Hindawi
Security and Communication Networks
Volume 2021, Article ID 3670101, 14 pages
https://doi.org/10.1155/2021/3670101

Research Article

Secrecy Capacity of Time Reversal Beamforming for Multi-User MIMO System under Spatial Correlation

Bingyan He,[1] **Tao Sun**,[2] **Chuanmu Li**,[1] **and Xingwang Huang**[1]

[1]*Computer Engineering College, Jimei University, Xiamen, China*
[2]*Wuhan University, Wuhan, China*

Correspondence should be addressed to Tao Sun; suntao@whu.edu.cn

Received 14 May 2021; Revised 16 October 2021; Accepted 2 November 2021; Published 18 December 2021

Academic Editor: Vijayakumar Pandi

In this paper, for strengthening the security of wireless transmission system, the time reversal (TR) beamforming method is proposed for the downlink of multi-user MIMO system with multiple users who potentially act as eavesdroppers. We develop a multi-input, single-output, multi-eavesdropper (MISOME) wiretap channel model in which Rayleigh fading and spatial correlation are taken into account. Using the proposed model, we further analyze the confidentiality provided by TR beamforming and we use achievable secrecy rates as our performance metrics. In particular, we derive novel closed-formed expressions for the average secrecy-SINR and the mean secrecy sum-rate in order to characterize the influences of propagation conditions on network secrecy metrics. These expressions provide deeper insights into the impact of network interference on communication confidentiality. We find that TR beamforming can deliver the maximum secrecy capacity potential in uncorrelated Rayleigh channels and achieve perfect confidential communication without any extra secrecy cost. On the other hand, even weak inter-user correlation may cause a significant loss of achievable secrecy sum-rate and therefore result in high secrecy cost. But benefiting more from larger signal bandwidth and rich-scattering environment, the TR beamforming technique is still an attractive and cost-effective solution for low-power indoor applications.

1. Introduction

As the diversity and the number of users in wireless networks keep growing, wireless security appears to be a crucial matter in today's communication systems. Due to the broadcast nature of wireless channels, wireless multi-user communications are very susceptible to eavesdropping. Traditionally, wireless security is ensured by data cryptography techniques, which mainly depend on secret keys and also rely on the limited computational power of eavesdroppers [1–4]. However, future wireless systems demand ubiquitous coverage and large-scale deployment of wireless radio devices. The market forecasts that in the era of the Internet of Things (IoT), billions of connected devices built with more than a trillion sensors will be installed worldwide [5]. The emergence of large-scale and dynamic networks imposes new challenges on conventional cryptographic techniques, due to the complexity of distributing and maintaining secret keys. To this end, physical-layer security has reemerged as an alternative to achieve perfect secrecy without the need for an encryption key and complex encryption/decryption algorithms [1–11].

The concept of communication secrecy is built on information-theoretic notion of perfect secrecy and was first postulated by Shannon in his ground-breaking treatise [12]. Based on this concept, Wyner in his work [13] introduced the discrete memory-less wiretap channel and showed that the secrecy capacity is determined by the difference between the capacity of the legitimate link and that of the eavesdropping link. In wireless environments, radio links are degraded by path loss, shadowing, and multi-path fading. The secrecy capacity in fading channels was investigated in [14–18]. Later on, secrecy capacity topic has been further studied in the context of multi-access channels,

multiple-input multiple-output (MIMO) communications [1, 19, 20], cooperative networks [21, 22], cellular networks [14, 23, 24], and IoT networks [5, 25, 26].

Recently, physical-layer security has also been extended to multi-user MIMO channels [22, 27, 28]. But most existing works only consider noise to evaluate secrecy capacity of multi-user networks and there is still a lack of fine-grained investigation of interference impact on network secrecy [19, 22, 29]. In fact, in multi-user networks, more users cause more severe inter-user interference (IUI) imposed on the receiver, which is considered deleterious for communications. Moreover, as signal bandwidth increases, more multi-path components can be resolved in a rich-scattering environment, such as indoors or in metropolitan areas [30]. Essentially, multi-path components are naturally existing degrees of freedom in the environment and channel capacity grows linearly with the available degrees of freedom [30–32]. But in practical communication systems, strong multi-path propagation causes severe inter-symbol interference (ISI) and then causes crucial system performance degradation, especially when the symbol rate is very high. Therefore, it is of critical importance to characterize the impact of interference (i.e., ISI and IUI) on secrecy capacity achievable in multi-user MIMO system over multi-path channels. We advocate the exploitation of wireless channel intrinsic properties (e.g., multi-path propagation) to strengthen communication secrecy.

As a linear precoding technique, TR beamforming can fully harvest energy from a rich-scattering environment and achieve superior focusing effect in both time and spatial domains, which can effectively suppress interference and improve the energy efficiency of wireless transmission [33–38]. In addition, thanks to its high-resolution spatial focusing effect, the TR-based system can achieve low probability of intercept. In other words, spatial focusing effect can also improve the system security [39–43].

In this paper, the secrecy performance of the multi-user MIMO TR-based system is presented and mainly studied in terms of achievable secrecy rates and secrecy cost. We take into account a multi-user MIMO TR-based system model that is generalized by considering (i) the frequency selective channel that has arbitrary power in each tap, (ii) the correlation at the transmitter side, and (iii) the correlation at the user side. Moreover, the average effective secrecy-SINR is derived using exact power expressions of desired signal, inter-symbol interference, and inter-user interference terms at both legitimate and illegitimate nodes. Finally, the validity of our analysis is verified by means of Monte Carlo simulation. The key contributions of the paper can be summarized as follows:

(1) We develop a framework for design and analysis of a multi-user MIMO TR-based system with intrinsic secrecy that accounts for propagation conditions and aggregates network interference.

(2) We derive approximations for the average secrecy-SINR and the mean per-user secrecy rate achievable by TR beamforming, the accuracies of which are verified by Monte Carlo simulations.

(3) The upper and lower bounds on mean per-user secrecy rate are determined. We find that the secrecy rate in a multi-user network does not grow unbounded with the transmit power.

(4) We find that the secrecy performance of TR beamforming depends highly on the degrees of freedom in the environment, i.e., multi-path components in a Rayleigh channel. The larger the number of multi-path components, the higher the TR focusing gain and thus the larger the secrecy capacity of TR-based system.

(5) We examine quantitatively the impact of spatial correlation on secrecy performance of the multi-user MIMO TR-based system.

The remainder of the paper is organized as follows. In Section 2, the system model is formulated. The secrecy rate achievable by the TR-based system is characterized in Section 3. In Section 4, numerical simulation results and corresponding discussions are provided. Finally, concluding remarks are drawn in Section 5.

Notation. E, $*$, and $\otimes$ denote expectation, discrete-time convolution, and the Kronecker product, respectively. The boldface lowercase $\mathbf{a}$ and uppercase $\mathbf{A}$ indicate vectors and matrices, respectively. In addition, the superscripts $(.)^T$ and $(.)^H$ represent the transpose and transpose conjugate, respectively. For a complex value, we denote Re $\{.\}$ as the real part. The notation $\mathbb{C}^{m\times n}$ denotes $m \times n$ complex matrix.

2. System Model

2.1. Preliminaries. The TR-based system under consideration is comprised of a base station (BS) with M antennas which simultaneously transmits N independent confidential messages to N single-antenna users. Our model is based on the assumption of a static (i.e., block fading) channel with perfect channel state information (CSI) available at the BS. This assumption is particularly appropriate for indoor wireless communications.

In order to develop an analytical expression, we only consider discrete-time signals. Tapped delay line (TDL) is used for modeling multi-path fading channel in a rich-scattering environment. Every tap in a tapped delay line represents a resolved path in a multi-path fading channel. In the multi-path fading channel, we assume that the length of channel impulse response (CIR) is L. Thus, the CIR between the i-th transmit antenna and the n-th user is

$$h_{ni}[k] = \sum_{l=1}^{L} \alpha_{ni,l}\,\delta(k-l), \tag{1}$$

where $\alpha_{ni,l}$ is the complex path gain of the l-th tap in the CIR while l represents the corresponding path delay. Additionally, we assume the following: (i) each $h_{ni}[l]$ is independent circular symmetric complex Gaussian (CSCG) random variable with zero mean ($E[h_{ni}[l]] = 0$, $E[|h_{ni}[l]|^2] = \sigma^2_{ni,l}$); (ii) the average power of each tap decays exponentially described as $E[|h_{ni}[l]|^2] = e^{-lT/\sigma_T}$, where T is

the sampling period of the system such that $1/T$ equals the channel bandwidth B and σ_T is the delay spread of the channel. In practice, the CIR can be expressed as a vector $h_{ni} \in \mathbb{C}^{L\times 1}$. Then, the channel matrix of the whole system can be written as

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \\ \cdots \\ \mathbf{H}_N \end{bmatrix} = \begin{bmatrix} \mathbf{h}_{11} & \mathbf{h}_{12} & \cdots & \mathbf{h}_{1M} \\ \mathbf{h}_{21} & \mathbf{h}_{22} & \cdots & \mathbf{h}_{2M} \\ \cdots & \cdots & \ddots & \cdots \\ \mathbf{h}_{N1} & \mathbf{h}_{N2} & \cdots & \mathbf{h}_{NM} \end{bmatrix}, \tag{2}$$

where $\mathbf{H}_i$ is the channel matrix of dimension $L \times M$ from the BS to the i-th user. As mentioned above, when signal bandwidth increases, L will increase correspondingly. Let the transmitted signal x_j for the j-th user be complex random variable with zero mean and variance of θ. This signal is obtained at the BS by performing a linear processing on the confidential messages $u_n, n = 1, \ldots, N$. Thus, the received signal vector at user n is given by

$$y_n = \sum_{i=1}^{M}\sum_{j=1}^{N} x_j * h_{ni} + z_n, \tag{3}$$

where z_n represents additive white Gaussian noise with variance σ^2 ($z_n \sim CN(0, \sigma^2)$).

It is required that the BS securely transmits each confidential message u_n, ensuring that the unintended users receive no information for other users. This is performed at the secrecy rate $R_{n,s}$, defined as follows. The secrecy capacity is the largest secrecy rate of communication between the source and the destination nodes with the eavesdropper knowing no information of the messages. In general, the behavior of the users cannot be known by the BS. Considering a worst-case scenario in our system, we assume that for each user n, the remaining $N-1$ users can cooperate to jointly eavesdrop on the message u_n. For each user n, the alliance of the $N-1$ eavesdroppers is equivalent to a single eavesdropper with $N-1$ receiving antennas, which is denoted by $\overline{n}$ [29].

2.2. TR Beamforming. The TR-based system model is depicted in Figure 1. We assume that the CIRs are stationary for at least one probing-and-transmitting cycle. During channel probing phase, the BS records the CIR of each link, also known as CSI. After the channel probing phase, the system starts its transmission phase and the BS applies the complex-conjugated time-reversed version of the CIR to prefilter the transmitted signal at the transmitter. Such prefiltering acting as a beamformer in the spatial domain focuses the RF power on the receiver and therefore can control the amount of crosstalk between the users [30, 40]. TR beamforming is particularly interesting because it can allow low-complexity implementation. If h_{ni} is supposed to be perfectly known at the BS and the channel is static, we define the prefiltering vector $f_{ni} \in \mathbb{C}^{L\times 1}$ for the link h_{ni}. Each tap of f_{ni} can be given by

$$f_{ni}[k] = \frac{h_{ni}^H[L+1-k]}{\sqrt{P_h}}, \tag{4}$$

$$P_h = \sum_{i=1}^{M}\sum_{l=1}^{L} \left|h_{ni}[l]\right|^2, \tag{5}$$

where $h_{ni}^H[L+1-k]$ is the time-reversed conjugate version of $h_{ni}[k]$ and P_h is a power normalization factor introduced to make sure that the total transmitted power remains constant in every realization. Let F denote the global prefiltering matrix for the channel matrix H, which is expressed as

$$\mathbf{F} = \begin{bmatrix} \mathbf{F}_1 \\ \mathbf{F}_2 \\ \cdots \\ \mathbf{F}_N \end{bmatrix} = \begin{bmatrix} \mathbf{f}_{11} & \mathbf{f}_{12} & \cdots & \mathbf{f}_{1M} \\ \mathbf{f}_{21} & \mathbf{f}_{22} & \cdots & \mathbf{f}_{2M} \\ \cdots & \cdots & \ddots & \cdots \\ \mathbf{f}_{N1} & \mathbf{f}_{N2} & \cdots & \mathbf{f}_{NM} \end{bmatrix}, \tag{6}$$

where $\mathbf{F}_i \in \mathbb{C}^{L\times M}$ is the prefiltering matrix matched for the channel matrix $\mathbf{H}_i$ shown in (2). Let confidential messages $\mathbf{u} = [u_1, u_2, \ldots, u_N]$ go through TR precoder, and u_n is assumed to have unit power (i.e., $E[|u_n|^2] = 1$). After that, the transmitted signal from the i-th antenna to the n-th user is

$$x_n = \sqrt{\theta} u_n * f_{ni}, \tag{7}$$

where θ is the transmit power and $x_n \in \mathbb{C}^{L\times 1}$.

By employing linear prefiltering in (4), the received signals at users n and $\overline{n}$ are, respectively,

$$\begin{aligned} y_n &= \sum_{j=1}^{N}\sum_{i=1}^{M} x_j * h_{ni} + z_n = \sqrt{\theta}\sum_{j=1}^{N}\sum_{i=1}^{M} u_j * f_{ji} * h_{ni} + z_n \\ &= \sqrt{\theta}\sum_{i=1}^{M} u_n * f_{ni} * h_{ni} + \sqrt{\theta}\sum_{j=1,j\neq n}^{N}\sum_{i=1}^{M} u_j * f_{ji} * h_{ni} + z_n \\ &= \underbrace{\sqrt{\theta}\sum_{i=1}^{M} u_n * (f_{ni} * h_{ni})[L]}_{\text{desired signal}} \\ &\quad + \underbrace{\sqrt{\theta}\sum_{k=1,k\neq L}^{2L-1}\sum_{i=1}^{M} u_n * (f_{ni} * h_{ni})[k]}_{ISI} \\ &\quad + \underbrace{\sqrt{\theta}\sum_{j=1,j\neq n}^{N}\sum_{i=1}^{M} u_j * f_{ji} * h_{ni}}_{IUI} + \underbrace{z_n}_{\text{Noise}}, \end{aligned} \tag{8}$$

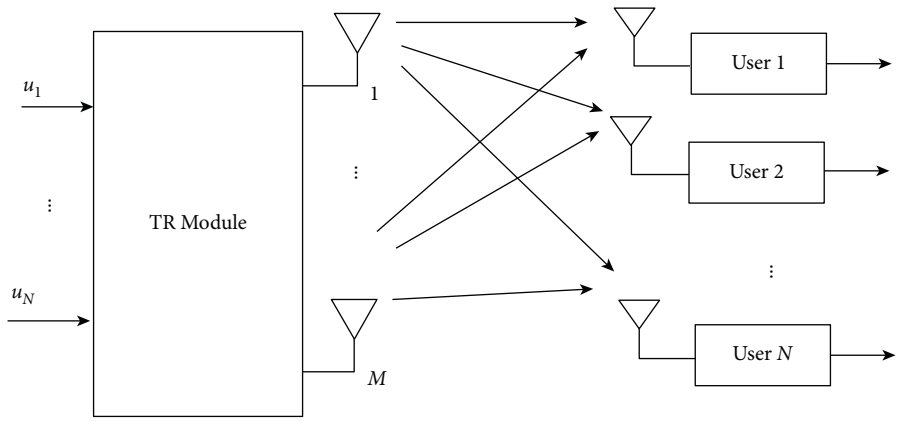

Figure 1: The block diagram of TR-based system.

$$
\begin{aligned}
y_{\overline{n}} &= \sqrt{\theta}\sum_{j=1,j\neq n}^{N}\sum_{i=1}^{M} u_n * f_{ni} * h_{ji} + \sum_{j=1,j\neq n}^{N}\sum_{i=1}^{M} x_j * h_{ji} + \sum_{j=1 j\neq n}^{N} z_j \\
&= \sqrt{\theta}\sum_{j=1,j\neq n}^{N}\sum_{i=1}^{M}\left(u_n * f_{ni} * h_{ji} + u_j * f_{ji} * h_{ji}\right) + \sum_{j=1,j\neq n}^{N} z_j \\
&= \underbrace{\sqrt{\theta}\sum_{j=1,j\neq n}^{N}\sum_{i=1}^{M} u_n * \left(f_{ni} * h_{ji}\right)[L]}_{\text{desired signal}} \\
&\quad + \underbrace{\sqrt{\theta}\sum_{j=1,j\neq n}^{N}\sum_{k=1,k\neq L}^{2L-1}\sum_{i=1}^{M} u_n * \left(f_{ni} * h_{ji}\right)[k]}_{ISI} \\
&\quad + \underbrace{\sqrt{\theta}\sum_{j=1,j\neq n}^{N}\sum_{i=1}^{M} u_j * f_{ji} * h_{ji}}_{IUI} + \underbrace{\sum_{j=1,j\neq n}^{N} z_j}_{\text{Noise}},
\end{aligned}
\tag{9}
$$

where $z_n, z_j \sim CN(0, \sigma^2)$ and $y_n, y_{\overline{n}} \in \mathbb{C}^{(2L-1)\times 1}$. Note that each user n, along with its own eavesdropper $\overline{n}$ and the transmitter at the BS, forms an equivalent multi-input, single-output, multi-eavesdropper (MISOME) wiretap channel [44]. The transmitter, the intended receiver, and the eavesdropper of this MISOME wiretap channel are equipped with M, 1, and $N-1$ virtual antennas, respectively.

Due to the simultaneous transmission of the N messages at the BS, the signal from the message u_n is desired for user n, and user n experiences inter-user interference from all u_j, $j \neq n$ as seen in (8). In addition, because the eavesdropper $\overline{n}$ wants to intercept the message u_n, the signal from all the u_j is regarded as IUI for the message u_n as seen in (9).

We have the equivalent time-reversed CIR (TR-CIR) formula from the i-th transmit antenna to the n-th user as

$$
\left(f_{ni} * h_{ni}\right)[k] = \frac{\sum_{l=1}^{k} h_{ni}^{H}[L+1-l]\, h_{in}[k+1-l]}{\sqrt{P_h}}, \tag{10}
$$

with $k = 1, 2, \ldots, 2L-1$ (i.e., $f_{ni} * h_{ni} \in \mathbb{C}^{(2L-1)\times 1}$).

So, the peak amplitude of the equivalent TR-CIR is

$$
\left(f_{ni} * h_{ni}\right)[L] = \frac{\sum_{l=1}^{L} \left|h_{ni}[l]\right|^2}{\sqrt{P_h}}. \tag{11}
$$

The energy is concentrated at the center tap (i.e., $k = L$) of equivalent TR-CIR and is zero (or very low power) elsewhere (i.e., $k \in \{1, 2\cdots, 2L-1\}, k \neq L$). Thus, only one-tap detection is needed at the receiver and the sampling point is just at the center tap. This will effectively reduce computational complexity at the terminal devices. Because the CIRs associated with different users are uncorrelated or weakly correlated, the power of $(f_{ji} * h_{ni})[k]\,(k \neq L)$ is also very small compared to the power of $(f_{ni} * h_{ni})[L]$. Thanks to TR prefiltering, ISI and IUI can be effectively mitigated.

2.3. Channel Correlation Model. In a rich-scattering environment, we usually assume a model of independent channels because the channels of different users are often spatially uncorrelated. However, channels may become correlated when the environment is less scattering and users are very close to each other. In our system, we assume that the distances between the BS and users are large and only antennas from the same equipment (either the transmitter or the receiver) are spatially correlated due to scattering and electromagnetic coupling. The correlation can be included into the channel model by introducing fixed transmit antenna and inter-user correlation matrices following the well-known Kronecker model [45]. The $M \times N$ spatially correlated channels are therefore given by

$$
H[k] = \left(\left(R_r^{1/2}\right)^T\right) \otimes \left(\left(R_t^{1/2}\right)\right) H_w[k], \tag{12}
$$

where $H_w[k] \in \mathbb{C}^{MN\times L}$ is the channel matrix containing the independent CIRs for a given k. $[H[k]]_{ni} = h_{ni}[k]$, $i \in \{1\cdots M\}$, $n \in \{1\cdots N\}$, and $k \in \{1\cdots L\}$. R_t is the transmit antenna correlation matrix with dimension $M \times M$ and R_r is the inter-user correlation matrix with dimension $N \times N$. The correlation matrix follows the general model with arbitrary positive coefficients (i.e., $\rho_{t,ii'} \geq 0$). We give an example of transmit antenna correlation matrix R_t:

$$R_t = \begin{bmatrix} 1 & \rho_{t,12} & \cdots & \rho_{t,1M} \\ \rho_{t,21} & 1 & \cdots & \rho_{t,2M} \\ \cdots & \cdots & \ddots & \cdots \\ \rho_{t,M1} & \rho_{t,M2} & \cdots & 1 \end{bmatrix}. \quad (13)$$

3. Achievable Secrecy Rates

In this section, we derive secrecy sum-rate for the multi-user MIMO TR-based system.

3.1. SINR at a Typical User. For the n-th equivalent MISOME wiretap channel in (8) and (9), we denote P_s^n, P_{isi}^n, and P_{iui}^n as the powers of the desired signal and the ISI and the IUI terms, respectively. Using these notations, we propose the following closed-form expression of the SINR for the message u_n at user n:

$$\begin{aligned} \gamma_n &= E\frac{P_s^n}{P_{isi}^n + P_{iui}^n + \sigma^2}, \\ P_s^n &= \theta\left|\sum_{i=1}^{M}\left(f_{ni} * h_{ni}\right)[L]\right|^2, \\ P_{\text{isi}}^n &= \theta\sum_{k=1,k\neq L}^{2L-1}\left|\sum_{i=1}^{M}\left(f_{ni} * h_{ni}\right)[k]\right|^2, \\ P_{\text{iui}}^n &= \theta\sum_{j=1,j\neq n}^{N}\sum_{k=1}^{2L-1}\left|\sum_{i=1}^{M}\left(f_{ji} * h_{ni}\right)[k]\right|^2. \end{aligned} \quad (14)$$

For simplicity of calculation, we ignore the difference between $(f_{ji} * h_{ni})[k]$ and $(f_{j_1 i} * h_{ni})[k]$ and let $\sum_{k=1}^{2L-1}|\sum_{i=1}^{M}(f_{ji} * h_{ni})[k]|^2$ represent the IUI power caused by a single eavesdropper to user n. So, P_{iui}^n can be rewritten as

$$P_{\text{iui}}^n = \theta(N-1)\sum_{k=1}^{2L-1}\left|\sum_{i=1}^{M}\left(f_{ji} * h_{ni}\right)[k]\right|^2, \quad j \neq n. \quad (15)$$

Note that P_{iui}^n denotes maximum cumulative interference power imposed on user n from the alliance of the $N-1$ cooperating eavesdroppers.

3.2. SINR at the Malicious Users. Here, eavesdropper $\overline{n}$ attempts to intercept the message u_n. Based on (9), the instantaneous effective SINR for the message u_n at eavesdropper $\overline{n}$ is usually formulated as

$$\gamma_{\overline{n}} = \frac{P_s^{\overline{n}}}{P_{\text{isi}}^{\overline{n}} + P_{\text{iui}}^{\overline{n}} + \sigma^2}, \quad (16)$$

$$\begin{aligned} P_s^{\overline{n}} &= \theta\sum_{j=1,j\neq n}^{N}\left|\sum_{i=1}^{M}\left(f_{ni} * h_{ji}\right)[L]\right|^2 \\ &= \theta(N-1)\left|\sum_{i=1}^{M}\left(f_{ni} * h_{ji}\right)[L]\right|^2, \quad j \neq n, \end{aligned} \quad (17)$$

$$P_{\text{isi}}^{\overline{n}} = \theta\sum_{j=1,j\neq n}^{N}\sum_{k=1,k\neq L}^{2L-1}\left|\sum_{i=1}^{M}\left(f_{ni} * h_{ji}\right)[k]\right|^2, \quad (18)$$

$$P_{\text{iui}}^{\overline{n}} = \theta\sum_{j=1,j\neq n}^{N}\sum_{k=1}^{2L-1}\left|\sum_{i=1}^{M}\left(f_{ji} * h_{ji}\right)[k]\right|^2. \quad (19)$$

Considering the worst-case scenario where all the malicious users can cooperate to eavesdrop on the message intended for the typical user, each malicious user is likely to decode his own message and can indirectly pass this information to all the other malicious users. This will lead to the worst results that all the malicious users can therefore subtract the IUI generated by all the messages u_j, $j \neq n$ [29]. In this case, the term $P_{\text{iui}}^{\overline{n}}$ in (16) may be omitted. A simplified expression for (16) is obtained:

$$\gamma_{\overline{n}} = \frac{P_s^{\overline{n}}}{P_{\text{isi}}^{\overline{n}} + \sigma^2}. \quad (20)$$

3.3. Achievable Secrecy Rates

Lemma 1. *An instantaneous achievable secrecy sum-rate R_s for the multi-user MIMO system with malicious users is given by*

$$R_s = \sum_{n=1}^{N} R_{n,s}, \quad (21)$$

where $R_{n,s}$ is achievable per-user secrecy rate for the n-th MISOME wiretap channel in (8) and (9), $n = 1, \ldots, N$.

Lemma 2. *An instantaneous per-user secrecy rate $R_{n,s}$ for the MISOME wiretap channel in (8) and (9) is given by*

$$\begin{aligned} R_{n,s} &= \left[\log_2(1+\gamma_n) - \log_2(1+\gamma_{\overline{n}})\right]^+ \\ &= \left[\log_2\left(\frac{1+\gamma_n}{1+\gamma_{\overline{n}}}\right)\right]^+ = \left[\log_2\left(1+\frac{\gamma_n-\gamma_{\overline{n}}}{1+\gamma_{\overline{n}}}\right)\right]^+ \\ &= \left[\log_2\left(1+\gamma_{n,s}\right)\right]^+, \end{aligned} \quad (22)$$

where $\gamma_{n,s} = (\gamma_n - \gamma_{\overline{n}})/(1+\gamma_{\overline{n}})$ is the secrecy-SINR. $R_{n,s}$ is the secrecy rate achievable by user n in the presence of eavesdropper $\overline{n}$. From (22), it is clearly observed that for secrecy rate maximization, maximizing γ_n and minimizing $\gamma_{\overline{n}}$ are required.

Then, the secrecy-SINR expression is given by

$$\gamma_{n,s} = \begin{cases} \dfrac{\gamma_n - \gamma_{\overline{n}}}{1+\gamma_{\overline{n}}}, & \gamma_n > \gamma_{\overline{n}}, \\ 0, & \text{otherwise.} \end{cases} \quad (23)$$

In more detail, $\gamma_{n,s}$ can be expressed as

$$\gamma_{n,s} = \frac{P_s^n/\left(P_{\text{isi}}^n + P_{\text{iui}}^n + \sigma^2\right) - P_s^{\overline{n}}/\left(P_{\text{isi}}^{\overline{n}} + \sigma^2\right)}{1 + P_s^{\overline{n}}/\left(P_{\text{isi}}^{\overline{n}} + \sigma^2\right)}. \quad (24)$$

According to (24), the expectation of secrecy-SINR can be formulated as

$$\overline{\gamma}_{n,s} = E\left[\gamma_{n,s}\right] = E\left[\frac{P_s^n/\left(P_{\text{isi}}^n + P_{\text{iui}}^n + \sigma^2\right) - P_s^{\overline{n}}/\left(P_{\text{isi}}^{\overline{n}} + \sigma^2\right)}{1 + P_s^{\overline{n}}/\left(P_{\text{isi}}^{\overline{n}} + \sigma^2\right)}\right]. \tag{25}$$

The closed-form expression for (25) is hard to obtain. With the help of [46, 47], we define an approximation for average secrecy-SINR as

$$\widehat{\overline{\gamma}}_{n,s} = \frac{E\left[P_s^n\right]/\left(E\left[P_{\text{isi}}^n\right] + E\left[P_{\text{iui}}^n\right] + \sigma^2\right) - E\left[P_s^{\overline{n}}\right]/\left(E\left[P_{\text{isi}}^{\overline{n}}\right] + \sigma^2\right)}{1 + E\left[P_s^{\overline{n}}\right]/\left(E\left[P_{\text{isi}}^{\overline{n}}\right] + \sigma^2\right)}. \tag{26}$$

More details are described in Appendix A. Averaging (22) over all realizations of the random ergodic channels, the expected value of the instantaneous achievable secrecy rate is a good reference of the long-term performance.

Theorem 1. *The mean per-user secrecy rate can be approximated as*

$$\overline{R}_{n,s} = E\left[\log_2\left(1 + \gamma_{n,s}\right)\right]^+ \approx \widehat{\overline{R}}_{n,s} = \left[\log_2\left(1 + \widehat{\overline{\gamma}}_{n,s}\right)\right]^+. \tag{27}$$

Then, the mean secrecy sum-rate can be approximated as

$$\overline{R}_s = E\left(\sum_{n=1}^{N}\left[\log_2\left(1 + \gamma_{n,s}\right)\right]^+\right) \approx N \times \widehat{\overline{R}}_{n,s}. \tag{28}$$

4. Simulation Experiments and Numerical Analysis

In this section, we present the secrecy performance of the multi-user MIMO TR-based system. First, the focusing property of TR beamforming is assessed by analyzing the CIR under different propagation conditions. Then, the evaluation of network secrecy metric defined in Section 3 is provided and fully discussed. The channel model is used with bandwidth (B)~20 MHz to 125 MHz and the number of taps $(L) \sim 5$ to 33. All the experimental results were obtained by averaging 10000 random channel realizations.

4.1. Time Compression Validation Test. The temporal focusing property of TR beamforming is presented in Figure 2 by comparing the amplitudes of both original CIRs and the equivalent TR-CIRs at the receiver, respectively. The power of each CIR has been normalized to 1 (i.e., $\sum_{l=1}^{L} |h_{ni}[l]|^2 = 1$). The original CIRs before TR demonstrate dispersive effects of multi-path channels under different bandwidth conditions. The more the multi-path components resolved in the channel are, the more quickly the signal strength fades as shown in Figures 2(a) and 2(b). Multi-path effects are particularly relevant in high data rate communication systems. Typically, this problem can be solved with equalization method at the receiver. But this would increase computational complexity at the receiver [48]. In Figure 2(c), the equivalent CIR after TR shows that most of signal energy is aggregated at the center tap (i.e., $k = L = 11$) while ISI components at the other taps (i.e., $k \in \{1, 2 \cdots, 2L-1\}, k \neq L$) have been suppressed as much as possible. This indicates that there is temporal focusing and therefore ISI can be mitigated. Thanks to the superior focusing effect in time domain, the receiver can perform a simple one-tap detection at the center tap and achieve good energy efficiency.

From Figure 2(d), one can see that for the multi-path channels with strong transmit antenna correlation ($\rho_t = 0.9$), there is only minor degradation in focusing effect of TR beamforming at the intended user. Comparing Figure 2(e) with Figure 2(f), we can observe that for the multi-path channels with inter-user correlation, as the inter-user correlation increases, the signal for the message u_n at the eavesdropper is markedly enhanced at the center tap while suppressed at other taps. Obvious, due to the presence of inter-user correlation, the focusing effect of TR beamforming also occurs at the eavesdropper. Unfortunately, this will lead to more interception of confidential information of legitimate user by the eavesdropper. Unlike inter-user correlation, transmit antenna correlation does not improve the CIR of the eavesdropper.

4.2. Mean Secrecy Capacity. In this part, we investigate the secrecy performance of the multi-user MIMO TR-based system. We evaluate quantitatively and discuss the influence of propagation conditions, such as the number of taps, the number of transmit antennas, and the number of eavesdroppers on the mean per-user secrecy rate achieved by TR beamforming. To facilitate the discussion, we presume the ratio β between the number of users N and the number of transmit antennas M, i.e., $\beta = N/M$.

All the results from Sections 4.2 to 4.4 assume that the channels of different users are spatially uncorrelated.

Figure 3 depicts the simulation results obtained with the mean per-user secrecy rate $\overline{R}_{n,s}$ and the analytical results achieved with the approximation $\widehat{\overline{R}}_{n,s}$ given in Theorem 1. One can see that the analytical results approximate well the simulation results, which proves the reasonableness and effectiveness of the approximation $\widehat{\overline{R}}_{n,s}$.

In addition, Figure 3(a) gives the upper bound of mean per-user secrecy rate $\overline{R}_{n,s}$ under different system configurations, ignoring the effects of IUI and spatial correlation. Note that for a given N, smaller β implies more transmit antennas deployed at the BS. More transmit antennas deployed at the BS also indicate higher per-user secrecy rate achieved, especially notable at high SNR. When the SNR is up to 20 dB, $\overline{R}_{n,s}$ reaches its peak. Thereafter, even if further increasing SNR, $\overline{R}_{n,s}$ still remains unchanged. The reason for this situation lies in the fact that as the SNR increases, the noise power gradually becomes weaker. When the SNR reaches 20 dB, the ISI power far exceeds the noise power so that the noise power can be ignored. The expression for $\gamma_{n,s}$ shown in (24) can be rewritten as

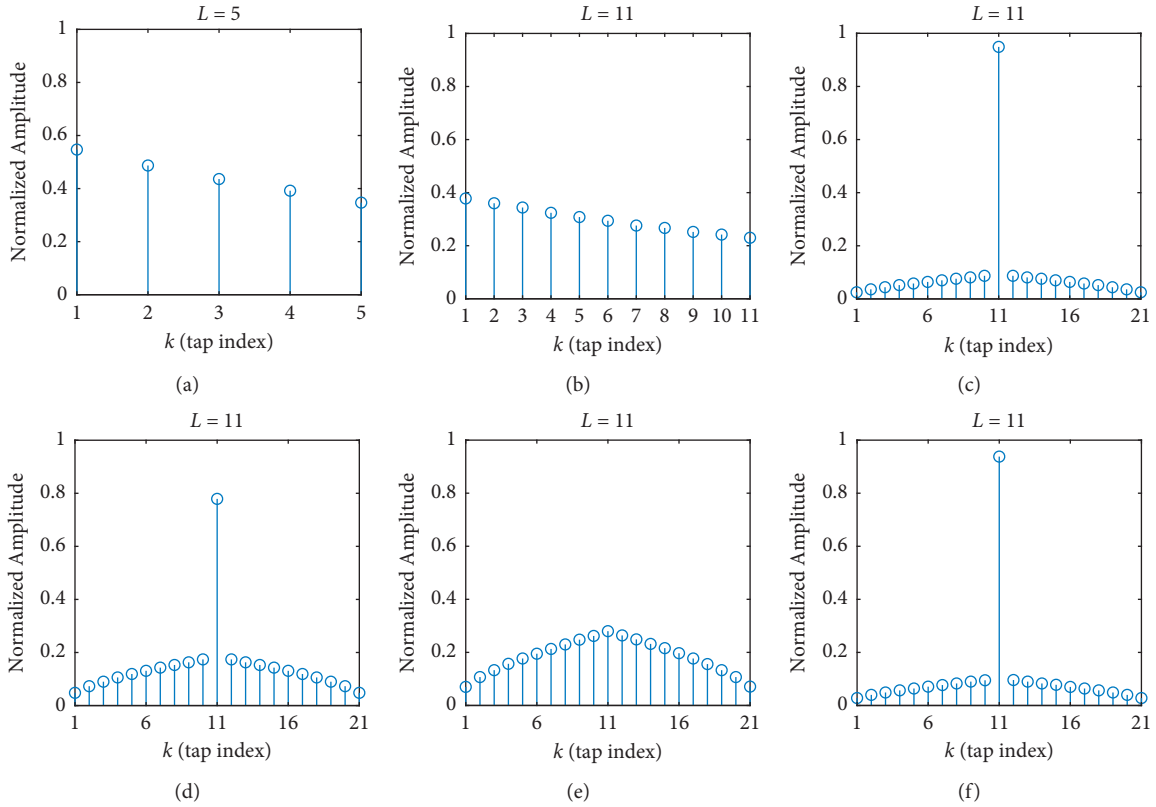

FIGURE 2: An illustration of CIR vs. multi-path channel. (a) The original CIR for $B = 20$ MHz. (b) The original CIR for $B = 40$ MHz. (c) The equivalent TR-CIR at the intended user for $\rho_t = 0$ and $\rho_r = 0$. (d) The equivalent TR-CIR at the intended user for $\rho_t = 0.9$ and $\rho_r = 0$. (e) The equivalent TR-CIR at the eavesdropper for $\rho_t = 0$ and $\rho_r = 0$. (f) The equivalent TR-CIR at the eavesdropper for $\rho_t = 0$ and $\rho_r = 0.9$.

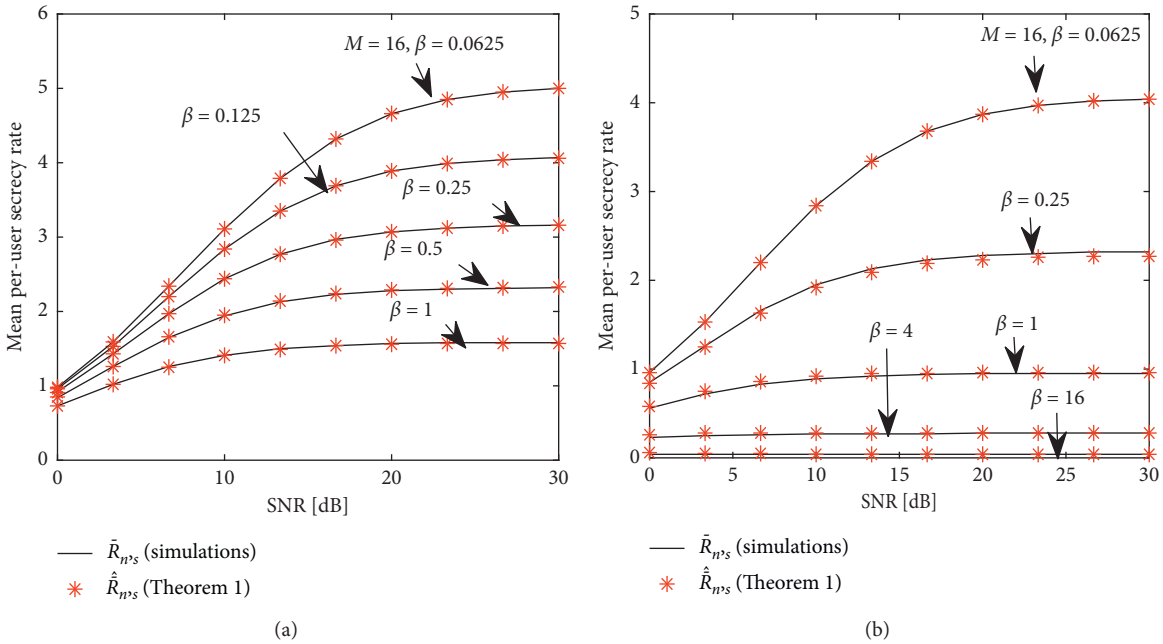

FIGURE 3: (a) Mean per-user secrecy rate vs. SNR for $L = 33$ and $N = 2$. (b) The impact of IUI on mean per-user secrecy rate for $L = 33$ and $N = 2$.

$$\gamma_{n,s} \approx \frac{P_s^n / P_{isi}^n - P_s^{\overline{n}} / P_{isi}^{\overline{n}}}{1 + P_s^{\overline{n}} / P_{isi}^{\overline{n}}}. \quad (29)$$

Eventually, both the desired signal power and the ISI power determine an upper bound on $\overline{R}_{n,s}$. Unlike Figure 3(a), Figure 3(b) considers the effects of the IUI on the mean per-user secrecy rate and gives the lower bound of mean per-user secrecy rate $\overline{R}_{n,s}$. Compared with Figure 3(a), it can be observed that IUI causes $\overline{R}_{n,s}$ to fall by about 0.3~1 bps/Hz.

In Figure 4, we have fixed SNR = 20 dB. Figure 4 shows the mean per-user secrecy rat as a function of β for different values of L. As expected, the mean per-user secrecy rate $\overline{R}_{n,s}$ increases as the length of CIR L increases (larger L implies more multi-path components in the channel and stronger scattering in the channel). This figure clearly shows the remarkable benefit of richer multi-path environment on network secrecy capacity. For example, for $L = 5$, the network goes into secrecy outage (i.e., $\overline{R}_{n,s} = 0$) at $\beta = 4$, whereas for $L = 11$, secrecy outage occurs at $\beta = 16$. This behavior can be attributed to the fact that by fully exploiting degrees of freedom provided by the environment, i.e., the abundant multi-path components in the channel, the TR-based system can support more coexisting users with non-zero secrecy rate and the secrecy performance of the system is significantly improved.

Table 1 displays the distributions of the mean per-user secrecy rate and the mean secrecy sum-rate achieved by TR beamforming, for different combinations of M and N, respectively. All the results in Table 1 were obtained at the SNR of 20 dB, for $L = 33$. As indicated in Table 1, this implies a trade-off between the network capacity (in terms of the number of serviced users) and the secrecy rate at each user. When N takes 2, 4, and 8 in turn and M is successively 8, 16, and 32, the mean per-user secrecy rates are 2.25 bps/Hz, 2.24 bps/Hz, and 2.24 bps/Hz, respectively. In the cases, the number of N as well as M is different each time, but the ratios of N to M remain the same (i.e., $\beta = N/M = 2/8 = 4/16 = 8/32 = 0.25$). These results demonstrate that in the absence of spatial correlation, the mean per-user secrecy rate is just a function of the SNR, L, and β, and thus the average secrecy sum-rate is a function of the SNR, L, β, and N.

4.3. Power Control Strategy. In Figure 3(b), it can be seen that for $\beta \leq 1$, $\overline{R}_{n,s}$ is always positive and monotonically increasing with the SNR until the SNR goes up to 20 dB, whereas for $\beta > 1$, the per-user secrecy rate is irrespective of the SNR. This indicates that the mean per-user secrecy rate does not grow unbounded with the increase of transmit power. Moreover, TR beamforming performs poorly in the high-SNR regime. When increasing the SNR from 10 dB up to 20 dB, only a minor increase in $R_{n,s}$ is achieved. Therefore, a power control strategy is introduced by reducing the transmit power properly to control the SNR to the value that can maximize the mean secrecy sum-rate (e.g., SNR at 10 dB) and works well for most of the cases. This power control strategy can save transmit power, thus effectively improving energy efficiency. For $1 < \beta < 32$, the TR-based system with power reduction strategy would achieve an optimal non-negative secrecy sum-rate. However, for $\beta \geq 31$, the secrecy sum-rate is always zero irrespective of the SNR and this strategy would not be effective.

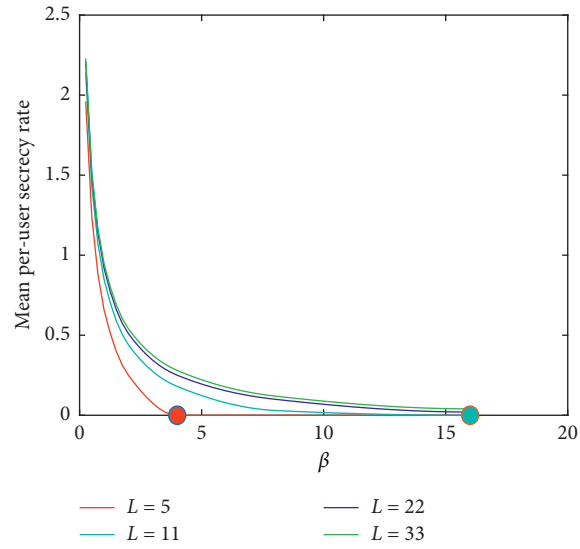

Figure 4: Per-user secrecy rate as a function of β, for different values of L. Circles denote secrecy outage.

Table 1: Secrecy rate comparison.

	$\overline{R}_s/\overline{R}_{n,s}$ (bps/Hz)				
M	$N = 2$	$N = 4$	$N = 8$	$N = 16$	$N = 32$
2	1.94/0.97	2.20/0.55	2.22/0.28	1.92/0.12	1.28/0.04
4	3.08/1.54	3.84/0.96	4.32/0.54	4.48/0.28	3.84/0.12
8	4.50/2.25	6.12/1.53	7.60/0.95	8.64/0.54	8.64/0.27
16	6.10/3.05	8.96/2.24	12.16/1.52	15.2/0.95	17.28/0.54
32	7.74/3.87	12.16/3.04	17.92/2.24	24.32/1.52	30.4/0.95

Figure 3 also shows that the mean per-user secrecy rate $\overline{R}_{n,s}$ is always a decreasing function of β. The main reason for this phenomenon lies in the fact that when $\beta > 1$, the intended user n suffered from a larger amount of IUI caused by more coexisting eavesdroppers while the alliance of cooperating eavesdroppers $\overline{n}$ is always free from IUI, as shown in (20). Therefore, the secrecy-SINR and the per-user secrecy rate are both interference-limited, especially limited by the IUI caused by the alliance of cooperating eavesdroppers.

4.4. Secrecy Cost. Guaranteeing secrecy and serving multiple (potentially malicious) users at the same time may come at a cost in terms of the per-user transmission rate. We discuss the cost of achieving physical-layer security in the multi-user MIMO TR-based system, which is the sum-rate loss due to the secrecy requirements. It can be obtained by comparing the mean secrecy sum-rate $\overline{R}_s$ achievable by TR beamforming to the mean sum-rate $\overline{R}$ without secrecy requirements. The gap between $\overline{R}_s$ and $\overline{R}$ represents how much guaranteeing secrecy costs in terms of the achievable sum-rate.

$$\overline{R} = N\overline{R}_n = N\log_2(1+\overline{\gamma}_n). \quad (30)$$

Figure 5 compares $\overline{R}_s$ and $\overline{R}$ of TR beamforming with and without secrecy requirements, respectively, for different values of β. For the uncorrelated multi-user Rayleigh channels, the difference between $\overline{R}_s$ and $\overline{R}$ (i.e., $\overline{R}$-$\overline{R}_s$) is negligible, which demonstrates that TR beamforming can achieve secure communication without sacrificing achievable sum-rate.

4.5. Secrecy Rate Loss due to Spatial Correlation. In the preceding sections, we assume a model of independent channels which is suitable for the rich-scattering multi-path environment. For the case when users are near to each other and the environment is less scattering, the channels of different users may become spatially correlated and the effect of spatial correlation on the system performance cannot be ignored. To gain a more comprehensive understanding of TR beamforming for secrecy transmission, it is important to develop a quantitative assessment of its performance degradation due to transmit antenna correlation or inter-user correlation, respectively. Figure 6 displays the mean per-user secrecy rate loss due to transmit antenna correlation. It is noticeable that low-to-moderate correlation among transmit antennas (i.e., $\rho_t < 0.4$) already causes a remarkable loss in the mean per-user secrecy rate. When ρ_t rises from 0 to 0.2, the mean per-user secrecy rate decreases to 30% of the original. Transmit antenna correlation causes poor performance of TR beamforming, particularly at high SNR. In such case, the power control strategy can be adapted to prevent the secrecy rate from decreasing fast.

Figure 7 displays the mean per-user secrecy rate loss due to inter-user correlation. From Figure 7, it can be observed that when ρ_r reaches 0.2, $\overline{R}_{n,s}$ all drop to zero, which means that the BS cannot transmit to any typical user at a non-zero secrecy rate and the network goes into secrecy outage. Obviously, inter-user correlation causes a severe degradation in the secrecy performance of the TR-based system. The worst part is that the inter-user correlation is much more destructive to $\overline{R}_{n,s}$ than transmit antenna correlation.

In fact, inter-user correlation not only causes much stronger IUI imposed on the intended user n but also helps the eavesdropper $\overline{n}$ gain the focusing effect of TR beamforming that significantly improves $\gamma_{\overline{n}}$ (i.e., the SINR at the eavesdropper $\overline{n}$) in (16). These are major reasons for a drastic degradation in $\overline{R}_{n,s}$ in the presence of inter-user correlation. Moreover, the improved SINR at the eavesdropper $\overline{n}$ enables him to intercept more confidential information of user n. On the other hand, Figures 6 and 7 also demonstrate that smaller β causes a faster secrecy rate loss. This implies that when channel correlation is present, more transmit antennas cannot improve the system performance any more.

More details are listed in Table 2, in which $\overline{R}_{n,s}^{\rho_t}$ stands for $\overline{R}_{n,s}$ in the presence of transmit antenna correlation and $\overline{R}_{n,s}^{\rho_r}$ stands for $\overline{R}_{n,s}$ in the presence of inter-user correlation.

Figures 8 and 9 reveal the secrecy costs of $\overline{R}_{n,s}$ in the presence of transmit antenna correlation and $\overline{R}_{n,s}$ in the presence of inter-user correlation, respectively. Note that in Figures 8 and 9, the red solid lines represent $\overline{R}_{n,s}$ and the red dashed lines represent $\overline{R}_n$, which plot the cases of uncorrelated Rayleigh channels (i.e., $\rho_t = 0$ and $\rho_r = 0$). Similarly, the blue lines plot the cases of correlated multi-user channels ($\rho_t = 0.1$ or $\rho_r = 0.1$). It can be seen that in the presence of transmit antenna correlation, the gap between $\overline{R}_{n,s}$ and $\overline{R}_n$ is very small in all cases, and thus the secrecy cost (i.e., $\overline{R}_n$-$\overline{R}_{n,s}$) is close to zero, as shown in Figure 8. In Figure 9, when ρ_r slightly rises from 0 to 0.1, the secrecy cost increases from 0 to 0.7 bps/Hz and the secrecy cost is very high. Worst of all, when ρ_r reaches 0.2, the network goes into secrecy outage (i.e., $\overline{R}_{n,s} = 0$), whereas $\overline{R}_n$ is always greater than 0.6 bps/Hz.

Furthermore, Figure 10 depicts the effects of the number of users on the $\overline{R}_{n,s}$ in the presence of transmit antenna correlation. In Figure 10, M takes 8, 16, 32, and 64 in turn

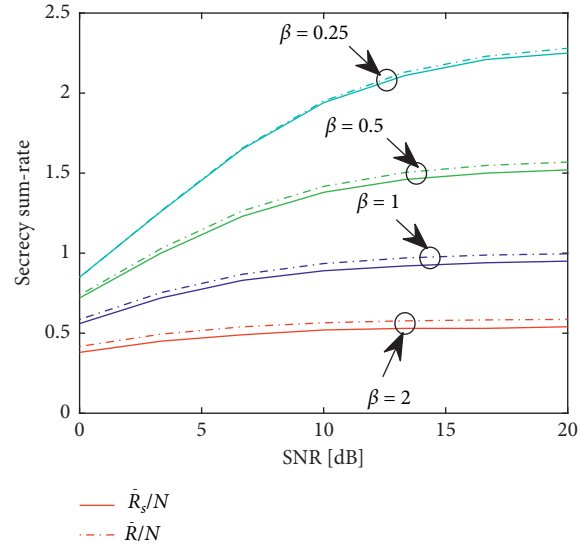

Figure 5: Comparison between the per-user secrecy rate (solid) and the per-user rate without secrecy requirements (dashed).

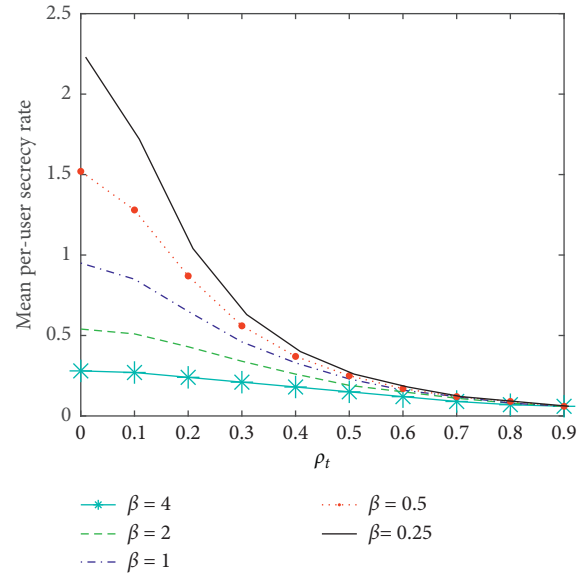

Figure 6: Per-user secrecy rate vs. ρ_t, for SNR = 20 dB and $N = 16$.

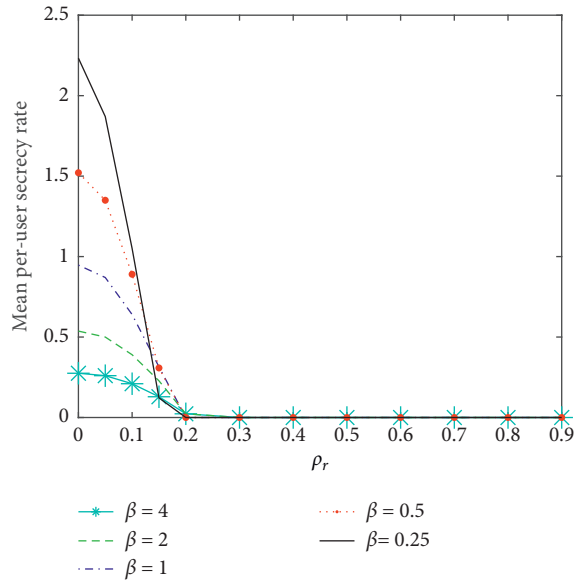

Figure 7: Per-user secrecy rate vs. ρ_r, for SNR = 20 dB and $N = 16$.

Table 2: Secrecy rate loss due to channel correlation.

Coefficient	$\overline{R}_{n,s}^{\rho_t}/\overline{R}_{n,s}^{\rho_r}$ (bps/Hz), $\beta = 0.25$									
ρ_t/ρ_r	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
$N = 2$	2.25/2.25	2.09/2.11	1.75/1.72	1.38/1.18	1.08/0.6	0.84/0.02	0.66/0	0.53/0	0.42/0	0.35/0
$N = 8$	2.24/2.24	1.95/1.58	1.42/0.31	0.99/0	0.69/0	0.5/0	0.37/0	0.28/0	0.21/0	0.16/0
$N = 16$	2.23/2.23	1.72/1.05	1.04/0	0.63/0	0.40/0	0.26/0	0.18/0	0.12/0	0.09/0	0.06/0

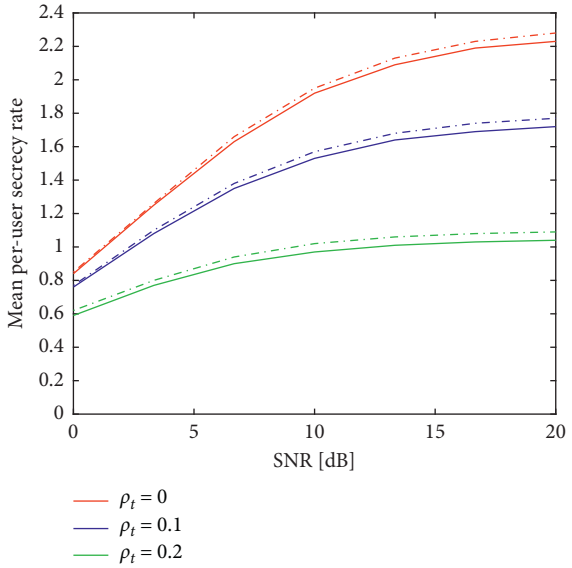

Figure 8: Comparison between the per-user secrecy rate (solid) and the per-user rate without secrecy requirements (dashed) under transmit antenna correlation, for $N = 16$, $\beta = 0.25$, and $\rho_r = 0$.

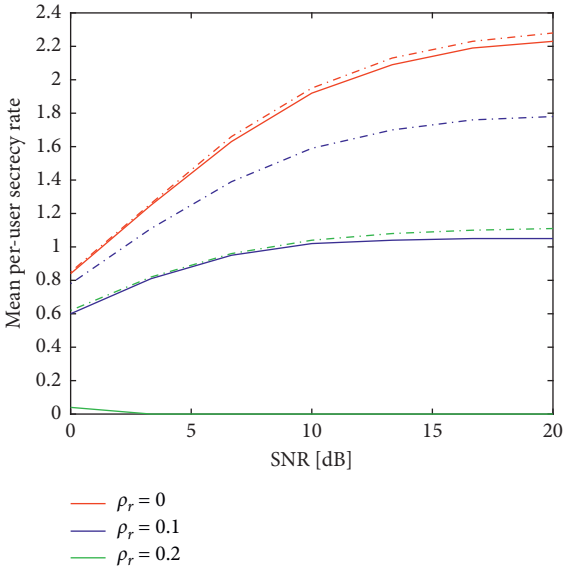

Figure 9: Comparison between the per-user secrecy rate (solid) and the per-user rate without secrecy requirements (dashed) under inter-user correlation, for $N = 16$, $\beta = 0.25$, and $\rho_t = 0$.

and N takes 2, 4, 8, and 16 in turn such that $\beta = N/M$ always remain constant. When no spatial correlation is present (i.e., $\rho_t = \rho_r = 0$), the original per-user secrecy rates are equal to each other and at its peak, no matter how big N is. This indicates that for uncorrelated Rayleigh channels, the number of users N has no effect on $\overline{R}_{n,s}$, and hence $\overline{R}_{n,s}$ is only related to L, β, and the SNR. In fact, a larger N means more users and stronger cumulative IUI. Why the original

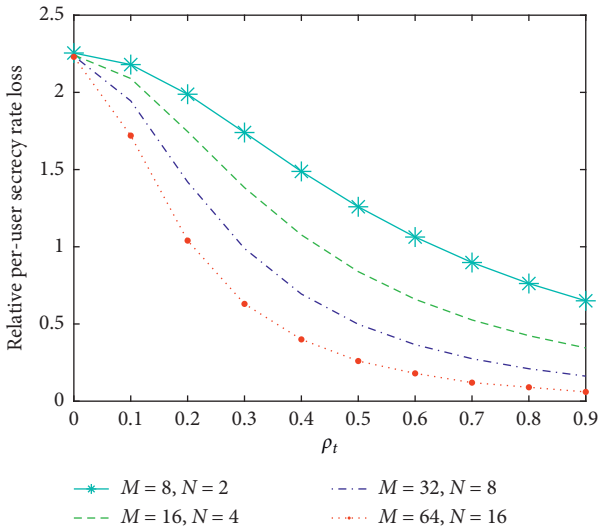

FIGURE 10: The impact of the number of users on the per-user secrecy rate, for SNR = 20 dB and $\beta = 0.25$.

per-user rates for different number of users are the same? This is because more transmit antennas compensate for the adverse effects of substantial increasing of cumulative IUI caused by more users. This also proves that when no spatial correlation is present, TR beamforming has good focusing performance and can effectively eliminate the interference.

Unfortunately, when ρ_t is greater than zero but still in the lower range (e.g., from 0 to 0.2), there is a significant reduction in $\overline{R}_{n,s}$. Both transmit antenna correlation and more users jointly give rise to the sharp increase of the cumulative IUI interference imposed on user n, which eventually leads to severe degradation in $\overline{R}_{n,s}$. When spatial correlation is present, the per-user secrecy rate is the function of L, β, ρ_t, ρ_r, N, and the SNR.

5. Conclusions

This paper has examined TR beamforming strategy for providing confidentiality at the physical layer in the multi-user MIMO system. This work enables a deeper understanding of how intrinsic properties of wireless networks can be exploited to enhance the network secrecy. Our study demonstrates that when no spatial correlation is present, TR beamforming can achieve perfect zero-cost secure communication and rich-scattering environment can be beneficial for network secrecy. We also found that in the presence of inter-user correlation, achievable mean secrecy sum-rate decreases so quickly that there is significant increase in secrecy cost in terms of the achievable sum-rate.

Fortunately, as 5G communication and future 6G communication are expected to adopt high-frequency band and larger signal bandwidth, these will greatly improve the spatial resolution and time resolution of the channels and therefore more abundant degrees of freedom can be resolved. In addition, with the increase of frequency band and the reduction of signal wavelength, the channels' difference of users will be more intense so that spatial correlation may be minimized almost to zero. By virtue of its good focusing property in the richer scattering environment and its low complexity, TR beamforming is still an ideal solution for enhancing the system security in the future indoor wireless communications.

Appendix

A. Derivations of (26)

Considering the correlated channel matrix, the expectation of product of two random variables can be derived as

$$E\left[h_{ni}[l]h_{n'i}^{H}[l]\right] = \sigma_{ni,l}\sigma_{n_t i_t,l}\left(R_t\right)_{ii'}\left(R_r\right)_{nn'}. \tag{A.1}$$

Accordingly, we also have

$$E\left[h_{n'i}^{H}[L+1-l]h_{ni}[k+1-l]\right] = \begin{cases} \left(R_r\right)_{nn'}\sigma_{ni,L+1-l}^{2}, & k = L, \\ 0, & \text{otherwise.} \end{cases} \tag{A.2}$$

Then, the expectation of product of four random variables which are jointly Gaussian distributed is given by [49]

$$\begin{aligned} E\left[X_1X_2X_3X_4\right] = {} & E\left[X_1X_2\right]E\left[X_3X_4\right] \\ & + E\left[X_1X_3\right]E\left[X_2X_4\right] + E\left[X_1X_4\right]E\left[X_2X_3\right] \\ & - 2E\left[X_1\right]E\left[X_2\right]E\left[X_3\right]E\left[X_4\right]. \end{aligned} \tag{A.3}$$

In addition, the following analytic expression is defined: $\xi = 1/\sum_{i=1}^{M}\sum_{l=1}^{L}\sigma_{ni,l}^{2}$.

A.1. Approximations for $E[P_s^n]$ at the Typical User

$$\begin{aligned} E\left[P_s^n\right] &= \theta E\left[\left|\sum_{i=1}^{M}\left(f_{ni} * h_{ni}\right)[L]\right|^2\right] \\ &= \theta\sum_{i=1}^{M}E\left[\left|\left(f_{ni} * h_{ni}\right)[L]\right|^2\right] \\ &\quad + \theta\xi E\left[\mathrm{Re}\left[\sum_{i'=1,i'\neq i}^{M}\sum_{i=1}^{M}\sum_{l=1}^{L}h_{ni}^{H}[l]h_{ni}[l]\sum_{l'=1}^{L}h_{ni'}[l']h_{ni'}^{H}[l']\right]\right]. \end{aligned} \tag{A.4}$$

Note that in (A.4), we have

$$\begin{aligned} E\left[\left|\left(f_{ni} * h_{ni}\right)[L]\right|^2\right] &= \xi E\left[\left|\sum_{l=1}^{L}h_{ni}^{H}[l]h_{ni}[l]\right|^2\right] \\ &= \xi\sum_{l=1}^{L}E\left[\left|h_{ni}^{H}[l]h_{ni}[l]\right|^2\right] \\ &\quad + \xi\sum_{l'=1,l'\neq l}^{L}\sum_{l=1}^{L}E\left[h_{ni}^{H}[l]h_{ni}[l]h_{ni}[l']h_{ni}^{H}[l']\right] \\ &= \xi\left(2\sum_{l=1}^{L}\sigma_{ni,l}^{4} + \left(\sum_{l=1}^{L}\sigma_{ni,l}^{2}\right)^2\right), \end{aligned} \tag{A.5}$$

where $E[|h_{ni}^{H}[l]h_{ni}[l]|^2] = 2\sigma_{ni,l}^{4}$ and $E[h_{ni}^{H}[l]h_{ni}[l]h_{ni}[l']h_{ni}^{H}[l']] = \sigma_{ni,l}^{2}\sigma_{ni,l'}^{2}$, $(l \neq l')$.

Then, in the second term on the right-hand side (RHS) of (A.4), we have

$$E\left[\sum_{l=1}^{L} h_{ni}^{H}[l]h_{ni}[l]\sum_{l'=1}^{L} h_{ni'}[l']h_{ni'}^{H}[l']\right] = \sum_{l=1}^{L}\sum_{l'=1}^{L}\sigma_{ni',l'}^{2}\sigma_{ni,l}^{2} + \sum_{l=1}^{L}(R_t)_{ii}^{2}\sigma_{ni,l}^{2}\sigma_{ni',l}^{2}. \tag{A.6}$$

$$E[P_s^n] = \frac{\theta\sum_{i=1}^{M}\left(2\sum_{l=1}^{L}\sigma_{ni,l}^{4} + \left(\sum_{l=1}^{L}\sigma_{ni,l}^{2}\right)^{2}\right)}{\sum_{i=1}^{M}\sum_{l=1}^{L}\sigma_{ni,l}^{2}} + \frac{\theta\sum_{i'=1,i'\neq i}^{M}\sum_{i=1}^{M}\left(\sum_{l'=1}^{L}\sum_{l=1}^{L}\sigma_{ni,l}^{2}\sigma_{ni',l}^{2} + \sum_{l=1}^{L}(R_t)_{ii}^{2}\sigma_{ni,l}^{2}\sigma_{ni',l}^{2}\right)}{\sum_{i=1}^{M}\sum_{l=1}^{L}\sigma_{ni,l}^{2}}.$$

The derivation processes for $E[P_{isi}^n]$ and $E[P_{iui}^n]$ are similar to $E[P_s^n]$ and are omitted due to space limitations. For the same reason, the derivation process for the malicious user $\overline{n}$ is omitted as well.

$$\begin{aligned} E[P_{isi}^n] &= \theta E\left[\sum_{k=1k\neq L}^{2L-1}\left|\sum_{i=1}^{M}(f_{ni} * h_{ni})[k]\right|^2\right] = 2\theta E\left[\sum_{k=1}^{L-1}\left|\sum_{i=1}^{M}(f_{ni} * h_{ni})[k]\right|^2\right] \\ &= 2\theta\sum_{k=1}^{L-1}\left\{\sum_{i=1}^{M}E\left[\left|(f_{ni} * h_{ni})[k]\right|^2\right] + \sum_{i'=1,i'\neq i}^{M}\sum_{i=1}^{M}E\left[\mathrm{Re}\left[(f_{ni} * h_{ni})[k]\left(f_{ni'} * h_{ni'}\right)^{*}t[k]\right]\right]\right\}. \end{aligned} \tag{A.7}$$

In (A.7), we have

$$\begin{aligned} E\left[\left|(f_{ni} * h_{ni})[k]\right|^2\right] &= \xi E\left[\left|\sum_{l=1}^{k}h_{ni}^{*}[L+1-l]h_{ni}[k+1-l]\right|^2\right] \\ &= \xi\sum_{l=1}^{k}E\left[\left|h_{ni}^{*}[L+1-l]h_{ni}[k+1-l]\right|^2\right] \\ &\quad + \xi\sum_{l'=1,l'\neq l}^{k}\sum_{l=1}^{k}E\left[h_{ni}^{*}[L+1-l]h_{ni}[k+1-l]h_{ni}[L+1-l']h_{ni}^{*}[k+1-l']\right] \\ &= \xi\sum_{l=1}^{k}\sigma_{ni,k+1-l}^{2}\sigma_{ni,L+1-l}^{2}, k\neq L, \end{aligned} \tag{A.8}$$

where $E[|h_{ni}^{*}[L+1-l]h_{ni}[k+1-l]|^2] = \sigma_{ni,k+1-l}^{2}\sigma_{ni,L+1-l}^{2}$ and $E[h_{ni}^{*}[L+1-l]h_{ni}[k+1-l]h_{ni}[L+1-l']h_{ni}^{*}[k+1-l']] = 0, k\neq L, l'\neq l$.

$$\begin{aligned} &E\left[\mathrm{Re}\left\{(f_{ni} * h_{ni})[k]\left(f_{ni'} * h_{ni'}\right)^{*}[k]\right\}\right] \\ &= \xi\sum_{l=1}^{k}E\left[h_{ni}^{*}[L+1-l]h_{ni}[k+1-l]h_{ni'} \cdot [L+1-l]h_{ni'}^{*}[k+1-l]\right] \\ &= \xi\sum_{l=1}^{k}(R_t)_{ii'}^{2}\left(\sigma_{ni,L+1-l}\sigma_{ni',L+1-l}\sigma_{ni,k+1-l}\sigma_{ni',k+1-l}\right). \end{aligned} \tag{A.9}$$

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported in part by the National Key Research and Development Program of China (no. 2020YFF0304903), Natural Science Foundation of

Fujian Province of China (nos. 2020J01700, 2020J01699, and 2021J01857), and Scientific Research Project of Middle-Aged and Young Teachers in Fujian Province (no. JAT190320).

References

[1] S. H. Chae, I. Bang, and H. Lee, "Physical layer security of QSTBC with power scaling in MIMO wiretap channels," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5647–5651, 2020.

[2] A. S. Khan, I. Chatzigeorgiou, G. Zheng, B. Basutli, J. M. Chuma, and S. Lambotharan, "Random linear network coding based physical layer security for relay-aided device-to-device communication," *IET Communications*, vol. 14, no. 7, pp. 1155–1161, 2020.

[3] S. N. Islam, Z. Baig, and S. Zeadally, "Physical layer security for the smart grid: vulnerabilities, threats, and countermeasures," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6522–6530, 2019.

[4] Y. Ai, M. Cheffena, T. Ohtsuki, and H. Zhuang, "Secrecy performance analysis of wireless sensor networks," *IEEE Sensors Letters*, vol. 3, no. 5, pp. 1–4, May 2019.

[5] M. A. Kishk and H. S. Dhillon, "Coexistence of rf-powered iot and a primary wireless network with secrecy guard zones," *IEEE Transactions on Wireless Communications*, vol. 17, no. 3, pp. 1460–1473, 2018.

[6] F. Jameel, S. Wyne, and I. Krikidis, "Secrecy outage for wireless sensor networks," *IEEE Communications Letters*, vol. 21, no. 7, pp. 1565–1568, Apr 2017.

[7] S. Vuppala, S. Biswas, and T. Ratnarajah, "Secrecy outage analysis of k-th best link in random wireless networks," *IEEE Transactions on Communications*, vol. 65, no. 10, pp. 4478–4491, Oct 2017.

[8] G. Chen, J. P. Coon, and M. Di Renzo, "Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 5, pp. 1195–1206, 2017.

[9] T. Somleewong and K. Maichalernnukul, "Secure multiple-antenna ultrawideband system: a wireless physical-layer security perspective," *I. J. Network Security*, vol. 21, no. 2, pp. 236–242, 2019.

[10] H. Alves, C. H. M. de Lima, P. H. J. Nardelli, R. D. Souza, and M. Latva-aho, "On the secrecy of interference-limited networks under composite fading channels," *IEEE Signal Processing Letters*, vol. 22, no. 9, pp. 1306–1310, 2015.

[11] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[12] C. E. Shannon, "Communication theory of secrecy systems∗," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[13] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[14] Y. J. Tolossa, S. Vuppala, G. Kaddoum, and G. Abreu, "On the uplink secrecy capacity analysis in d2d-enabled cellular network," *IEEE Systems Journal*, vol. 12, no. 3, pp. 2297–2307, 2018.

[15] S. Sreekumar, A. Bunin, Z. Goldfeld, H. H. Permuter, and S. Shamai, "The secrecy capacity of cost-constrained wiretap channels," *IEEE Transactions on Information Theory*, vol. 67, no. 3, pp. 1433–1445, 2021.

[16] F. Rottenberg, P. De Doncker, F. Horlin, and J. Louveaux, "Secrecy capacity of FBMC-OQAM modulation over frequency selective channel," *IEEE Wireless Communications Letters*, vol. 9, no. 8, pp. 1230–1234, 2020.

[17] M. Srinivasan and S. Kalyani, "Secrecy capacity of $\kappa-\mu$ shadowed fading channels," *IEEE Communications Letters*, vol. 22, no. 8, pp. 1728–1731, 2018.

[18] S. S. Chauhan, G. Verma, A. Singh, S. Singh, and A. Singh, "Average secrecy rate and probability of non-zero secrecy capacity of wiretap generalised gamma fading channels," *International Journal of Wireless and Mobile Computing*, vol. 18, no. 4, pp. 403–409, 2020.

[19] J. Zhu, Y. Zou, G. Wang, Y.-D. Yao, and G. K. Karagiannidis, "On secrecy performance of antenna-selection-aided MIMO systems against eavesdropping," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 214–225, 2016.

[20] S. Majhi and N. Nandan, "Secrecy capacity analysis of MIMO system over multiple destinations and multiple eavesdroppers," *Wireless Personal Communications*, vol. 100, no. 3, pp. 1009–1022, 2018.

[21] V. P. Tuan, N. Q. Sang, and H. Y. Kong, "Secrecy capacity maximization for untrusted uav-assisted cooperative communications with wireless information and power transfer," *Wireless Networks*, vol. 26, no. 4, pp. 2999–3010, 2020.

[22] L. Kong, S. Vuppala, and G. Kaddoum, "Secrecy analysis of random MIMO wireless networks over α - μ fading channels," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 11654–11666, 2018.

[23] S. Vuppala, Y. J. Tolossa, G. Kaddoum, and G. Abreu, "On the physical layer security analysis of hybrid millimeter wave networks," *IEEE Transactions on Communications*, vol. 66, no. 3, pp. 1139–1152, 2018.

[24] X. Luo, H. Chen, and W. Meng, "How much can radio resource allocation help to improve secrecy capacity of V2V underlay cellular networks?" *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 14932–14944, 2020.

[25] J. Guo, Y. Chen, H. Yang et al., "Study on secrecy capacity of wireless sensor networks in internet of things based on the amplify-and-forward compressed sensing scheme," *IEEE Access*, vol. 7, pp. 185580–185589, 2019.

[26] A. Jaiswal, S. Kumar, O. Kaiwartya, N. Kumar, H. Song, and J. Lloret, "Secrecy rate maximization in virtual-mimo enabled SWIPT for 5g centric iot applications," *IEEE Systems Journal*, vol. 15, no. 2, pp. 2810–2821, 2021.

[27] W. Son, H. Nam, W.-Y. Shin, and B. C. Jung, "Secrecy outage analysis of multiuser downlink wiretap networks with potential eavesdroppers," *IEEE Systems Journal*, vol. 15, no. 2, pp. 3093–3096, 2021.

[28] L. Wei, Y. Yang, and B. Jiao, "Secrecy throughput in full-duplex multiuser MIMO short-packet communications," *IEEE Wireless Communications Letters*, vol. 10, no. 6, pp. 1339–1343, 2021.

[29] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Transactions on Communications*, vol. 62, no. 6, pp. 2006–2021, 2014.

[30] B. Wang, Q. Xu, C. Chen, F. Zhang, and K. J. R. Liu, "The promise of radio analytics: a future paradigm of wireless positioning, tracking, and sensing," *IEEE Signal Processing Magazine*, vol. 35, no. 3, pp. 59–80, May 2018.

[31] F. Zhang, C. Wu, B. Wang, and K. J. R. Liu, "mmeye: super-resolution millimeter wave imaging," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6995–7008, 2021.

[32] S. D. Regani, C. Wu, B. Wang, M. Wu, and K. J. R. Liu, "mmWrite: passive handwriting tracking using a single millimeter-wave radio," *IEEE Internet of Things Journal*, vol. 8, no. 17, pp. 13291–13305, 2021.

[33] A. Dezfooliyan and A. M. Weiner, "Spatiotemporal focusing of phase compensation and time reversal in ultrawideband systems with limited rate feedback," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 4, pp. 1998–2006, 2016.

[34] B. Fall, F. Elbahhar, M. Heddebaut, A. Rivenq, and M. G. Di Benedetto, "Assessment of the contribution of time reversal on a UWB localization system for railway applications," *International Journal of Intelligent Transportation Systems Research*, vol. 14, no. 3, pp. 139–151, 2016.

[35] G. Caso, L. D. Nardis, M. T. Phuong Le, F. Maschietti, J. Fiorina, and M.-G. D. Benedetto, "Performance evaluation of non-prefiltering vs. time reversal prefiltering in distributed and uncoordinated IR-UWB ad-hoc networks," *Mobile Networks and Applications*, vol. 22, no. 5, pp. 796–805, 2017.

[36] U. Zia, M. Uppal, and I. H. Naqvi, "Robust feedback design for time reversal UWB communication systems under CSIT imperfections," *IEEE Communications Letters*, vol. 19, no. 1, pp. 102–105, 2015.

[37] S. M. Moghadasi and M. Dehmollaian, "Buried-object time-reversal imaging using UWB near-ground scattered fields," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 52, no. 11, pp. 7317–7326, 2014.

[38] D. Abbasi-Moghadam, A. Mohebbi, and Z. Mohades, "Performance analysis of time reversal UWB communication with non-coherent energy detector," *Wireless Personal Communications*, vol. 77, no. 3, pp. 2291–2303, 2014.

[39] W. Cao, J. Lei, W. Hu, and W. Li, "Secrecy capacity achievable time reversal pre-filter in MISO communication system and the unequal secrecy protection application," *Wireless Personal Communications*, vol. 97, no. 4, pp. 5427–5437, 2017.

[40] Y. Chen, B. Wang, Y. Han, H.-Q. Lai, Z. Safar, and K. J. R. Liu, "Why time reversal for future 5g wireless? [perspectives]," *IEEE Signal Processing Magazine*, vol. 33, no. 2, pp. 17–26, 2016.

[41] W. Lei, W. Zhang, M. Yang, H. Lei, and X. Xie, "Optimization of pre-processing filter for time-reversal multi-user secure transmission systems based on artificial noise," *Digital Signal Processing*, vol. 109, Article ID 102933, 2021.

[42] H. Tran, H. Tran, G. Kaddoum, D. Tran, and D. Ha, "Effective secrecy-sinr analysis of time reversal-employed systems over correlated multi-path channel," in *Proceedings of the IEEE 11th International Conference on Wireless and Mobile Computing Networking and Communications*, pp. 527–532, Abu Dhabi, United Arab Emirates, Oct. 2015.

[43] H. El-Sallabi, P. Kyritsi, A. Paulraj, and G. Papanicolaou, "Experimental investigation on time reversal precoding for space-time focusing in wireless communications," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 6, pp. 1537–1543, 2010.

[44] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: the MISOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, aug 2010.

[45] C. Oestges, "Validity of the kronecker model for MIMO correlated channels," in *Proceedings of the 63rd IEEE Vehicular Technology Conference, VTC Spring*, pp. 2818–2822, Melbourne, Australia, May 2006.

[46] S. H. Rice, "The expected value of the ratio of correlated random variables," *Ratio Derive*, vol. 1, pp. 1–3, 2015.

[47] H.-V. Tran, H. Nguyen, and E.-K. Hong, "Generalized analysis of mu-miso time reversal-based systems over correlated multipath channels with estimation error," *AEU - International Journal of Electronics and Communications*, vol. 69, no. 10, pp. 1541–1549, 2015.

[48] C. A. Viteri-Mera and F. L. Teixeira, "Equalized time reversal beamforming for frequency-selective indoor MISO channels," *IEEE Access*, vol. 5, pp. 3944–3957, 2017.

[49] P. H. M. Janssen and P. Stoica, "On the expectation of the product of four matrix-valued Gaussian random variables," *IEEE Transactions on Automatic Control*, vol. 33, no. 9, pp. 867–870, 1988.