introduces the system model of secure MIMO wireless communications. In Section III, we propose secure STLC systems for single-antenna and two-antenna users and design the AN signals for the two-antenna users, providing sum secrecy rate analysis. Numerical evaluations verifying the

TABLE I
VARIABLES USED IN THIS ARTICLE

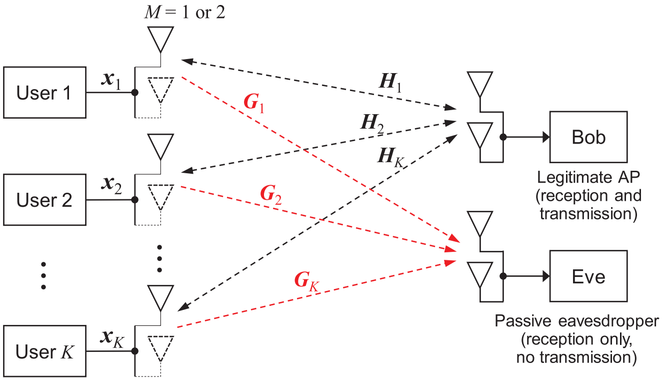
| Variable | Description |
|---|---|
| $T_D L$ | DL block duration |
| $T_U L$ | UL block duration |
| $L$ | Number of UL blocks in a subframe |
| $\tau$ | UL time ratio |
| $K$ | Number of users |
| $M$ | Number of transmit antennas at users |
| $\mathcal{E}_k$ | Transmit symbol power for user $k$ |
| $C_B$ | Sum achievable rate at Bob |
| $C_E$ | Sum achievable rate at Eve |
| $C_s$ | Sum secrecy rate |
| $\boldsymbol{H}_k \in \mathbb{C}^{2\times M}$ | Channel matrix between user $k$ and Bob |
| $\boldsymbol{G}_k \in \mathbb{C}^{2\times M}$ | channel matrix between user $k$ and Eve |
| $\boldsymbol{Q}_k \in \mathbb{C}^{2\times 2}$ | Effective channel between user $k$ and Eve |
| $\tilde{\boldsymbol{H}}_k \in \mathbb{C}^{2\times M}$ | The estimate of $\boldsymbol{H}_k$ |
| $\hat{\boldsymbol{Q}}_k \in \mathbb{C}^{2\times 2}$ | Effective channel at Eve in the previous frame |
| $\boldsymbol{s}_k \in \mathbb{C}^{2\times 1}$ | Transmit symbol vector for user $k$ |
| $\boldsymbol{w}_k \in \mathbb{C}^{2\times 1}$ | Noise vector at Bob with $\mathcal{CN}(\mathbf{0}, \sigma_B^2 \boldsymbol{I}_2)$ |
| $\boldsymbol{v}_k \in \mathbb{C}^{2\times 1}$ | Noise vector at Eve with $\mathcal{CN}(\mathbf{0}, \sigma_E^2 \boldsymbol{I}_2)$ |
| $\boldsymbol{X}_k \in \mathbb{C}^{2\times M}$ | Transmit matrix for two time intervals |
| $\boldsymbol{P} \in \mathbb{R}^{2\times 2}$ | STBC encoding matrix |
| $\alpha_k$ | Correlation between $\boldsymbol{H}_k$ and $\tilde{\boldsymbol{H}}_k$ |
| $\beta_k$ | Correlation between $\boldsymbol{Q}_k$ and $\hat{\boldsymbol{Q}}_k$ |
| $\gamma_k$ | Frobenius norm of $\tilde{\boldsymbol{H}}_k$ |
| $p_k$ | Power ratio between desired symbols and AN |
| $\boldsymbol{A}_k \in \mathbb{C}^{2\times 2}$ | AN signal matrix for user $k$ |
| $f_d T_B$ | Block normalized Doppler frequency |

proposed method are provided in Sections IV, and V concludes this article.

*Notation:* $\boldsymbol{A}^*$, $\boldsymbol{A}^T$, $\boldsymbol{A}^H$, and $\|\boldsymbol{A}\|_F$ denote the complex conjugate, the transposition, the complex conjugate transposition, and the Frobenius norm of a matrix $\boldsymbol{A}$, respectively; $\|\mathbf{a}\|$ is the 2-norm of vector $\mathbf{a}$; for a square matrix $\boldsymbol{B}$, $\mathrm{tr}(\boldsymbol{B})$ and $|\boldsymbol{B}|$ represent the trace and determinant operators; $\boldsymbol{I}_N$ means an $N$-by-$N$ identity matrix; $\mathbf{0}$ represents a vector or a matrix with all zero elements; $\mathbb{R}^{M\times N}$ and $\mathbb{C}^{M\times N}$ are the sets composed of $M$-by-$N$ real- and complex-valued matrices, respectively; and $E[\cdot]$ denotes the expectation operator. In addition, the variables used in this article are summarized as Table I.

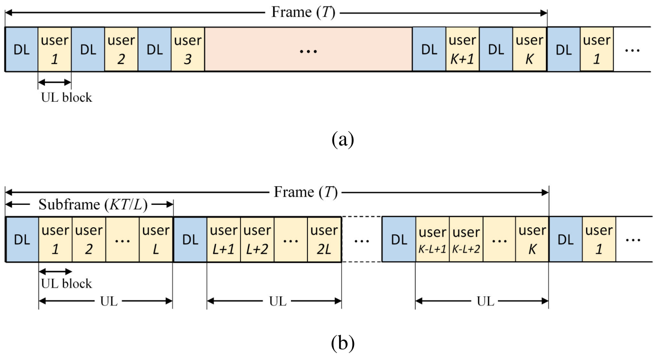
## II. SYSTEM MODEL

As shown in Fig. 2, we consider a MIMO wireless communication link composed of a legitimate AP (Bob) with two antennas, a passive eavesdropper (Eve) with two antennas, and $K$ users with $M$ antennas, where $M \in \{1, 2\}$. We assume that the passive eavesdropper only receives signals from nearby devices and transmits no signal to hide wiretapping. $\{\boldsymbol{H}_k \in \mathbb{C}^{2\times M}\}$ describe main channels from users to Bob, and $\{\boldsymbol{G}_k \in \mathbb{C}^{2\times M}\}$ denote eavesdropper channels from users to Eve, and the channels $\boldsymbol{H}_k$ and $\boldsymbol{G}_k$ are modeled as flat fading. We assume that the channels among different users are independent, and also that the main channel $\boldsymbol{H}_k$ is independent of the eavesdropper channel $\boldsymbol{G}_k$. Moreover, it is assumed that the DL and UL channels are reciprocal in both main and eavesdropping links.



M = 1 or 2
User 1
$x_1$
User 2
$x_2$
User K
$x_K$
$H_1$
$H_2$
$H_K$
$G_1$
$G_2$
$G_K$
Bob
Legitimate AP (reception and transmission)
Eve
Passive eavesdropper (reception only, no transmission)

Fig. 2. System model composed of $K$ users with $M$ antennas, a legitimate access point (AP) with two antennas, and an eavesdropper with two antennas.



(a)

(b)

Fig. 3. Time division duplexing between Bob and $K$ users, (a) when frame structure 1 is used and (b) when frame structure 2 is used.

Fig. 3 describes two frame structures based on time-division duplexing (TDD) and time-division multiplexing (TDM) to exchange data between the users and Bob. It is assumed that a DL block includes pilot symbols and a DL payload, and that a UL block has only a UL payload without a pilot for secure transmission. For simplicity, we assume that the UL block duration is identical to all users. In frame structure 1, $K$ users sequentially transmit a UL block as soon as receiving a DL block, based on TDD and TDM. In frame structure 2, Bob periodically transmits a DL block during the DL transmission interval denoted as “DL,” and $K$ users transmit UL data blocks through TDM during the UL transmission interval denoted as “UL” in Fig. 3(b). Define the frame duration as $T$. $L$ users contiguously transmit UL blocks between two consecutive DL blocks, and DL blocks are conveyed $\frac{K}{L}$ times per frame. Also, define a subframe composed of a DL block and $L$ UL blocks whose duration is $\frac{LT}{K}$. Suppose that $T_{DL}$ and $T_{UL}$ are time intervals for transmission of one DL and UL block, respectively. When UL and DL transmission intervals are denoted as $\tau T$ and $(1-\tau)T$ for $0 < \tau < 1$, respectively, $\tau = \frac{T_{UL}}{T_{DL}+T_{UL}}$ for frame structure 1 and $\tau = \frac{LT_{UL}}{T_{DL}+LT_{UL}}$ for frame structure 2.

We consider a communication scenario where confidential and/or proprietary information is transferred from user $k$ to Bob in the UL, while the pilot and normal data are carried on the DL. It is assumed that the DL pilot and data are perfectly transferred to users without active attacks such as jamming and spoofing.

A block fading channel model is used for $\boldsymbol{H}_k$ and $\boldsymbol{G}_k$, i.e., the channel gains are constant during a block and then changed to new random values in the following block. User *k* achieves the CSI of the main channel $\boldsymbol{H}_k$ using the DL pilot, and however, the CSI of the eavesdropper channel $\boldsymbol{G}_k$ is not available because Eve, a passive eavesdropper, only receives signals from nearby devices and transmits no signal.

When user *k* sends a UL data block at symbol time *n*, the received signals at Bob and Eve, $\boldsymbol{y}_k(n) \in \mathbb{C}^{2\times 1}$ and $\boldsymbol{z}_k(n) \in \mathbb{C}^{2\times 1}$, are given by

$$\boldsymbol{y}_k(n) = \boldsymbol{H}_k \boldsymbol{x}_k(n) + \boldsymbol{w}_k(n) \tag{1a}$$

$$\boldsymbol{z}_k(n) = \boldsymbol{G}_k \boldsymbol{x}_k(n) + \boldsymbol{v}_k(n) \tag{1b}$$

respectively, where $\boldsymbol{x}_k(n) \in \mathbb{C}^{M\times 1}$ is a transmit symbol vector satisfying $E[\boldsymbol{x}_k^H(n)\boldsymbol{x}_k(n)] = \mathcal{E}_k$; and $\boldsymbol{w}_k(n) \in \mathbb{C}^{2\times 1}$ and $\boldsymbol{v}_k(n) \in \mathbb{C}^{2\times 1}$ represent the noise vectors at Bob and Eve, respectively, with $\boldsymbol{w}_k \sim \mathcal{CN}(\boldsymbol{0}, \sigma_B^2 \boldsymbol{I}_2)$ and $\boldsymbol{v}_k \sim \mathcal{CN}(\boldsymbol{0}, \sigma_E^2 \boldsymbol{I}_2)$. As a performance measure of information-theoretic security, the secrecy capacity is defined as

$$C_s = [C_B - C_E]^+ \tag{2}$$

where $C_B$ and $C_E$ are the sum-rate capacities of all users at Bob and Eve, respectively, and $[x]^+ = \max(x, 0)$. Note that $C_B$ and $C_E$ depend on the design method of transmit vectors $\{\boldsymbol{x}_k(n)\}$.

## III. Proposed STLC-Based Secure Transmission

A new STLC-based transmission method is proposed for secure communications in multiuser MIMO systems as shown in Fig. 2. The STLC with two receive antennas in [49] is employed, and no pilot or training symbol is transmitted in the UL to make it difficult for Eve to estimate the eavesdropper channels. For this reason, Bob recovers the UL data through noncoherent detection. In the following sections, we first introduce an STLC-based transmission technique for single-antenna users, i.e., $M = 1$, and then propose an AN injection method for the STLC with two-antenna users, i.e., $M = 2$.

### *A. STLC for Single-Antenna Users*

A single-antenna user *k* transmits an STLC-encoded symbol vector $\boldsymbol{X}_k = [x_k(1), x_k(2)]$ to Bob with two receive antennas for secure communications. In this case, $\boldsymbol{H}_k$ and $\boldsymbol{G}_k$ are denoted as $2 \times 1$ vectors $\boldsymbol{h}_k$ and $\boldsymbol{g}_k$, respectively. When $\boldsymbol{X}_k$ is transmitted for two consecutive time intervals, it is expressed as [49]

$$\boldsymbol{X}_k = \frac{1}{\|\tilde{\boldsymbol{h}}_k\|} \tilde{\boldsymbol{h}}_k^H \boldsymbol{S}_k \in \mathbb{C}^{1\times 2} \tag{3}$$

where $\boldsymbol{S}_k = [\begin{smallmatrix} s_{k,1} & -s_{k,2}^* \\ s_{k,2} & s_{k,1}^* \end{smallmatrix}]$, $s_{k,1}$ and $s_{k,2}$ are transmit symbols for user *k* with $E[|s_{k,1}|^2] = E[|s_{k,2}|^2] = \mathcal{E}_k$, and $\tilde{\boldsymbol{h}}_k$ is the estimate of the main channel obtained from most recently transmitted DL pilot symbols. By substituting (3) into (1a) and replacing $\boldsymbol{H}_k$ with $\boldsymbol{h}_k$, the received signal matrix at Bob is written as

$$\boldsymbol{Y}_k = \frac{1}{\|\tilde{\boldsymbol{h}}_k\|} \boldsymbol{h}_k \tilde{\boldsymbol{h}}_k^H \boldsymbol{S}_k + \boldsymbol{W}_k \tag{4}$$

where $\boldsymbol{Y}_k = [\boldsymbol{y}_k(1), \boldsymbol{y}_k(2)] \in \mathbb{C}^{2\times 2}$ and $\boldsymbol{W}_k = [\boldsymbol{w}_k(1), \boldsymbol{w}_k(2)] \in \mathbb{C}^{2\times 2}$. For noncoherent detection, the received signal is rearranged as

$$\begin{bmatrix} \boldsymbol{y}_k(1) \\ \boldsymbol{y}_k^*(2) \end{bmatrix} = \frac{1}{\|\tilde{\boldsymbol{h}}_k\|} \begin{bmatrix} \boldsymbol{h}_k \tilde{\boldsymbol{h}}_k^H \\ (\boldsymbol{h}_k \tilde{\boldsymbol{h}}_k^H)^* \boldsymbol{P} \end{bmatrix} \boldsymbol{s}_k + \begin{bmatrix} \boldsymbol{w}_k(1) \\ \boldsymbol{w}_k^*(2) \end{bmatrix} \in \mathbb{C}^{4\times 1} \tag{5}$$

where $\boldsymbol{P} = [0 \quad -1 \quad 1 \quad 0]$ and $\boldsymbol{s}_k = [s_{k,1}, s_{k,2}]^T$. Using $\tilde{\boldsymbol{h}}_k$, the main channel vector $\boldsymbol{h}_k$ can be modeled as follows [59]:

$$\boldsymbol{h}_k = \alpha_k \tilde{\boldsymbol{h}}_k + \sqrt{1 - \alpha_k^2}\, \boldsymbol{e}_{h,k} \in \mathbb{C}^{2\times 1} \tag{6}$$

where $\alpha_k = 2\pi f_{B,k} T_k$ is the correlation between $\boldsymbol{h}_k$ and $\tilde{\boldsymbol{h}}_k$, $f_{B,k}$ is the normalized Doppler frequency of user *k* at Bob, $T_k$ is the time interval between the UL block for user *k*, and the most recent DL block, and $\boldsymbol{e}_{h,k} \in \mathbb{C}^{2\times 1}$ is an error vector whose elements are independent and identically distributed (i.i.d.) random variables with $\mathcal{CN}(0, \frac{1}{2}\|\tilde{\boldsymbol{h}}_k\|^2)$.

By combining the receive signals in (5) for detecting $s_1$ and $s_2$, we have

$$\begin{aligned} \boldsymbol{r}_k &\triangleq \begin{bmatrix} \boldsymbol{I}_2 & \boldsymbol{P}^T \end{bmatrix} \begin{bmatrix} \boldsymbol{y}_k(1) \\ \boldsymbol{y}_k^*(2) \end{bmatrix} \\ &= \alpha_k \|\tilde{\boldsymbol{h}}_k\| \boldsymbol{s}_k + \boldsymbol{q}_{B,k} + \tilde{\boldsymbol{w}}_k \in \mathbb{C}^{2\times 1} \end{aligned} \tag{7}$$

where $\tilde{\boldsymbol{w}}_k = \boldsymbol{w}_k(1) + \boldsymbol{P}^T \boldsymbol{w}_k^*(2)$ is a combined noise with $\mathcal{CN}(\boldsymbol{0}, 2\sigma_B^2 \boldsymbol{I}_2)$ and the interference $\boldsymbol{q}_{B,k}$ is given by

$$\boldsymbol{q}_{B,k} = \frac{\sqrt{1-\alpha_k^2}}{\|\tilde{\boldsymbol{h}}_k\|} \left( \boldsymbol{e}_{h,k} \tilde{\boldsymbol{h}}_k^H + \boldsymbol{P}^T \boldsymbol{e}_{h,k}^* \tilde{\boldsymbol{h}}_k^T \boldsymbol{P} \right) \boldsymbol{s}_k \in \mathbb{C}^{2\times 1}. \tag{8}$$

Here, $\boldsymbol{q}_{B,k}$ is distributed with $\mathcal{CN}(\boldsymbol{0}, \mathcal{E}_k(1-\alpha_k^2)\|\tilde{\boldsymbol{h}}_k\|^2 \boldsymbol{I}_2)$. From (7), the estimate of $\boldsymbol{s}_k$ is obtained as

$$\hat{\boldsymbol{s}}_k = \frac{1}{\alpha_k \|\tilde{\boldsymbol{h}}_k\|} \boldsymbol{r}_k. \tag{9}$$

When phase shift-keying (PSK) is used for modulation, the scaling factor $\alpha_k \|\tilde{\boldsymbol{h}}_k\|$ is not required for symbol detection. If non-PSK constellations are used, the scaling factor can be estimated by using a blind signal-to-noise ratio (SNR) estimation techniques whose Cramer–Rao lower bounds (CRLBs) are derived in [60]–[62]. Since the CRLB of $\alpha_k \|\tilde{\boldsymbol{h}}_k\|$ estimate is approximately given by multiplication of the CRLB of SNR estimate and the noise variance, the estimation error of the scaling factor is relatively small compared to the CSI error except the low SNR region. For this reason, the estimation error of the scaling factor is ignored in (9). From the receive signals with CSI uncertainty in (7) and (8), we have the detection signal-to-interference-plus-noise ratio (SINR) for user *k* as follows:

$$\mathrm{SINR}_{B,k} = \frac{\mathcal{E}_k \alpha_k^2 \|\tilde{\boldsymbol{h}}_k\|^2}{\mathcal{E}_k (1-\alpha_k^2)\|\tilde{\boldsymbol{h}}_k\|^2 + 2\sigma_B^2} \tag{10}$$

and the sum achievable rate at Bob is given by

$$C_B = \frac{\tau}{K} \sum_{k=1}^{K} \log_2 \left( 1 + \frac{\mathcal{E}_k \alpha_k^2 \|\tilde{\boldsymbol{h}}_k\|^2}{\mathcal{E}_k (1-\alpha_k^2)\|\tilde{\boldsymbol{h}}_k\|^2 + 2\sigma_B^2} \right). \tag{11}$$

When perfect CSI is available at the transmitter (i.e., $\alpha_k = 1$), the SINR for user *k* in (10) is equal to $\frac{\mathcal{E}_k \|\boldsymbol{h}_k\|^2}{2\sigma_B^2}$ as shown in [49].

On the other hand, the received signal at Eve is expressed as

$$\boldsymbol{Z}_k = \frac{1}{\|\tilde{\boldsymbol{h}}_k\|} \boldsymbol{g}_k \tilde{\boldsymbol{h}}_k^H \boldsymbol{S}_k + \boldsymbol{V}_k \tag{12}$$

where $\boldsymbol{Z}_k = [\boldsymbol{z}_k(1), \boldsymbol{z}_k(2)] \in \mathbb{C}^{2\times 2}$ and $\boldsymbol{V}_k = [\boldsymbol{v}_k(1), \boldsymbol{v}_k(2)] \in \mathbb{C}^{2\times 2}$. By rearranging (12) in a similar way to (5), we have

$$\boldsymbol{z}_{t,k} = \begin{bmatrix} \boldsymbol{z}_k(1) \\ \boldsymbol{z}_k^*(2) \end{bmatrix} = \frac{1}{\|\tilde{\boldsymbol{h}}_k\|} \begin{bmatrix} \boldsymbol{Q}_k \\ \boldsymbol{Q}_k^* \boldsymbol{P} \end{bmatrix} \boldsymbol{s}_k + \boldsymbol{v}_{t,k} \in \mathbb{C}^{4\times 1} \tag{13}$$

where $\boldsymbol{Q}_k = \boldsymbol{g}_k \tilde{\boldsymbol{h}}_k^H \in \mathbb{C}^{2\times 2}$ and $\boldsymbol{v}_{t,k} = [\boldsymbol{v}_k^T(1), \boldsymbol{v}_k^H(2)]^T$. In (13), the effective channel $\boldsymbol{Q}_k$ cannot be explicitly obtained at Eve, because no pilot or training symbol is transmitted from user *k*. The only way for achieving the CSI about $\boldsymbol{Q}_k$ is to use the UL blocks transmitted from user *k* in previous frames. It is intractable to obtain an accurate CSI of $\boldsymbol{Q}_k$ in previous frames due to the lack of pilot symbols. However, we assume that the CSI of $\boldsymbol{Q}_k$ is available from the most recent previous frame to consider the worst-case scenario.[1] In this case, we can write

$$\boldsymbol{Q}_k = \beta_k \hat{\boldsymbol{Q}}_k + \sqrt{1-\beta_k^2}\boldsymbol{E}_{Q,k} \in \mathbb{C}^{2\times 2} \tag{14}$$

where $\hat{\boldsymbol{Q}}_k$ is the CSI of the previous frame available at Eve, $\beta_k = (2\pi)^2 f_{B,k} T f_{E,k} T_k$ is the correlation between $\boldsymbol{Q}_k$ and $\hat{\boldsymbol{Q}}_k$, $f_{E,k}$ is the normalized Doppler frequency of user *k* at Eve, and $\boldsymbol{E}_{Q,k} \in \mathbb{C}^{2\times 2}$ is an error matrix whose elements are i.i.d. random variables with $\mathcal{CN}(0, \frac{1}{4}\|\hat{\boldsymbol{Q}}_k\|_F^2)$. By substituting (14) into (13), we obtain

$$\boldsymbol{z}_{t,k} = \frac{\beta_k}{\|\tilde{\boldsymbol{h}}_k\|} \begin{bmatrix} \hat{\boldsymbol{Q}}_k \\ \hat{\boldsymbol{Q}}_k^* \boldsymbol{P} \end{bmatrix} \boldsymbol{s}_k + \boldsymbol{q}_{E,k} + \boldsymbol{v}_{t,k} \in \mathbb{C}^{4\times 1} \tag{15}$$

where $\boldsymbol{q}_{E,k} = \frac{\sqrt{1-\beta_k^2}}{\|\tilde{\boldsymbol{h}}_k\|} [ \begin{smallmatrix} \boldsymbol{E}_{Q,k} \\ \boldsymbol{E}_{Q,k}^* \boldsymbol{P} \end{smallmatrix} ] \boldsymbol{s}_k$. Here, $\boldsymbol{q}_{E,k} + \boldsymbol{v}_{t,k}$ is the interference plus noise term distributed with $\mathcal{CN}(\boldsymbol{0}, \tilde{\sigma}_{E,k}^2 \boldsymbol{I}_4)$, where $\tilde{\sigma}_{E,k}^2$ is given by

$$\tilde{\sigma}_{E,k}^2 = \frac{(1-\beta_k^2)\|\hat{\boldsymbol{Q}}_k\|_F^2 \mathcal{E}_k}{2\|\tilde{\boldsymbol{h}}_k\|^2} + \sigma_E^2. \tag{16}$$

From (15), the sum achievable rate of Eve is derived as follows:

$$\begin{aligned} C_E = &\frac{\tau}{2K} \sum_{k=1}^{K} \log_2 \\ &\times \left| \boldsymbol{I}_2 + \frac{\mathcal{E}_k \beta_k^2{}^2}{\tilde{\sigma}}{}_{E,k} \|\tilde{\boldsymbol{h}}_k\|^2 \left( \hat{\boldsymbol{Q}}_k^H \hat{\boldsymbol{Q}}_k + \boldsymbol{P}^T \hat{\boldsymbol{Q}}_k^T \hat{\boldsymbol{Q}}_k^* \boldsymbol{P} \right) \right| \end{aligned}$$

$$= \frac{\tau}{2K} \sum_{k=1}^{K} \log_2 \left| \boldsymbol{I}_2 + \frac{\mathcal{E}_k \beta_k^2 \|\hat{\boldsymbol{g}}_k\|^2}{\tilde{\sigma}_{E,k}^2 \|\tilde{\boldsymbol{h}}_k\|^2} (\hat{\boldsymbol{h}}_k \hat{\boldsymbol{h}}_k^H + \boldsymbol{P}^T \hat{\boldsymbol{h}}_k^* \hat{\boldsymbol{h}}_k^T \boldsymbol{P}) \right|$$

$$= \frac{\tau}{K} \sum_{k=1}^{K} \log_2 \left( 1 + \frac{\mathcal{E}_k \beta_k^2 \|\hat{\boldsymbol{h}}_k\|^2}{\tilde{\sigma}_{E,k}^2 \|\tilde{\boldsymbol{h}}_k\|^2} \|\hat{\boldsymbol{g}}_k\|^2 \right) \tag{17}$$

where $\hat{\boldsymbol{h}}_k$ and $\hat{\boldsymbol{g}}_k$ are the main channel and eavesdropper channel for user *k* in the previous frame, respectively. From (17), the detection SINR at Eve is expressed as

$$\mathrm{SINR}_{E,k} = \frac{\mathcal{E}_k \beta_k^2 \|\hat{\boldsymbol{h}}_k\|^2}{\tilde{\sigma}_{E,k}^2 \|\tilde{\boldsymbol{h}}_k\|^2} \|\hat{\boldsymbol{g}}_k\|^2. \tag{18}$$

Finally, by substituting (11) and (17) into (2), the sum secrecy rate $C_s$ is computed.

Since the eigen-beamforming combined with AN injection proposed in [33] exploits the nullspace of the main channel $\boldsymbol{H}_k$, it is used when the number of transmit antennas is greater than the number of receive antennas or there is an eigenspace unused for data transmission. In other words, it does not applicable to a $1 \times 2$ SIMO channel, in which users have a single antenna. The proposed method improves the sum secrecy rate through STLC encoding at users and noncoherent decoding at Bob.

### *B. STLC for Two-Antenna Users With AN*

In this section, we extend the STLC-based secure transmission method to the two-antenna users, i.e., $M = 2$. To further enhance the secrecy rate, we design AN signals as in the eigen-beamforming and STBC schemes [33], [36], and optimize the power ratio between information-bearing symbols and AN signals. When user *k* transmits STLC-encoded symbols with AN using two antennas, the transmit symbols for two consecutive time intervals are written as

$$\boldsymbol{X}_k = \frac{\sqrt{p_k}}{\gamma_k} \tilde{\boldsymbol{H}}_k^H \boldsymbol{S}_k + \frac{\sqrt{1-p_k}}{\gamma_k} \boldsymbol{A}_k \in \mathbb{C}^{2\times 2} \tag{19}$$

where $\tilde{\boldsymbol{H}}_k$ is the estimate of the main channel matrix obtained from the most recently transmitted DL pilot, $\gamma_k = \|\tilde{\boldsymbol{H}}_k\|_F$, $\boldsymbol{A}_k \in \mathbb{C}^{2\times 2}$ is an AN signal matrix for user *k* satisfying $\|\boldsymbol{A}_k\|_F^2 = \|\tilde{\boldsymbol{H}}_k^H \boldsymbol{S}_k\|_F^2 = 2\mathcal{E}_s \gamma_k^2$, and $0 < p_k \leq 1$ is the power ratio between STLC-encoded symbols and AN signals for user *k*. Our goal is to find a low-complexity AN design scheme that utilizes the noncoherent detection structure of STLC in Section III-A. From (19), the received signal at Bob is expressed as

$$\boldsymbol{Y}_k = \frac{\sqrt{p_k}}{\gamma_k} \boldsymbol{H}_k \tilde{\boldsymbol{H}}_k^H \boldsymbol{S}_k + \frac{\sqrt{1-p_k}}{\gamma_k} \boldsymbol{H}_k \boldsymbol{A}_k + \boldsymbol{W}_k. \tag{20}$$

As in (6), the main channel $\boldsymbol{H}_k$ is modeled as

$$\boldsymbol{H}_k = \alpha_k \tilde{\boldsymbol{H}}_k + \sqrt{1-\alpha_k^2}\boldsymbol{E}_{H,k} \tag{21}$$

where $\boldsymbol{E}_{H,k} \in \mathbb{C}^{2\times 2}$ is an error matrix whose elements are i.i.d. random variables with $\mathcal{CN}(0, \frac{1}{4}\gamma_k^2)$. In a similar manner to (4)–(7), we can rearrange $\boldsymbol{Y}_k$ for noncoherent detection as

[1] In the worst-case scenario, Eve initially tries to decode the UL signals from user *k* using a blind channel estimation method (see [63] and references therein). If Eve successfully decodes the transmit symbols for user *k* at the $(m-1)$th frame, the channel between user *k* and Eve $\hat{\boldsymbol{Q}}_k$ can be estimated by utilizing the decoded symbols as pilot sequences. Then, $\hat{\boldsymbol{Q}}_k$ can be used for decoding the symbols from user *k* at the *m*th frame. It is assumed that Eve always successfully decodes the symbols for user *k* at the previous frame, in order to evaluate the worst-case sum secrecy rate.

follows:

$$\begin{aligned}\boldsymbol{r}_k &\triangleq \begin{bmatrix}\boldsymbol{I}_2 & \boldsymbol{P}^T\end{bmatrix}\begin{bmatrix}\boldsymbol{y}_k(1)\\ \boldsymbol{y}_k^*(2)\end{bmatrix}\\ &= \alpha_k\gamma_k\sqrt{p_k}\boldsymbol{s}_k + \frac{\sqrt{1-p_k}}{\gamma_k}\boldsymbol{b}_k + \sqrt{p_k}\boldsymbol{q}_{B,k} + \tilde{\boldsymbol{w}}_k \qquad (22)\end{aligned}$$

where $\boldsymbol{b}_k = \boldsymbol{H}_k[a_{k,1,1}\ \ a_{k,2,1}]^T + \boldsymbol{P}^T\boldsymbol{H}_k^*[a_{k,1,2}\ \ a_{k,2,2}]^H \in \mathbb{C}^{2\times 1}$; $a_{k,i,j}$ is the $(i,j)$th element of $\boldsymbol{A}_k$; $\boldsymbol{q}_{B,k}$ is the interference by CSI error described as

$$\boldsymbol{q}_{B,k} = \frac{\sqrt{1-\alpha_k^2}}{\gamma_k}\left(\boldsymbol{E}_{H,k}\tilde{\boldsymbol{H}}_k^H + \boldsymbol{P}^T\boldsymbol{E}_{H,k}^*\tilde{\boldsymbol{H}}_k^T\boldsymbol{P}\right)\boldsymbol{s}_k \qquad (23)$$

and the per-symbol variance of $\boldsymbol{q}_{B,k}$ is given by

$$\begin{aligned}\sigma_{q,k}^2 &= \frac{1}{2}\operatorname{tr}\left(E[\boldsymbol{q}_{B,k}\boldsymbol{q}_{B,k}^H]\right)\\ &= \frac{\mathcal{E}_k(1-\alpha_k^2)}{2\gamma_k^2}\operatorname{tr}\left(E\left[\left(\boldsymbol{E}_{H,k}\tilde{\boldsymbol{H}}_k^H + \boldsymbol{P}^T\boldsymbol{E}_{H,k}^*\tilde{\boldsymbol{H}}_k^T\boldsymbol{P}\right)\right.\right.\\ &\qquad \left.\left.\times\left(\boldsymbol{E}_{H,k}\tilde{\boldsymbol{H}}_k^H + \boldsymbol{P}^T\boldsymbol{E}_{H,k}^*\tilde{\boldsymbol{H}}_k^T\boldsymbol{P}\right)^H\right]\right)\\ &= \frac{\mathcal{E}_k(1-\alpha_k^2)\gamma_k^2}{2}. \qquad (24)\end{aligned}$$

Now, we design the AN signal matrix $\boldsymbol{A}_k$ such that the AN component $\boldsymbol{b}_k$ is completely eliminated from the Bob's received signal in (22). From the definition of $\boldsymbol{b}_k$, the AN signal vectors should fulfill the following condition:

$$\boldsymbol{b}_k = \boldsymbol{H}_k\boldsymbol{a}_{k,1} + \boldsymbol{P}^T\boldsymbol{H}_k^*\boldsymbol{a}_{k,2}^* = \boldsymbol{0} \in \mathbb{C}^{2\times 1} \qquad (25)$$

where $\boldsymbol{a}_{k,m} = [a_{k,m,1}, a_{k,m,2}]^T$ for $m \in \{1,2\}$. Because $\boldsymbol{H}_k$ is not available at user *k*, $\boldsymbol{H}_k$ is replaced with the channel estimate $\tilde{\boldsymbol{H}}_k$. Then, by expanding the left-hand side of (25), the AN nulling condition is modified as follows:

$$\boldsymbol{H}_{k,1}^c\boldsymbol{a}_{k,1}^c + \boldsymbol{H}_{k,2}^c\boldsymbol{a}_{k,2}^c = \boldsymbol{0} \qquad (26)$$

where $\boldsymbol{a}_{k,m}^c = [a_{k,m,1}, a_{k,m,2}^*]^T$ for $m \in \{1,2\}$ and $\boldsymbol{H}_{k,m}^c$ is given by

$$\boldsymbol{H}_{k,m}^c = \begin{bmatrix}\tilde{h}_{k,1,m} & \tilde{h}_{k,2,m}^*\\ \tilde{h}_{k,2,m} & -\tilde{h}_{k,1,m}^*\end{bmatrix}. \qquad (27)$$

Here, $\tilde{h}_{k,i,j}$ is the $(i,j)$th element of $\tilde{\boldsymbol{H}}_k$. Using the property that the columns of $\boldsymbol{H}_{k,m}^c$ are orthogonal, we can construct the vectors $\boldsymbol{a}_{k,1}^c$ and $\boldsymbol{a}_{k,2}^c$ to meet (26) in a concise form as follows:

$$\boldsymbol{a}_{k,1}^c = \frac{\|\tilde{\boldsymbol{h}}_{k,2}\|}{\|\tilde{\boldsymbol{h}}_{k,1}\|}(\boldsymbol{H}_{k,1}^c)^H\boldsymbol{\epsilon}_k \in \mathbb{C}^{2\times 1} \qquad (28a)$$

$$\boldsymbol{a}_{k,2}^c = -\frac{\|\tilde{\boldsymbol{h}}_{k,1}\|}{\|\tilde{\boldsymbol{h}}_{k,2}\|}(\boldsymbol{H}_{k,2}^c)^H\boldsymbol{\epsilon}_k \in \mathbb{C}^{2\times 1} \qquad (28b)$$

where $\tilde{\boldsymbol{h}}_{k,m}$ is the *m*th column of $\tilde{\boldsymbol{H}}_k$ and $\boldsymbol{\epsilon}_k \in \mathbb{C}^{2\times 1}$ is a random vector distributed with $\mathcal{CN}(\boldsymbol{0}, \mathcal{E}_k\boldsymbol{I}_2)$. From our AN design of (28), it is easily shown that $\|\boldsymbol{A}_k\|_F^2 = \|\boldsymbol{a}_{k,1}\|^2 + \|\boldsymbol{a}_{k,2}\|^2 = 2\mathcal{E}_s\gamma_k^2$.

When the user has the perfect CSI of the main channel, i.e., $\tilde{\boldsymbol{H}}_k = \boldsymbol{H}_k$, it is readily shown that $\boldsymbol{b}_k$ is thoroughly eliminated from the combined signal $\boldsymbol{r}_k$ in (22). In a practical system, the AN signal is not completely removed due to the imperfect CSI, and from (21) and (25), the combined AN signal is written as

$$\begin{aligned}\boldsymbol{b}_k &= \sum_{m=1}^{2}\left(\alpha_k\boldsymbol{H}_{k,m}^c + \sqrt{1-\alpha_k^2}\boldsymbol{E}_{k,m}^c\right)\boldsymbol{a}_{k,m}^c\\ &= \sqrt{1-\alpha_k^2}\sum_{m=1}^{2}\boldsymbol{E}_{k,m}^c\boldsymbol{a}_{k,m}^c \qquad (29)\end{aligned}$$

where $\boldsymbol{E}_{k,m}^c = [\begin{smallmatrix}e_{k,1,m} & e_{k,2,m}^*\\ e_{k,2,m} & -e_{k,1,m}^*\end{smallmatrix}]$ and $e_{k,i,j}$ is the $(i,j)$th element of $\boldsymbol{E}_{H,k}$. Note that $E[\boldsymbol{b}_k] = \boldsymbol{0}$ and the correlation matrix of $\boldsymbol{b}_k$ is given by

$$E[\boldsymbol{b}_k\boldsymbol{b}_k^H] = \frac{1}{2}\mathcal{E}_k(1-\alpha_k^2)\gamma_k^4\boldsymbol{I}_2. \qquad (30)$$

Using (29), the combined received signal at Bob is rewritten as

$$\begin{aligned}\boldsymbol{r}_k &= \alpha_k\gamma_k\sqrt{p_k}\boldsymbol{s}_k + \frac{\sqrt{(1-p_k)(1-\alpha_k^2)}}{\gamma_k}\sum_{m=1}^{2}\boldsymbol{E}_{k,m}^c\boldsymbol{a}_{k,m}^c\\ &\quad + \sqrt{p_k}\boldsymbol{q}_{B,k} + \tilde{\boldsymbol{w}}_k. \qquad (31)\end{aligned}$$

Therefore, by employing (24), (30), and $\tilde{\boldsymbol{w}}_k \sim \mathcal{CN}(\boldsymbol{0}, 2\sigma_B^2\boldsymbol{I}_2)$, the detection SINR of Bob is expressed as

$$\begin{aligned}\mathrm{SINR}_{B,k} &= \frac{\mathcal{E}_k\alpha_k^2\gamma_k^2p_k}{\frac{1}{2}\mathcal{E}_k(1-\alpha_k^2)\gamma_k^2\{(1-p_k)+p_k\} + 2\sigma_B^2}\\ &= \frac{\mathcal{E}_k\alpha_k^2\gamma_k^2p_k}{\frac{1}{2}\mathcal{E}_k(1-\alpha_k^2)\gamma_k^2 + 2\sigma_B^2} \qquad (32)\end{aligned}$$

and the sum achievable rate at Bob is derived as follows:

$$C_B = \frac{\tau}{K}\sum_{k=1}^{K}\log_2\left(1 + \frac{\mathcal{E}_k\alpha_k^2\gamma_k^2p_k}{\frac{1}{2}\mathcal{E}_k(1-\alpha_k^2)\gamma_k^2 + 2\sigma_B^2}\right). \qquad (33)$$

As the next step, we evaluate the sum achievable rate at Eve when the AN signal in (28) is used. The received signal at Eve is written as

$$\boldsymbol{Z}_k = \frac{\sqrt{p_k}}{\gamma_k}\boldsymbol{G}_k\tilde{\boldsymbol{H}}_k^H\boldsymbol{S}_k + \frac{\sqrt{1-p_k}}{\gamma_k}\boldsymbol{G}_k\boldsymbol{A}_k + \boldsymbol{V}_k \qquad (34)$$

where $\boldsymbol{Z}_k = [\boldsymbol{z}_k(1), \boldsymbol{z}_k(2)]$ and $\boldsymbol{V}_k = [\boldsymbol{v}_k(1), \boldsymbol{v}_k(2)]$. As in (13), the received signal in (34) is rearranged as

$$\boldsymbol{z}_{t,k} = \frac{\sqrt{p_k}}{\gamma_k}\begin{bmatrix}\boldsymbol{Q}_k\\ \boldsymbol{Q}_k^*\boldsymbol{P}\end{bmatrix}\boldsymbol{s}_k + \frac{\sqrt{1-p_k}}{\gamma_k}\boldsymbol{f}_k + \boldsymbol{v}_{t,k} \qquad (35)$$

where $\boldsymbol{Q}_k = \boldsymbol{G}_k\tilde{\boldsymbol{H}}_k^H$, $\boldsymbol{f}_k = [\begin{smallmatrix}\boldsymbol{G}_k\boldsymbol{a}_{k,1}\\ \boldsymbol{G}_k^*\boldsymbol{a}_{k,2}^*\end{smallmatrix}]$, and $\boldsymbol{a}_{k,m}$ is the *m*th column of $\boldsymbol{A}_k$. Suppose that the CSI of $\boldsymbol{Q}_k$ is obtained from the most recent previous frame to consider the worse case as in the single-antenna users, i.e., $\boldsymbol{Q}_k$ is denoted as (14). Then, we can rewrite (35) as

$$\begin{aligned}\boldsymbol{z}_{t,k} &= \frac{\beta_k\sqrt{p_k}}{\gamma_k}\begin{bmatrix}\hat{\boldsymbol{Q}}_k\\ \hat{\boldsymbol{Q}}_k^*\boldsymbol{P}\end{bmatrix}\boldsymbol{s}_k + \frac{\sqrt{1-p_k}}{\gamma_k}\boldsymbol{f}_k + \sqrt{p_k}\boldsymbol{q}_{E,k} + \boldsymbol{v}_{t,k}\\ &= \frac{\beta_k\sqrt{p_k}}{\gamma_k}\hat{\boldsymbol{Q}}_k^c\boldsymbol{s}_k + \frac{\sqrt{1-p_k}}{\gamma_k}\boldsymbol{f}_k + \tilde{\boldsymbol{v}}_{t,k} \qquad (36)\end{aligned}$$

where $\hat{\boldsymbol{Q}}_k^c = [\begin{smallmatrix}\hat{\boldsymbol{Q}}_k \\ \hat{\boldsymbol{Q}}_k^*\boldsymbol{P}\end{smallmatrix}]$, $\tilde{\boldsymbol{v}}_{t,k} = \sqrt{p_k}\boldsymbol{q}_{E,k} + \boldsymbol{v}_{t,k}$ is the sum of the interference vector by CSI error and the noise vector, and $\boldsymbol{q}_{E,k}$ is the same as in (15). From the definition of $\boldsymbol{a}_{k,1}^c$ and $\boldsymbol{a}_{k,2}^c$ in (28), the correlation matrices between $\boldsymbol{a}_{k,m}$ and $\boldsymbol{a}_{k,n}$ are obtained as follows (see Appendix A for details):

$$E[\boldsymbol{a}_{k,1}(\boldsymbol{a}_{k,1})^H] = \mathcal{E}_k \boldsymbol{P}^T \tilde{\boldsymbol{H}}_k^T \tilde{\boldsymbol{H}}_k^* \boldsymbol{P} \tag{37a}$$

$$E[\boldsymbol{a}_{k,2}^*(\boldsymbol{a}_{k,2})^T] = \mathcal{E}_k \boldsymbol{P}^T \tilde{\boldsymbol{H}}_k^H \tilde{\boldsymbol{H}}_k \boldsymbol{P} \tag{37b}$$

$$E[\boldsymbol{a}_{k,1}(\boldsymbol{a}_{k,2})^T] = \mathcal{E}_k |\tilde{\boldsymbol{H}}_k^*| \boldsymbol{P}. \tag{37c}$$

Using (37a), the correlation matrix of $\boldsymbol{f}_k$, $\boldsymbol{F}_k = E[\boldsymbol{f}_k \boldsymbol{f}_k^H]$, is given by

$$\begin{aligned}\boldsymbol{F}_k &= \begin{bmatrix} \boldsymbol{G}_k E[\boldsymbol{a}_{k,1}\boldsymbol{a}_{k,1}^H]\boldsymbol{G}_k^H & \boldsymbol{G}_k E[\boldsymbol{a}_{k,1}\boldsymbol{a}_{k,2}^T]\boldsymbol{G}_k^T \\ \boldsymbol{G}_k^* E[\boldsymbol{a}_{k,2}^*\boldsymbol{a}_{k,1}^H]\boldsymbol{G}_k^H & \boldsymbol{G}_k^* E[\boldsymbol{a}_{k,2}^*\boldsymbol{a}_{k,2}^T]\boldsymbol{G}_k^T \end{bmatrix} \\ &= \mathcal{E}_k \begin{bmatrix} \boldsymbol{G}_k \boldsymbol{P}^T \tilde{\boldsymbol{H}}_k^T \tilde{\boldsymbol{H}}_k^* \boldsymbol{P} \boldsymbol{G}_k^H & |\tilde{\boldsymbol{H}}_k^*| \boldsymbol{G}_k \boldsymbol{P} \boldsymbol{G}_k^T \\ |\tilde{\boldsymbol{H}}_k| \boldsymbol{G}_k^* \boldsymbol{P}^T \boldsymbol{G}_k^H & \boldsymbol{G}_k^* \boldsymbol{P}^T \tilde{\boldsymbol{H}}_k^H \tilde{\boldsymbol{H}}_k \boldsymbol{P} \boldsymbol{G}_k^T \end{bmatrix}.\end{aligned} \tag{38}$$

Moreover, $\hat{\boldsymbol{v}}_{t,k}$ of (36) has the distribution of $\mathcal{CN}(\boldsymbol{0}, \tilde{\sigma}_{E,k}^2 \boldsymbol{I}_4)$, where $\tilde{\sigma}_{E,k}^2$ is given by

$$\tilde{\sigma}_{E,k}^2 = \frac{p_k(1-\beta_k^2)\|\hat{\boldsymbol{Q}}_k\|_F^2 \mathcal{E}_k}{2\gamma_k^2} + \sigma_E^2. \tag{39}$$

Now, from (36), (38), and (39), the sum achievable rate at Eve is derived as

$$\begin{aligned} C_E = \frac{\tau}{2K}\sum_{k=1}^{K} \Bigg\{ &\log_2 \left| \tilde{\sigma}_{E,k}^2 \boldsymbol{I}_4 + \frac{1-p_k}{\gamma_k^2}\boldsymbol{F}_k + \frac{p_k \beta_k^2 \mathcal{E}_k}{\gamma_k^2}\boldsymbol{\Psi}_k \right| \\ &- \log_2 \left| \tilde{\sigma}_{E,k}^2 \boldsymbol{I}_4 + \frac{1-p_k}{\gamma_k^2}\boldsymbol{F}_k \right| \Bigg\} \end{aligned} \tag{40}$$

where $\boldsymbol{\Psi}_k = \hat{\boldsymbol{Q}}_k^c (\hat{\boldsymbol{Q}}_k^c)^H$. Finally, the sum secrecy rate is evaluated by substituting (33) and (40) into (2).

As shown in (40), $C_E$ depends on $\boldsymbol{G}_k$, which is not available at the user of the proposed STLC-based method. To determine the optimal power ratio $p_k$ maximizing the sum secrecy rate, it is assumed that the elements of $\boldsymbol{G}_k$ are i.i.d. random variables with zero mean and variance of $\mathcal{E}_g$. Then, we evaluate $E[\boldsymbol{F}_k]$ and $E[(\hat{\boldsymbol{Q}}_k^c)^H \hat{\boldsymbol{Q}}_k^c]$ with respect to $\boldsymbol{G}_k$ to approximately compute $C_E$ without using $\boldsymbol{G}_k$. From (38), we have

$$\begin{aligned} &E\left[\boldsymbol{G}_k \boldsymbol{P}^T \tilde{\boldsymbol{H}}_k^T \tilde{\boldsymbol{H}}_k^* \boldsymbol{P} \boldsymbol{G}_k^H\right] \\ &\quad = E[\boldsymbol{G}_k \boldsymbol{\Phi}_k \boldsymbol{D}_k \boldsymbol{\Phi}_k^H \boldsymbol{G}_H] = E\left[\lambda_1 \tilde{\boldsymbol{\phi}}_1 \tilde{\boldsymbol{\phi}}_1^H + \lambda_2 \tilde{\boldsymbol{\phi}}_2 \tilde{\boldsymbol{\phi}}_2^H\right] \\ &\quad = \mathcal{E}_g(\lambda_1 + \lambda_2)\boldsymbol{I}_2 = \mathcal{E}_g \|\tilde{\boldsymbol{H}}_k\|_F^2 \boldsymbol{I}_2 \end{aligned} \tag{41}$$

where $\boldsymbol{P}^T \tilde{\boldsymbol{H}}_k^T \tilde{\boldsymbol{H}}_k^* \boldsymbol{P} = \boldsymbol{\Phi}_k \boldsymbol{D}_k \boldsymbol{\Phi}_k^H$ is the eigen-decomposition by a $2 \times 2$ unitary matrix $\boldsymbol{\Phi}_k$ and a diagonal matrix $\boldsymbol{D}_k = \mathrm{diag}[\lambda_1, \lambda_2]$, and $\tilde{\boldsymbol{\phi}}_m$ is the *m*th column of $\boldsymbol{G}_k \boldsymbol{\Phi}_k$. Note that we used the property $E[\boldsymbol{G}_k \boldsymbol{\Phi}_k \boldsymbol{\Phi}_k^H \boldsymbol{G}_H] = \mathcal{E}_g \boldsymbol{I}_2$. Again from (38), we obtain

$$E[|\tilde{\boldsymbol{H}}_k^*| \boldsymbol{G}_k \boldsymbol{P} \boldsymbol{G}_k^T] = E[|\tilde{\boldsymbol{H}}_k^*||\boldsymbol{G}_k|\boldsymbol{P}] = \boldsymbol{0} \tag{42}$$

because $E[|\boldsymbol{G}_k|] = 0$. Using (41) and (42), the expectation of $\boldsymbol{F}_k$ is given by

$$E[\boldsymbol{F}_k] = \mathcal{E}_k \mathcal{E}_g \|\tilde{\boldsymbol{H}}_k\|_F^2 \boldsymbol{I}_4. \tag{43}$$

Moreover, the expectation of $(\hat{\boldsymbol{Q}}_k^c)^H \hat{\boldsymbol{Q}}_k^c$ is derived as follows:

$$\begin{aligned} E[\boldsymbol{\Phi}_k] &\triangleq E\left[\left(\hat{\boldsymbol{Q}}_k^c\right)^H \hat{\boldsymbol{Q}}_k^c\right] = E\left[\hat{\boldsymbol{Q}}_k^H \hat{\boldsymbol{Q}}_k + \boldsymbol{P}^T \hat{\boldsymbol{Q}}_k^T \hat{\boldsymbol{Q}}_k^* \boldsymbol{P}\right] \\ &= E[\|\hat{\boldsymbol{Q}}_k\|_F^2]\boldsymbol{I}_2 = E[\|\tilde{\boldsymbol{Q}}_k\|_F^2]\boldsymbol{I}_2 \\ &= 2\mathcal{E}_g \|\tilde{\boldsymbol{H}}_k\|_F^2 \boldsymbol{I}_2. \end{aligned} \tag{44}$$

By replacing $\boldsymbol{F}_k$, $\boldsymbol{\Psi}_k$, and $\tilde{\sigma}_{E,k}^2$ with the expectations with respect to $\boldsymbol{G}_k$ in (40), we have

$$\begin{aligned} \widetilde{C}_E &= \frac{\tau}{2K}\sum_{k=1}^{K} \log_2 \left| \boldsymbol{I}_4 + \frac{p_k \beta_k^2 \mathcal{E}_k}{(1-p_k)\mathcal{E}_k \mathcal{E}_g + E[\tilde{\sigma}_{E,k}^2]} \frac{E[\boldsymbol{\Psi}_k]}{\gamma_k^2} \right| \\ &= \frac{\tau}{2K}\sum_{k=1}^{K} \log_2 \left| \boldsymbol{I}_2 + \frac{p_k \beta_k^2 \mathcal{E}_k}{(1-p_k)\mathcal{E}_k \mathcal{E}_g + E[\tilde{\sigma}_{E,k}^2]} \frac{E[\boldsymbol{\Phi}_k]}{\gamma_k^2} \right| \\ &= \frac{\tau}{K}\sum_{k=1}^{K} \log_2 \left( 1 + \frac{2 p_k \beta_k^2 \mathcal{E}_k \mathcal{E}_g}{(1-p_k)\mathcal{E}_k \mathcal{E}_g + E[\tilde{\sigma}_{E,k}^2]} \right) \end{aligned} \tag{45}$$

where $E[\tilde{\sigma}_{E,k}^2] = p_k(1-\beta_k^2)\mathcal{E}_g \mathcal{E}_k + \sigma_E^2$. Notice that we used the property that $|\boldsymbol{I} + \boldsymbol{A}\boldsymbol{A}^H| = |\boldsymbol{I} + \boldsymbol{A}^H \boldsymbol{A}|$. Since (45) still requires the knowledge of $\mathcal{E}_g$, it is also assumed that the average SINR of Eve is identical to the SINR of Bob, i.e., $\frac{E[\|\boldsymbol{G}_k\|_F^2]}{\sigma_E^2} = \frac{\|\tilde{\boldsymbol{H}}_k\|_F^2}{\sigma_B^2}$. In this case, we get $\frac{4\mathcal{E}_g}{\sigma_E^2} = \frac{\gamma_k^2}{\sigma_B^2}$, and thus (45) is rewritten as

$$\widetilde{C}_E = \frac{\tau}{K}\sum_{k=1}^{K} \log_2 \left( 1 + \frac{2 p_k \beta_k^2 \mathcal{E}_k \gamma_k^2}{(1 - p_k \beta_k^2)\mathcal{E}_k \gamma_k^2 + 4\sigma_B^2} \right). \tag{46}$$

From (46), the detection SINR at Eve is denoted as

$$\mathrm{SINR}_{E,k} = \frac{2 p_k \beta_k^2 \mathcal{E}_k \gamma_k^2}{(1 - p_k \beta_k^2)\mathcal{E}_k \gamma_k^2 + 4\sigma_B^2}. \tag{47}$$

Now, the sum secrecy rate is modified as $C_s = C_B - \widetilde{C}_E$ using (33) and (46), and the optimal $p_k$ can be found by solving $\frac{\partial C_s}{\partial p_k} = 0$ as follows (see Appendix B for details):

$$p_k^o = \min\left( -d_k + \sqrt{2d_k^2 - 2c_k d_k},\ 1 \right) \tag{48}$$

where $c_k = \frac{1-\alpha_k^2}{2\alpha_k^2} + \frac{2\sigma_B^2}{\mathcal{E}_k \alpha_k^2 \gamma_k^2}$ and $d_k = \frac{1}{\beta_k^2} + \frac{4\sigma_B^2}{\mathcal{E}_k \beta_k^2 \gamma_k^2}$.

## IV. Numerical Secrecy Rate Evaluation

Through numerical simulations, we compare the sum secrecy rate of the proposed STLC method with conventional secrecy transmission schemes for $1 \times 2$ SIMO and $2 \times 2$ MIMO systems, respectively. It is assumed that the DL block duration is the same as the UL block duration, i.e., $T_B \triangleq T_{DL} = T_{UL}$, and also assumed that the Doppler frequency of user *k* is identical for Bob and Eve, i.e., $f_d \triangleq f_{B,k} = f_{E,k}$. The channel matrices $\{\boldsymbol{H}_k\}$ and $\{\boldsymbol{G}_k\}$ are i.i.d. complex Gaussian random variables with zero mean and unit variance; and the channel gain for each transmit and receive antenna pair is modeled as block flat fading so that it is changed in every block according to the block normalized Doppler frequency $f_dT_B$, where $T_B$ is the DL or UL block duration. We set $K = 20$ and $L = 4$ in Fig. 3(b). Thus, $\tau = \frac{1}{2}$ for frame structure 1 (FS1) and $\tau = \frac{4}{5}$ for frame structure 2 (FS2). Besides, $T_B$ is the same in FS1 and FS2, and the frame duration is given by $T = 40T_B$ and $T = 25T_B$ for FS1 and FS2, respectively. Every point representing the average of a sum secrecy rate is obtained by averaging over more than 100 channel realizations.

### A. *Performance Comparison for* $1 \times 2$ *SIMO*

We evaluate the sum secrecy rate of the proposed STLC-based transmission method for single-antenna users in Section III-A. For comparison, we consider the two-step method in [29] and the maximal ratio combining (MRC) for SIMO systems as well as the maximal ratio transmission (MRT) for MISO systems. Numerical simulations are performed for the following secure communication methods considering FS1 and FS2 in Fig. 3.

1) *Proposed STLC:* Proposed STLC-based method for $1 \times 2$ SIMO in Section III-A.
2) *Two-step method [29]:* Two-step method for $1 \times 2$ SIMO, transmits an arbitrary reference symbol using the eigen-beamforming with AN in the DL and modulates the data symbol by multiplying the reference symbol in the UL. The sum secrecy rate is computed accounting for the achievable rate loss for the transmission of the reference symbol.
3) *MRT [64] ($2 \times 1$ MISO):* The conventional MRT scheme maximizes the detection SNR of the $2 \times 1$ MISO systems through beamforming. This method is used to compare the sum secrecy rate of the proposed method and the MRT when the CSI is available only at the transmitter. For fairness, the CSI error by fading is considered as in the proposed method.
4) *MRC [64]:* The conventional MRC method for $1 \times 2$ SIMO maximizes the detection SNRs at both Bob and Eve, respectively. It is assumed that both Bob and Eve have perfect CSIs.

The average sum secrecy rate for various secure transmission methods is shown across the SNR when the block normalized Doppler frequency ($f_dT_B$) = 0.01 in Fig. 4, and across the $f_dT_B$ when SNR = 30 dB in Fig. 5. In Fig. 4, the proposed method outperforms conventional secure transmission schemes in all SNR regions irrespective of a frame structure. In Fig. 5, the proposed scheme with FS1 performs better than the two-step method, MRT, and the MRC when $f_dT_B > 0.0014$, and the proposed technique with FS2 shows better performance than conventional methods when $f_dT_B > 0.0018$. It is assumed that Eve achieves the CSI of $\boldsymbol{G}_k$ from the most previously transmitted UL block to take into account the worst-case scenario, and thus $C_E$ of the proposed method in (17) becomes large when $f_dT_B$ is small. If $f_dT_B$ increases, $C_E$ decreases due to the reduction of channel correlation between consecutive UL blocks from the same user, and therefore the secrecy rate gain of the proposed STLC method increases compared to existing secure transmission schemes. When $f_dT_B$ is very large, the sum rate of the main channel $C_B$ decreases because the CSI error of $\boldsymbol{H}_k$ increases, and thereby causing the decrease of the average sum secrecy rate in all secure transmission methods. Since $\tau = \frac{1}{2}$ for FS1 and $\tau = \frac{4}{5}$ for FS2, the proposed STLC with FS2 has better sum secrecy rate than that with FS1 when $f_dT_B < 0.04$. FS1 is more robust to channel variation, because the UL block is transferred just after the reception of a DL block. When the channel fade rate is very large ($f_dT_B > 0.04$), FS1 presents better performance than FS2.

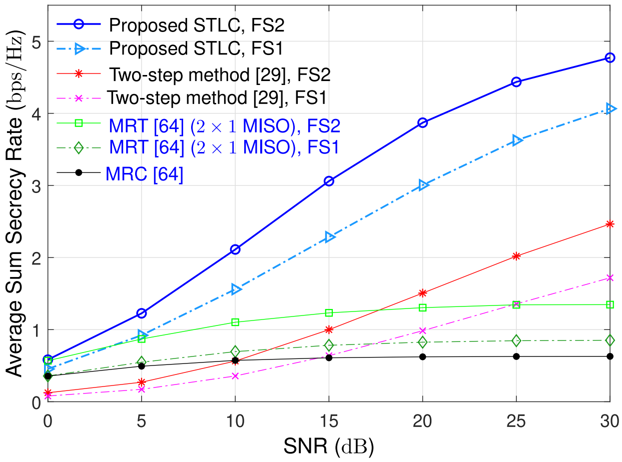


Fig. 4. Average of sum secrecy rate for various secure transmission methods across the SNR, when $f_dT_B = 0.01$.

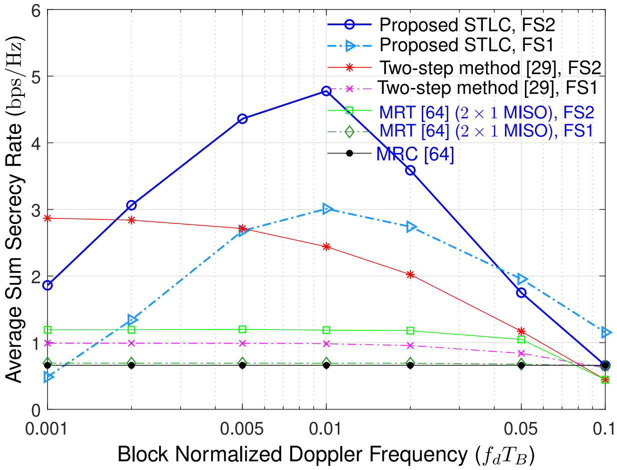


Fig. 5. Average of sum secrecy rate for various secure transmission methods across $f_dT_B$, when SNR = 30 dB.

Fig. 6 presents the outage probability of the sum secrecy rate when SNR= 20 dB and $f_dT_B = 0.01$. As expected in Figs. 4 and 5, the proposed STLC method shows the huge gain in terms of the outage probability compared to conventional secure transmission schemes. The two-step method achieves a full secrecy rate in the UL, yet it requires the prior transfer of the reference symbol in the DL using a MISO secure transmission method,

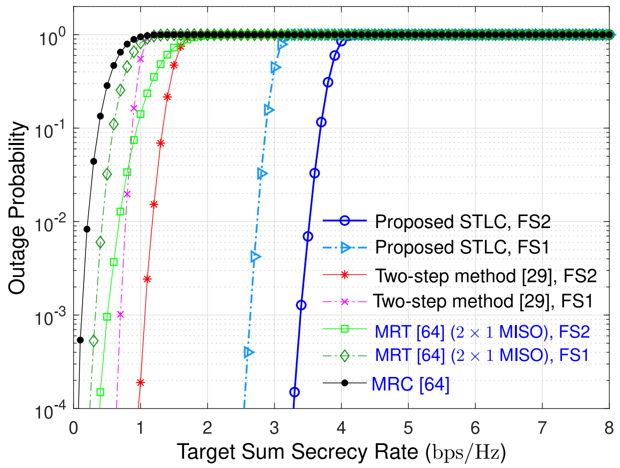


Fig. 6. Outage probability of various secure transmission methods, when SNR $= 20$ dB and $f_d T_B = 0.01$.

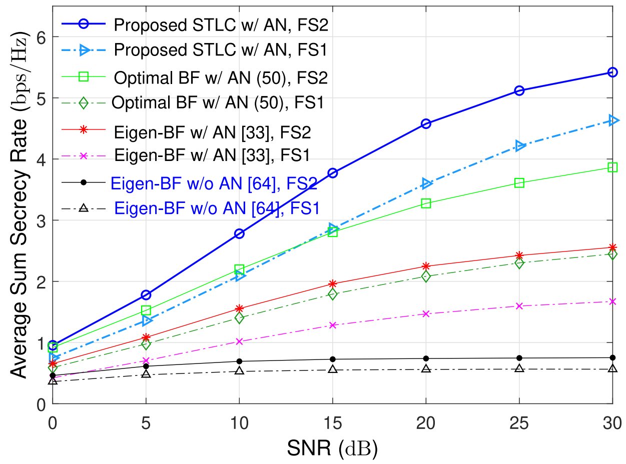


Fig. 7. Average of sum secrecy rate for various secure transmission methods for 2 × 2 MIMO systems, when $f_d T_B = 0.01$.

and thus the overall sum secrecy rate is reduced. The MRT and the MRC methods provide limited secrecy rates because Eve can detect the UL symbols similarly to Bob. As mentioned before, FS1 has smaller $\tau$ than FS2 in the proposed STLC method. Therefore, when the target outage probability is 0.001, the proposed STLC with FS2 has better sum secrecy rate than that with FS1 by 0.6 bps/Hz.

### *B. Performance Comparison for* 2 × 2 *MIMO*

The sum secrecy rate of 2 × 2 MIMO systems is evaluated for the proposed STLC-based method with AN in Section III-B and existing secure transmission schemes. As baseline secure transmission methods, we consider the optimal beamforming with AN and the eigen-beamforming with AN in [33]. In the optimal beamforming with AN, the transmit signal is defined as

$$\boldsymbol{x}_k = \boldsymbol{u}_k^s s_k + \boldsymbol{u}_k^a a_k \tag{49}$$

where $s_k$ and $a_k$ are the desired symbol and the AN signal for user $k$ satisfying $E[|s_k|^2] = E[|a_k|^2] = \mathcal{E}_s$ and $E[s_k^* a_k] = 0$; and $\boldsymbol{u}_k^s \in \mathcal{C}^{2\times 1}$ and $\boldsymbol{u}_k^a \in \mathcal{C}^{2\times 1}$ are the beamforming vectors for the desired symbol and the AN signal, respectively. Then, the secrecy rate maximization problem for user $k$ is formulated as follows:

$$\max_{\boldsymbol{u}_k^s, \boldsymbol{u}_k^a} \log_2\left(1 + \frac{\mathcal{E}_s \|\boldsymbol{H}_k \boldsymbol{u}_k^s\|^2}{\sigma_B^2}\right) - \log_2\left(1 + \frac{\mathcal{E}_s \|\boldsymbol{G}_k \boldsymbol{u}_k^s\|^2}{\mathcal{E}_s \|\boldsymbol{G}_k \boldsymbol{u}_k^a\|^2 + \sigma_E^2}\right) \tag{50a}$$

$$\text{s.t.} \quad \|\boldsymbol{u}_k^s\|^2 + \|\boldsymbol{u}_k^a\|^2 = 1. \tag{50b}$$

When $\boldsymbol{H}_k$ and $\boldsymbol{G}_k$ are available at user $k$ without CSI error, the optimal beamforming vectors for the desired symbol and AN can be found by solving (50a) using the interior-point method [65]. Note that this method is the performance upper bound of the beamforming with AN. We perform numerical simulations for the following secure transmission methods in 2 × 2 MIMO channels considering FS1 and FS2 in Fig. 3.

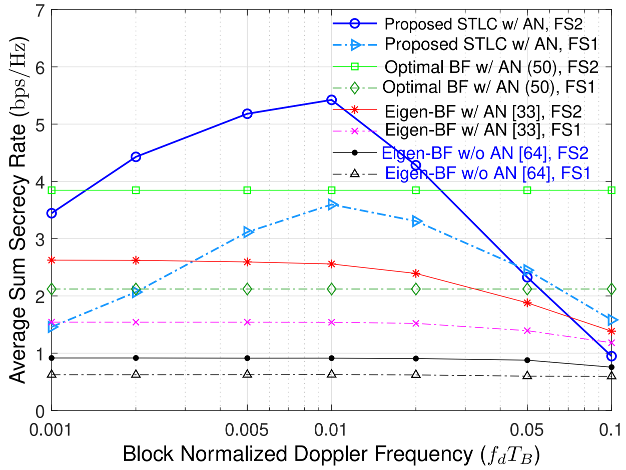


Fig. 8. Average of sum secrecy rate for various secure transmission methods for 2 × 2 MIMO systems, when SNR $= 30$ dB.

1) Proposed STLC w/AN: Proposed STLC-based method with AN in Section III-B whose transmit power ratio is determined by (48).
2) Optimal BF w/AN: Optimal beamforming (BF) with AN which finds the optimal beamforming vectors from (50a) using perfect knowledge of $\{\boldsymbol{H}_k\}$ and $\{\boldsymbol{G}_k\}$.
3) Eigen-BF w/AN: Eigen-beamforming with AN in [33]. The transmit power ratio is optimized by a grid search in the range of $0 < p_k \leq 1$ with a grid size 0.01, assuming that $\tilde{\boldsymbol{H}}_k$ and $\boldsymbol{G}_k$ are known to user $k$.
4) Eigen-BF w/o AN [64]: Eigen-beamforming without AN injection whose beamforming vector is the dominant right singular vector of $\tilde{\boldsymbol{H}}_k$.

The average sum secrecy rate of secure transmission methods is compared for 2 × 2 MIMO systems across SNR when $f_d T_B = 0.01$ in Fig. 7 and across $f_d T_B$ when SNR= 30 dB in Fig. 8, respectively. The proposed STLC-based method shows the best performance in all SNR regions without respect to a frame structure in Fig. 7. In Fig. 8, the proposed STLC with FS2

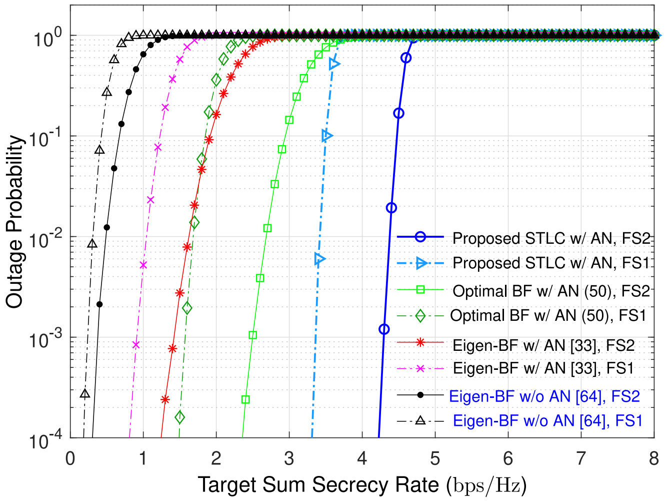


Fig. 9. Outage probability for $2 \times 2$ MIMO systems, when SNR $= 20$ dB and $f_d T_B = 0.01$.

outperforms the optimal BF without AN and eigen-BF methods with and without AN when $0.0013 < f_d T_B < 0.23$, and the proposed STLC with FS1 performs better than other methods when $0.0031 < f_d T_B < 0.63$. Since the optimal beamforming with AN finds the beamforming vectors using the perfect $\boldsymbol{H}_k$ and $\boldsymbol{G}_k$, its sum secrecy rate is identical irrespective of $f_d T_B$ and changed by a frame structure (i.e., by $\tau$). As in Fig. 5, the sum secrecy rate of the proposed method decreases when $f_d T_B$ is small, and the proposed STLC with FS2 presents better sum secrecy rate than that with FS1 because FS2 has a larger $\tau$ than FS1. When $f_d T_B > 0.01$, the sum secrecy rate decreases in all secure transmission methods except the optimal beamforming with AN, because the sum rate of the main channel is reduced by the increment of CSI error.

Fig. 9 presents the outage probability of the sum secrecy rate when SNR $= 20$ dB and $f_d T_B = 0.01$. The proposed method exhibits much lower outage probability than the conventional MIMO secure transmission methods. Also, the slope of the proposed method is steepest among the secure transmission schemes, in other words, the proposed method has smaller variation of the sum secrecy rate than the existing techniques. As in Fig. 6, the proposed STLC with FS2 has greater sum secrecy rate than that with FS1 by 0.9 bps/Hz when the target outage probability is 0.001.

## V. Conclusion

When the CSI of the main channel is only available at users and no CSIs are available at Bob and Eve, we proposed a new STLC-based secure transmission method that achieves full spatial diversity at Bob. When users have a single antenna, conventional secure transmission methods cannot be directly used, however the proposed method improves the sum secrecy rate through STLC encoding and noncoherent decoding. When users have two antennas, the proposed STLC-based method can be further enhanced in combination with AN injection, by applying a low-complexity AN design scheme and optimizing the transmit power ratio between the desired symbols and the AN signals. Through theoretical analysis of the sum secrecy rate and numerical evaluations two types of the frame structure, it was shown that the proposed methods have better performance than conventional secure transmission methods in terms of the average and outage probability of the sum secrecy rate, except the case that the channel fade rate is very low or very high. Thus, the proposed STLC transmission method can enhance secure communications for both UL and DL in combination with conventional DL secure transmission techniques, and can be used for future communication systems such as sensor networks that require confidential and private data transfer from multiple users. By transmitting multiple STLC streams and/or using more than two transmit antennas, it is expected that the secrecy rate is further improved.

## Appendix A
## Derivation of Correlation Matrices in (37a)

From the definition of $\boldsymbol{a}_{k,1}^c$ and $\boldsymbol{a}_{k,2}^c$ in (28), we can obtain the following correlation matrices:

$$E[\boldsymbol{a}_{k,1}^c(\boldsymbol{a}_{k,1}^c)^H] = \mathcal{E}_s \|\tilde{\boldsymbol{h}}_{k,2}\|^2 \tag{A.1a}$$

$$E[\boldsymbol{a}_{k,2}^c(\boldsymbol{a}_{k,2}^c)^H] = \mathcal{E}_s \|\tilde{\boldsymbol{h}}_{k,1}\|^2 \tag{A.1b}$$

$$E[\boldsymbol{a}_{k,1}^c(\boldsymbol{a}_{k,2}^c)^H] = -\mathcal{E}_s \boldsymbol{C}_{k,1}^H \boldsymbol{C}_{k,2}. \tag{A.1c}$$

Note that we used the property $(\boldsymbol{H}_{k,m}^c)^H \boldsymbol{H}_{k,m}^c = \|\tilde{\boldsymbol{h}}_{k,m}\|^2 \boldsymbol{I}_2$ for $m \in \{1, 2\}$. Also, from the definitions of $\boldsymbol{a}_{k,m}$ and $\boldsymbol{a}_{k,m}^c$, we can write

$$\left[\boldsymbol{a}_{k,1}^H, \boldsymbol{a}_{k,2}^T\right] = \left[(\boldsymbol{a}_{k,1}^c)^H, (\boldsymbol{a}_{k,2}^c)^H\right] \boldsymbol{P}_4 \tag{A.2}$$

where $\boldsymbol{P}_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$. Using (A.1a) and (A.2), the correlation matrix of $\begin{bmatrix} \boldsymbol{a}_{k,1} \\ \boldsymbol{a}_{k,2}^* \end{bmatrix}$ is denoted as

$$\begin{aligned} E\left[\begin{bmatrix} \boldsymbol{a}_{k,1} \\ \boldsymbol{a}_{k,2}^* \end{bmatrix} \begin{bmatrix} \boldsymbol{a}_{k,1} \\ \boldsymbol{a}_{k,2}^* \end{bmatrix}^H\right] &= \boldsymbol{P}_4^T E\left[\begin{bmatrix} \boldsymbol{a}_{k,1}^c \\ \boldsymbol{a}_{k,2}^c \end{bmatrix} \begin{bmatrix} \boldsymbol{a}_{k,1}^c \\ \boldsymbol{a}_{k,2}^c \end{bmatrix}^H\right] \boldsymbol{P}_4 \\ &= \mathcal{E}_s \begin{bmatrix} \|\tilde{\boldsymbol{h}}_{k,2}\|^2 & d_k & 0 & -|\tilde{\boldsymbol{H}}_k^*| \\ d_k^* & \|\tilde{\boldsymbol{h}}_{k,2}\|^2 & |\tilde{\boldsymbol{H}}_k^*| & 0 \\ 0 & |\tilde{\boldsymbol{H}}_k| & \|\tilde{\boldsymbol{h}}_{k,1}\|^2 & d_k^* \\ -|\tilde{\boldsymbol{H}}_k| & 0 & d_k & \|\tilde{\boldsymbol{h}}_{k,1}\|^2 \end{bmatrix} \\ &= \mathcal{E}_s \begin{bmatrix} \boldsymbol{P}^T \tilde{\boldsymbol{H}}_k^T \tilde{\boldsymbol{H}}_k^* \boldsymbol{P} & |\tilde{\boldsymbol{H}}_k^*| \boldsymbol{P} \\ |\tilde{\boldsymbol{H}}_k| \boldsymbol{P}^T & \boldsymbol{P}^T \tilde{\boldsymbol{H}}_k^H \tilde{\boldsymbol{H}}_k \boldsymbol{P} \end{bmatrix} \end{aligned} \tag{A.3}$$

where $d_k = -\tilde{h}_{k,1,1}^* \tilde{h}_{k,1,2} - \tilde{h}_{k,2,1}^* \tilde{h}_{k,2,2}$. Therefore, the correlation matrix between $\boldsymbol{a}_{k,m}$ and $\boldsymbol{a}_{k,n}$ are denoted as (37a).

## APPENDIX B
## DERIVATION OF OPTIMAL POWER RATIO IN (48)

The sum secrecy rate is given by $C_s = C_B - \widetilde{C}_E$, where $C_B$ and $\widetilde{C}_E$ are defined as (33) and (46), respectively. The first-order optimality condition, i.e., $\frac{\partial C_s}{\partial p_k} = 0$, is derived as follows:

$$\begin{aligned}
&\frac{K\log(2)}{\tau}\frac{\partial C_s}{\partial p_k} \\
&= \frac{2\mathcal{E}_k\alpha_k^2\gamma_k^2}{2\mathcal{E}_k\alpha_k^2\gamma_k^2 p_k + \mathcal{E}_k(1-\alpha_k^2)\gamma_k^2 + 4\sigma_B^2} \\
&\quad - \frac{\beta_k^2\mathcal{E}_k\gamma_k^2}{(1+\beta_k^2 p_k)\mathcal{E}_k\gamma_k^2 + 4\sigma_B^2} - \frac{\beta_k^2\mathcal{E}_k\gamma_k^2}{(1-\beta_k^2 p_k)\mathcal{E}_k\gamma_k^2 + 4\sigma_B^2} \\
&= \frac{1}{p_k + c_k} - \frac{1}{p_k + d_k} + \frac{1}{p_k - d_k} = 0 \qquad \text{(B.1)}
\end{aligned}$$

where $c_k = \frac{1-\alpha_k^2}{2\alpha_k^2} + \frac{2\sigma_B^2}{\mathcal{E}_k\alpha_k^2\gamma_k^2}$ and $d_k = \frac{1}{\beta_k^2} + \frac{4\sigma_B^2}{\mathcal{E}_k\beta_k^2\gamma_k^2}$. Since $\frac{\partial^2 C_s}{\partial p_k^2} < 0$ for $0 < p_k \leq 1$ and $d_k > 2c_k$, the optimal $p_k$ maximizing $C_s$ is given by (48).

## REFERENCES

[1] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun., Surv. Tut.*, vol. 19, no. 1, pp. 347–376, Jan.–Mar. 2017.

[2] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun., Surv. Tut.*, vol. 19, no. 2, pp. 1027–1053, Apr.–Jun. 2017.

[3] B. Li, Z. Fei, Z. Chu, and Y. Zhang, "Secure transmission for heterogeneous cellular networks with wireless information and power transfer," *IEEE Syst. J.*, vol. 12, no. 4, pp. 3755–3766, Dec. 2018.

[4] H. Yu, S. Guo, Y. Yang, and B. Xiao, "Optimal target secrecy rate and power allocation policy for a SWIPT system over a fading wiretap channel," *IEEE Syst. J.*, vol. 12, no. 4, pp. 3291–3302, Dec. 2018.

[5] M. R. A. Khandaker, K. Wong, Y. Zhang, and Z. Zheng, "Probabilistically robust SWIPT for secrecy MISOME systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 1, pp. 211–226, Jan. 2017.

[6] C. Guo, B. Liao, D. Feng, C. He, and X. Ma, "Minimum secrecy throughput maximization in wireless powered secure communications," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2571–2581, Mar. 2018.

[7] M. J. Saber, A. Keshavarz, J. Mazloum, A. M. Sazdar, and M. J. Piran, "Physical-layer security analysis of mixed SIMO SWIPT RF and FSO fixed-gain relaying systems," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2851–2858, Sep. 2019.

[8] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sep. 2014.

[9] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245–2261, Mar. 2016.

[10] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3880–3900, Jul. 2016.

[11] X. Zhang, D. Guo, K. An, and B. Zhang, "Secure communications over cell-free massive MIMO networks with hardware impairments," *IEEE Syst. J.*, vol. 14, no. 2, pp. 1909–1920, Jun. 2020.

[12] X. Tian, Q. Liu, Z. Wang, and M. Li, "Secure hybrid beamformers design in mmWave MIMO wiretap systems," *IEEE Syst. J.*, vol. 14, no. 1, pp. 548–559, Mar. 2020.

[13] Y. Zhu, L. Wang, K.-K. Wong, and R. W. Heath, "Secure communications in millimeter wave Ad Hoc networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 3205–3217, May 2017.

[14] Y. Zhu, G. Zheng, and M. Fitch, "Secrecy rate analysis of UAV-enabled mmwave networks using Matérn hardcore point processes," *IEEE J. Select. Areas Commun.*, vol. 36, no. 7, pp. 1397–1409, Jul. 2018.

[15] A. Li, Q. Wu, and R. Zhang, "UAV-enabled cooperative jamming for improving secrecy of ground wiretap channel," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 181–184, Feb. 2019.

[16] H. Kang, J. Joung, J. Ahn, and J. Kang, "Secrecy-aware altitude optimization for quasi-static UAV base station without eavesdropper location information," *IEEE Commun. Lett.*, vol. 23, no. 5, pp. 851–854, May 2019.

[17] D. Hu, Q. Zhang, Q. Li, and J. Qin, "Joint position, decoding order, and power allocation optimization in UAV-based NOMA downlink communications," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2949–2960, Jun. 2020.

[18] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[19] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[20] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[21] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[22] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[23] A. O. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[24] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 2470–2492, Sep. 2009.

[25] A. Khisti and G. W. Wornell, "Secure transmissionwith multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[26] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[27] M. Z. I. Sarkar and T. Ratnarajah, "Secure communications through Rayleigh fading SIMO channel with multiple eavesdroppers," in *Proc. IEEE Int. Conf. Commun.*, May 2010, pp. 1–5.

[28] C. Wang, H. Wang, and B. Wang, "Low-overhead distributed jamming for SIMO secrecy transmission with statistical CSI," *IEEE Signal Process. Lett.*, vol. 22, no. 12, pp. 2294–2298, Dec. 2015.

[29] W. Bo, M. P. Cheng, Y. P. Zhi, Y. P. Zhi, and Y. Q. Ye, "Two-step transmission with artificial noise for secure wireless SIMO communications," *Sci. China Inf. Sci.*, vol. 58, pp. 042 308:1–13, Apr. 2015.

[30] P. Zhao, M. Zhang, H. Yu, H. Luo, and W. Chen, "Robust beamforming design for sum secrecy rate optimization in MU-MIMO networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 9, pp. 1812–1823, Sep. 2015.

[31] F. S. Al-Qahtani, Y. Huang, S. Hessien, R. M. Radaydeh, C. Zhong, and H. M. Alnuweiri, "Secrecy analysis of MIMO wiretap channels with low-complexity receivers under imperfect channel estimation," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 2, pp. 257–270, Feb. 2017.

[32] T. Yang, R. Zhang, X. Cheng, and L. Yang, "Secure massive MIMO under imperfect CSI: Performance analysis and channel prediction," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 6, pp. 1610–1623, Jun. 2019.

[33] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[34] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[35] S. A. A. Fakoorian, H. Jafarkhani, and A. L. Swindlehurst, "Secure space-time block coding via artificial noise alignment," in *Proc. IEEE Asilomar Conf., Signals, Syst. Comput.*, Nov. 2011, pp. 651–655.

[36] T. Allen, A. Tajer, and N. Al-Dhahir, "Secure Alamouti MAC transmissions," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3674–3687, Jun. 2017.

[37] K. Cumanan, G. C. Alexandropoulos, Z. Ding, and G. K. Karagiannidis, "Secure communications with cooperative jamming: Optimal power allocation and secrecy outage analysis," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7495–7505, Aug. 2017.

[38] Y. Liu, H. Chen, L. Wang, and W. Meng, "Artificial noisy MIMO systems under correlated scattering Rayleigh fading–A physical layer security approach," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2121–2132, Jun. 2020.

[39] H. Yu and T. Kim, "Training and data structures for AN-aided secure communication," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2869–2872, Sep. 2019.

[40] M. Pei, J. Wei, K.-K. Wong, and X. Wang, "Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 544–549, Feb. 2012.

[41] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[42] Y. Wu, C. Xiao, Z. Ding, X. Gao, and S. Jin, "Linear precoding for finite-alphabet signaling over MIMOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2599–2612, Jul. 2012.

[43] S. A. A. Fakoorian and A. L. Swindlehurst, "On the optimality of linear precoding for secrecy in the MIMO broadcast channel," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1701–1713, Sep. 2013.

[44] C. Zhang, J. Ge, F. Gong, Y. Ji, and J. Li, "Improving physical-layer security for wireless communication systems using duality-aware two-way relay cooperation," *IEEE Syst. J.*, vol. 13, no. 2, pp. 1241–1249, Jun. 2019.

[45] A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[46] M. Andersson, R. Schaefer, T. Oechtering, and M. Skoglund, "Polar coding for bidirectional broadcast channels with common and confidential messages," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1901–1908, Sep. 2013.

[47] X. He and A. Yener, "Providing secrecy with structured codes: Two-user Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2121–2138, Apr. 2014.

[48] X. Zhou, B. Maham, and A. Hjørungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.

[49] J. Joung, "Spacetime line code," *IEEE Access*, vol. 6, pp. 1023–1041, Nov. 2018.

[50] J. Joung, "Spacetime line code for massive MIMO and multiuser systems with antenna allocation," *IEEE Access*, vol. 6, pp. 962–979, Nov. 2018.

[51] J. Joung and E.-R. Jeong, "Multiuser space-time line code with optimal and suboptimal power allocation methods," *IEEE Access*, vol. 6, pp. 51 766–51 775, Oct. 2018.

[52] J. Joung and J. Choi, "Uneven power amplifier shuffling for space-time line code (STLC) systems," *IEEE Access*, vol. 6, pp. 58 491–58 500, Oct. 2018.

[53] J. Joung and B. C. Jung, "Machine learning based blind decoding for spacetime line code (STLC) systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 5, pp. 5154–5158, May 2019.

[54] J. Joung, "Energy efficient space-time line coded regenerative two-way relay under per-antenna power constraints," *IEEE Access*, vol. 6, pp. 47026–47035, Sep. 2018.

[55] J. Joung and J. Choi, "Spacetime line codes with power allocation for regenerative two-way relay systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 5, pp. 4884–4893, May 2019.

[56] J. Joung, B. C. Jung, and J. Choi, "Spacetime line coded regenerative two-way relay systems with power control," *Electron. Lett.*, vol. 55, no. 12, pp. 694–696, Jun. 2019.

[57] J. Joung, J. Choi, and B. C. Jung, "Double spacetime line codes," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 2316–2321, Feb. 2020.

[58] J. Joung, J. Choi, B. C. Jung, and S. Yu, "Artificial noise injection and its power loading methods for secure space-time line coded systems," *Entropy*, vol. 21, no. 515, pp. 1–12, May 2019.

[59] J. Choi and R. W. Heath, "Interpolation based transmit beamforming for MIMO-OFDM with limited feedback," *IEEE Trans. Signal Process.*, vol. 53, no. 11, pp. 4125–4135, Nov. 2005.

[60] F. Bellili, A. Methenni, and S. Affes, "Closed-form CRLBs for SNR estimation from Turbo-coded BPSK-, MSK-, and square-QAM-modulated signals," *IEEE Trans. Signal Process.*, vol. 62, no. 15, pp. 4018–4033, Aug. 2014.

[61] F. Bellili, A. Stephenne, and S. Affes, "Cramer–Rao lower bounds for NDA SNR estimates of square QAM modulated transmissions," *IEEE Trans. Commun.*, vol. 58, no. 11, pp. 3211–3218, Nov. 2010.

[62] P. Gao and C. Tepedelenlioğlu, "SNR estimation for nonconstant modulus constellations," *IEEE Trans. Signal Process.*, vol. 53, no. 3, pp. 865–870, Mar. 2005.

[63] Z. Ding and L. Qiu, "Blind MIMO channel identification from second order statistics using rank deficient channel convolution matrix," *IEEE Trans. Signal Process.*, vol. 51, no. 2, pp. 535–544, Feb. 2003.

[64] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[65] S. Boyd and L. Vandenberghe, *Convex Optimization*. 1st ed. Cambridge, U.K.: Cambridge Univ. Press, 2004.

**Jihoon Choi** (Senior Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electrical engineering from Korea Advanced Institute for Science and Technology (KAIST), Daejeon, South Korea, in 1997, 1999, and 2003, respectively.

From 2003 to 2004, he was with the Department of Electrical and Computer Engineering, The University of Texas at Austin, where he performed research on MIMO-OFDM systems as a Postdoctoral Fellow. From 2004 to 2008, he was with the Samsung Electronics, Korea, where he worked on developments of radio access stations for M-WiMAX and base stations for CDMA 1xEV-DO Rev.A/B. In 2008, he joined Korea Aerospace University (KAU), Goyang, South Korea, as a Faculty Member. He is currently a Professor with the School of Electronics and Information Engineering, KAU, where he is also the Chief Investigator of the Intelligent Signal Processing Laboratory. His research interests include MIMO communication techniques, signal processing algorithms, secure transmission in the physical layer, radar signal processing, and modem design for future cellular networks, wireless LANs, IoT devices, and digital broadcasting systems.

**Jingon Joung** (Senior Member, IEEE) received the B.S. degree in radio communication engineering from Yonsei University, Seoul, South Korea, in 2001, and the M.S. and Ph.D. degrees in electrical engineering and computer science from Korea Advanced Institute for Science and Technology (KAIST), Daejeon, South Korea, in 2003 and 2007, respectively.

He was a Postdoctoral Fellow with KAIST, South Korea and UCLA, CA, USA, in 2007 and 2008, respectively. He was a Scientist with the Institute for Infocomm Research (I$^2$R), Agency for Science, Technology and Research (A*STAR), Singapore, from 2009 to 2015, and joined Chung-Ang University (CAU), Seoul, South Korea, in 2016, as a Faculty Member. He is currently an Associate Professor with the School of Electrical and Electronics Engineering, CAU, where he is also the Principal Investigator of the Intelligent Wireless Systems Laboratory. His research interests include wireless communication signal processing, numerical analysis, algorithms, and machine learning.

Dr. Joung was a recipient of the First Prize of the Intel-ITRC Student Paper Contest in 2006. He was recognized as the Exemplary Reviewers of the IEEE Communications Letters in 2012 and the IEEE Wireless Communications Letters in 2012, 2013, 2014, and 2019. He served as the Guest Editor for the IEEE Access in 2016, as the Editorial Board Member of the *APSIPA Transactions on Signal and Information Processing* from 2014 to 2019, and as a Guest Editor for the *MDPI Electronics* in 2019. He is currently an Associate Editor for the IEEE Transactions on Vehicular Technology and *MDPI Sensors*.

**Bang Chul Jung** (Senior Member, IEEE) received the B.S. degree in electronics engineering from Ajou University, Suwon, South Korea, in 2002, and the M.S. and Ph.D. degrees in electrical and computer engineering from the Korea Advanced Institute for Science and Technology (KAIST), Daejeon, South Korea, in 2004 and 2008, respectively.

He was a Senior Researcher/Research Professor with the KAIST Institute for Information Technology Convergence, Daejeon, from 2009 to 2010. From 2010 to 2015, he was a Faculty Member of Gyeongsang National University, Tongyeong, South Korea. He is currently a Professor with the Department of Electronics Engineering, Chungnam National University, Daejeon. His research interests include wireless communication systems, Internet-of-Things (IoT) communications, statistical signal processing, information theory, interference management, radio resource management, spectrum sharing techniques, and machine learning.

Dr. Jung was a recipient of the Fifth IEEE Communication Society AsiaPacific Outstanding Young Researcher Award in 2011, the Bronze Prize of Intel Student Paper Contest in 2005, the First Prize of KAISTs Invention Idea Contest in 2008, and the Bronze Prize of Samsung Humantech Paper Contest in 2009. He has been selected as a winner of Haedong Young Scholar Award in 2015, which is sponsored by the Haedong foundation and given by KICS. He has been selected as a winner of the 29th Science and Technology Best Paper Award in 2019, which is sponsored by the Korean Federation of Science and Technology Societies. He has served as an Associate Editor of IEEE Vehicular Technology Magazine since 2020 and he has also served as an Associate Editor for the *IEICE Transactions on Fundamentals of Electronics, Communications, and Computer Sciences* since 2018.