

Iterative Antenna Selection for Secrecy Enhancement in Massive MIMO Wiretap Channels

(Invited Paper)

Ali Bereyhi*, Saba Asaad*, Rafael F. Schaefer[†] and Ralf R. Müller*

*Institute for Digital Communications (IDC), Friedrich-Alexander Universität Erlangen-Nürnberg (FAU)

[†]Information Theory and Applications Chair, Technische Universität Berlin (TUB)

ali.bereyhi@fau.de, saba.asaad@fau.de, rafael.schaefer@tu-berlin.de, ralf.r.mueller@fau.de

Abstract—The growth of interest in massive MIMO systems is accompanied with hardware cost and computational complexity. Antenna selection is an efficient approach to overcome this cost-plus-complexity issue which also enhances the secrecy performance in wiretap settings. Optimal antenna selection requires exhaustive search which is computationally infeasible for settings with large dimensions. This paper develops an iterative algorithm for antenna selection in massive multiuser MIMO wiretap settings. The algorithm takes a stepwise approach to find a suitable subset of transmit antennas. Numerical investigations depict a significant enhancement in the secrecy performance.

Index Terms—Massive MIMO wiretap channel, transmit antenna selection, stepwise regression

I. INTRODUCTION

Motivated by emerging increasing traffic demands as well as multi antenna devices and terminals, physical layer security in Multiple-Input Multiple-Output (MIMO) wiretap channels has drawn significant attentions from information-theoretic points of view [1]–[3]. The investigations have demonstrated the promising secrecy performance of these settings and depicted that the growth in system dimensions can significantly boost this performance [4]. Such large-scale setups however suffer from high Radio Frequency (RF) cost and computational complexity. Therefore, classical approaches such as antenna selection [5], [6], load modulated arrays [7] and hybrid analog-digital precoding [8] have been proposed to alleviate this issue.

The idea of antenna selection is to transmit or receive via a subset of available antennas. By proper selection of the subset, this approach can provide significant advantages in terms of the overall RF cost and hardware complexity without significant degradation in the performance [9]–[11]. The optimal approach for antenna selection requires an exhaustive search which is computationally impractical particularly in massive MIMO settings [12]. Hence, there are several studies devoted to find sub-optimal greedy algorithms with polynomial complexity; see for example [10], [13] and references therein for some recent studies.

Antenna selection is a special case of the general problem of subset selection arising in several applications such as pattern classification [14] and data mining [15]. An efficient low-complexity approach in these applications is stepwise regres-

sion in which the selected subset is iteratively constructed such that the growth of a given metric is maximized in each step. Although this strategy does not necessarily result in the optimal subset, it constitutes an effective and low-complexity approach.

The stepwise approach can be employed for antenna selection considering various selection metrics. For example in [16]–[18], iterative stepwise selection algorithms are proposed in which channel capacity was taken as the measure of performance. Simulation results demonstrated that the performance of this algorithm almost captures the optimal performance for moderate number of transmit antennas. The approach is further extended in recent studies, e.g., [13], [19], [20], considering some other performance metrics such as energy efficiency and receive signal-to-noise ratio.

Recent studies have demonstrated that antenna selection can be employed as an effective means for secrecy enhancement in massive MIMO wiretap settings [21], [22]. Such studies, however, do not provide algorithmic approaches which exploit this property. In this paper, we develop a stepwise algorithm for antenna selection in massive multiuser MIMO wiretap settings. Our investigations demonstrate that stepwise antenna selection can considerably enhance the secrecy performance without imposing a computational burden onto the system.

Notations: Scalars, vectors and matrices are shown with non-bold, bold lower case and bold upper case letters, respectively. The complex plain is shown by \mathbb{C} . \mathbf{H}^H , \mathbf{H}^* and \mathbf{H}^T indicate the Hermitian, complex conjugate and transpose of \mathbf{H} , respectively. $\log(\cdot)$ indicates the binary logarithm, and \mathbb{E} represents the expectation operator. For brevity, we define $[x]^+ = \max\{0, x\}$ and abbreviate $\{1, \dots, N\}$ by $[N]$.

II. PROBLEM FORMULATION

We consider secure downlink transmission in a massive multiuser MIMO wiretap setting consisting of a Base Station (BS) with M transmit antennas, K single-antenna legitimate receivers and an eavesdropper equipped with N receive antennas. The BS is assumed to be equipped with L_{\max} RF-chains with $L_{\max} \leq M$. For this setting, uplink channel coefficients from the users to the antenna array at the BS are enclosed in the matrix $\mathbf{H} \in \mathbb{C}^{M \times K}$. $\mathbf{G} \in \mathbb{C}^{M \times N}$ represents the channel from the eavesdropper to the BS. The system is assumed to operate in standard Time Division Duplexing (TDD) mode

meaning that the channels are reciprocal. The BS intends to transmit confidential messages to the users over this wiretap channel while the eavesdropper seeks to recover information conveyed from the BS to the legitimate users. The Channel State Information (CSI) of the main and the eavesdropper's channel is assumed to be known at the BS.

A. System Model

At the beginning of each coherence interval, the BS selects $L \leq L_{\max}$ transmit antennas based on the CSI of the main and the eavesdropper's channel. Let $\mathbf{s} = [s_1, \dots, s_K]^T$ be the vector of information symbols. The BS precodes \mathbf{s} linearly as

$$\mathbf{x} = \sqrt{P} \mathbf{W}_L \mathbf{s}. \quad (1)$$

for some P . $\mathbf{W}_L \in \mathbb{C}^{L \times K}$ is the signal shaping matrix which satisfies $\text{E tr}\{\mathbf{W}_L \mathbf{W}_L^H\} = 1$. The subscript L indicates the number of active transmit antennas. Assuming $\text{E} \mathbf{s} \mathbf{s}^H = \mathbf{I}_K$, the transmit power reads $\text{E} \mathbf{x}^H \mathbf{x} = P$. We further assume that the transmit power is constrained by $P \leq P_{\max}$.

The precoded signal $\mathbf{x} \in \mathbb{C}^L$ is transmitted over the selected antennas. Denoting the indices of the selected antennas with $\mathbb{L} = \{i_1, \dots, i_L\}$, the signals received at user terminals read

$$\mathbf{y} = \mathbf{H}_{\mathbb{L}}^T \mathbf{x} + \mathbf{n}_m \quad (2)$$

where $\mathbf{y} = [y_1, \dots, y_K]^T$ with y_k being the received signal at user k , $\mathbf{H}_{\mathbb{L}} \in \mathbb{C}^{L \times K}$ denotes the effective channel enclosing the rows of \mathbf{H} indexed by \mathbb{L} and \mathbf{n}_m encloses independent and identically distributed (i.i.d.) zero-mean Gaussian noise at user terminals whose variances are σ_m^2 , i.e., $\mathbf{n}_m \sim \mathcal{CN}(\mathbf{0}, \sigma_m^2 \mathbf{I}_K)$.

The received signal at the eavesdropper moreover reads

$$\mathbf{z} = \mathbf{G}_{\mathbb{L}}^T \mathbf{x} + \mathbf{n}_e \quad (3)$$

where $\mathbf{G}_{\mathbb{L}} \in \mathbb{C}^{L \times N}$ is the effective eavesdropper channel corresponding to \mathbb{L} and $\mathbf{n}_e \in \mathbb{C}^N$ denotes zero-mean complex Gaussian noise with variance σ_e^2 , i.e., $\mathbf{n}_e \sim \mathcal{CN}(\mathbf{0}, \sigma_e^2 \mathbf{I}_N)$.

B. Secrecy Performance Metric

From information-theoretic points of view, the secrecy performance is properly quantified via the achievable secrecy rate. For the setting under study, the achievable secrecy rate for user k is given by [1], [2]

$$\mathcal{R}_k^s(P, \mathbb{L}) = [\mathcal{R}_k^m(P, \mathbb{L}) - \mathcal{R}_k^e(P, \mathbb{L})]^+. \quad (4)$$

Here, the arguments P and \mathbb{L} indicate the dependency on the transmit power and selected antennas. $\mathcal{R}_k^m(P, \mathbb{L})$ denotes the rate to user k achieved over the main channel and $\mathcal{R}_k^e(P, \mathbb{L})$ is the information leakage from user k to the eavesdropper.

Assuming that the CSIs of the both channels are available at the receiving terminals, the maximum achievable rate for user k over the main channel is lower-bounded by [23], [24]

$$\mathcal{R}_k^m(P, \mathbb{L}) = \log(1 + \gamma_k^m(P, \mathbb{L})) \quad (5)$$

where $\gamma_k^m(P, \mathbb{L})$ denotes the Signal-to-Interference-plus-Noise Ratio (SINR) at user k and is given by

$$\gamma_k^m(P, \mathbb{L}) = \frac{\rho_m t_k(\mathbf{H}_{\mathbb{L}}, \mathbf{W}_L)}{1 + \rho_m u_k(\mathbf{H}_{\mathbb{L}}, \mathbf{W}_L)}. \quad (6)$$

Here, $\rho_m := P/\sigma_m^2$ and $t_k(\mathbf{H}_{\mathbb{L}}, \mathbf{W}_L)$ and $u_k(\mathbf{H}_{\mathbb{L}}, \mathbf{W}_L)$ are

$$t_k(\mathbf{H}_{\mathbb{L}}, \mathbf{W}_L) := |\mathbf{h}_{\mathbb{L}k}^T \mathbf{w}_{Lk}|^2 \quad (7a)$$

$$u_k(\mathbf{H}_{\mathbb{L}}, \mathbf{W}_L) := \sum_{j=1, j \neq k}^K |\mathbf{h}_{\mathbb{L}j}^T \mathbf{w}_{Lj}|^2 \quad (7b)$$

where $\mathbf{h}_{\mathbb{L}j}$ and \mathbf{w}_{Lj} denote the j -th columns of $\mathbf{H}_{\mathbb{L}}$ and \mathbf{W}_L , respectively.

The information leakage from user k is upper-bounded by considering the worst-case scenario in which the eavesdropper is able to cancel out all the interfering signals while overhearing the message of user k . The maximum information leakage from user k to the eavesdropper is bounded from above as

$$\mathcal{R}_k^e(P, \mathbb{L}) = \log(1 + \gamma_k^e(P, \mathbb{L})) \quad (8)$$

where $\gamma_k^e(P, \mathbb{L})$ is the SINR at the eavesdropper while overhearing the message of user k and is given by

$$\gamma_k^e(P, \mathbb{L}) = \rho_e t_k(\mathbf{G}_{\mathbb{L}}, \mathbf{W}_L) \quad (9)$$

with $\rho_e = P/\sigma_e^2$ and $t_k(\mathbf{G}_{\mathbb{L}}, \mathbf{W}_L)$ reading

$$t_k(\mathbf{G}_{\mathbb{L}}, \mathbf{W}_L) := \|\mathbf{G}_{\mathbb{L}}^T \mathbf{w}_{Lk}\|^2. \quad (10)$$

This bound is tight when other users cooperate with the eavesdropper such that it retrieves the interfered signals [25].

From (5) and (8), one concludes that the secrecy rate achievable for user k is bounded from below by

$$\mathcal{R}_k^s(P, \mathbb{L}) = \left[\log \frac{1 + \gamma_k^m(P, \mathbb{L})}{1 + \gamma_k^e(P, \mathbb{L})} \right]^+. \quad (11)$$

Consequently, the average achievable secrecy rate with respect to the weighting vector $\mathbf{w} = [w_1, \dots, w_K]$ is given by

$$\bar{\mathcal{R}}^s(P, \mathbb{L} | \mathbf{w}) = \sum_{k=1}^K w_k \mathcal{R}_k^s(P, \mathbb{L}). \quad (12)$$

Throughout the paper, we consider $\bar{\mathcal{R}}^s(P, \mathbb{L} | \mathbf{w})$ to be the secrecy performance metric of this multiuser setting. Our main objective is to develop an iterative algorithm which effectively selects a subset of transmit antennas and controls the transmit power with respect to this performance metric.

III. JOINT ANTENNA SELECTION AND POWER CONTROL

We find the optimal power level P and the optimal selection subset \mathbb{L} for given \mathbf{w} as

$$(P, \mathbb{L}) = \underset{0 \leq P \leq P_{\max}, \mathbb{L} \subseteq [M], |\mathbb{L}| \leq L_{\max}}{\operatorname{argmax}} \bar{\mathcal{R}}^s(Q, \mathbb{S} | \mathbf{w}). \quad (13)$$

The combinatorial optimization problem (13) is not practical for large M . Consequently, one may employ an alternative approach with feasible computational complexity at the expense of suboptimality. In this section, we develop an iterative algorithm for antenna selection and power control via stepwise regression. For the sake of brevity, we assume that the BS employs Maximum Ratio Transmission (MRT) precoding whose

signal shaping matrix for L active transmit antennas indexed with \mathbb{L} is given by

$$\mathbf{W}_L = \beta_L \mathbf{H}_{\mathbb{L}}^* \quad (14)$$

with $\beta_L := \text{tr}\{\mathbf{H}_{\mathbb{L}} \mathbf{H}_{\mathbb{L}}^H\}^{-1/2}$. Nevertheless, the results can be extended to other linear precoding schemes by standard lines of derivations. The extension is briefly discussed later on.

A. Transmit Antenna Selection (TAS) via Stepwise Regression

In the stepwise approach, the transmit antennas are iteratively selected. Starting from a single active antenna, assume that $\ell < L_{\max}$ antennas have been already selected, and we intend to select the $(\ell + 1)$ -st transmit antenna. Denoting the index set of ℓ selected antennas with \mathbb{L}_0 , the set of indices in the next step is $\mathbb{L}_1 = \mathbb{L}_0 \cup \{i_{\ell+1}\}$ where $i_{\ell+1}$ denotes the index of the transmit antenna being selected in step $\ell + 1$. The effective channels and the signal shaping matrix read

$$\mathbf{H}_{\mathbb{L}_1}^T = [\mathbf{H}_{\mathbb{L}_0}^T, \mathbf{h}_{\ell+1}] \quad (15a)$$

$$\mathbf{G}_{\mathbb{L}_1}^T = [\mathbf{G}_{\mathbb{L}_0}^T, \mathbf{g}_{\ell+1}] \quad (15b)$$

$$\mathbf{W}_{\ell+1}^T = \alpha(i_{\ell+1}) [\mathbf{W}_{\ell}^T, \beta_{\ell} \mathbf{h}_{\ell+1}^*] \quad (15c)$$

where $\mathbf{h}_{\ell+1} = [h_1, \dots, h_K]^T$ and $\mathbf{g}_{\ell+1}$ are the column vectors in \mathbf{H}^T and \mathbf{G}^T indexed by $i_{\ell+1}$, and $\alpha(i_{\ell+1}) := \beta_{\ell+1}/\beta_{\ell}$ is determined as

$$\alpha(i_{\ell+1}) = 1/\sqrt{1 + \beta_{\ell}^2 \|\mathbf{h}_{\ell+1}\|^2}. \quad (16)$$

Moreover, $\mathbf{H}_{\mathbb{L}_0}$ and $\mathbf{G}_{\mathbb{L}_0}$ denote the effective uplink channels in step ℓ , $\mathbf{H}_{\mathbb{L}_1}$ and $\mathbf{G}_{\mathbb{L}_1}$ are the effective channels in step $\ell + 1$, and \mathbf{W}_{ℓ} and $\mathbf{W}_{\ell+1}$ represent the MRT signal shaping matrices before and after selecting the new antenna, respectively.

Considering (15b)-(15c), the performance of the setting in step $\ell + 1$ is described as a stepwise update of the performance in step ℓ . To illustrate this statement, assume fixed power P at the transmitter. In this case, one can write $\gamma_k^m(P, \mathbb{L}_1)$ and $\gamma_k^e(P, \mathbb{L}_1)$ in terms of the SINR in step ℓ as

$$1 + \gamma^m(P, \mathbb{L}_1) = \theta_k^m(P, i_{\ell+1}) (1 + \gamma^m(P, \mathbb{L}_0)) \quad (17a)$$

$$1 + \gamma^e(P, \mathbb{L}_1) = \theta_k^e(P, i_{\ell+1}) (1 + \gamma^e(P, \mathbb{L}_0)) \quad (17b)$$

where $\theta_k^m(P, \ell + 1)$ and $\theta_k^e(P, \ell + 1)$ are given by

$$\theta_k^m(P, i_{\ell+1}) = \frac{\alpha^2(i_{\ell+1}) + \epsilon_k^m(P, i_{\ell+1})}{\alpha^2(i_{\ell+1}) + \psi_k^m(P, i_{\ell+1})} \quad (18a)$$

$$\theta_k^e(P, i_{\ell+1}) = \alpha^2(i_{\ell+1}) + \epsilon_k^e(P, i_{\ell+1}) \quad (18b)$$

where $\epsilon_k^m(P, i_{\ell+1})$, $\psi_k^m(P, i_{\ell+1})$ and $\epsilon_k^e(P, i_{\ell+1})$ are given by (19a)-(19c) on the top of the next page.

Consequently, the average achievable secrecy rate in step $\ell + 1$, i.e., $\bar{\mathcal{R}}^s(P, \mathbb{L}_1|\mathbf{w})$, can be written as

$$\bar{\mathcal{R}}^s(P, \mathbb{L}_1|\mathbf{w}) = \bar{\mathcal{R}}^s(P, \mathbb{L}_0|\mathbf{w}) + \Theta(P, i_{\ell+1}|\mathbf{w}) \quad (20)$$

where $\Theta(P, i_{\ell+1}|\mathbf{w})$ is defined as

$$\Theta(P, i_{\ell+1}|\mathbf{w}) := \sum_{k=1}^K w_k \log \frac{\theta_k^m(P, i_{\ell+1})}{\theta_k^e(P, i_{\ell+1})}. \quad (21)$$

From (20), one observes that the performance metric in step $\ell + 1$ is given by an update of the metric in step ℓ via a single term depending on $i_{\ell+1}$. Stepwise regression suggests that in each step, we select the transmit antenna which maximizes this single update term. In this case, the active antennas are selected such that the growth in the performance is optimized in *each step*. In contrast to optimal TAS, this stepwise approach has linear complexity which is computationally feasible in practice. Nevertheless, one should note that it does not necessarily lead to the globally optimal solution given by (13).

B. Iterative TAS and Power Control Algorithm

We develop an iterative algorithm for joint power control and TAS in this section. The algorithm employs the stepwise TAS approach while iteratively updating the transmit power in each step. It is given in Algorithm 1 and its details are illustrated in the sequel.

Initialization: For a given \mathbf{w} , the algorithm starts with the following initialization:

- The index of the first active antenna is set to i_1 such that

$$i_1 = \arg\max_{i \in [M]} \frac{\|\mathbf{H}_{\{i\}}\|}{\|\mathbf{G}_{\{i\}}\|}. \quad (22)$$

- The transmit power is set to P_1 such that the average achievable secrecy rate for $\mathbb{L} = \{i_1\}$ is maximized.

Iterative TAS: At step $\ell \in [L_{\max}]$, the algorithm selects the transmit antenna indexed with $i_{\ell+1}$ from the non-selected antennas such that the growth term $\Theta(P_{\ell}, i_{\ell+1}|\mathbf{w})$ is maximized where P_{ℓ} is the transmit power being set at the end of step ℓ .

Iterative Power Control: The transmit power is updated in each iteration after antenna selection such that the average secrecy rate, achieved via the selected antennas, is optimized with respect to P . This means that in step ℓ , after selection of the $(\ell + 1)$ -st transmit antenna, the selection subset is expanded by $\mathbb{L} = \mathbb{L} \cup \{i_{\ell+1}\}$ and the power is updated as

$$P_{\ell+1} = \arg\max_{0 \leq P \leq P_{\max}} \bar{\mathcal{R}}^s(P, \mathbb{L}|\mathbf{w}). \quad (23)$$

Stopping Criteria: When the performance metric monotonically increases with respect to the number of selected antennas, the stepwise selection is continued until L_{\max} transmit antennas are set active. There exist, however, scenarios for which the increase in number of active antennas does not necessarily enhance the performance metric [22]. In this case, the optimal stepwise update term, i.e., $\Theta(P_{\ell}, i_{\ell+1}|\mathbf{w})$, does not return a positive value after some iterations. We therefore stop the algorithm either when the number of active antennas is L_{\max} or when the optimal stepwise update term is non-positive, i.e., $\Theta(P_{\ell}, i_{\ell+1}|\mathbf{w}) \leq 0$ the latter criteria is labeled by STC in Algorithm 1.

C. Further Extensions

Although the results have been derived for MRT precoding and average secrecy rate, the approach can be extended to other linear precoders and performance metrics; see discussions in [13]. For other linear precoders, the rank-one updates, similar

$$\epsilon_k^m(P, i_{\ell+1}) = \frac{1 + \rho_m \alpha^2(i_{\ell+1}) \beta_\ell \left(\sum_{j=1}^K \beta_\ell |h_k h_j^*|^2 + 2 \operatorname{Re} \{ \mathbf{h}_{\mathbb{L}_0 k}^\top \mathbf{w}_{\ell j} h_k h_j^* \} \right) - \alpha^2(i_{\ell+1})}{1 + \rho_m (t_k(\mathbf{H}_{\mathbb{L}_0}, \mathbf{W}_\ell) + u_k(\mathbf{H}_{\mathbb{L}_0}, \mathbf{W}_\ell))} \quad (19a)$$

$$\psi_k^m(P, i_{\ell+1}) = \frac{1 + \rho_m \alpha^2(i_{\ell+1}) \beta_\ell \left(\sum_{j=1, j \neq k}^K \beta_\ell |h_k h_j^*|^2 + 2 \operatorname{Re} \{ \mathbf{h}_{\mathbb{L}_0 k}^\top \mathbf{w}_{\ell j} h_k h_j^* \} \right) - \alpha^2(i_{\ell+1})}{1 + \rho_m u_k(\mathbf{H}_{\mathbb{L}_0}, \mathbf{W}_\ell)} \quad (19b)$$

$$\epsilon_k^e(P, i_{\ell+1}) = \frac{1 + \rho_e \alpha^2(i_{\ell+1}) \beta_\ell (\beta_\ell |h_k|^2 \|\mathbf{g}_{\ell+1}\|^2 + 2 \operatorname{Re} \{ h_k \mathbf{g}_{\ell+1}^\top \mathbf{G}_{\mathbb{L}_0}^\top \mathbf{w}_{\ell k} \}) - \alpha^2(i_{\ell+1})}{1 + \rho_e t_k(\mathbf{G}_{\mathbb{L}_0}, \mathbf{W}_\ell)} \quad (19c)$$

Algorithm 1 Iterative Joint TAS and Power Control

Input: Channel matrices \mathbf{H} and \mathbf{G} , and P_{\max} , L_{\max} and \mathbf{w}
Initiate Let $\ell = 1$ and

$$i_1 = \operatorname{argmax}_{i \in [M]} \frac{\|\mathbf{H}_{\{i\}}\|}{\|\mathbf{G}_{\{i\}}\|}. \quad (24)$$

Set $\mathbb{L} = \{i_1\}$, $\mathbf{H}_{\mathbb{L}} = \mathbf{H}(i_1, :)$, $\mathbf{G}_{\mathbb{L}} = \mathbf{G}(i_1, :)$ and

$$P_1 = \operatorname{argmax}_{0 \leq P \leq P_{\max}} \bar{\mathcal{R}}^s(P, \mathbb{L} | \mathbf{w}). \quad (25)$$

while $\ell < L_{\max}$

$$i_{\ell+1} = \operatorname{argmax}_{i \in [M] \setminus \mathbb{L}} \Theta(P_\ell, i | \mathbf{w}). \quad (26)$$

if $\Theta(P_\ell, i_{\ell+1} | \mathbf{w}) \leq 0$ **then** STC
 break
end if

Set $\mathbf{H}_{\mathbb{L}} = [\mathbf{H}_{\mathbb{L}}^\top, \mathbf{H}(i_{\ell+1}, :)]^\top$ and update the precoder as

$$\mathbf{W}_{\ell+1} = \alpha_{\ell+1} \begin{bmatrix} \mathbf{W}_\ell \\ \beta_\ell \mathbf{H}^*(i_{\ell+1}, :) \end{bmatrix}. \quad (27)$$

Update $\mathbb{L} = \mathbb{L} \cup \{i_{\ell+1}\}$ and the transmit power as

$$P_{\ell+1} = \operatorname{argmax}_{0 \leq P \leq P_{\max}} \bar{\mathcal{R}}^s(P, \mathbb{L} | \mathbf{w}). \quad (28)$$

Set $\ell = \ell + 1$.

end while

Output: $L = \ell$, $P = P_\ell$ and \mathbb{L} .

to the one derived for MRT precoding in (15c), are derived using the Sherman-Morrison formula [26]. By similar lines of derivations, the stepwise update rule is extended to multiple performance metrics. Due to lack of space, further derivations are skipped and left for the extended version of the manuscript.

IV. NUMERICAL INVESTIGATIONS

We investigate the proposed algorithm numerically by considering the following sample setting: The BS has a transmit antenna array of size $M = 64$ and L_{\max} RF-chains. Moreover, the eavesdropper is equipped with $N = 8$ receive antennas. The number of users is set to $K = 4$. For simplicity, the main channel and the eavesdropper's channel are assumed to be i.i.d. unit-variance Rayleigh fading meaning that their entries are i.i.d. zero-mean and unit-variance complex Gaussian random

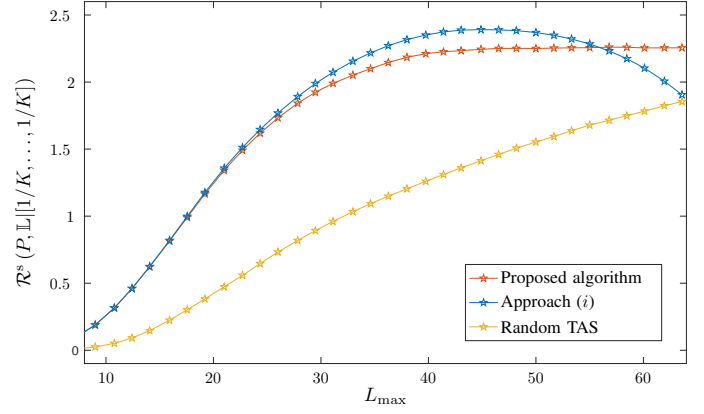


Fig. 1: Performance of the TAS approaches for $M = 64$, $K = 4$, $P_{\max} = 1$, $\sigma_m^2 = \sigma_e^2 = 0.1$ and $N = 8$. The proposed algorithm stops selecting antennas at $L = 37$, since further selection degrades the performance. Such degradation is observed in approach (i).

variables. The noise variances at the user terminals and the eavesdropper are set to $\sigma_m^2 = \sigma_e^2 = 0.1$, and the transmit power P is constrained by $P_{\max} = 1$. The weighting factors w_k are set to $1/K$ for all the users.

In Fig. 1, the average achievable secrecy rate $\bar{\mathcal{R}}^s(P, \mathbb{L} | \mathbf{w})$ is given as a function of the number of RF-chains L_{\max} for three different approaches: (i) The stepwise approach given in Algorithm 1 without the stopping criteria STC. (ii) The proposed iterative algorithm with the stopping criteria STC. (iii) Random TAS. As the figure depicts, the secrecy rate is not an increasing function of L_{\max} in the stepwise approach. Such an observation is also reported in [22] via large-system analyses. The optimal choice for the number of active transmit antennas is some $L < L_{\max}$ which is approximated by the proposed iterative approach. As the figure depicts, the proposed algorithm stops selecting antennas around $L = 37$, due to the fact that further selection degrades the performance. The slight degradation in the performance of the algorithm with the stopping criteria STC is due to fact that the algorithm solves the coupled problems of power control and TAS separately. For the sake of comparison, we have also evaluated the performance of random TAS for this setting. The figure shows a significantly degraded performance.

V. CONCLUSION AND OUTLOOK

The proposed iterative algorithm for joint TAS and power control in massive MIMO wiretap settings selects the active

transmit antennas using the forward selection method from stepwise regression. The proposed algorithm significantly enhances the secrecy performance while enjoying low computational complexity.

The large-system performance characterization of the proposed algorithm is an interesting direction for future work. The work in this direction is currently ongoing.

REFERENCES

- [1] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.
- [2] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. on Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.
- [3] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2547–2553, 2009.
- [4] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 21–27, 2015.
- [5] A. F. Molisch, M. Z. Win, Y.-S. Choi, and J. H. Winters, "Capacity of MIMO systems with antenna selection," *IEEE Transactions on Wireless Communications*, vol. 4, no. 4, pp. 1759–1772, 2005.
- [6] S. Asaad, A. Bereyhi, R. R. Müller, and A. M. Rabiei, "Asymptotics of transmit antenna selection: Impact of multiple receive antennas," *IEEE International Conference on Communications (ICC)*, 2017.
- [7] M. A. Sedaghat, V. I. Barousis, R. R. Müller, and C. B. Papadias, "Load modulated arrays: a low-complexity antenna," *IEEE Communications Magazine*, vol. 54, no. 3, pp. 46–52, 2016.
- [8] L. Liang, W. Xu, and X. Dong, "Low-complexity hybrid precoding in massive multiuser MIMO systems," *IEEE Wireless Communications Letters*, vol. 3, no. 6, pp. 653–656, 2014.
- [9] S. Sanayei and A. Nosratinia, "Antenna selection in MIMO systems," *IEEE Communications Magazine*, vol. 42, no. 10, pp. 68–73, 2004.
- [10] A. Bereyhi, M. A. Sedaghat, and R. R. Müller, "Asymptotics of nonlinear LSE precoders with applications to transmit antenna selection," in *IEEE International Symposium on Information Theory (ISIT)*, pp. 81–85, 2017.
- [11] A. Bereyhi, M. A. Sedaghat, S. Asaad, and R. R. Müller, "Nonlinear precoders for massive MIMO systems with general constraints," *International ITG Workshop on Smart Antennas (WSA)*, 2017.
- [12] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3590–3600, 2010.
- [13] A. Bereyhi, S. Asaad, and R. R. Müller, "Stepwise transmit antenna selection in downlink massive multiuser MIMO," *International ITG Workshop on Smart Antennas (WSA)*; available on arXiv, arXiv:1802.05148, 2018.
- [14] R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern classification*. John Wiley & Sons, 2012.
- [15] J. Han, J. Pei, and M. Kamber, *Data mining: concepts and techniques*. Elsevier, 2011.
- [16] A. Gorokhov, D. A. Gore, and A. J. Paulraj, "Receive antenna selection for MIMO spatial multiplexing: theory and algorithms," *IEEE Transactions on Signal Processing*, vol. 51, no. 11, pp. 2796–2807, 2003.
- [17] M. Gharavi-Alkhansari and A. B. Gershman, "Fast antenna subset selection in MIMO systems," *IEEE Transactions on Signal Processing*, vol. 52, no. 2, pp. 339–347, 2004.
- [18] S. Sanayei and A. Nosratinia, "Capacity maximizing algorithms for joint transmit-receive antenna selection," in *38th Asilomar Conference on Signals, Systems and Computers*, vol. 2, pp. 1773–1776, 2004.
- [19] X. Zhou, B. Bai, and W. Chen, "An iterative algorithm for joint antenna selection and power adaptation in energy efficient MIMO," in *IEEE International Conference on Communications (ICC)*, pp. 3812–3816, 2014.
- [20] M. Gkizeli and G. N. Karystinos, "Maximum-SNR antenna selection among a large number of transmit antennas," *IEEE Journal of Selected Topics in Signal Processing*, vol. 8, no. 5, pp. 891–901, 2014.
- [21] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," *IEEE Transactions on Communications*, vol. 63, no. 8, pp. 2959–2971, 2015.
- [22] S. Asaad, A. Bereyhi, R. R. Müller, R. F. Schaefer, and A. M. Rabiei, "Optimal number of transmit antennas for secrecy enhancement in massive MIMOME channels," *IEEE Global Communications Conference (GLOBECOM)*, 2017.
- [23] G. Caire, N. Jindal, M. Kobayashi, and N. Ravindran, "Multiuser MIMO achievable rates with downlink training and channel state feedback," *IEEE Transactions on Information Theory*, vol. 56, no. 6, pp. 2845–2866, 2010.
- [24] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Processing Letters*, vol. 19, no. 6, pp. 372–375, 2012.
- [25] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2245–2261, 2016.
- [26] M. S. Bartlett, "An inverse matrix adjustment arising in discriminant analysis," *The Annals of Mathematical Statistics*, vol. 22, no. 1, pp. 107–111, 1951.