IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 19, 2017, accepted December 21, 2017, date of publication January 1, 2018,
date of current version February 28, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2789162

Randomized Beamforming With Generalized Selection Transmission for Security Enhancement in MISO Wiretap Channels

MORTEZA SOLTANI[1], (Student Member, IEEE), AND HÜSEYIN ARSLAN[2], (Fellow, IEEE)
[1]School of Engineering and Natural Sciences, Istanbul Medipol University, 34810 Istanbul, Turkey
[2]Department of Electrical Engineering, University of South Florida, Tampa, FL 33620, USA

Corresponding author: Morteza Soltani (msoltani@st.medipol.edu.tr)

This work was supported by the Scientific and Technological Research Council of Turkey under Grant 114E244.

ABSTRACT Transmit beamforming (TBF) has been proposed as an effective approach to enhance the security performance of multiple-input single-output (MISO) wiretap channels. However, this secrecy enhancement comes at some expenses, such as power consumption and the amount of signal processing. In addition, in block fading channels, TBF fails to deliver secure communication against intelligent eavesdroppers equipped with advanced channel estimation techniques. Considering these issues associated with TBF, we propose and study randomized beamforming with generalized selection transmission (RBF/GST) to enhance physical layer security in MISO wiretap channels. With GST, Q antennas out of N antennas are selected at the transmitter to maximize the signal to noise ratio at the legitimate receiver. Moreover, RBF is responsible for delivering secure communications in the presence of advanced eavesdroppers. We characterize the physical layer secrecy of RBF/GST under passive and active eavesdropping scenarios, via our closed-form expressions for the ergodic secrecy rate and the exact and asymptotic secrecy outage probabilities. We demonstrate that RBF/GST can effectively improve communication secrecy with a reasonable amount of signal processing and power consumption.

INDEX TERMS Physical layer security, MISO wiretap channels, randomized beamforming.

I. INTRODUCTION

Broadcast nature of wireless communications enables reaching multiple parties simultaneously. However, due to this property, the security of information transmission is prone to eavesdropping of unauthorized receivers. Therefore, physical layer security has emerged as a promising solution aiming at delivering secure communications over the physical layer of the communication network. It enables the possibility of secure communications by only exploiting the characteristics of wireless channels (e.g., fading, noise, and interference) without relying on encryption at higher layers of the communication network.

Recently, it has been shown that degrees of freedom in achieving secure communication remarkably increase in the presence of multiple antenna techniques [1]. A promising approach in multiple antenna enabled physical layer security is to design a transmit beamformer (TBF) via direction selection and power allocation [2]. The secrecy performance of multiple antenna beamforming methods is mainly governed by the amount of channel state information (CSI) available at the transmitter. Under the assumption of perfect CSI availability of both main and wiretap channels at the transmitter, authors in [3] showed that the secrecy capacity-achieving beamformer has a direction along the generalized eigenvector corresponding to the maximum generalized eigenvalues of the main and wiretap channel. In the case that full main CSI and partial or none wiretap CSI are available at the transmitter, the optimal beamformer is aligned with the main channel direction [4]. However, in this case, a secrecy outage is unavoidable. The secrecy outage probability of the latter case was investigated in [5] for block fading channels. Although TBF can be seen as an optimal approach, there are two major problems associated with such a transmission method. Firstly, the number of radio frequency (RF) chains connected to each antenna and the amount of required signal processing are relatively high. Secondly, under the assumption of block fading channels, an intelligent eavesdropper equipped with blind equalization techniques can detect the

confidential data and violate the secure communications. The former problem has been partially addressed by adopting transmit antenna selection (TAS) scheme to reduce the power consumption and amount of signal processing [6]. However, in [7], it was proved that TAS is not an optimal approach in terms of secrecy performance. The latter problem has been investigated by [8], where an approach called artificial fast fading (AFF) is used to randomize the received signal at eavesdroppers and prevent them from capturing any confidential data. Nevertheless, the first problem of TBF scheme holds for AFF approach due to the transmission from all of the available transmit antennas.

In this paper, we propose a generalized selection transmission scheme with randomized beamforming (RBF/GST) to address both of the problems of TBF simultaneously. With GST, instead of choosing all the available antennas for beamforming, provided by the possession of perfect CSI of the main channel at the transmitter, only a subset of antennas are chosen for transmission (a subset of Q transmit antennas with strongest fading channel gains out of N total transmit antennas). Thus, GST reduces the amount of signal processing and power consumption to a reasonable level. Besides, RBF provides robust secure transmission against intelligent eavesdroppers. Assuming a passive eavesdropping scenario, where only the statistical CSI of the eavesdropper's channel is available to the transmitter [9], we first derive closed-form expressions for the exact and asymptotic secrecy outage probabilities with GST and RBF/GST schemes. Our asymptotic results reveal that GST achieves the same secrecy outage diversity gain as TBF in MISO wiretap channels. We then consider an active eavesdropping scenario, where the perfect CSI of the eavesdropper's channel is known at the transmitter [9] (this can be considered as a cellular network case where Eve is another user in the coverage area of the cellular base station and its CSI can be known at the base station) and we derive the expression of the ergodic secrecy rate of GST and RBF/GST under the assumption of active eavesdropping. These results indicate that RBF/GST outperforms GST in terms of ergodic secrecy rate performance and can significantly enhance the security in MISO wiretap channel. Finally, we show that by reducing the number of antennas for transmission to a certain level, the secrecy performance of RBF/GST is not considerably affected.

II. ALGORITHM DESCRIPTION

This section presents GST and RBF/GST algorithms for delivering secure communications in MISO wiretap channels. We first present the studied system model and then delve into the details of GST and RBF/GST techniques.

A. SYSTEM MODEL

Consider a MISO wiretap channel in which the transmitter (Alice) is equipped with N antennas, whereas the legitimate receiver (Bob) and an eavesdropper (Eve) are equipped with a single antenna. We focus on quasi-static fading channels with independent identically distributed (i.i.d.) block Rayleigh fading in the main channel from Alice to Bob, and in the wiretap channel from Alice to Eve.

B. GENERALIZED SELECTION TRANSMISSION (GST)

This subsection describes the signal model of the GST scheme. Here, we consider that Bob feedbacks the perfect CSI of the main channel to Alice. With the availability of CSI of the main channel, Alice selects $Q (1 \leq Q \leq N)$ transmit antennas among N antennas that maximize the output signal to noise ratio (SNR) at Bob. Based on this selection scheme, Alice first ranks the transmit antennas in terms of their instantaneous fading gain in an ascending format. We denote the complex channel coefficient from Alice's kth transmit antenna to the receive antenna of Bob as h_k, where $1 \leq k \leq N$. Let $|h_1|^2 \leq |h_2|^2 \leq \cdots \leq |h_N|^2$ be the order statistics from arranging $\left\{|h_k|^2\right\}_{k=1}^{N}$ in ascending order of magnitude. Then Alice selects the last Q variable(s) in the order statistics. We denote $\mathcal{A}$ as a set that contains the indexes of the chosen antennas. Finally, Alice beamforms the confidential data using the vector $\mathbf{w}(i) = \mathbf{h}_Q/\|\mathbf{h}_Q\|$, where $\mathbf{h}_Q = [h_1, h_2, \cdots, h_Q]^T$ denotes the main channel vector between Q selected transmit antennas at Alice and the receive antenna at Bob and $\|\cdot\|$ indicates the Euclidean norm.

In order to transmit confidential message $\mathbf{s}$, Alice encodes it into a codeword $\mathbf{x} = [x(1), \cdots, x(i), \cdots, x(m)]$, where m is the length of $\mathbf{x}$. The transmitted codeword is subject to an average power constraint $\frac{1}{m}\sum_{i=1}^{m}\mathbb{E}\left[|x(i)|^2\right] \leq P$, where $\mathbb{E}\{\cdot\}$ is the expectation operator. In the main channel, the received signal at Bob at time i is given by

$$y_M(i) = \mathbf{h}_Q^H \mathbf{w}(i)x(i) + n_M(i) = \|\mathbf{h}_Q\|x(i) + n_M(i), \quad (1)$$

where $n_M(i)$ denotes the additive white Gaussian noise (AWGN) component with zero mean and variance σ_M^2. In the wiretap channel, the received signal at Eve at time i can be written as

$$y_W(i) = \mathbf{g}_Q^H \mathbf{w}(i)x(i) + n_W(i), \quad (2)$$

and $\mathbf{g}_Q = [g_1, g_2, \cdots, g_Q]^T$ is the eavesdropper's channel vector between Q selected transmit antennas at Alice and the receive antenna at Eve, and $n_W(i)$ is the AWGN term at Eve with variance σ_W^2.

Since the selected antennas at Alice are independent of $\mathbf{g}_Q$, the Q strongest transmit antennas for Bob corresponds to a random transmit antennas for Eve.

C. RANDOMIZED BEAMFORMING WITH GENERALIZED SELECTION TRANSMISSION (RBF/GST)

As mentioned, when the main and wiretap channels are block fading, Eve can exploit some advanced blind channel estimation techniques to attain the effective CSI (the product of beamforming vector and the wiretap channel coefficients) and coherently detect the confidential data. Hence, to enhance the security of GST, we adopt a randomized beamforming transmission technique to corrupt the received signal of the eavesdropper by a time varying multiplicative noise.

The basic idea is to make $\mathbf{h}_Q^H\mathbf{w}(i)$ deterministic but $\mathbf{g}_Q^H\mathbf{w}(i)$ changes randomly in each symbol interval. As such, Eve experiences an equivalent fast fading channel which prevents the blind channel estimation.

As for designing time varying weighting coefficients, Alice selects the beamforming vector $\mathbf{w}(i) = \left[w_1(i), w_2(i), \cdots, w_Q(i)\right]^T$, where the first $Q-1$ elements of vector $\mathbf{w}(i)$ are randomly generated while the last element of the vector is determined using the constraint $\mathbf{h}_Q^H\mathbf{w}(i) = 1$. We assume that $w_k(i)$, $k = 1, \cdots, Q-1$ are i.i.d. complex Gaussian distributed random variables with zero mean and variance σ_0^2 and the last element is given by

$$w_Q(i) = \frac{1 - \sum_{k\in\mathcal{A},k=1}^{Q-1} h_k^* w_k(i)}{h_Q^*}. \tag{3}$$

With RBF/GST, the received signal at Bob is

$$y_B^{RBF}(i) = x(i) + n_M(i), \tag{4}$$

however, the received signal at Eve is given by

$$y_E^{RBF}(i) = \mathbf{g}_Q^H\mathbf{w}(i)x(i) + n_W(i) = g_E(i)x(i) + n_W(i), \tag{5}$$

where $g_E(i) \triangleq \mathbf{g}_Q^H\mathbf{w}(i)$ is the effective channel between Alice and Eve (effective wiretap channel). We note that the effect of large scale fading (path loss and shadowing) can be incorporated in the received average signal to noise ratios at Bob and Eve.

Next, we prove that the effective wiretap channel $g_E(i)$ can be modeled as a Rician fading channel.

Theorem 1: The effective wiretap channel $g_E(i)$, under the usage of Randomized Beamforming at Alice, is equivalent to a Rician fading channel with parameters $|\mu_E|$ and σ_E, where $\mu_E = \frac{g_Q^*}{h_Q^*}$ and $\sigma_E^2 = \sum_{k\in\mathcal{A},k=1}^{Q-1}\left|g_k^* - \frac{g_Q^* h_k^*}{h_Q^*}\right|^2\sigma_0^2$.

Proof: We start the proof by expanding $\mathbf{g}_Q^H\mathbf{w}(i)$ using (3). This expansion will result in

$$\begin{aligned} g_E(i) &= \sum_{k\in\mathcal{A},k=1}^{Q} g_k^*(i)w_k(i) \\ &= \frac{g_Q^*}{h_Q^*}\left(1 - \sum_{k\in\mathcal{A},k=1}^{Q-1} h_k^*(i)w_k(i)\right) + \sum_{k\in\mathcal{A},k=1}^{Q-1} g_k^*(i)w_k(i) \\ &= \frac{g_Q^*}{h_Q^*} + \sum_{k\in\mathcal{A},k=1}^{Q-1}\left(g_k^* - \frac{g_Q^*}{h_Q^*}h_k^*\right)w_k(i). \end{aligned} \tag{6}$$

We note that $w_k(i)$ are i.i.d complex Gaussian random variables. Thus, based on (6), one can easily show that $g_E(i)$ is a complex Gaussian random variable with mean $\mu_E = \frac{g_Q^*}{h_Q^*}$ and variance $\sigma_E^2 = \sum_{k\in\mathcal{A},k=1}^{Q-1}\left|g_k^* - \frac{g_Q^* h_k^*}{h_Q^*}\right|^2\sigma_0^2$. This further implies that the envelope of $g_E(i)$ follows a Rician distribution with parameters $|\mu_E|$ and σ_E. □

Theorem 1 suggests that over each fading block of the original channels $\mathbf{h}_Q$ and $\mathbf{g}_Q$, the effective wiretap channel $g_E(i)$ is a Rician fading channel. The introduced fast fading considerably degrades the channel estimation performance of Eve and prevents coherent detection of confidential data.

Finally, since $\mathbf{h}_Q$ is a block fading channel, due to the inversion behavior of the RBF/GST weighting vector as indicated in (3), the average transmit power of Alice can be extremely large. To resolve this issue, Alice chooses $|h_Q| = \max\left\{|h_k|\right\}_{k=1}^N$, i.e., choose the antenna with the largest fading gain as h_Q in (3).

III. SECRECY PERFORMANCE

This section characterizes the secrecy performances of the GST and RBF/GST beamforming schemes under the passive and active eavesdropping scenarios. We first consider a passive eavesdropper and assume that only the statistical CSI of the eavesdropper's channel is known at Alice. In such a scenario, we adopt the secrecy outage probability as the main performance measure to quantify the secrecy performances of GST and RBF/GST. Moreover, we provide asymptotic analysis for GST and show that this scheme achieves the same secrecy diversity gain as TBF. We then study GST and RBF/GST schemes for the active eavesdropping scenario and adopt ergodic secrecy rate to quantify the secrecy performances of the mentioned schemes.

A. SECRECY PERFORMANCE OF GST

1) PASSIVE EAVESDROPPING SCENARIO

In this section, we derive the asymptotic and exact secrecy outage probabilities of GST in closed form for the passive eavesdropping scenario. To this end, we first present the statistics of the instantaneous received signal to noise ratios (SNR) at Bob and Eve. The instantaneous SNR at Bob with GST is $\gamma_M = \overline{\gamma}_M\|\mathbf{h}_Q^H\mathbf{w}(i)\|^2 = \overline{\gamma}_M\|\mathbf{h}_Q\|^2$, with $\overline{\gamma}_M = P/\sigma_M^2$. Likewise, the instantaneous received SNR at Eve is $\gamma_W = \overline{\gamma}_W\|\mathbf{g}_Q^H\mathbf{w}(i)\|^2$, where $\overline{\gamma}_W = P/\sigma_W^2$. The cumulative distribution function (CDF) of γ_M can be derived as [10]

$$F_{\gamma_M}(z) = \epsilon_0 + \sum_{k=1}^{Q}\epsilon_k\frac{z^{(k-1)}e^{\frac{-z}{\overline{\gamma}_M}}}{\Gamma(k)} + \sum_{k=Q+1}^{N}\epsilon_k e^{\frac{-kz}{Q\overline{\gamma}_M}}, \tag{7}$$

where $\Gamma(\cdot)$ stands for the Gamma function and ϵ_k is

$$\epsilon_k = \begin{cases} 1 & k = 0 \\ \overline{\gamma}_M^{1-k}\Big[-1 + \sum_{\ell=Q+1}^{N}(-1)^{\ell-k} \\ \quad\times\frac{\binom{N}{N-\ell}\binom{\ell-1}{\ell-Q-1}}{\left(\frac{\ell}{Q}-1\right)^{Q-k+1}}\Big] & 1 \le k < Q \\ -\overline{\gamma}_M^{1-Q}\binom{N}{N-Q} & k = Q \\ \frac{(-1)^k\binom{N}{N-Q}\binom{k-1}{k-Q-1}}{\left(\frac{k}{Q}-1\right)^Q} & Q < k \le N. \end{cases} \tag{8}$$

It can be proved that γ_W is exponentially distributed due to the fact that the beamforming vector at Alice is independent

from eavesdropper's channel [5], yielding

$$F_{\gamma_W}(z) = 1 - e^{\frac{-z}{\overline{\gamma}_W}}. \tag{9}$$

The instantaneous secrecy rate of GST is given by $R_{Sec} = [R_M - R_W]^+$, where $[x]^+$ denotes $\max\{0, x\}$, $R_M = \log_2(1+\gamma_M)$ is the instantaneous rate of the main channel and $R_W = \log_2(1+\gamma_W)$ stands for the instantaneous rate of the wiretap channel. Based on the instantaneous secrecy rate, we define the outage probability of the secrecy rate R_S as

$$\begin{aligned} P_{out}(R_S) &= \Pr\{R_{Sec} < R_S\} \\ &= \int_0^\infty F_{\gamma_M}\left[2^{R_S}(1+z)-1\right] f_{\gamma_W}(z)\, dz, \end{aligned} \tag{10}$$

where $f_{\gamma_W}(\cdot)$ denote the probability density function (pdf) of γ_W and it is obtained by taking the first derivative of F_{γ_W} in (9). Substituting this pdf and (7) into (10) and solving the integral, we derive the secrecy outage probability of GST in closed-form as

$$P_{out}(R_S) = 1 + \theta_1 + \theta_2, \tag{11}$$

where θ_1 and θ_2 are given by

$$\theta_1 = \sum_{k=1}^{Q} \frac{\epsilon_k}{\overline{\gamma}_W \Gamma(k)} \sum_{j=0}^{k-1} \frac{\xi \Gamma(j+1)}{\left(\frac{1}{\overline{\gamma}_W} + \frac{2^{R_S}}{\overline{\gamma}_M}\right)^{(j+1)}}, \tag{12}$$

$$\theta_2 = \sum_{k=Q+1}^{N} \epsilon_k \frac{e^{-\frac{\left(2^{R_S}-1\right)k}{Q\overline{\gamma}_M}}}{\overline{\gamma}_W} \left(\frac{1}{\overline{\gamma}_W} + \frac{2^{R_S}k}{Q\overline{\gamma}_M}\right)^{-1}. \tag{13}$$

In (12), we define ξ as

$$\xi = \binom{k-1}{j} \left(2^{R_S}-1\right)^{k-1} e^{-\frac{\left(2^{R_S}-1\right)}{\overline{\gamma}_M}} \left(\frac{2^{R_S}}{2^{R_S}-1}\right)^{j}. \tag{14}$$

Notice that, when $N = Q$, (11) reduces to

$$P_{out}(R_S) = 1 - \sum_{k=1}^{N} \sum_{j=0}^{k-1} \frac{\xi \Gamma(j+1)}{\overline{\gamma}_M^{(k-1)} \overline{\gamma}_W \Gamma(k) \left(\frac{1}{\overline{\gamma}_W} + \frac{2^{R_S}}{\overline{\gamma}_M}\right)^{(j+1)}}, \tag{15}$$

which is the same result as that in [7, eq. (12)].

Since in the high SNR regime of the main channel (i.e., $\gamma_B \to \infty$), the secrecy outage diversity gain and the secrecy outage SNR gain govern the secrecy outage probability, we derive an asymptotic secrecy outage expression. To do so, we proceed by deriving the first order expansion of $F_{\gamma_M}(z)$ in (7). This can be derived as $F_{\gamma_M}(z) \approx 1/\left(Q^{(N-Q)}Q!\right)\left(z/\overline{\gamma}_M\right)^N$. Accordingly, we find the asymptotic secrecy outage probability as

$$P_{out}^{\infty}(R_S) = \left(\Delta \overline{\gamma}_M\right)^{-G_D}, \tag{16}$$

where $G_D = N$ is the secrecy outage diversity gain and Δ is the secrecy outage SNR gain. In (16), Δ is given by

$$\Delta = \left[\sum_{u=0}^{N} \binom{N}{u} \frac{2^{uR_S}\left(2^{R_S}-1\right)^{N-u} u! \overline{\gamma}_W^u}{Q^{(N-Q)}Q!}\right]^{-\frac{1}{N}}. \tag{17}$$

According to (16), the following points provide insights into the use of GST in the main channel. (I) The secrecy outage probability approaches zero as $\overline{\gamma}_M$ approaches infinity. (II) The maximum secrecy outage diversity gain of N is achieved and thus GST has the same secrecy outage diversity gain as TBF. (III) The secrecy outage diversity gain is not affected by the choice of Q. The impact of Q is only reflected in the secrecy outage SNR gain.

2) ACTIVE EAVESDROPPING SCENARIO

When the CSI of the wiretap channel is available at Alice, ergodic secrecy rate should be considered as the secrecy performance metric [9]. To this end, we derive the ergodic secrecy rate of GST scheme as

$$\overline{R}_{Sec}^{GST} = \left\{I(y_B; x) - I(y_E; x)\right\}^+, \tag{18}$$

where $I(y_B; x)$ and $I(y_E; x)$ represent the average mutual information of the main channel and wiretap channel, respectively. Based on (1), $I(y_B; x)$ can be written as

$$\begin{aligned} I(y_B; x) &= \mathbb{E}\left\{\log_2(1+\gamma_M)\right\} \\ &= \frac{1}{\ln 2} \int_0^\infty \ln(1+\gamma_M) f(\gamma_M)\, d\gamma_M, \end{aligned} \tag{19}$$

where $f(\gamma_M)$ is the pdf of γ_M and is derived by taking the first derivative of (7). Substituting this pdf into (19) and solving the integral, we calculate the ergodic rate of the main channel as

$$\begin{aligned} I(y_B; x) = \frac{1}{\ln 2} \Bigg\{ &- \sum_{k=1}^{Q} \epsilon_k \overline{\gamma}_M^{(k-1)} e^{\frac{1}{\overline{\gamma}_M}} E_k\left(\frac{1}{\overline{\gamma}_M}\right) \\ &- \sum_{k=Q+1}^{N} \epsilon_k e^{\frac{k}{Q\overline{\gamma}_M}} E_1\left(\frac{k}{Q\overline{\gamma}_M}\right) \Bigg\}, \end{aligned} \tag{20}$$

where $E_k(\cdot)$ is the generalized exponential integral function. Similarly, the average mutual information of the wiretap channel under GST scheme is given by

$$I(y_E; x) = \frac{1}{\ln 2} e^{\frac{1}{\overline{\gamma}_W}} E_1\left(\frac{1}{\overline{\gamma}_W}\right). \tag{21}$$

Hence the ergodic secrecy rate of GST is given by substituting (20) and (21) into (18).

B. SECRECY PERFORMANCE OF RBF/GST

1) PASSIVE EAVESDROPPING SCENARIO

Considering a passive eavesdropping scenario, the secrecy performance of RBF/GST is studied with respect to the secrecy outage probability. To this end, we first quantify the statistics of the received SNRs at Bob and Eve under the usage of RBF/GST at Alice. We then derive the secrecy outage probability of RBF/GST beamformer scheme. Based on (4), the received SNR at Bob with RBF/GST is $\gamma_M^{RBF} = \overline{\gamma}_M$. On the other hand, (5) implies that the received SNR at Eve with RBF/GST is $\gamma_W^{RBF} = \overline{\gamma}_W |g_E(i)|^2$. As mentioned, the envelope of $g_E(i)$ follows a Rician distribution

with parameters $|\mu_E|$ and σ_E and its CDF is given by

$$F_{|g_E|}(z) = 1 - Q_1\left(\frac{|\mu_E|}{\sigma_E}, \frac{z}{\sigma_E}\right), \tag{22}$$

where $Q_1(\cdot,\cdot)$ is the Marcum Q-function and is given by [11]

$$Q_1(a,b) = \int_b^\infty x \exp\left(-\frac{x^2+a^2}{2}\right) I_0(ax)\, dx, \tag{23}$$

where $I_0(x)$ is the Modified Bessel function of the first kind. Therefore, $|g_E(i)|^2$ has the following CDF

$$F_{|g_E|^2}(z) = 1 - Q_1\left(\frac{|\mu_E|}{\sigma_E}, \frac{\sqrt{z}}{\sigma_E}\right), \tag{24}$$

Thus, the CDFs of γ_M^{RBF} and γ_W^{RBF} are derived as

$$F_{\gamma_M^{RBF}}(z) = u\left(z - \overline{\gamma}_M\right), \tag{25}$$

$$F_{\gamma_W^{RBF}}(z) = 1 - Q_1\left(\frac{|\mu_E|}{\sigma_E}, \frac{1}{\sigma_E}\sqrt{\frac{z}{\overline{\gamma}_W}}\right), \tag{26}$$

where $u(\cdot)$ is the unit step function. Now, we are ready to derive the secrecy outage probability of RBF/GST. To this end, we first note that

$$\overline{P}_{out}(R_S) = \mathbb{E}_{\mathbf{h_Q},\mathbf{g_Q}}\left\{P_{out}(R_S) \,\middle|\, \mathbf{h_Q}, \mathbf{g_Q}\right\}. \tag{27}$$

Hence, for each realization of $\mathbf{h_Q}$ and $\mathbf{g_Q}$, $P_{out}\left(R_S\right)$ can be derived using (10). Substituting (25) into (10), we can write

$$\begin{aligned} P_{out}(R_S) &= \int_0^\infty u\left[2^{R_S}(1+z) - 1 - \overline{\gamma}_M\right] f_{\gamma_W^{RBF}}(z)\, dz \\ &= \int_{2^{-R_S}(1+\overline{\gamma}_M)-1}^\infty f_{\gamma_W^{RBF}}(z)\, dz \\ &= 1 - F_{\gamma_W^{RBF}}\left(2^{-R_S}(1+\overline{\gamma}_M) - 1\right) \\ &= Q_1\left(\frac{|\mu_E|}{\sigma_E}, \frac{1}{\sigma_E}\sqrt{\frac{2^{-R_S}(1+\overline{\gamma}_M)-1}{\overline{\gamma}_W}}\right). \end{aligned} \tag{28}$$

As can be seen from (28), the secrecy outage probability of RBF/GST depends on the design parameter σ_0, the variance of the randomizing vector elements, through σ_E. Since the function $Q_1(\cdot,\cdot)$ is an increasing function in σ_E and $\sigma_E \propto \sigma_0$, lower values of σ_0 implies in a lower values of secrecy outage probability and this, in turn, implies in a better secrecy performance. Finally, averaging (28) over all the realizations of $\mathbf{h_Q}$ and $\mathbf{g_Q}$ gives $\overline{P}_{out}\left(R_S\right)$. Based on (27), we are able to calculate other secrecy performance metrics. For example, the probability of positive secrecy rate is given by $\overline{\Pr}\,(C_S > 0) = \Pr\left(\gamma_M^{RBF} > \gamma_W^{RBF}\right) = 1 - \overline{P}_{out}(0)$.

Finally, we observe that the work in [8] does neither perform GST nor does it consider a passive eavesdropping scenario. Therefore, the secrecy outage probability performance of RBF/GST is not shown in this work.

2) ACTIVE EAVESDROPPING SCENARIO

In order to derive the ergodic secrecy rate, we first note that if we use (4) as our model for the received signal at Bob from Alice, the ergodic secrecy rate is given by the result presented in [8]. Note that by using (4) as the received signal model at Bob, the received signal does not benefit from the diversity gain offered by the multiple antenna array transmission and results into a poor secrecy rate performance as shown in Section IV. Hence, we rearrange (3) as

$$w_Q(i) = \frac{\|\mathbf{h_Q}\| - \sum_{k\in\mathcal{A},k=1}^{Q-1} h_k^* w_k(i)}{h_Q^*}. \tag{29}$$

which results into a signal model as (1). Clearly, (1) benefits from the diversity gain of the multiple antenna transmission and results in a better secrecy performance. Under the usage of (29), $g_E(i)$ in (5) will be distributed as $g_E(i) \sim \mathcal{CN}\left(\mu_E, \sigma_E^2\right)$, where $\mu_E = \frac{g_Q^*}{h_Q^*}\|\mathbf{h}_Q\|$ and $\sigma_E^2 = \sum_{k\in\mathcal{A},k=1}^{Q-1}\left|g_k^* - \frac{g_Q^* h_k^*}{h_Q^*}\right|^2 \sigma_0^2$. Now, the ergodic secrecy capacity of RBF/GST is given by

$$\overline{R}_{Sec}^{RBF} = \left\{I(y_B;x) - I\left(y_E^{RBF};x\right)\right\}^+, \tag{30}$$

where $I(y_B;x)$ is given by (20) and $I\left(y_E^{RBF};x\right)$ is

$$I\left(y_E^{RBF};x\right) = \mathbb{E}_{\mathbf{h}_Q,\mathbf{g}_Q}\left\{h\left(y_E^{RBF}\right) - h\left(y_E^{RBF}|x\right)\middle|\mathbf{h_Q},\mathbf{g_Q}\right\}, \tag{31}$$

where $h(\cdot)$ is the differential entropy. Based on [8, eqs. (28) and (30)], when x is Gaussian distributed ($x \sim \mathcal{CN}(0,P)$), $h\left(y_E^{RBF}\right)$ and $h\left(y_E^{RBF}|x\right)$ are found respectively as

$$h(y_E^{RBF}) = -2\pi\int_0^\infty \log_2 P_y(\alpha_y) P_y(\alpha_y)\alpha_y\, d\alpha_y, \tag{32}$$

$$h\left(y_E^{RBF}|x\right) = \log_2\left(\pi e \sigma_W^2\right) + \frac{1}{\ln 2} e^{\frac{1}{\beta}} E_1\left(\frac{1}{\beta}\right), \tag{33}$$

where $\beta = \sigma_E^2\overline{\gamma}_W$, $\alpha_y = |y_E^{RBF}|$ and $P_y(y)$ is

$$\begin{aligned} P_y(y) = \int_0^\infty &\frac{2\alpha}{\pi\sigma_W^2\sigma_E^2\left(\alpha^2\overline{\gamma}_W+1\right)} I_0\left(\frac{2\alpha\alpha_\mu}{\sigma_E^2}\right) \\ &\times \exp\left(-\frac{|y|^2}{\left(\alpha^2\overline{\gamma}_W+1\right)\sigma_W^2} - \frac{\alpha^2+\alpha_\mu^2}{\sigma_E^2}\right) d\alpha, \end{aligned} \tag{34}$$

where $I_0(\cdot)$ is the zero order modified Bessel function of the first kind, $\alpha = |g_E|$ and $\alpha_\mu = |\mu_E|$. Finally, the ergodic secrecy rate of RBF/GST is given by subtracting (31) from (20).

IV. NUMERICAL RESULTS

In this section, simulation results are presented to evaluate the secrecy performances of the GST and RBF/GST. In the simulations, the secrecy outage probability and ergodic secrecy rate of GST and RBF/GST are illustrated. The secrecy outage

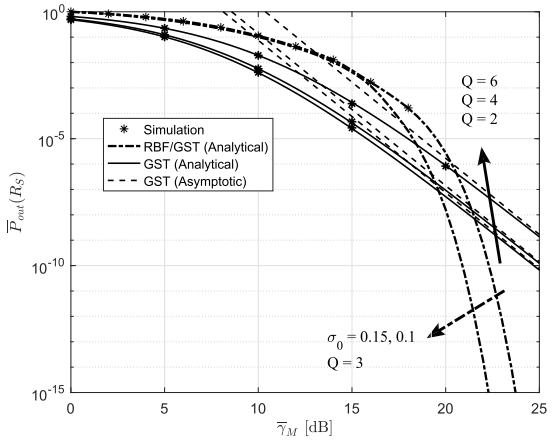

FIGURE 1. Secrecy outage probability performance of GST and RBF/GST versus $\overline{\gamma}_M$ for $\overline{\gamma}_W = 5$ dB, $R_S = 1$ and $N = 6$.

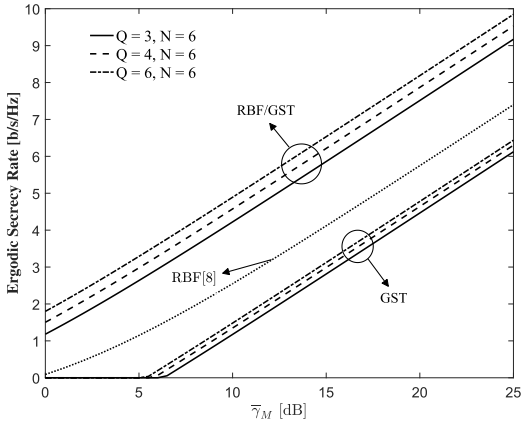

FIGURE 2. Comparison of the ergodic secrecy rate between RBF/GST and GST versus $\overline{\gamma}_M$ for $\overline{\gamma}_W = 15$ dB and $\sigma_0 = 1$.

probability and ergodic secrecy rate of RBF/GST is obtained by averaging 1000 Monte Carlo simulations.

Figure 1 plots the secrecy outage probability of GST and RBF/GST versus $\overline{\gamma}_M$ for $\overline{\gamma}_W = 5$ dB, $R_S = 1$ and $N = 6$. From the figure, we see that the asymptotic secrecy outage probability obtained from (16) accurately predicts the secrecy outage diversity and SNR gains. We also observe that the secrecy outage probability of GST and RBF/GST given in (11) and (28) are in precise agreement with the Monte Carlo simulations marked with '$*$'. Moreover, we observe that increasing Q in GST implies in a better secrecy performance. However, the secrecy performance of GST when not all the N antennas are used, is not considerably worse than the case where all N antennas are exploited. Specifically, there is approximately 0.3 dB difference in secrecy performance of GST when $Q = 4$ and $Q = N = 6$. Additionally, we see that after a certain value for $\overline{\gamma}_M$, RBF/GST can outperform GST. More importantly, we observe that with GST, even when all of the antennas are used at Alice, i.e., $Q = N = 6$, the secrecy performance is still worse than that of with RBF/GST and $Q = 3$. Thus, RBF/GST can effectively improve secrecy performance in MISO wiretap channels with lower amount of signal processing and power consumption compared to TBF. Additionally, we observe that the decrease of σ_0 results in a better secrecy outage performance of RBF/GST due to the fact that $Q_1(\cdot, \cdot)$ in (28) is an increasing function in σ_0.

Figure 2 compares the ergodic secrecy rate of RBF/GST with that of GST versus $\overline{\gamma}_M$ for different Q, $\overline{\gamma}_W = 15$ dB and $\sigma_0 = 1$. We first observe that RBF/GST outperforms GST in terms of ergodic secrecy rate performance. We also note that ergodic secrecy rate increases with increasing Q. We observe that the difference between the ergodic secrecy rate with $Q = N = 6$ and $Q = 4, N = 6$ is not considerable. Thus, by decreasing Q to a certain number, which in turn reduces the amount of signal processing and power consumption, the ergodic secrecy rate is not considerably affected. Hence, RBF/GST can provide higher secrecy than GST with a reasonable amount of signal processing and power consumption. Moreover, for the sake of comparison, we plot the ergodic secrecy rate of RBF studied in [8] with $Q = N = 6$. We observe that the proposed RBF/GST outperforms this approach and implies in a better secrecy performance.

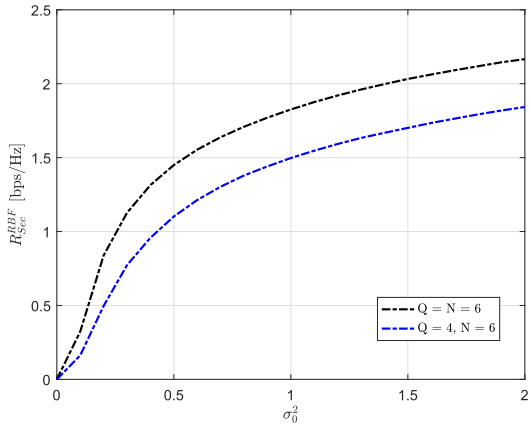

FIGURE 3. Comparison of the ergodic secrecy rate of RBF/GST for $\overline{\gamma}_M = 0$ dB and $\overline{\gamma}_W = 15$ dB versus σ_0.

Finally, Figure 3 demonstrates the effect of σ_0 on the ergodic secrecy rate of RBF/GST for different number of active antennas Q. We observe that the increase in σ_0 results in a better ergodic secrecy rate. This is on the contrary to the secrecy outage results due to the fact that for the case of secrecy outage, increasing σ_0 improves the received SNR at Eve ((28) is an increasing function in σ_0) and results in a worse secrecy outage performance. However, the ergodic rate of Eve under usage of RBF/GST given in (31) is a decreasing function in σ_0 and hence, increasing σ_0 always implies in a better ergodic secrecy rate performance.

V. CONCLUSIONS

We proposed RBF/GST to enhance security performance in block fading MISO wiretap channels. We examined the secrecy performances of GST and RBF/GST with respect to

secrecy outage probability and ergodic secrecy rate performance metrics. Our results indicated that GST achieves the same maximum secrecy outage diversity gain as TBF. Moreover, the results indicated that RBF/GST outperforms GST and results in a better secrecy performance. Furthermore, we observed that the secrecy performance of RBF/GST can be improved by carefully choosing the design parameters of the randomizing beamformer. Finally, we conclude that that RBF/GST achieves better security performance with lower power consumption and amount of signal processing compared to TBF.

REFERENCES

[1] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[2] C. Jeong, I.-M. Kim, and D. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jan. 2012.

[3] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 2471–2475.

[4] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 2466–2470.

[5] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 704–716, Apr. 2012.

[6] 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, Jun. 2012.

[7] N. S. Ferdinand, D. B. da Costa, A. L. F. de Almeida, and M. Latva-Aho, "Secrecy outage performance of MISO wiretap channels with outdated CSI," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2014, pp. 789–793.

[8] H. M. Wang, T. Zheng, and X. G. Xia, "Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 94–106, Jan. 2015.

[9] A. Chorti, S. M. Perlaza, Z. Han, and H. V. Poor, "Physical layer security in wireless networks with passive and active eavesdroppers," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2012, pp. 4868–4873.

[10] X. Cai and G. B. Giannakis, "Performance analysis of combined transmit selection diversity and receive generalized selection combining in Rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 3, no. 6, pp. 1980–1983, Nov. 2004.

[11] D. Morales-Jimenez, F. J. Lopez-Martinez, E. Martos-Naya, J. F. Paris, and A. Lozano, "Connections between the generalized Marcum Q-function and a class of hypergeometric functions," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1077–1082, Feb. 2014.

MORTEZA SOLTANI was born in Mashhad, Iran, in 1991. He received the B.S. degree in electrical engineering from the Ferdowsi University of Mashhad, Mashhad, Iran, in 2013, and the M.S. degree in electrical engineering from Istanbul Medipol University, Istanbul, Turkey, in 2013. He is currently pursuing the Ph.D. degree in electrical engineering with the Department of Electrical and Computer Engineering, University of Idaho, Moscow, ID, USA.

His research areas span a wide range of topics in wireless communications and networking, including physical layer security, cryptography, information theory, performance limits of communications at low and high power regime, multiple input multiple output communication systems, cognitive radio networks, and visible light communication.

HÜSEYIN ARSLAN received the B.S. degree from Middle East Technical University, Ankara, Turkey, in 1992; and the M.S. and Ph.D. degrees from Southern Methodist University, Dallas, TX, USA, in 1994 and 1998, respectively. From 1998 to 2002, he was with the research group of Ericsson Inc., NC, USA, where he was involved with several projects related to 2G and 3G wireless communication systems. From 2002 to 2013, he was with the Electrical Engineering Department, University of South Florida, Tampa, FL, USA. Since 2013, he has been with Istanbul Medipol University. He was a part time Consultant for various companies and institutions, including Anritsu Company, Savronik Inc., and The Scientific and Technological Research Council of Turkey.

His research interests are related to advanced signal processing techniques at the physical and medium access layers, with cross-layer design for networking adaptivity and quality of service control. He is interested in many forms of wireless technologies including cellular radio, wireless PAN/LAN/MANs, fixed wireless access, aeronautical networks, underwater networks, *in vivo* networks, and wireless sensors networks. His current research interests are on physical layer security, signal intelligence, cognitive radio, small cells, powerline communications, smart grid, UWB, multi-carrier wireless technologies, dynamic spectrum access, co-existence issues on heterogeneous networks, aeronautical (High Altitude Platform) communications, *in vivo* channel modeling and system design, and underwater acoustic communications. He has served as the technical program committee chair, a technical program committee member, a session and symposium organizer, and the workshop chair of several IEEE conferences. He has served eight years as a member on the editorial board for the *Wireless Communication and Mobile Computing Journal* (Wiley). He is currently a member on the Editorial Board for the IEEE TRANSACTIONS ON COMMUNICATIONS, the *Physical Communication Journal* (Elsevier), and the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS.