Effective Secrecy-SINR Analysis of Time Reversal-Employed Systems over Correlated Multi-path Channel

Ha-Vu Tran, Hung Tran and Georges Kaddoum
ETS Engineering School, University of Quebec
Montreal, Canada
E-mail: ha-vu.tran.1@ens.etsmtl.ca,
tranhungemail@gmail.com,
georges.kaddoum@etsmtl.ca

Duc-Dung Tran and Dac-Binh Ha
Faculty of Electrical and Electronics Engineering
Duy Tan University, Danang, Viet Nam
E-mail: dung.td.1227@gmail.com,
hadacbinh@duytan.edu.vn

Abstract—**Based on the capability of harvesting the energy of all paths in the multipath environment, time-reversal (TR) transmission technique offers a great potential of low-complexity energy-efficient communications for future wireless network. The TR-employed systems benefit from a significantly reduced leakage of message-bearing signal to unintended users or eavesdroppers. In this paper, we propose a term so-called average *effective secrecy signal-to-interference-plus-noise ratio (SINR)* which represents the secrecy performance of TR-employed systems. Furthermore, we also consider: (i) the channel correlation between transmit antennas, and (ii) the channel correlation between a legitimate user and an eavesdropper. Accordingly, we derive the average *effective secrecy-SINR* in a closed-form expression of TR-employed systems. The obtained expression is based on the exact power-averaged expressions of the desired signal and the inter-symbol interference (ISI) components at both the legitimate user and eavesdropper side. The analytical results confirmed by numerical simulations show that the average *effective secrecy-SINR* metric is preferred to the average *secrecy-SINR* term in the perspective of measuring secrecy performance over correlated multi-path channel.**

Keywords—*Time reversal, physical layer security, secrecy-SINR, correlation.*

I. INTRODUCTION

Over the past few years, physical layer security have been vastly studied in the literature [1]–[3]. This promising approach explores the characteristics of the wireless channel, such as multipath fading and spatial signatures, to enhance wireless transmission security. In practice, due to the differences in receivers' locations, the message-bearing signals obtained at receivers experience distinct propagation effects. Therefore, the multi-path delay profile or channel state information (CSI) can be measured and then encoded to produce a unique sercrecy key used between legitimate nodes.

TR technique is one of most prominent forms of linear precoding which can exploit the unique property of channel impulse response (CIR) by focusing the energy of all taps in the time and space domains on the intended terminals [4]–[9]. By utilizing the time-reversed version of CIR to prefilter transmit signals, TR is equivalent to a special beamforming technique. The focalization property of the TR technique, which leads to improving the system security, is one of its most notable features. In particular, in traditional TR systems, certain wideband channel have been considered where the average power of each tap decays exponentially [5], [8]. Regarding secrecy aspects, the experimental outcome in [10] shows that the achieved signal power at the eavesdroppers is significantly lower compared with the power at the legitimate receiver, regardless of whether the eavesdroppers is located near the legitimate receiver or not. Based on the spatial focusing effect, the earlier work in [7] also exhibits that the TR-based transmission can limit the leakage of the information to the unintended user or the eavesdroppers significantly. In the aspect of secrecy analysis, the results reported in [11] provide the asymptotic capacity analysis. It is assumed that the central tap has a complex Gaussian distribution to reduce the complexity of analytical derivations, however, this hypothesis leads to a rather large gap between analytical and simulation results.

To the best authors' knowledge, the exact analyses of average channel-capacity and average SINR have not been investigated due to the mathematical complexity. It is found to be complicated to provide the closed-form expression of average *secrecy-capacity* and average *secrecy-SINR*. In this paper, we propose a new definition of average *effective secrecy-SINR* term to evaluate the secrecy performance of TR-applied systems. In general, the average *effective secrecy-SINR* has the same characteristics as the average *secrecy-SINR*, in which *secrecy-SINR* can be inferred from the *secrecy-capacity*. In reality, the eavesdropper is frequently located at an unknown position near the legitimate user, whereas the distance between the eavesdropper and the legitimate user can estimate how much information can be eavesdropped. On the other hand, if the transmission bandwidth is limited and the amount of scattering in the propagation channel is poor, the transmit correlation and the correlation between the illegitimate and legitimate channels have a strong effect on the secrecy performance. In this paper, we present a security performance of well-known model with two practical assumptions including (i) the channel correlation between transmit antennas, and (ii) the channel correlation between the legitimate user and the eavesdropper. The analysis of average *effective secrecy-SINR* can be derived using exact closed-form expressions of desired signal and inter-symbol interference (ISI) terms at both legitimate and illegitimate nodes. We show that the average *ef-*
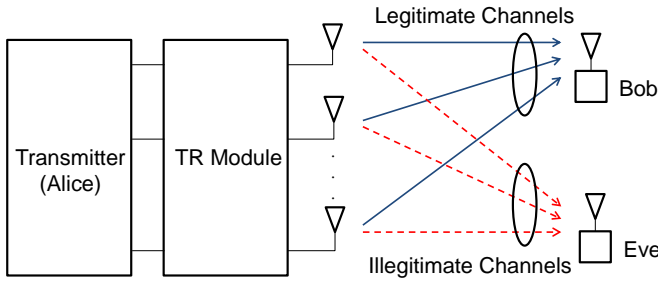
Fig. 1. System model.

fective secrecy-SINR term is more interesting than the average secrecy-SINR term for measuring secrecy performance due to simpler mathematical computations. Finally, the validity of our analysis is verified using a Monte-Carlo simulation.

The rest of this paper is organized as follows: the system model is described in Section II. Section III presents the secrecy performance analysis. We show the numerical results in Section IV. Finally, the conclusion is inferred in Section V.

Notation: the notation $\mathbb{C}^{m \times n}$ denotes the set of $m \times n$ complex matrix. The boldface lowercase letters and uppercase letters indicate vectors and matrices respectively. The superscript T represent the transpose. $|\cdot|$ and $\|\cdot\|$ stand for the absolute value and the vector Euclidean norm respectively. For a comlex value, we denote $\text{Re}\{\cdot\}$ as the real part. Moreover, $\text{E}[\cdot]$ represents the expectation calculation. $\otimes$ and $*$ denote the Kronecker product and the convolution operator respectively.

II. SYSTEM MODEL

Let us consider the TR-based system model as shown in Fig. 1 where Alice transmits the information-bearing signal through a base station equipped with M antennas and TR module to Bob (legitimate users). In this network, Eve's (eavesdropper) receiver is equipped with one single antenna device. For notational conveniences, we refer to legitimate user Bob as user 0 and the eavesdropper Eve as user 1. In the multipath channel, we assume the maximum length of each CIR is L. Thus, the CIR between the transmit antenna m ($0 \leq m \leq M$) and the user n ($n = \{0; 1\}$) can be formulated as

$$h_{mn}(t) = \sum_{l=1}^{L} \sigma_{mn,l} \delta(t - \tau_{mn,l}), \quad (1 \leq l \leq L) \quad (1)$$

where $\sigma_{mn,l}$ and $\tau_{mn,l}$ are the amplitude and the delay of the $l-th$ tap, respectively. The CIR can be discretized in the time domain as a vector $\mathbf{h}_{mn} \in \mathbb{C}^{L \times 1}$ in which $\text{E}[h_{mn}[l]] = 0$ and $\text{E}\left[|h_{mn}[l]|^2\right] = \sigma_{mn,l}^2$.

We can arrange the propagation channels in an $2M \times L$ matrix form as

$$\mathbf{H} = [\mathbf{h}_{10} \ldots \mathbf{h}_{M0} \mathbf{h}_{11} \ldots \mathbf{h}_{M1}]^T. \quad (2)$$

According to Kronecker model [12], the channel matrix with the correlation following the Kronecker model can be given by

$$\mathbf{H} = \left(\left(\mathbf{R}_D^{1/2}\right)^T \otimes \mathbf{R}_T^{1/2}\right) \mathbf{H}_w, \quad (3)$$

where the correlation between legal and illegal users and the correlation between transmit antennas are represented by the 2×2 positive-define matrix $\mathbf{R}_D$ and the $M \times M$ positive-define matrix $\mathbf{R}_T$, respectively. $\mathbf{H}_w \in \mathbb{C}^{2M \times L}$ is the channel matrix of the independent CIRs. Note that the correlation matrix follows the general model with arbitrary positive coefficients (i.e. $\rho_{U,nn'} \geq 0$). For an example, a matrix $\mathbf{R}_D$ can be illustrated as

$$\mathbf{R}_D = \begin{bmatrix} 1 & \rho_{D,12} \\ \rho_{D,21} & 1 \end{bmatrix}. \quad (4)$$

In the TR scheme [7], first, Bob (i.e. the legitimate user) sends a pilot signal to Alice (i.e. the base station). In the second step, Alice estimates the pilot signal to infer the information of CIR which can be considered as the secret key for the data transmission between Alice and Bob. In the third step, the time reversed and conjugate version of the CIR is used as a matched filter (or pre-filter) at Alice side. The modulated transmit signals conveyed to Bob is very tightly focused at one specific time and one location. Therefore, TR technique greatly improves the secrecy performance.

Based on the TR scheme, we define $\mathbf{g}_{m0} \in \mathbb{C}^{L \times 1}$ as the pre-filtering vector for the message-bearing signal. Each tap of $\mathbf{g}_{m0}$ can be given by

$$g_{m0}[l] = \sqrt{p} h_{m0}^*[L + 1 - l] \Big/ \sqrt{\sum_{m=1}^{M} \text{E}\left[\|\mathbf{h}_{m0}\|^2\right]}. \quad (5)$$

in which $h_{m0}^*[L + 1 - l]$ represents the conjugate of $h_{m0}[L + 1 - l]$ and p is the transmit power. After some mathematical manipulations, the $(2L - 1) \times 1$ received signal vectors at the legitimate user and the eavesdropper can be derived as

$$\mathbf{y}_0 = \sum_{m=1}^{M} s\left(\mathbf{g}_{m0} * \mathbf{h}_{m0}\right) + \mathbf{n}_0, \quad (6)$$

$$\mathbf{y}_1 = \sum_{m=1}^{M} s\left(\mathbf{g}_{m0} * \mathbf{h}_{m1}\right) + \mathbf{n}_1, \quad (7)$$

respectively. In each equation, the first and second terms are the obtained signal and the additive white Gaussian noise, respectively. In which, $s \in \mathbb{C}$ is the transmitted signal, each element of $\mathbf{n}_0$ and $\mathbf{n}_1$ vectors are zero mean Gaussian noise with variances $\sigma_{Gauss,0}^2$ and $\sigma_{Gauss,1}^2$ respectively.

Due to the focalization property of TR, the receiver is expected to take one sample at the central tap, i.e. the L-th tap. The instantaneous SINR derivations at the legitimate user and the eavesdropper can be expressed as follows

$$\gamma_0 = \frac{\underbrace{\left|\sum_{m=1}^{M} (g_{m0} * h_{m0})[L]\right|^2}_{P_{sig}^{(0)}}}{\underbrace{\sum_{\substack{k=1 \\ k \neq L}}^{2L-1} \left|\sum_{m=1}^{M} (g_{m0} * h_{m0})[k]\right|^2 + |\mathbf{n}_0[L]|^2}_{P_{isi}^{(0)}}}, \quad (8)$$

$$\gamma_1 = \frac{\underbrace{\left| \sum_{m=1}^{M} (g_{m0} * h_{m1})[L] \right|^2}_{P_{sig}^{(1)}}}{\underbrace{\sum_{\substack{k=1 \\ k \neq L}}^{2L-1} \left| \sum_{m=1}^{M} (g_{m0} * h_{m1})[k] \right|^2 + |n_1[L]|^2}_{P_{isi}^{(1)}}}. \qquad (9)$$

Note that $P_{sig}^{(n)}$ and $P_{isi}^{(n)}$ are the received signal power and interference power due to ISI respectively.

III. SECRECY PERFORMANCE ANALYSIS

A. Secrecy-SINR for the TR-based System

In this section, we are interested in *secrecy-SINR* which can be inferred from *secrecy-capacity*. Since *secrecy-capacity* is defined as the difference between capacity of the main channel and the eavesdroppers channel, the fomula of *secrecy-capacity* can be rewritten as

$$
\begin{aligned}
C_S &= \log_2(1+\gamma_0) - \log_2(1+\gamma_1), \quad \gamma_0 > \gamma_1 \\
&= \log_2\left(1 + \frac{\gamma_0 - \gamma_1}{1+\gamma_1}\right) \qquad (10) \\
&= \log_2(1+\gamma_S),
\end{aligned}
$$

where $\gamma_S = \frac{\gamma_0 - \gamma_1}{1+\gamma_1}$ is the *secrecy-SINR*. As a result, the *secrecy-SINR* expression is given by

$$\gamma_S = \{\gamma_0 - \gamma_1\}^+ = \begin{cases} \dfrac{\gamma_0 - \gamma_1}{1+\gamma_1}, & \gamma_0 > \gamma_1 \\ 0, & \gamma_0 \leq \gamma_1. \end{cases} \qquad (11)$$

B. Analysis of Effective Secrecy-SINR

According to (11), the expectation of *secrecy-SINR* can be formulated as

$$\bar{\gamma}_S = \mathrm{E}[\gamma_S] = \mathrm{E}\left[\frac{\gamma_0 - \gamma_1}{1+\gamma_1}\right]. \qquad (12)$$

To the best author's knowledge, closed-form expression for (12) is impossible to obtain. However, we can rewrite it by using the help of [13] as follows

$$\mathrm{E}\left[\frac{\gamma_0 - \gamma_1}{1+\gamma_1}\right] = \frac{\mathrm{E}[\gamma_0 - \gamma_1]}{\mathrm{E}[1+\gamma_1]} \qquad (13)$$
$$+ \frac{\sum_{i=1}^{\infty} (-1)^i \mathrm{E}[\gamma_0 - \gamma_1]\langle^i(1+\gamma_1)\rangle + \langle\gamma_0 - \gamma_1, ^i(1+\gamma_1)\rangle}{\mathrm{E}[1+\gamma_1]^{i+1}},$$

where $\langle^i(1+\gamma_1)\rangle = \mathrm{E}\left[(1+\gamma_1 - \mathrm{E}[1+\gamma_1])^i\right]$ is the i-th central moment of $(1+\gamma_1)$, and $\langle\gamma_0 - \gamma_1, ^i(1+\gamma_1)\rangle = \mathrm{E}\left[(\gamma_0 - \gamma_1 - \mathrm{E}[\gamma_0 - \gamma_1])(1+\gamma_1 - \mathrm{E}[1+\gamma_1])^i\right]$ is the i-th mixed central moment of $(1+\gamma_1)$ and $(\gamma_0 - \gamma_1)$.

Based on [8], [14], the value of the first term on the right-side part of equation (13) should be small. In this case, this term can be neglected. Thus, we can define the average *effective secrecy-SINR* as follows

$$\hat{\gamma}_S = \frac{\dfrac{\mathrm{E}\left[P_{sig}^{(0)}\right]}{\mathrm{E}\left[P_{isi}^{(0)}\right] + \sigma_{Gauss,0}^2} - \dfrac{\mathrm{E}\left[P_{sig}^{(1)}\right]}{\mathrm{E}\left[P_{isi}^{(1)}\right] + \sigma_{Gauss,1}^2}}{1 + \dfrac{\mathrm{E}\left[P_{sig}^{(1)}\right]}{\mathrm{E}\left[P_{isi}^{(1)}\right] + \sigma_{Gauss,1}^2}}, \qquad (14)$$

To demonstrate that the average *effective secrecy-SINR* can replace the average *secrecy-SINR* to evaluate the secrecy performance, a comparison between them is discussed in Section IV.

Theorem 1: Relying on (14), we can observe that the average *effective secrecy-SINR* consists of $\mathrm{E}\left[P_{sig}^{(0)}\right]$, $\mathrm{E}\left[P_{isi}^{(0)}\right]$, $\mathrm{E}\left[P_{sig}^{(1)}\right]$ and $\mathrm{E}\left[P_{isi}^{(1)}\right]$ terms. Therefore, the closed-form derivation of *effective secrecy-SINR* can be achieved through the expressions as (15)-(18).

Proof: We start with considering the expectation of $P_{sig}^{(0)}$ which can be decomposed into two components as follows

$$
\mathrm{E}\left[\left|\sum_{m=1}^{M}(g_{mn} * h_{mn})[L]\right|^2\right] = \mathrm{E}\left[\left|\sum_{m=1}^{M}\Delta_{mn}[L]\right|^2\right]
$$
$$
= \mathrm{E}\left[\sum_{m=1}^{M}|\Delta_{mn}[L]|^2 + \mathrm{Re}\left\{\sum_{\substack{m'=1 \\ m' \neq m}}^{M}\sum_{m=1}^{M}\Delta_{mn}[L]\Delta_{m'n}^*[L]\right\}\right],
$$
$$(19)$$

where $\Delta_{mn} = g_{mn} * h_{mn}$.

It can be observed that (19) implies the components of $\mathrm{E}\left[|h_{mn}[l]h_{mn}^*[l]|^2\right]$ and $\mathrm{E}\left[(h_{mn} * h_{m'n})[k](h_{mn} * h_{m'n})^*[k]\right]$. Therefore, to solve the expectation of each term on the right side in (19), it is necessary to provide some useful formulations in the general form as below

$$
\begin{aligned}
\mathrm{E}\left[|h_{mn}[l]h_{m'n'}^*[l']|^2\right] &= \mathrm{E}\left[|h_{mn}[l]|^2\right]\mathrm{E}\left[|h_{m'n'}[l']|^2\right] \\
&- |\mathrm{E}[h_{mn}[l]h_{m'n'}^*[l']]|^2, \qquad (20)
\end{aligned}
$$

$$
\begin{aligned}
&\mathrm{E}\left[(h_{mn} * h_{m'n'})[k](h_{mn} * h_{m'n'})^*[k']\right] \\
&= \sum_{l=1}^{k}\mathrm{E}[h_{mn}^*[L+1-l]h_{mn}[k+1-l]... \qquad (21) \\
&...h_{m'n'}[L+1-l]h_{m'n'}^*[k'+1-l]].
\end{aligned}
$$

Furthermore, since we consider the correlated channel matrix, we can derive the expectation of product of two random variables as

$$\mathrm{E}[h_{mn}[l]h_{m'n'}^*[l']] = \sigma_{mn,l}\sigma_{m'n',l'}(\mathbf{R}_T)_{mm'}(\mathbf{R}_D)_{nn'}. \qquad (22)$$

In the case of the expectation of product of four random variables, we can further express by the manner as in [15]. For an example, that is,

$$
\begin{aligned}
&\mathrm{E}[X_1 X_2 X_3 X_4] \\
&= \mathrm{E}[X_1 X_2]\mathrm{E}[X_3 X_4] + \mathrm{E}[X_1 X_3]\mathrm{E}[X_2 X_4] \\
&+ \mathrm{E}[X_1 X_4]\mathrm{E}[X_2 X_3] - 2\mathrm{E}[X_1]\mathrm{E}[X_2]\mathrm{E}[X_3]\mathrm{E}[X_4],
\end{aligned}
$$
$$(23)$$

$$E\left[P_{sig}^{(0)}\right] = \frac{p\sum_{m=1}^{M}\left(\sum_{l=1}^{L}\sigma_{mn,l}^{4}+\left(\sum_{l=1}^{L}\sigma_{mn,l}^{2}\right)^{2}\right)}{\sum_{m=1}^{M}\sum_{l=1}^{L}\sigma_{mn,l}^{2}} + \frac{p\sum_{\substack{m'=1\\m'\neq m}}^{M}\sum_{m=1}^{M}\left(\sum_{l'=1}^{L}\sum_{l=1}^{L}\sigma_{mn,l}^{2}\sigma_{m'n,l}^{2}+\sum_{l=1}^{L}\sigma_{mn,l}^{2}\sigma_{m'n,l}^{2}\left(\mathbf{R}_{T}\right)_{mm'}^{2}\right)}{\sum_{m=1}^{M}\sum_{l=1}^{L}\sigma_{mn,l}^{2}}, \quad (15)$$

$$\mathrm{E}\left[P_{isi}^{(0)}\right] = 2p\sum_{k=1}^{L-1}\left(\frac{\sum_{m=1}^{M}\left(\sum_{l=1}^{k}\sigma_{mn,k+1-l}^{2}\sigma_{mn,L+1-l}^{2}\right)+\sum_{\substack{m'=1\\m'\neq m}}^{M}\sum_{m=1}^{M}\left(\sum_{l=1}^{k}\left(\sigma_{mn,l}\sigma_{mn',l}\sigma_{m'n,l}\sigma_{m'n',l}\right)\left(\mathbf{R}_{T}\right)_{mm'}^{2}\right)}{\sum_{m=1}^{M}\sum_{l=1}^{L}\sigma_{mn,l}^{2}}\right), \quad (16)$$

$$
\begin{aligned}
\mathrm{E}\left[P_{sig}^{(1)}\right] = {} & p\frac{\sum_{m=1}^{M}\left(\left(1+\left(\mathbf{R}_{U}\right)_{nn'}^{2}\right)\sum_{l=1}^{L}\sigma_{mn,l}^{2}\sigma_{mn',l}^{2}+\sum_{\substack{l'=1\\l'\neq l}}^{L}\sum_{l=1}^{L}\left(\sigma_{mn,l}\sigma_{mn',l}\sigma_{m'n,l'}\sigma_{m'n',l'}\right)\left(\mathbf{R}_{D}\right)_{nn'}^{2}\right)}{\sum_{m=1}^{M}\sum_{l=1}^{L}\sigma_{mn,l}^{2}} \\
+ {} & p\frac{\sum_{\substack{m'=1\\m'\neq m}}^{M}\sum_{m=1}^{M}\left(\sum_{\substack{l'=1\\l'\neq l}}^{L}\sum_{l=1}^{L}\left(\sigma_{mn,l}\sigma_{mn',l}\sigma_{m'n,l'}\sigma_{m'n',l'}\right)\left(\mathbf{R}_{D}\right)_{nn'}^{2}+\sum_{l=1}^{L}\left(\sigma_{mn,l}\sigma_{mn',l}\sigma_{m'n,l}\sigma_{m'n',l}\right)\left(\left(\mathbf{R}_{D}\right)_{nn'}^{2}+\left(\mathbf{R}_{T}\right)_{mm'}^{2}\right)\right)}{\sum_{m=1}^{M}\sum_{l=1}^{L}\sigma_{mn,l}^{2}},
\end{aligned}
$$
$$(17)$$

$$\mathrm{E}\left[P_{isi}^{(1)}\right] = 2p\sum_{k=1}^{L-1}\left(\frac{\sum_{m=1}^{M}\sum_{l=1}^{k}\sigma_{mn,k+1-l}^{2}\sigma_{mn',L+1-l}^{2}+\sum_{\substack{m'=1\\m'\neq m}}^{M}\sum_{m=1}^{M}\sum_{l=1}^{k}\left(\sigma_{mn,l}\sigma_{mn',l'}\sigma_{m'n,l}\sigma_{m'n',l'}\right)\left(\mathbf{R}_{T}\right)_{mm'}^{2}}{\sum_{m=1}^{M}\sum_{l=1}^{L}\sigma_{mn',l}^{2}}\right). \quad (18)$$

where X_1, X_2, X_3 and X_4 are jointly Gaussian random variables.

After some mathematical derivations using equations (20)-(23), we obtain the results of (24) and (25) as

$$
\begin{aligned}
\mathrm{E}\left[\left|\Delta_{mn}\left[L\right]\right|^{2}\right] &= p\mathrm{E}\left[\frac{\left|\sum_{l=1}^{L}h_{mn}\left[l\right]h_{mn}^{*}\left[l\right]\right|^{2}}{\sum_{m=1}^{M}\sum_{l=1}^{L}\sigma_{mn,l}^{2}}\right] \quad (24)\\
&= p\frac{\sum_{l=1}^{L}\sigma_{mn,l}^{4}+\left(\sum_{l=1}^{L}\sigma_{mn,l}^{2}\right)^{2}}{\sum_{m=1}^{M}\sum_{l=1}^{L}\sigma_{mn,l}^{2}},
\end{aligned}
$$

$$
\begin{aligned}
&\mathrm{E}\left[\,\Delta_{mn}\left[L\right]\Delta_{m'n}^{*}\left[L\right]\right]\\
&= p\mathrm{E}\left[\frac{\sum_{l=1}^{L}h_{mn}\left[l\right]h_{mn}^{*}\left[l\right]\sum_{l'=1}^{L}h_{m'n}^{*}\left[l'\right]h_{m'n}\left[l'\right]}{\sum_{m=1}^{M}\sum_{l=1}^{L}\sigma_{mn,l}^{2}}\right]\\
&= p\frac{\sum_{l'=1}^{L}\sum_{l=1}^{L}\sigma_{mn,l}^{2}\sigma_{m'n,l'}^{2}+\sum_{l=1}^{L}\sigma_{mn,l}^{2}\sigma_{m'n,l}^{2}\left(\mathbf{R}_{T}\right)_{mm'}^{2}}{\sum_{m=1}^{M}\sum_{l=1}^{L}\sigma_{mn,l}^{2}}.
\end{aligned}
$$
$$(25)$$

Substituting (24) and (25) into (23), we achieve the expected value of signal power component as (15).

Futhermore, the expected value of $P_{isi}^{(0)}$ can be defined as

$$\mathrm{E}\left[\sum_{\substack{k=1\\k\neq L}}^{2L-1}\left|\sum_{m=1}^{M}\left(g_{mn}*h_{mn}\right)\left[k\right]\right|^{2}\right] = 2\sum_{k=1}^{L-1}\mathrm{E}\left[\left|\sum_{m=1}^{M}\Delta_{mn}\left[k\right]\right|^{2}\right]. \quad (26)$$

In the similar way to (19), we divide $\mathrm{E}\left[\left|\sum_{m=1}^{M}\Delta_{mn}[k]\right|^2\right]$ into two terms as follows

$$\mathrm{E}\left[\left|\sum_{m=1}^{M}\Delta_{mn}[k]\right|^2\right]$$
$$= \mathrm{E}\left[\sum_{m=1}^{M}|\Delta_{mn}[k]|^2 + \mathrm{Re}\left\{\sum_{\substack{m'=1\\m'\neq m}}^{M}\sum_{m=1}^{M}\Delta_{mn}[k]\Delta_{m'n}^{*}[k]\right\}\right].$$
(27)

By applying the (20)-(23) for (27), we can infer the formulations of (28) and (29). Then the closed-form expression of $P_{isi}^{(0)}$, i.e. equation (16), can be computed by substituting (28) and (29) into (27).

$$\mathrm{E}\left[|\Delta_{mn}[k]|^2\right] = p\mathrm{E}\left[\left|\frac{\sum_{l=1}^{k}h_{mn}[k+1-l]h_{mn}^{*}[L+1-l]}{\sum_{m=1}^{M}\sum_{l=1}^{L}\sigma_{mn,l}^2}\right|^2\right]$$
$$= p\frac{\sum_{l=1}^{k}\sigma_{mn,k+1-l}^2\sigma_{mn,L+1-l}^2}{\sum_{m=1}^{M}\sum_{l=1}^{L}\sigma_{mn,l}^2},$$
(28)

$$\mathrm{E}\left[\Delta_{mn}[k]\Delta_{m'n}^{*}[k]\right]$$
$$= p\mathrm{E}\left[\frac{\sum_{l=1}^{k}h_{mn}[k+1-l]h_{mn}^{*}[L+1-l]}{\sum_{m=1}^{M}\sum_{l=1}^{L}\sigma_{mn,l}^2}\right]$$
$$\times\mathrm{E}\left[\sum_{l=1}^{k}h_{m'n}^{*}[k+1-l]h_{m'n}[L+1-l]\right]$$
$$= p\frac{\sum_{l=1}^{k}\left(\sigma_{mn,l}\sigma_{mn',l'}\sigma_{m'n,l}\sigma_{m'n',l'}\right)(\mathbf{R}_T)_{mm'}^2}{\sum_{m=1}^{M}\sum_{l=1}^{L}\sigma_{mn,l}^2}.$$
(29)

For $\mathrm{E}\left[P_{sig}^{(1)}\right]$ and $\mathrm{E}\left[P_{isi}^{(1)}\right]$, their exact analysis can be derived in a similar manner to $\mathrm{E}\left[P_{sig}^{(0)}\right]$ and $\mathrm{E}\left[P_{isi}^{(0)}\right]$, respectively. ∎

IV. NUMERICAL RESULTS

In this section, numerical results are presented to evaluate the system performance.

For simplicity, we use the inter-class correlation model described as below

$$(\mathbf{R}_T)_{mm'} = \begin{cases} 1, & m = m' \\ \rho_T, & m \neq m'. \end{cases}$$
(30)

The same model can be used for $(\mathbf{R}_D)_{nn'}$ with the correlation factor ρ_D. Furthermore, similar to [8], we set channel's bandwidth to $B = 500$ MHz, the number of tap $L = 110$ and root mean square delay spread $\theta_T = 100/B$ and sampling time of
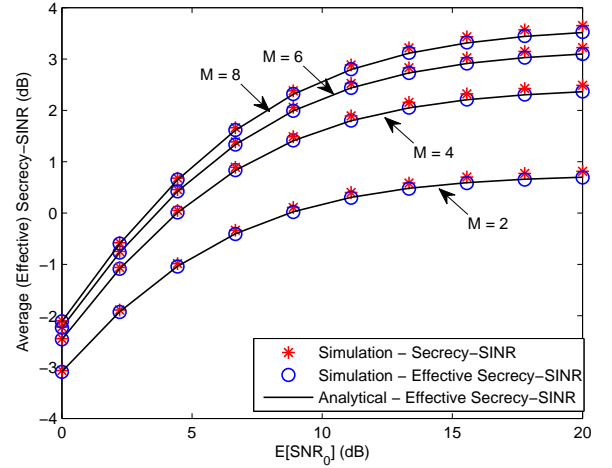

Fig. 2. *Average effective secrecy-SINR* and average *secrecy-SINR* vs. $\mathrm{E}[\mathrm{SNR}_0]$ ($\rho_T = 0.3, \rho_D = 0.4$).
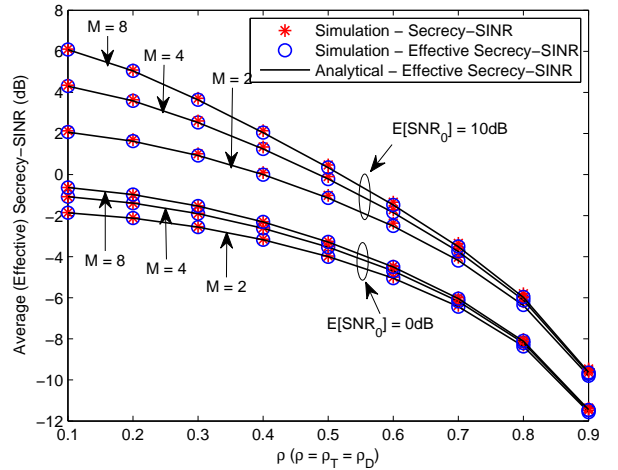

Fig. 3. Average *effective secrecy-SINR* and average *secrecy-SINR* vs. correlations.

the system $T_S = 1/B$. The average power of each tap decays exponentially described as follows

$$\mathrm{E}\left[|h_{mn}[l]|^2\right] = \sigma_{mn,l}^2 = e^{-\frac{lT_S}{\theta_T}}.$$
(31)

Note that all channels convey the same average power.

In general, Fig. 2 and 3 show a good agreement between average *secrecy-SINR* and average *effective secrecy-SINR*. In fact, these two parameters have very similar properties. It means that it is efficient to replace average *secrecy-SINR* by average *effective secrecy-SINR* for measuring the secrecy performance. Especially, in case of average *effective secrecy-SINR*, one can observe that the analytical results are the same as the simulation results. And hence our analysis is validated.

In more details, we can evaluate in Fig. 2 the secrecy performance in term of average *secrecy-SINR* and average *effective secrecy-SINR* under different values of average signal-

to-noise-ratio (SNR) at the legitimate user defined as follows

$$\mathrm{E}\left[\mathrm{SNR}_0\right] = \frac{\mathrm{E}\left[P_{sig}^{(0)}\right]}{\sigma_{Gauss}^2}. \qquad (32)$$

Without loss of generality, we assume in this paper that the noise variances in the system are equal. It means that $\sigma_{Gauss}^2 = \sigma_{Gauss,0}^2 = \sigma_{Gauss,1}^2$.

By using TR technique, Fig. 2 indicates that when the number of transmit antennas increases, the achieved secrecy performance is significantly improved. It can be explain that the $\mathrm{E}\left[P_{sig}^{(0)}\right]$ increase faster than that of $\mathrm{E}\left[P_{sig}^{(1)}\right]$. In Fig. 3, we can observe the average *secrecy-SINR* and average *effective secrecy-SINR* as a function of correlations. Clearly, the growth of $\mathrm{E}\left[P_{sig}^{(1)}\right]$ induces a reduction in the secercy performance. This implies that the amount of scattering of environment has a strong impact on the secrecy performance.

V. CONCLUSION

In this paper, the secrecy performance of TR-based system has been analyzed using the exact closed-form expression of average *effective secrecy-SINR*, in presence of (i) the channel correlation between transmit antennas and (ii) the channel correlation between a legitimate user and an eavesdropper. Based on the analysis, it can be concluded that the performance can be improved when the number of transmit antennas increases, and the correlations is one of main metric which causes to the decrease in performance significantly. Our framework also demonstrates the proposed average *effective secrecy-SINR* can replace the average *secrecy-SINR* to measure the secrecy performance of the system efficiently.

REFERENCES

[1] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, 2012.

[2] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 254–259, 2013.

[3] D.-D. Tran, D.-B. Ha, V. Tran-Ha, and E.-K. Hong, "Secrecy analysis with MRC/SC-based eavesdropper over heterogeneous channels," *IETE Journal of Research*, 2015, (to be published). [Online]. Available: http://www.tandfonline.com/doi/pdf/10.1080/03772063.2015.1021389

[4] M. Fink, "Time reversal of ultrasonic fields. i. basic principles," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 39, no. 5, pp. 555–566, 1992.

[5] B. Wang, Y. Wu, F. Han, Y.-H. Yang, and K. J. R. Liu, "Green wireless communications: A time-reversal paradigm," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 8, pp. 1698–1710, 2011.

[6] M.-A. Bouzigues, I. Siaud, M. Hlard, and A.-M. Ulmer-Moll, "Turn back the clock: Time reversal for green radio communications," *IEEE Trans. Veh. Technol.*, vol. 8, no. 1, pp. 49–56, 2013.

[7] V. Tran-Ha, Q.-D. Vu, and E.-K. Hong, "Time reversal-based transmissions with distributed power allocation for two-tier networks," in *Proc. of IEEE International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, Gwangju, South Korea, March 2015, pp. 181–186.

[8] F. Han, Y.-H. Yang, B. Wang, Y. Wu, and L. K.J.R, "Time-reversal division multiple access over multi-path channels," *IEEE Trans. Commun.*, vol. 60, no. 7, pp. 1953–1965, 2012.

[9] H.-V. Tran, D.-B. Ha, H. Nguyen, and E.-K. Hong, "Robust time reversal-based transmit optimization for green heterogeneous networks," *Elektronika ir Elektrotechnika (Electronics and Electrical Engineering)*, vol. 21, no. 3, pp. 66–72, 2015.

[10] X. Zhou, P. Eggers, P. Kyritsi, J. Andersen, G. Perdersen, and J. Nilsen, "Spatial focusing and interference reduction using miso time reversal in an indoor application," in *Proc. of IEEE Workshop on Statistical Signal Processing (SSP)*, Madison, WI, USA, August 2007, pp. 307–311.

[11] T. Koike-Akino, A. F. Molisch, C. Duan, Z. Tao, and P. Orlik, "Capacity, MSE and secrecy analysis of linear block precoding for distributed antenna systems in multi-user frequency-selective fading channels," *IEEE Trans. Commun.*, vol. 59, no. 3, pp. 888–900, 2011.

[12] C. Oestges, "Validity of the kronecker model for MIMO correlated channels," in *Proc. of IEEE Vehicular Technology Conference (VTC)-Spring*, vol. 6, Melbourne, Australia, May 2006, pp. 2818–2822.

[13] S. H. Rice, "The expected value of the ratio of correlated random variables," Texas Tech University, Tech. Rep., 2009. [Online]. Available: http://www.faculty.biol.ttu.edu/Rice/ratio-derive.pdf

[14] 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," *International Journal of Electronics and Communications*, 2015, (to be published). [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1434841115001739

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