Proceedings Paper:
Romero-Zurita, N, Ghogho, M, McLernon, D et al. (2015) Can Bob enhance the security of the multiple antenna wiretap channel? In: 2015 IEEE International Conference on Communication Workshop, ICCW 2015. IEEE International Conference on Communications, 08-12 Jun 2015, London. , pp. 447-452. ISBN: 9781467363051.

https://doi.org/10.1109/ICCW.2015.7247220

Can Bob Enhance the Security of the Multiple Antenna Wiretap Channel?

Nabil Romero-Zurita*†, Mounir Ghogho*‡, Des McLernon*, Ananthram Swami§
*School of Electronic and Electrical Engineering, University of Leeds, Leeds, UK.
†Cambridge Silicon Radio Ltd., Cambridge, UK.
‡International University of Rabat, Morocco.
§US Army Research Lab, Adelphi, MD, USA.
Email: leonabil@ieee.org, m.ghogho@leeds.ac.uk, d.c.mclernon@leeds.ac.uk, a.swami@ieee.org

***Abstract*—We address the physical layer security question of whether a multiple antenna receiver can enhance the secrecy rate of the multiple-input multiple-output wiretap channel by transmitting artificial noise from some of its antennas to jam a multiple antenna eavesdropper. To answer this question we use a QoS-MMSE approach to formulate a global constrained optimisation problem that is efficiently solved after approximating it by a semidefinite program. Results suggest that an improvement in secrecy rate is possible by transmitting artificial noise from an appropriately chosen number of the receiver's antennas. We introduce two antenna configuration selection strategies to reduce system complexity and obtain the best secrecy performance.**

***Index Terms*—Artificial noise, precoding, secrecy rate, multiple antennas, physical layer security, wireless secrecy, semidefinite programming.**

I. Introduction

In this paper we study physical (PHY) layer approaches to improve security in wireless systems, without relying on upper-layer encryption to tackle the intrinsic vulnerabilities arising from the broadcast nature of the wireless channel. We address security in the multiple antenna wiretap channel; specifically, we investigate how the transmission of artificial noise (AN) by the intended receiver can improve the overall security of the system.

There has been a remarkable increase in multiple antenna signal processing approaches attempting to secure wireless networks at the PHY-layer [1]. Optimal transmission strategies for the multiple-input single-output (MISO) case have been widely studied [2], while the multiple-input multiple-output (MIMO) case has not received as much attention mostly due to its complexity. The MIMO wiretap channel, also known as the multiple-input multiple-output multiple-antenna eavesdropper, was first studied in [3] and [4] where suboptimal secure transmission strategies were introduced. A minimum mean square error (MMSE) approach was used in [5]. More recently, in [6] the transmission solution for the MIMO wiretap channel was characterized for a full-rank input covariance matrix under an average power constraint. The general transmit solution that achieves the MIMO wiretap channel's secrecy capacity (C_S) through alternating optimisation was introduced in [7]. All these papers have shown that generating AN from the transmitter is counter-effective to enhance the secrecy rate in the presence of one fully determined multiple antenna active eavesdropper; i.e., its channel state information (CSI) is available at the transmitter.

The aforementioned studies consider the transmitter as the unique source of the jamming signal and not a different AN source to potentially enhance the secrecy rate of the system. This idea, originally proposed by Goel and Negi in [8], consists of using *'cooperative jammers'* as an alternative to generate AN [9]–[11]. However, cooperative jamming introduces important confidentiality issues arising from relying on third-party cooperative nodes that might behave maliciously [12]. Secure cooperation presents a technical challenge by requiring both synchronisation between the transmission/jamming parties and the availability of global CSI at all entities [13]. Moreover, in a practical network, the AN generated from the cooperative jammers may interfere the intended receiver due to the error-prone available CSI.

In contrast to cooperative jamming, in this paper we address the question of whether the transmission of AN from the receiver, known in the secrecy literature as *Bob*, can enhance security in multiple antenna systems. This idea has recently been suggested to secure a single antenna device's transmission to a two-antenna receiver in the presence of a single antenna eavesdropper [14]. We took this idea further in [15] by considering that both the transmitter and the receiver can jointly transmit AN to confuse a single antenna eavesdropper. Here, we address the general case of the MIMO wiretap channel and study the security performance of the joint AN transmission when the eavesdropper is equipped with multiple antennas. Our objective is to understand whether, and under what conditions, joint AN generation can enhance the MIMO wiretap channel's secrecy capacity introduced in [7]. With this objective, we formulate an optimisation problem that seeks the transmission covariance matrices that maximise the secrecy rate (R_S) in a globally power constrained system. Our results suggest that a remarkable improvement in the R_S can be achieved by generating AN solely from the receiver. This strategy becomes particularly useful when the eavesdropper's channel is better than the main link's counterpart. This scenario can occur when the eavesdropper is equipped with a large number of antennas, when it experiences good channel fading conditions or when it is located close to the transmitter. Moreover, this technique, compared to cooperative

jamming, does not require an external party to generate the AN; therefore, it reduces overall system complexity without compromising confidentiality.

The security improvement resulting from AN broadcasting by Bob is obtained by judiciously choosing the subset of Bob's antennas to transmit AN. This raises questions about the optimal receiver antenna configuration and requires careful criteria to partition the receiver's antennas between reception and AN generation. Unfortunately, this procedure introduces a great level of complexity into the solution; hence, in this paper we devise two practical criteria to choose the best antenna configuration for the receiver.

II. System and Signal Model

Following the standard wireless secrecy model, we name the transmitter, the legitimate receiver and the eavesdropper as "Alice", "Bob" and "Eve". They are respectively equipped with $N_a \geq 2$, $N_b \geq 2$ and $N_e \geq 1$ antennas. The MIMO Alice-to-Bob and Alice-to-Eve channels are denoted by $\mathbf{H} \in \mathbb{C}^{N_a \times N_b}$ and $\mathbf{G}_a \in \mathbb{C}^{N_a \times N_e}$, respectively. We account for path-loss effect by setting $\mathbf{H} = r_{ab}^{-\frac{\alpha}{2}} \tilde{\mathbf{H}}$ and $\mathbf{G}_a = r_{ae}^{-\frac{\alpha}{2}} \tilde{\mathbf{G}}_a$ where r_{ab} and r_{ae} respectively denote the Alice-to-Bob and Alice-to-Eve distances, with $\alpha \geq 2$ being the path loss exponent, and $\tilde{\mathbf{H}} \sim \mathcal{CN}(\mathbf{0}, \sigma^2_{\tilde{H}} \mathbf{I})$ and $\tilde{\mathbf{G}}_a \sim \mathcal{CN}(\mathbf{0}, \sigma^2_{\tilde{G}_a} \mathbf{I})$ are the independent small-scale fading channels[1].

Bob receives Alice's signal and transmits AN at the same time. So, he allocates $N_r \geq 1$ antennas for receiving information and $N_n = N_b - N_r$ antennas for AN generation. We denote the *actual* Alice-to-Bob channel by $\mathbf{H}_a \in \mathbb{C}^{N_a \times N_r}$, which is a submatrix of the full channel $\mathbf{H}$ consisting of only the N_r channel vectors associated with the information-receiving antennas. Similarly, we denote the Bob-to-Eve channel by $\mathbf{G}_b \in \mathbb{C}^{N_n \times N_e}$ which also takes into account the path-loss effect due to the Bob-to-Eve distance r_{be}; i.e., $\mathbf{G}_b = r_{be}^{-\frac{\alpha}{2}} \tilde{\mathbf{G}}_b$ where $\tilde{\mathbf{G}}_b \sim \mathcal{CN}(\mathbf{0}, \sigma^2_{\tilde{G}_b} \mathbf{I})$.

Alice transmits a signal vector $\mathbf{s} \in \mathbb{C}^{N_a}$, given by $\mathbf{s} = \mathbf{w} + \boldsymbol{\eta}_a$, where $\mathbf{w}$ is the information bearing vector using an idealised Gaussian codebook with covariance matrix $\mathbf{C}_w = \mathbb{E}\{\mathbf{w}\mathbf{w}^H\}$ and $\boldsymbol{\eta}_a$ is Alice's AN vector with covariance matrix $\mathbf{C}_{\eta_a} = \mathbb{E}\{\boldsymbol{\eta}_a \boldsymbol{\eta}_a^H\}$. Likewise, Bob's AN vector is $\boldsymbol{\eta}_b \in \mathbb{C}^{N_n}$ with $\mathbf{C}_{\eta_b} = \mathbb{E}\{\boldsymbol{\eta}_b \boldsymbol{\eta}_b^H\}$. The AN transmitted by Bob is cancelled at his receiving antennas by using self-interference full duplex techniques [14], [15]. This can be understood by noting that Bob can perfectly cancel the effect of its own AN by making two reasonable assumptions: i) it has a perfect estimate of the channel between its transmitting/receiving antennas and ii) it knows exactly the AN that it broadcasts. It is worth pointing out that we assume that both legitimate transmission parties are aware of each other's transmission strategy; therefore, we let $P = \mathrm{Tr}\{\mathbf{C}_w\} + \mathrm{Tr}\{\mathbf{C}_{\eta_a}\} + \mathrm{Tr}\{\mathbf{C}_{\eta_b}\}$ denote the global transmit power. We should point out that we consider a global power constraint for the sake of fairness when comparing our system's performance against the traditional wiretap channel where only the transmitter has transmission power available (equivalent to the global power constraint).

We assume that all the transmission parties' CSI are perfectly available; therefore, the secrecy rate (in bps/Hz) is[2]

$$\mathrm{R}_S = \Big[\log_2 \det\left(\mathbf{I}_{N_b} + \mathbf{W}_1 \tilde{\mathbf{H}}_a^H \mathbf{C}_w \tilde{\mathbf{H}}_a\right) - \log_2 \det\left(\mathbf{I}_{N_e} + \mathbf{W}_2 \tilde{\mathbf{G}}_a^H \mathbf{C}_w \tilde{\mathbf{G}}_a\right)\Big]^+ \quad (1)$$

where we define

$$\mathbf{W}_1 = \left\{\tilde{\mathbf{H}}_a^H \mathbf{C}_{\eta_a} \tilde{\mathbf{H}}_a + r_{ab}^{\alpha} \sigma_b^2 \mathbf{I}_{N_r}\right\}^{-1} \quad (2)$$

$$\mathbf{W}_2 = \left\{\tilde{\mathbf{G}}_a^H \mathbf{C}_{\eta_a} \tilde{\mathbf{G}}_a + \rho^{\alpha} \tilde{\mathbf{G}}_b^H \mathbf{C}_{\eta_b} \tilde{\mathbf{G}}_b + r_{ae}^{\alpha} \sigma_e^2 \mathbf{I}_{N_e}\right\}^{-1} \quad (3)$$

with $\rho = {}^{r_{ae}}/_{r_{be}}$, and σ_b^2 and σ_e^2 are respectively the AWGN variances at the receiving antennas of Bob and Eve.

III. Optimisation Problem

We seek the information and AN (from Bob and Alice) transmission covariance matrices to maximise the secrecy rate. We consider the optimisation problem subject to a global power constraint P_{max} that can be written as follows

$$\max_{\substack{\mathbf{C}_w \succeq \mathbf{0}, \mathbf{C}_{\eta_a} \succeq \mathbf{0}, \\ \mathbf{C}_{\eta_b} \succeq \mathbf{0}}} \quad \mathrm{R}_S, \quad \text{s.t.} \;\; P \leq P_{max}. \quad (4)$$

The problem (4) is hard to solve due to the non-convex nature of the objective function in (1). Therefore, we introduce a sub-optimal approach to approximate (4) by an efficient solvable program.

A. A QoS-MMSE approach to maximise the secrecy rate

We consider an MMSE approach for Eve, which yields a tractable pathway to study the performance. Although suboptimal, this formulation brings up the advantage of providing an answer to the question posed earlier in the paper with a reasonable level of complexity. We introduce the metric $\bar{\mathrm{R}}_S$ to obtain a suboptimal but tractable version of (4), and so we approximate (1) as

$$\bar{\mathrm{R}}_S = \Big[\log_2 \det\left(\mathbf{I}_{N_r} + \mathbf{W}_1 \tilde{\mathbf{H}}_a^H \mathbf{C}_w \tilde{\mathbf{H}}_a\right) - \log_2\left(1 + \mathrm{SNR}_e\right)\Big]^+ \quad (5)$$

where

$$\mathrm{SNR}_e = \mathrm{Tr}\left\{\tilde{\mathbf{G}}_a^H \mathbf{W}_2 \tilde{\mathbf{G}}_a \mathbf{C}_w\right\} \quad (6)$$

is the signal-to-noise ratio at Eve after considering an MMSE approach; i.e., Eve recovers the signal by using an MMSE receiver beamforming vector to maximise her SNR. As in [16], we consider the worst case for security; i.e., Eve is perfectly aware of the transmission strategy given by $\mathbf{C}_w, \mathbf{C}_{\eta_a}$ and $\mathbf{C}_{\eta_b}$.

[1] $\mathbf{a} \sim \mathcal{CN}(\boldsymbol{\alpha}, \boldsymbol{\Sigma})$ means that $\mathbf{a}$ is a random vector following a complex circular Gaussian distribution with mean $\boldsymbol{\alpha}$ and covariance matrix $\boldsymbol{\Sigma}$.

[2] $[a]^+$ represents $\max\{a, 0\}$.

We now maximise $\bar{\mathrm{R}}_S$, and so we rewrite the problem in (4) for $\bar{\mathrm{R}}_S$ by introducing the slack variable β as follows

$$\max_{\substack{\mathbf{C}_w,\mathbf{C}_{\eta_a},\\ \mathbf{C}_{\eta_b},\beta}} \quad \log_2 \det\left(\mathbf{I}_{N_b}+\mathbf{W}_1\tilde{\mathbf{H}}_a^H\mathbf{C}_w\tilde{\mathbf{H}}_a\right)-\log_2(\beta) \tag{7a}$$

$$\text{s.t.} \quad \log_2(\beta)\geq \log_2\left(1+\mathrm{SNR}_e\right) \tag{7b}$$

$$\mathbf{C}_w\succeq\mathbf{0},\mathbf{C}_{\eta_a}\succeq\mathbf{0},\mathbf{C}_{\eta_b}\succeq\mathbf{0},\beta>1 \tag{7c}$$

$$P\leq P_{max}. \tag{7d}$$

The problem above is still non-convex, so we fix $\beta > 1$ to a given value. This is equivalent to introduce a Quality of Service (QoS) constraint to set the maximum admissible SNR at Eve. Therefore, the problem has to be solved iteratively to find the value of β that delivers the largest $\bar{\mathrm{R}}_S$. We use the inequality

$$\det\left(\mathbf{I}+\mathbf{\Sigma}\right)=\prod_{i=1}^{r}\left(1+\lambda_i\right)\geq 1+\mathrm{Tr}(\mathbf{\Sigma}) \tag{8}$$

where $\mathbf{\Sigma}\succeq\mathbf{0}$, $r=\mathrm{rank}(\mathbf{\Sigma})$ and λ_i denotes the i^{th} positive eigenvalue of $\mathbf{\Sigma}$. The equality in (8) holds iff $r = 1$. Finally, we arrive at the following maximisation problem

$$\max_{\substack{\mathbf{C}_w,\mathbf{C}_{\eta_a},\\ \mathbf{C}_{\eta_b},\beta}} \quad \frac{1}{\beta}\left(1+\mathrm{Tr}\left\{\mathbf{W}_1\tilde{\mathbf{H}}_a^H\mathbf{C}_w\tilde{\mathbf{H}}_a\right\}\right) \tag{9a}$$

$$\text{s.t.} \quad \mathrm{Tr}\left\{\tilde{\mathbf{G}}_a^H\mathbf{W}_2\tilde{\mathbf{G}}_a\mathbf{C}_w\right\}\leq\beta-1 \tag{9b}$$

$$\mathbf{C}_w\succeq\mathbf{0},\mathbf{C}_{\eta_a}\succeq\mathbf{0},\mathbf{C}_{\eta_b}\succeq\mathbf{0},\beta>1 \tag{9c}$$

$$P\leq P_{max} \tag{9d}$$

for a fixed value of β.

We now recast (9) as a semidefinite program (SDP) by using the Charness-Cooper transformation [17]. Therefore, we introduce the slack variable $\xi > 0$, define $\mathbf{C}_w=\frac{\tilde{\mathbf{C}}_w}{\xi}$, $\mathbf{C}_{\eta_a}=\frac{\tilde{\mathbf{C}}_{\eta_a}}{\xi}$ and $\mathbf{C}_{\eta_b}=\frac{\tilde{\mathbf{C}}_{\eta_b}}{\xi}$ and set

$$\tilde{\mathbf{H}}_a^H\tilde{\mathbf{C}}_{\eta_a}\tilde{\mathbf{H}}_a+\xi r_{ab}^{\alpha}\sigma_b^2\mathbf{I}_{N_r}=\mathbf{I}_{N_r}. \tag{10}$$

Therefore, we obtain the SDP

$$\max_{\substack{\tilde{\mathbf{C}}_w,\tilde{\mathbf{C}}_{\eta_a},\\ \tilde{\mathbf{C}}_{\eta_b},\xi}} \frac{1}{\beta}\mathrm{Tr}\left\{\tilde{\mathbf{H}}_a^H\tilde{\mathbf{C}}_w\tilde{\mathbf{H}}_a\right\} \tag{11a}$$

$$\text{s.t. } \tilde{\mathbf{H}}_a^H\tilde{\mathbf{C}}_{\eta_a}\tilde{\mathbf{H}}_a+\left(\xi r_{ab}^{\alpha}\sigma_b^2-1\right)\mathbf{I}_{N_r}\preceq\mathbf{0} \tag{11b}$$

$$\tilde{\mathbf{G}}_a^H\left[\left(\frac{\beta-1}{N_e}\right)\tilde{\mathbf{C}}_{\eta_a}-\tilde{\mathbf{C}}_w\right]\tilde{\mathbf{G}}_a+\left(\frac{\beta-1}{N_e}\right)\times$$

$$\xi r_{ae}^{\alpha}\sigma_e^2\mathbf{I}_{N_b}+\left(\frac{\beta-1}{N_e}\right)\rho_k^{\alpha}\tilde{\mathbf{G}}_b^H\tilde{\mathbf{C}}_{\eta_b}\tilde{\mathbf{G}}_b\succeq\mathbf{0} \tag{11c}$$

$$\mathrm{Tr}\left\{\tilde{\mathbf{C}}_w\right\}+\mathrm{Tr}\left\{\tilde{\mathbf{C}}_{\eta_a}\right\}+\mathrm{Tr}\left\{\tilde{\mathbf{C}}_{\eta_b}\right\}\leq\xi P_{max} \tag{11d}$$

$$\tilde{\mathbf{C}}_w\succeq\mathbf{0},\tilde{\mathbf{C}}_{\eta_a}\succeq\mathbf{0},\tilde{\mathbf{C}}_{\eta_b}\succeq\mathbf{0},\xi\geq 0 \tag{11e}$$

where the linear matrix inequalities (LMIs) (11b) and (11c) result from relaxing the equality (10) and using the definition of $\mathbf{W}_2$ (from (3)) in (11c). Finally, $\xi > 0$ is relaxed to $\xi \geq 0$ without consequence since $\xi = 0$ is not feasible for (11d).

The SDP in (11) can be conveniently solved by using solvers based on interior-point algorithms such as SeDuMi [18].

TABLE I
Bob's antenna configurations for $N_b = 3$.

Conf.	Antenna 1	Antenna 2	Antenna 3
1	RX	AN	AN
2	AN	RX	AN
3	AN	AN	RX
4	AN	RX	RX
5	RX	AN	RX
6	RX	RX	AN
7	RX	RX	RX

RX stands for a reception antenna while AN represents an AN generating antenna.

It is worth recalling that the SDP in (11) is solved for a fixed value of β. Therefore, an iterative exhaustive linear search algorithm as in [19] can be used to find the value for β that delivers the largest $\bar{\mathrm{R}}_S$.

1) Numerical Results: To illustrate the performance of the technique we consider a numerical example in which $N_a = N_b = N_e = 3$. As a result, there are $2^{N_b}-1=7$ possible antenna configurations for Bob as illustrated in Table I.

As explained in Section II, in order to determine Bob's best antenna configuration that delivers the largest $\bar{\mathrm{R}}_S$, we need to solve the SDP in (11) for each one of the $2^{N_b}-1$ possible channel configurations and then select the best one. This is effectively done in Fig. 1.a which depicts the maximum $\bar{\mathrm{R}}_S$ of the sixteen random channel realisations and the antenna configuration number (from Table I) that attains it. The figure shows that joint AN generation can enhance the security of the system compared to the MIMO secrecy capacity C_S [7] that uses all of Bob's antennas for reception. Also we see that the best antenna configuration for Bob changes across channel realisations. The power allocation depicted in Fig. 1.b suggests that broadcasting AN from Bob is useful to enhance $\bar{\mathrm{R}}_S$ while transmitting AN from Alice is not necessary.

Two main questions rise from these results: i) under what circumstances is it convenient to transmit AN from Bob? ii) what is the antenna configuration that Bob should use to achieve the best security performance? We address these two questions in the following by introducing two antenna configuration selection criteria that will not only offer answers to these two questions but also reduce substantially the complexity of the transmission technique.

IV. Bob's Antenna Configuration Criteria

Although the potential benefits of transmitting AN from Bob are now clear, analysing all of the possible $2^{N_b}-1$ antenna configurations at the receiver to maximise $\bar{\mathrm{R}}_S$ is a cumbersome task. Indeed, for each antenna configuration the SDP (11) has to be solved. Therefore, a criterion to systematically choose the best configuration is desirable. This is not a trivial task due to the trade-off between using all of Bob's antennas for reception to enhance the transmission rate in the main link, and increasing the number of Bob's antennas devoted for broadcasting a more directive AN to further jam Eve.

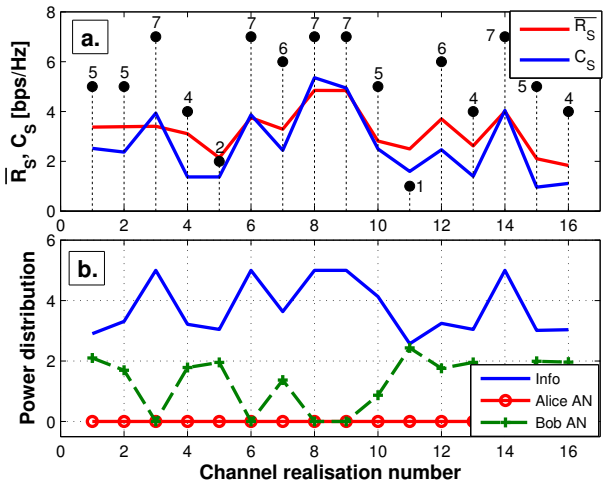

Fig. 1. Fig. a. Secrecy analysis for 16 random channel realisations and Bob's best antenna configuration for $r_{ab} = r_{ae} = r_{be} = 1$ and $N_a = N_b = N_e = 3$. The black numbered dots represent the best antenna configuration (see Table I) for each channel realisation. Fig. b. Power allocation for a global power constraint $P_{max} = 5$.

A. Degrees of Freedom Analysis

This criterion chooses the antenna configuration based on the analysis of the degrees of freedom (DoF) of the three wireless channels involved in the transmission between Alice, Bob and Eve. As pointed out in [6] and [7], the secrecy capability of the wiretap channel depends upon exploiting the DoF of $\mathbf{H}\mathbf{H}^H - \mathbf{G}_a\mathbf{G}_a^H$; indeed, the rank of the transmission covariance matrix corresponds to the number of positive eigenvalues of $\mathbf{H}\mathbf{H}^H - \mathbf{G}_a\mathbf{G}_a^H$. This implies that if $\mathbf{H}\mathbf{H}^H \preceq \mathbf{G}_a\mathbf{G}_a^H$ then achieving secrecy is not possible because the eavesdropping MIMO channel is more capable that the main channel. In this scenario, transmitting AN from Bob can deteriorate Eve's signal quality allowing a positive $\bar{\mathrm{R}}_S$. As we consider AN generation from Bob, we also take into account the analysis of the DoF of ${\mathbf{G}_b}^H\mathbf{G}_b - {\mathbf{G}_a}^H\mathbf{G}_a$ that gives the *difference* between the channels that Eve sees for receiving the AN from Bob and the information from Alice.

We analyse all the possible $k \in [1, 2^{N_b} - 1]$ antenna configurations at Bob and consider the channels $\mathbf{H}_a^k \in \mathbb{C}^{N_a \times N_r^k}$ and $\mathbf{G}_b^k \in \mathbb{C}^{N_n^k \times N_e}$ between Alice-to-Bob and Bob-to-Eve where N_r^k and N_n^k are respectively the number of Bob's antennas for reception and AN generation in the k^{th} configuration. Denote λ_i^k as the i^{th} positive eigenvalue of $\mathbf{H}_a^k{\mathbf{H}_a^k}^H - \mathbf{G}_a\mathbf{G}_a^H$ and let μ_j^k be the j^{th} positive eigenvalue of ${\mathbf{G}_b^k}^H\mathbf{G}_b^k - {\mathbf{G}_a}^H\mathbf{G}_a$. Then we form two column vectors:

$$\boldsymbol{\delta}_a^k = \left[\lambda_1^k \cdots \lambda_i^k, 0, \cdots, 0\right]^T \in \mathbb{R}^{N_t} \tag{12}$$

$$\boldsymbol{\delta}_b^k = \left[\mu_1^k \cdots \mu_j^k, 0, \cdots, 0\right]^T \in \mathbb{R}^{N_e} \tag{13}$$

which we combine into the matrix $\boldsymbol{\Delta} \in \mathbb{R}^{N_t+N_e \times 2^{N_b}-1}$

$$\boldsymbol{\Delta} = \begin{bmatrix} \boldsymbol{\delta}_a^1 & \boldsymbol{\delta}_a^2 & \cdots & \boldsymbol{\delta}_a^k & \cdots & \boldsymbol{\delta}_a^{2^{N_b}-1} \\ \alpha\boldsymbol{\delta}_b^1 & \alpha\boldsymbol{\delta}_b^2 & \cdots & \alpha\boldsymbol{\delta}_b^k & \cdots & \alpha\boldsymbol{\delta}_b^{2^{N_b}-1} \end{bmatrix} \tag{14}$$

for weight $\alpha < 1$. This parameter α allows us to weight the contribution of the eigenvalues corresponding to the difference between the AN and information received by Eve ($\boldsymbol{\delta}_b^k$) compared to those of the wiretap channel ($\boldsymbol{\delta}_a^k$). Subsequently, we perform the sum of the column vectors of the matrix $\boldsymbol{\Delta}$. This sum is now stored in a row vector $\bar{\boldsymbol{\delta}}_1$ all of whose elements have been normalised by the maximum component of $\bar{\boldsymbol{\delta}}_1$ and sorted in descending order. Vector $\bar{\boldsymbol{\delta}}_1$ effectively represents the sorted channel configurations where the first element corresponds to the antenna configuration that delivers the best performance considering the DoF analysis presented here.

B. Eigen-Transmission Analysis

The second configuration selection criterion is based on the analysis of an eigen-transmission strategy for the maximisation in (7). Again we analyse all the possible $k \in [1, 2^{N_b} - 1]$ antenna configurations at Bob; i.e., the k channels $\mathbf{H}_a^k$ and $\mathbf{G}_b^k$. Now, similar to the optimal MISO secrecy solution in [2], we obtain a beamforming vector $\mathbf{t}^k \in \mathbb{C}^{N_a}$ that corresponds to the principal eigenvector of the pencil $\left(\mathbf{I}_{N_a} + \mathbf{H}_a^k{\mathbf{H}_a^k}^H, \mathbf{I}_{N_a} + \mathbf{G}_a{\mathbf{G}_a}^H\right)$. Therefore, to simplify the problem, we effectively enforce a suboptimal rank-one transmission. We do not consider AN generation from Alice, a strategy consistent with [2]–[4], [6], [7]. Then, Bob beamforms AN over the principal eigenvector $\boldsymbol{\eta}^k \in \mathbb{C}^{N_n^k}$ associated with the largest eigenvalue of $\mathbf{G}_b^k{\mathbf{G}_b^k}^H$, considering again a rank-one transmission covariance matrix. This strategy yields the following secrecy rate

$$\tilde{\mathrm{R}}_S^k = \log_2\left(1 + \frac{\xi P_{max} r_{ab}^{-\alpha} {\mathbf{t}^k}^H \tilde{\mathbf{H}}_a^k {\tilde{\mathbf{H}}_a^k}^H \mathbf{t}^k}{\sigma_b^2}\right) - \log_2\left(1 + \frac{\xi P_{max} r_{ae}^{-\alpha} {\mathbf{t}^k}^H \tilde{\mathbf{G}}_a \tilde{\mathbf{G}}_a^H \mathbf{t}^k}{(1-\xi) P_{max} r_{be}^{-\alpha} {\boldsymbol{\eta}^k}^H \tilde{\mathbf{G}}_b^k {\tilde{\mathbf{G}}_b^k}^H \boldsymbol{\eta}^k + \sigma_e^2}\right) \tag{15}$$

where $\xi \in (0, 1]$ defines the global power distribution between Alice's transmitted information and Bob's AN. Then, we maximise $\tilde{\mathrm{R}}_S$ over ξ expressing this problem as

$$\max_{0<\xi\leq 1} \frac{\left(\sigma_b^2 + \xi P_{max} a^k\right)\left(P_{max}(1-\xi)c^k + \sigma_e^2\right)}{\sigma_b^2\left[\left(P_{max}(1-\xi)c^k + 1\right) + \xi P_{max} b^k\right]} \tag{16}$$

where we define

$$a^k = r_{ab}^{-\alpha} {\mathbf{t}^k}^H \tilde{\mathbf{H}}_a^k {\tilde{\mathbf{H}}_a^k}^H \mathbf{t}^k \tag{17}$$

$$b^k = r_{ae}^{-\alpha} {\mathbf{t}^k}^H \tilde{\mathbf{G}}_a \tilde{\mathbf{G}}_a^H \mathbf{t}^k \tag{18}$$

$$c^k = r_{be}^{-\alpha} {\boldsymbol{\eta}^k}^H \tilde{\mathbf{G}}_b^k {\tilde{\mathbf{G}}_b^k}^H \boldsymbol{\eta}^k. \tag{19}$$

The power allocation problem in (16) can be efficiently solved by linear search algorithms as in [20]. Finally, for the k^{th} configuration we store the maximum value of $\tilde{\mathrm{R}}_S^k$ in a normalised decreasing-order vector $\bar{\boldsymbol{\delta}}_2$, similarly to what we did for the normalised $\bar{\boldsymbol{\delta}}_1$. The first-element of $\bar{\boldsymbol{\delta}}_2$ effectively corresponds to the antenna configuration that delivers the best performance using the eigen-transmission strategy.

Remark 1: In the case where the resulting antenna configuration for either method is to use all of Bob's antennas for reception ($N_r = N_b$), then [7] offers the best performance due to the sub-optimality of the technique in Section III-A.

Remark 2: When $\mathbf{H}\mathbf{H}^H - \mathbf{G}_a\mathbf{G}_a^H \succ \mathbf{0}$, i.e., all the eigenvalues are positive and non-zero, then broadcasting AN from Bob is not necessary as it cannot outperform the MIMO C_S. In general, when the rank of the main channel is larger than the rank of the eavesdropping channel ($N_a > N_e$), there exists an effective null-space, and thus the best configuration is to use the full degrees of freedom of the MIMO channel such that all Bob's antennas are allocated for reception.

Remark 3: It is advisable to set a threshold $\tau \in [0, 1]$ to define the channel configurations achieving a selection criterion performance larger than τ to be considered in the analysis. The two introduced selection strategies are based on approximation mechanisms and therefore they are not totally accurate, in particular, when the performance obtained from different antenna configurations is similar. In this scenario the differences between the elements within either of the vectors $\bar{\boldsymbol{\delta}}_1$ and $\bar{\boldsymbol{\delta}}_2$ corresponding to these configurations are small and could lead to not choosing the antenna configuration that delivers the largest secrecy rate. As a countermeasure, it is advisable (but optional) to set a threshold ($\tau \in [0, 1]$) to introduce into the analysis the channel configurations achieving a selection criterion performance larger than τ. We recall that the elements of $\bar{\boldsymbol{\delta}}_1$ and $\bar{\boldsymbol{\delta}}_2$ are ordered in descending magnitude starting from 1; therefore we will consider the elements larger or equal to τ that correspond to the selected antenna configurations. For example, we could analyse the secrecy performance offered by all the antenna configurations attaining a performance larger than $\tau = 0.9$. This procedure improves the accuracy in selecting the best antenna configuration that will be used to solve the SDP in (11) but it increases the complexity of the strategy.

1) Numerical Results: We set $N_a = N_b = 3$ and normalise both the variance of the small-scale fading channel and the noise power (i.e., $\sigma^2_{\bar{G}_a} = \sigma^2_{\bar{G}_b} = \sigma^2_{\bar{H}_a} = 1$ and $\sigma^2_b = \sigma^2_e = 1$). The Alice-to-Bob distance is fixed to $r_{ab} = 1$ and the global power constraint is set at $P_{max} = 5$.

First, we investigate the joint AN technique performance when the number of antennas at Eve increases. In Fig. 2 we see that broadcasting AN from Bob is particularly useful when the eavesdropping channel's degrees of freedom increase. Indeed when $N_e < N_b$ our strategy is outperformed by the C_S in [7], and so allocating resources at Bob for AN generation is useless. In contrast, when $N_e \geq N_b$, broadcasting AN from Bob is useful. Interestingly, joint AN generation yields best performance at $N_e = 4$ because an eavesdropper equipped with a larger number of antennas can mitigate the effect of the AN thus reducing the effectiveness of an external interference.

We now turn our attention to the performance of the configuration selection strategies and their savings in complexity. As explained in Remark 3, in order to increase the successful channel configuration selection rate (SCCSR) we consider a threshold τ to analyse the configurations that potentially might

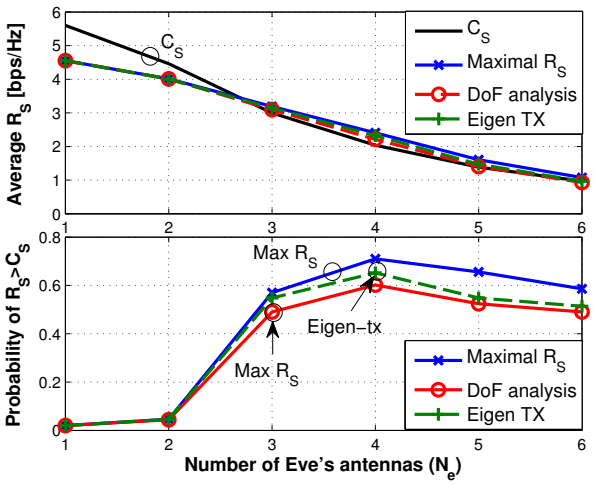

Fig. 2. Effect of the number of eavesdropper's antennas (N_e) on the average $\bar{\mathrm{R}}_S$ and the probability of $\bar{\mathrm{R}}_S > \mathrm{C}_S$ for $r_{ab} = r_{ae} = r_{be} = 1$. For DoF and eigen-transmission strategies $\tau = 0.75, 0.85$.

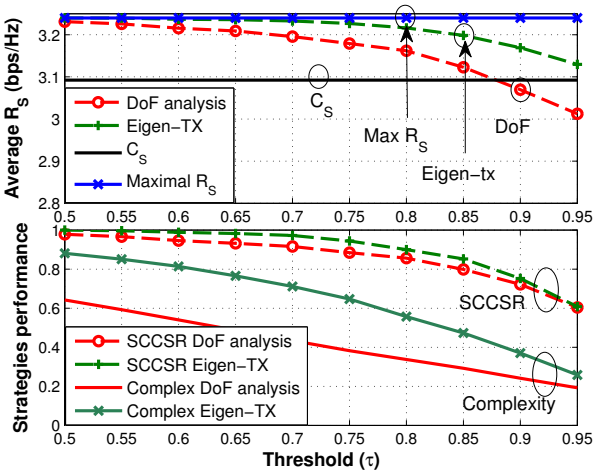

Fig. 3. Effect of τ on the average secrecy rate $\bar{\mathrm{R}}_S$ and the performance of antenna configuration selection strategy for $r_{ab} = r_{ae} = r_{be} = 1$ when $N_e = 3$. The bottom figure shows both the successful channel configuration selection rate (SCCSR) and the associated complexity.

deliver a larger $\bar{\mathrm{R}}_S$. We also study how τ affects the secrecy performance, the SCCSR and the associated complexity cost. Fig. 3 shows that the eigen-transmission method is better than the DoF analysis across all the values considered for τ in terms of choosing the best channel configuration (SCCSR); however, the associated complexity is considerably higher. It is worth pointing out that we measure the complexity by calculating the ratio between the number of channel configurations chosen by the channel selection strategy above τ to the total number of possible channel configurations; i.e., $2^{N_b} - 1$. Interestingly, the eigen-transmission method outperforms C_S even when $\tau \geq 0.9$. This behaviour is not found with the DoF analysis.

To analyse the effect of the location of the eavesdropper on security we consider a travelling eavesdropper moving in

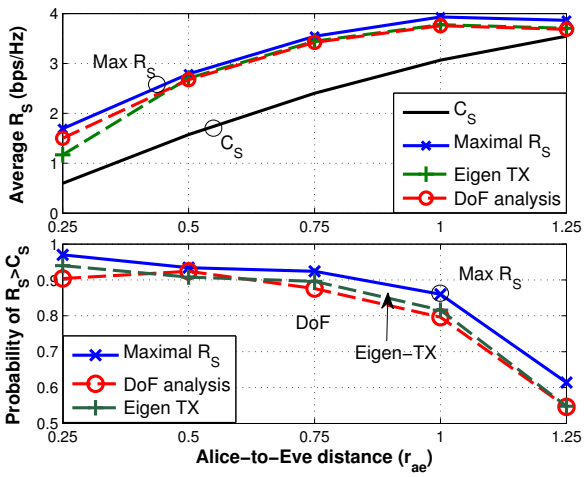

Fig. 4. Effect of the location of the eavesdropper on the average $\bar{\mathrm{R}}_S$ and the probability of $\bar{\mathrm{R}}_S > \mathrm{C}_S$ when $r_{ab} = 1$ and $N_e = 3$. The values of τ for DoF and eigen-transmission analysis has been set to 0.5 and 0.95 respectively.

a straight line from Alice towards Bob and beyond. Based on a normalised Alice-to-Bob distance $r_{ab} = 1$, the Bob-to-Eve distance (r_{be}) can be easily inferred from the Alice-to-Eve (r_{ae}) one. For the sake of clarity, in Fig. 4 we only plot the Alice-to-Eve distance, so Bob-to-Eve's distances are $r_{ae} = 0.25 \Rightarrow r_{be} = 0.75; r_{ae} = 1 \Rightarrow r_{be} \to 0; r_{ae} = 1.25 \Rightarrow r_{be} = 0.25$.

Fig. 4 shows the possible improvements in terms of secrecy rate by broadcasting AN from Bob when Eve is moving as described above. The gap between the maximal $\bar{\mathrm{R}}_S$ and the MIMO wiretap channel C_S is larger when Eve is closer to Alice due to the positive effect of jointly broadcasting AN that counters the smaller path losses that the eavesdropping link suffers under this condition. This gap decreases for $r_{ae} > r_{ab}$, meaning that it is not so useful to generate AN from Bob under this scenario because the eavesdropping channel is already poor due to large path losses because of Eve's greater distance from Alice. This behaviour is confirmed in the lower plot in Fig. 4 where the probability that the $\bar{\mathrm{R}}_S$ achieved by the joint AN strategy outperforms C_S is almost unity for Eve close to Alice. This verifies that the generation of AN from Bob is particularly useful when Eve is under favourable channel conditions compared to the main link. Fig. 4 also illustrates the good performance of the DoF and eigen-transmission strategies to select Bob's channel configuration. Here again, the eigen-transmission approach is the one that delivers the best performance.

V. Conclusion

In this paper we have answered positively to the question whether receiver 'Bob' can enhance the secrecy of the multiple antenna wiretap channel by transmitting artificial noise from some of his antennas. Indeed, a judicious allocation of Bob's antennas can provide a larger secrecy rate compared to the wiretap channel secrecy capacity obtained when Bob purely receives transmitted information. We have also introduced two low-complexity antenna selection techniques with minimum impact on secrecy performance. Transmitting artificial noise from the receiver is useful when the eavesdropping channel has a greater capacity than the main channel.

References

[1] Y.-W. Hong, P.-C. Lan, and C.-C. Kuo, "Enhancing Physical-Layer Secrecy in Multiantenna Wireless Systems: An Overview of Signal Processing Approaches," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 29–40, Sep. 2013.

[2] S. Shafiee and S. Ulukus, "Achievable Rates in Gaussian MISO Channels with Secrecy Constraints," in *IEEE International Symposium on Information Theory. ISIT 2007*, Jun. 2007, pp. 2466–2470.

[3] A. Khisti and G. Wornell, "Secure Transmission With Multiple Antennas II: The MIMOME Wiretap Channel," *IEEE Trans. on Information Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[4] F. Oggier and B. Hassibi, "The Secrecy Capacity of the MIMO Wiretap Channe," *IEEE Trans. on Information Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[5] R. Bustin, R. Liu, H. V. Poor, and S. Shamai, "An MMSE Approach to the Secrecy Capacity of the MIMO Gaussian Wiretap Channel," *EURASIP Journal in Wireless Comms. Networks.*, vol. 2009, pp. 3:1–3:8, Mar. 2009.

[6] S. Fakoorian and A. Swindlehurst, "Full Rank Solutions for the MIMO Gaussian Wiretap Channel with an Average Power Constraint," *IEEE Trans. on Signal Processing*, vol. 61, no. 10, pp. 2620–2631, May 2013.

[7] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, "Transmit Solutions for MIMO Wiretap Channels using Alternating Optimization," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1714–1727, Sep. 2013.

[8] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," *IEEE Trans. on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[9] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. Bloch, S. Ulukus, and A. Yener, "Cooperative Security at the Physical Layer: A Summary of Recent Advances," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 16–28, Sep. 2013.

[10] J. Huang and A. Swindlehurst, "Cooperative Jamming for Secure Communications in MIMO Relay Networks," *IEEE Trans. on Signal Processing*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[11] S. Fakoorian and A. Swindlehurst, "Solutions for the MIMO Gaussian Wiretap Channel with a Cooperative Jammer," *IEEE Trans. on Signal Processing*, vol. 59, no. 10, pp. 5013–5022, Oct. 2011.

[12] X. He and A. Yener, "Cooperation with an Untrusted Relay: A Secrecy Perspective," *IEEE Trans. on Information Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[13] Z. Ding, K. Leung, D. Goeckel, and D. Towsley, "On the Application of Cooperative Transmission to Secrecy Communications," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 2, pp. 359–368, Feb. 2012.

[14] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Communications Letters*, vol. 16, no. 10, pp. 1628–1631, Oct. 2012.

[15] N. Romero-Zurita, D. McLernon, and M. Ghogho, "PHY Layer Security in Multiple Antenna Systems by Joint Transmitter/Receiver Artificial Noise Generation through Semidefinite Programming," in *IET Intelligent Signal Processing Conference 2013 (ISP 2013)*, Dec. 2013, pp. 1–6.

[16] A. Mukherjee and A. Swindlehurst, "Robust Beamforming for Security in MIMO Wiretap Channels with Imperfect CSI," *IEEE Trans. on Signal Processing*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[17] A. Charnes and W. W. Cooper, "Programming with linear fractional functionals," *Naval Research Logistics Quarterly*, vol. 9, no. 3-4, pp. 181–186, 1962.

[18] J. Sturm, "Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones," *Optimization Methods & Software*, vol. 11-2, no. 1-4, Sp. Iss. SI, pp. 625–653, 1999.

[19] N. Romero-Zurita, D. McLernon, and M. Ghogho, "Physical Layer Security by Robust Masked Beamforming and Protected Zone Optimisation," *IET Communications*, vol. 8, no. 8, pp. 1248–1257, May 2014.

[20] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "PHY Layer Security Based on Protected Zone and Artificial Noise," *IEEE Signal Processing Letters*, vol. 20, no. 5, pp. 487–490, May. 2013.