User Selection in Multiuser MIMO Systems with Secrecy Considerations

Amitav Mukherjee

Electrical Engineering and Computer Science
University of California
Irvine, CA 92697-2625
a.mukherjee@uci.edu

A. Lee Swindlehurst

Electrical Engineering and Computer Science
University of California
Irvine, CA 92697-2625
swindle@uci.edu

Abstract—This paper investigates simple user selection strategies in a multiuser downlink system with a single transmitter, multiple legitimate receivers, and a single eavesdropper, where all nodes are equipped with multiple antennas. No information regarding the eavesdropper is presumed at the transmitter, and we examine the MIMO downlink channel with either single or multiple data streams per receiver. The transmitter uses linear beamforming techniques based on generalized zero-forcing with a corresponding minimum SINR or rate requirement per receiver. In both cases the information signal is transmitted with just enough power to guarantee the desired Quality-of-Service (QoS) at the desired receivers, while the remainder of the power is used to broadcast artificial noise that selectively degrades the passive eavesdropper's signal. Numerical simulations displaying the power consumption and the number of selected users provided by each selection scheme demonstrate the effectiveness of the proposed schedulers in ensuring physical-layer security.

I. INTRODUCTION

The continuing evolution of multiuser wireless communication systems has led to significant interest in scheduling and resource sharing mechanisms. In the last decade, multiuser networks with multiple antennas (MIMO) at one or both ends of the transmit-receive links that provide the opportunity to serve multiple users simultaneously are the new resource allocation paradigm. As a result, several approaches have been proposed for the user scheduling problem in MIMO downlink channels [1]–[4]. In this case, the multiuser equivalent of the greedy selection scheme schedules the set of users with the most favorable channel conditions. However, wireless transmissions are inherently vulnerable to interception by unintended receivers, which can be exacerbated if the network is attacked by malicious eavesdroppers that listen passively without revealing their location. Therefore, secure transmission strategies that operate at the physical layer have recently been of great interest in the so-called ‘MIMO wiretap’ network setting.

This work presents simple user selection strategies that provide confidentiality in a MIMO downlink system with multiple legitimate receivers and one or more passive eavesdroppers, where all nodes possess multiple antennas. The transmitter is assumed to have perfect channel state information (CSI) of

the intended receivers, whereas the CSI of the eavesdropper is unavailable at the transmitter. Each receiver is assumed to have a minimum Quality-of-Service (QoS) requirement that must be met by the transmitter. For the case of a single data stream per receiver, the QoS is in terms of signal-to-noise-plus-interference ratio (SINR), whereas for multiple data streams per receiver the QoS is measured in rate. Unlike [5]–[7], it is not desired for the message of one receiver to be shielded from the others; instead we aim to provide protection for all messages from being overheard by external eavesdropper(s).

The general theme of the user scheduling schemes are as follows. Once the maximum number of users that can be supported in a transmission epoch have been selected, any remaining portion of the transmit power is used to broadcast an artificial interference signal in order to mask the desired signal from potential eavesdroppers [8]–[11]. For example, one of the proposed selection algorithms schedule users that minimize the overall transmit power while satisfying the pre-specified QoS thresholds. This approach differs from existing user selection algorithms in two ways. Firstly, existing MIMO user selection algorithms primarily focus on maximizing sum-rate or throughput [1]–[3], whereas user selection for guaranteed performance has received comparatively little attention [4]. Secondly, to the best knowledge of the authors, secrecy-based user selection in MIMO systems without any eavesdropper information has not been considered previously in the literature. [12] independently considered the case of user selection with secrecy capacity as the metric, i.e., with eavesdropper CSI known to the transmitter.

The remainder of this paper is organized as follows. The mathematical model of the MIMO downlink is presented next. In Sec. III we describe differing approaches to the secrecy-based user selection problem. Sec. IV contains numerical results, and we conclude in Sec. V.

II. SYSTEM MODEL

The network under consideration is comprised of a N_t -antenna transmitter broadcasting to a subset $\mathcal{K}$ of legitimate receivers out of the overall candidate set $\mathcal{S}$ with N_r antennas each, and C passive eavesdroppers with N_e antennas each in the vicinity of the network. The transmitter is assumed to have a total power constraint P encompassing information

transmission and artificial noise. The general representation of the received signal at the k^{th} active user is

$$\mathbf{y}_k = \mathbf{H}_k \mathbf{T}_k \mathbf{x}_k + \sum_{j=1, j \neq k}^K \mathbf{H}_j \mathbf{T}_j \mathbf{x}_j + \mathbf{H}_k \mathbf{z}' + \mathbf{n}_k, \quad (1)$$

where $\mathbf{H}_k$ is the corresponding full-rank $N_r \times N_t$ channel matrix between the transmitter and user k , $\mathbf{T}_k$ is a $N_r \times d_k$ linear precoder where d_k is the number of data streams, $\mathbf{x}_k$ is the $d_k \times 1$ information vector for user k , the $N_t \times 1$ vector $\mathbf{z}'$ is the artificial noise for jamming the eavesdropper, and $\mathbf{n}_k$ is the additive white Gaussian noise vector with covariance $\mathcal{E}\{\mathbf{n}_k \mathbf{n}_k^H\} = \sigma^2 \mathbf{I}$. The k^{th} receiver then applies a $d_k \times N_r$ linear post-processor $\mathbf{W}_k$ to its received signal.

Since the CSI of all receivers (except for the eavesdropper) is available to the transmitter, the artificial noise $\mathbf{z}'$ can be chosen from the nullspace of the effective downlink channel $\tilde{\mathbf{H}} = [\tilde{\mathbf{H}}_1 \dots \tilde{\mathbf{H}}_K]^T$, where $\tilde{\mathbf{H}}_k = (\mathbf{W}_k^H \mathbf{H}_k)^T$, in order to guarantee that it does not impact the desired receivers. Let $0 < \rho_k \leq 1$ be the fraction of the power devoted to the information signal of user k , and $\rho \equiv \sum_{k=1}^K \rho_k$ be the fraction of the total power used for information transmission.

Define the power fraction left for transmitting artificial noise as $\alpha = 1 - \rho$, which leads to

$$\mathcal{E}\{\mathbf{z}' \mathbf{z}'^H\} = \mathbf{Q}'_z \quad \text{Tr}(\mathbf{Q}'_z) = \alpha P.$$

While dirty paper coding achieves the capacity of the MIMO broadcast channel, we focus on more practical linear transmission techniques that have significantly reduced complexity requirements. The linear precoding and post-processing algorithm of choice is the coordinated transmit-receive beamforming (CBF) technique of [13], [14], for both the cases where a single data stream is to be sent to each receiver, i.e., $d_k = 1 \forall k$, or if $d_k > 1 \forall k$.

A brief description of CBF is provided next. For user k , define $\tilde{\mathbf{H}}_k$ as

$$\tilde{\mathbf{H}}_k = [\tilde{\mathbf{H}}_1 \dots \tilde{\mathbf{H}}_{k-1} \tilde{\mathbf{H}}_{k+1} \dots \tilde{\mathbf{H}}_K] \quad (2)$$

$$\tilde{\mathbf{H}}_l = (\mathbf{W}_l^H \mathbf{H}_l)^T.$$

The singular value decomposition of $\tilde{\mathbf{H}}_k$ yields

$$\tilde{\mathbf{H}}_k = \tilde{\mathbf{U}}_k \tilde{\mathbf{D}}_k \tilde{\mathbf{V}}_k^H, \quad (3)$$

where $\tilde{\mathbf{U}}_k$ is the matrix of left singular vectors, $\tilde{\mathbf{D}}_k$ is the diagonal matrix of singular values, and $\tilde{\mathbf{V}}_k$ is the collection of right singular vectors.

The CBF algorithm initializes the receive matrices as $\mathbf{W}_k$ as the d_k dominant left singular vectors of $\tilde{\mathbf{H}}_k$. Subsequently, the effective downlink channel is constructed as shown in (2), followed by the computation of the transmit matrices so as to block-diagonalize the effective downlink channel [13].

III. USER SELECTION STRATEGIES

The transmitter wishes to schedule a subset $\mathcal{K}$, $\mathcal{K} \subseteq \mathcal{S}$ of users, where the cardinality $|\mathcal{K}|$ of $\mathcal{K}$ is less than or equal to the maximum number of simultaneous users K_m . For the single-stream system with $d_k = 1 \forall k$, a common choice is to set $K_m = N_t$. Each active receiver in the selected set has a QoS requirement L_k that the transmitter must satisfy. For the single-stream system, the QoS threshold is a signal-to-noise-plus-interference ratio (SINR) $L_k \geq E_k$, whereas for multiple data streams per receiver the desired QoS is a rate $L_k \geq R_k$. Since the legitimate receivers do not perceive multiple-user interference under CBF and the artificial noise is nulled by the receive processing, we have

$$R_k = \log |\mathbf{I} + \mathbf{H}_k \mathbf{T}_k \mathbf{Q}_z \mathbf{T}_k^H \mathbf{H}_k^H / \sigma_k^2|. \quad (4)$$

As the CBF algorithm itself is iterative nature with computationally expensive singular value decomposition operations per iteration, it is of interest to develop simple heuristic selection methods instead of resorting to an exhaustive search, which has combinatorially increasing complexity as the size of the candidate set increases. In the sequel, we describe three such suboptimal schedulers that address differing aspects of the selection problem. However, the issue of selection fairness is not addressed explicitly in the proposed selection schemes, though it is worthy of further study.

A. Min-Power Scheduling

Define $\Psi = \mathcal{S} \setminus \mathcal{K}$ as the set of all unselected users. In brief, a simple greedy method that increases the selected user set one candidate at a time comprises the scheduling algorithm. Each new candidate is chosen so as to minimize the transmit sum power, thereby maximizing the power available for jamming the eavesdropper. We summarize the proposed suboptimal selection scheme for the multiple data-stream downlink based on CBF below.

Algorithm 1 Min-Power Selection Strategy for Guaranteed Rate

Require: $P > 0, R_k > 0$

Initialize $\mathcal{K}^{(0)} = \{\emptyset\}$, $\Psi = \mathcal{S}$

For $i = 1$ to K_m

Solve:

$$\arg \min_{s \in \Psi} \rho_s = \text{Tr}(\mathbf{Q}_s)$$

$$\text{s. t. } R_s = \log |\mathbf{I} + \mathbf{H}_s \mathbf{T}_s \mathbf{Q}_s \mathbf{T}_s^H \mathbf{H}_s^H / \sigma_s^2|.$$

end

Recompute CBF Transmit and Receive Beamforming Matrices and update overall power allocation ρ

$$\text{If } (|\mathcal{K}| \leq K_m) \text{ AND } \left(\sum_{s \in \mathcal{K}^{(i)}} \rho_s \leq P \right)$$

$$\mathcal{K}^{(i+1)} = \{\mathcal{K}^{(i)}, s\}, \Psi = \mathcal{S} \setminus s.$$

Else: TERMINATE

B. Max-User Scheduling

Depending upon user channel conditions and QoS requirements, the greedy scheduler proposed above may not always lead to an outcome where a non-zero fraction of power is left over for generating artificial interference. Consequently, it may be more prudent to set aside a fixed fraction of transmit power αP for artificial interference, while using the remaining fraction to accommodate as many users as possible given their pre-specified QoS thresholds. In effect, this is equivalent to the conventional MIMO downlink problem of selecting the largest possible user set with an effective transmit power constraint of ρP . For simplicity, assume a single data stream per user ($d_k = 1$) is permitted. Therefore, under CBF up to N_t legitimate users can be scheduled simultaneously given a sufficiently large power budget. The algorithmic description of the Max-User scheduler is very similar to that of Table 3, except now K_m is not predetermined and the stopping criterion is based on the transmit sum power.

Algorithm 2 Max-User Selection Strategy

Require: $P > 0, R_k > 0$

Initialize $\mathcal{K}^{(0)} = \{\emptyset\}, \Psi = \mathcal{S}$

While $\left(\sum_{s \in \mathcal{K}^{(i)}} \rho_s \leq (1 - \alpha)P \right)$

Solve:

$$\arg \min_s \rho_s = \text{Tr}(\mathbf{Q}_s)$$

$$\text{s. t. } R_s = \log |\mathbf{I} + \mathbf{H}_s \mathbf{T}_s \mathbf{Q}_s \mathbf{T}_s^H \mathbf{H}_s^H / \sigma^2|.$$

Recompute CBF Transmit and Receive Beamforming Matrices and update overall power allocation ρ

$\mathcal{K}^{(i+1)} = \{\mathcal{K}^{(i)}, s\}, \Psi = \mathcal{S} \setminus s.$

C. Max-Product Scheduling

Hitherto, the aspects of jamming power and selected user set size have been treated separately in the Min-Power and Max-User scheduling schemes. It is evident that a tradeoff exists between the two: increasing the power used for artificial interference leads to a reduction in the number of serviceable users and vice-versa. Therefore, a simple heuristic user selection scheme that considers both competing objectives simultaneously would be to maximize the product of the power fraction used for information transmission and the number of selected users.

IV. SIMULATION RESULTS

The channel matrices for all links are composed of independent Gaussian random variables with zero mean and unit variance. The transmitter power constraint is fixed as $P = 25\text{dB}$, and the background noise power is assumed to be the same for all receivers and the eavesdropper: $\sigma^2 = 1$. All of the displayed results are calculated based on an average of 500 trials with independent channel and noise realizations. For the first simulation, we assume a transmitter with $N_t = 4$

Algorithm 3 Max-Product Selection Strategy

Require: $P > 0, R_k > 0$

Initialize $\mathcal{K}^{(0)} = \{\emptyset\}, \Psi = \mathcal{S}$

For $M = 1$ to N_t

Solve:

$$\arg \min_s \rho_s(M) = \text{Tr}(\mathbf{Q}_s)$$

$$\text{s. t. } R_s = \log |\mathbf{I} + \mathbf{H}_s \mathbf{T}_s \mathbf{Q}_s \mathbf{T}_s^H \mathbf{H}_s^H / \sigma^2|.$$

Recompute CBF Transmit and Receive Beamforming Matrices and update overall power allocation

end

$N = \arg \min_M M \rho_s(M)$

$\rho = \rho_s(N)^M$

Fig. 1. Transmit sum power versus desired data rate for Min-Power selection of $K_m = 4$ out of $S = 12$ total users, $N_t = 4, N_r = 2, N_e = 4$ antennas.

antennas, selection of $K_m = 4$ out of $S = 12$ potential legitimate receivers with $N_r = 2$ antennas each, and an eavesdropper with $N_e = 4$ antennas. Fig. 1 displays the transmit sum power used for information transmission over a range of desired data rates. The random selection method arbitrarily picks K_m users out of S . The heuristic selection method incurs a slightly greater transmit sum power compared to the optimal exhaustive search, but requires significantly lower complexity. As expected, the performance loss due to random selection is much greater.

Fig. 2 displays the information BER at the eavesdropper over a range of desired data rates, assuming BPSK-modulated symbols and maximum-likelihood detection. Once again, the heuristic selection degrades eavesdropper capabilities almost as much as the optimal exhaustive search method.

Fig. 3 displays the performance of the Max-User and exhaustive schedulers over a range of jamming power fractions α . On average, the heuristic selection is able to accommodate as many users as the optimal scheduler for large data transmit powers, with a graceful degradation as α increases.

Fig. 2. Eavesdropper BER versus desired data rate for selection of $K_m = 6$ out of $S = 15$ total users, $N_t = 5$, $N_r = 3$, $N_e = 5$ antennas.

Fig. 3. Max-User selection with $S = 12$ total users, $N_t = 8$, $N_r = 2$, $N_e = 6$ antennas.

Fig. 4. Comparison of selection strategies for $S = 12$ total users, $N_t = 8$, $N_r = 2$, $N_e = 5$ antennas.

Fig. 4 exhibits the power fraction and user selection size provided by the Max-Product algorithm. The outcomes of the Min-Power scheme with $K_m = 4$ and Max-User scheme with $\alpha = 0.7$ are shown alongside. While a direct comparison of the different selection methodologies is difficult to make, the figure captures the intuitive trade-off offered by the Max-Product algorithm.

V. CONCLUSION

A number of low-complexity heuristic user selection algorithms for MIMO downlink channels that provide an enhanced level of physical-layer security have been proposed in this work. In the first approach, minimizing the sum transmit power required to achieve a certain level of QoS at the selected users maximizes the power available for jamming potential eavesdroppers. A complementary approach fixes the fraction of power reserved for jamming eavesdroppers and attempts to maximize the number of users that can be guaranteed their desired QoS. Finally, an ad hoc joint optimization of the product of the jamming power fraction and selected user set size is shown to offer a trade-off between the two previous approaches.

REFERENCES

- [1] Goran Dimic and N. D. Sidiropoulos, "On downlink beamforming with greedy user selection: performance analysis and a simple new algorithm," *IEEE Trans. Signal Process.*, vol. 53, no. 10, pp. 3857-3868, Oct. 2005.
- [2] Z. Shen, J. G. Andrews, R. W. Heath, and B. L. Evans, "Low complexity user selection algorithms for multiuser MIMO Systems with block diagonalization," *IEEE Trans. Signal Process.*, vol. 54, no. 9, pp. 3658-3663, Sep. 2006.
- [3] A. Bayesteh and A. K. Khandani, "On the user selection for MIMO broadcast channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 3, pp. 1086-1107, Mar. 2008.
- [4] X. Zhang, E. Jorswieck, B. Ottersten, and A. Paulraj, "User selection schemes in multiple antenna broadcast channels with guaranteed performance," *IEEE SPAWC*, pp. 1-5, Helsinki, June 2007.
- [5] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.
- [6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *IEEE Intl Symp. on Inf. Theory*, pp. 524-528, July 2008.
- [7] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453-2469, June 2008.
- [8] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, June 2008.
- [9] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas II: the MIMOME wiretap channel," submitted to *IEEE Trans. Inform. Theory*, Aug. 2008. [Online]. Available: <http://www.rle.mit.edu/sia/>.
- [10] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," *IEEE ICASSP*, pp. 2437-2440, April 2009, Taiwan.
- [11] A. Mukherjee and A. L. Swindlehurst, "Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels," to appear, *IEEE SPAWC*, Perugia, Italy, June 21-24, 2009.
- [12] M. Yanase and T. Ohtsuki, "Secrecy-based user selection in multiuser MIMO downlink system," *IEICE Tech. Rep.*, vol. 109, no. 105, RCS 2009-45, pp. 97-100, June 2009.
- [13] Q. H. Spencer, A. L. Swindlehurst, and M. Haardt, "Zero-forcing methods for downlink spatial multiplexing in multiuser MIMO channels," *IEEE Trans. Signal Process.*, vol. 52, no. 2, pp. 461-471, Feb. 2004.
- [14] Q. Spencer and A. Swindlehurst, "A hybrid approach to spatial multiplexing in multi-user MIMO downlinks," *EURASIP Journ. Wireless Commun. and Network.*, pp. 236-247, Dec. 2004.