Chunk-based User Selection and Resource Allocation in Distributed Secure MISO-OFDMA Systems

Bo Wu[1,2] , Yong Ding[1]
1.Zhongzhou University, Zhengzhou, China , 450044
2.Wuhan University, Wu Han, China , 430072
wuwubobo001@163.com

***Abstract*—The user selection and resource allocation problem for the downlink of Orthogonal Frequency Division Multiple Access (OFDMA) wireless systems is investigated. It is assumed that the Base Station (BS) consists of multiple antennas in a distributed Antenna System (DAS), while a single antenna is available to each user. The considered problem is modeled as an optimization problem which takes into account a multiple antenna eavesdropper and artificial noise generation for secure communications. Also, the user selection unit is not the subcarrier, as in conventional OFDMA systems, but a set of subcarriers (chunk). User selection based on chunk, power, secrecy data rate are optimized for security capacity in the proposed suboptimal but efficient algorithm. Simulation and complexity comparison are provided to show the benefits of chunk-based resource allocation to DASs.**

Keywords-User selection, distributed antenna system, MISO-OFDMA, chunks, physical-layer security, artificial noise

I. INTRODUCTION

Orthogonal frequency division multiple access (OFDMA) is a promising scheme that helps utilize multiuser diversity against multipath fading, which is also a candidate for high speed wireless networks, such as 3GPP Long Term Evolution (LTE), IEEE 802.16 Worldwide Interoperability for Microwave Access (WiMAX). Meanwhile, Multi-Input Single-Output (MISO) technology offers significant increase in communication capacity without additional bandwith and more power requirements. In such systems, the different channel conditions of each user can be exploited to boost system performance metrics such as the aggregate user throughput (sum rate) [1]. By combining OFDMA and MISO transmission, wireless systems can offer improved reliability. In a MISO-OFDMA system, the fadings of different subcarriers are independent for different users and the maximum system capacity can be achieved by using user selection and resource allocation.

In MIMO system, the system capacity can be further increased by placing BSs antennas at distributed locations [2]. In this DAS, resource allocation is performed centralized and the available resources are exploited more efficiently because of the different scattering environments across distributed antennas that enrich the wireless channels of users [3]. It was shown that Dirty Paper Coding (DPC) can achieve transmission on the boundary of the capacity region in [4]. And an iterative algorithm for the computation of the capacity was presented in [5]. Despite its optimality, it is unattractive in some practical scenarios for its high complexity. A Zero-Forcing DPC based technique (ZF-DPC) is proposed in [6]. The technique combines DPC with QR decomposition to completely eliminate the interference among transmitting users. Hence, although its complexity is lower than the optimal scheme, it can still be prohibitively high in realistic scenarios. Although information security is known to be vital in wireless communications, cryptography does not directly leverage the unique property of the wireless domain to address security threats. To further reduce the complexity and the overhead of signaling, chunk-based approaches have been proposed in [7] [8].

On the other hand, we should point out that a large number of work has been devoted to physical layer (PHY) security [9]-[11], as a complement to the traditional cryptographic encryption adopted in the upper layer. In 1975, Wyner [12]showed that a source and a destination can exchange perfectly secure messages if the desired receiver enjoys better channel conditions than the passive eavesdropper. Subsequently,secure communication systems with multiple antennas have been proposed, which degrade the channels of the eavesdroppers by artificial noise or signal randomization [10]. The authors study the power allocation problem for maximizing the ergodic secrecy capacity in single-user single-carrier systems for different system configurations [11]. However, the assumption of ergodic channels cannot be justified for delay sensitive applications in practice since the transmitted packets of these applications can only experience quasistatic fading [13]. Hence, a secrecy outage occurs whenever the secrecy data rate exceeds the secrecy capacity. At the same time, resource allocation in multi-carrier systems with PHY security considerations are studied in [14] and [15] for the case of single-user and multiuser systems, respectively. In these works, the channel state information (CSI) of the eavesdroppers is assumed to be known at the BS such that secure communication can be guaranteed. However, without considering interference suppression and resource allocation between different users, these methods are limited to single user systems and are incapable of deployment in multiuser downlink MISO-OFDMA systems.

In this paper, motivated by [1] [3], a suboptimal resource allocation algorithm, which enables secure communication in slow fading for for the MISO (Multiple Input Single Output)-OFDMA DAS downlink by introducing artificial noise with lower complexity. we formulate the resource allocation and scheduling problem for secure communication in OFDMA systems as an optimization problem.

Published by Atlantis Press, Paris, France.

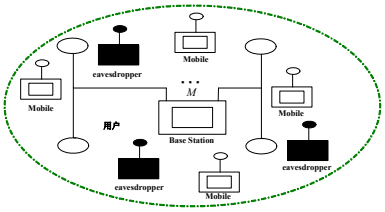

Figure 1. Chunk-Based Distributed Secure MISO-OFDMA Systems Model

The rest of the paper is organized as follows. In Section II, we outline the model for secure MISO-OFDMA communication systems with artificial noise generation as an optimization. In Sections III, we formulate the resource allocation design problem and solve the problem by Using Zero Forcing beamforming and on spatial correlation based on the method of [1] and [3]. Section IV presents numerical performance results for the proposed resource allocation and scheduling algorithm. In Section V, we conclude with a brief summary of our results.

II. System Model And Problem Formulation

Considering a MISO-OFDMA downlink transmission with N subcarriers, M distributed antennas at BS and K active users, each equipped with one receive antenna. And the eavesdropper has only one or more antennas, as figure 1. Let B be the overall available bandwidth, P be the total transmit power and $h_{k,n} = \left[h_{k,n}^1,...,h_{k,n}^M\right]^T$, $1 \le k \le K$, $1 \le n \le N$ be the $M \times 1$ channel vector between the BS and user k in subcarrier n. N subcarriers are divided into Q chunks, each with L contiguous subcarriers, that is N = Q × L, Thus, $\tilde{h}_{k,q} = \sum_{l=1}^{L} h_{k,(q-1)L+l}$ is the mean channel vector between user k and chunk q.

Using ZF transmit beamforming, the baseband equivalent model for the q-th chunk-based system is

$$y_q = \tilde{H}_q s_q + z_q \tag{1}$$

where y_q is a $K \times 1$ received signal vector and $\tilde{H}_q$ is a $K \times M$ channel matrix with complex entries. S_q is a $K \times 1$ transmiting signal vector, and z_q is a $K \times 1$ noise vector. At the same time, the baseband equivalent model for the eavesdropper is

$$y_{Eve,q} = G_{qSq} + z_{Eve,q} \tag{2}$$

We also assume that the CSI of the desired users are perfectly known at the BS due the accurate channel estimation. On the other hand, it is assumed that the transmitter only knows the number of eavesdroppers. Since the CSI of eavesdropper is hardly to achieved, in order to secure communication, an artificial noise is used to degrade the wireless of eavesdropper. Assume the transmit signal S_q as the linear combination of the information bearing signal u_q and artificial noise signal v_q, i.e.,

$$s_q = b_q u_q + w_q v_q \tag{3}$$

where v_q is a vector of the independent and identically distributed (i.i.d) complex Gaussian random variables with variance $\sigma_{v,q}^2$. b_q is the ZF beamforming matrix and w_q is a orthogonal basis for the null space of $\tilde{H}_q$, such that $\tilde{H}_q w_q v_q = 0$ and $w_q^* w_q = I_q$ where I_q is a $(M-1)\times(M-1)$ identity matrix and $[\bullet]^*$ represents the conjugate transpose operation. So the noise does not affect the desired users. Hence, the received signals can be rewritten as

$$y_q = \tilde{H}_q b_q u_q + z_q \tag{4}$$

$$y_{Eve,q} = G_q b_q u_q + G_q w_q v_q + z_{Eve,q} \tag{5}$$

Suppose the total transmit power on subcarrier chunks p is p_p. We define the following variables

$$P_q = p_q + (M-1)\sigma_{v,q}^2 \tag{6}$$

$$p_q = \alpha_q P_q \tag{7}$$

$$\sigma_{v,q}^2 = \frac{(1-\alpha_q)P_q}{(M-1)} \tag{8}$$

where P_q denotes the power allocated to the desired signal on chunk p and $0 < \alpha_q \le 1$ represents the fraction of power devoted to the information bearing signal on chunk p.

As in [3], when $K > M$ it is necessary to select $t < M$ out of K users in each chunk. So, there are $I = \sum_{t=1}^{M}\binom{K}{t}$ possible combinations of users transmitting in the same chunk denoted as $A_{i,p} = \{s_1,...,s_t\}$ and notice that each subcarrier of chunk $q = 1,2,...,Q$ is assigned to the same set of users. Then the capacity of chunk q is

$$c_{k,i,q} = \frac{B}{Q}\log\left(1 + \frac{\rho_{k,i,q}\left\|\tilde{h}_{k,q}\right\|_2^2}{\sigma_{k,q}^2}\right) \tag{9}$$

where $\rho_{k,i,q}$ is the chunk allocation indicator such that $\rho_{k,i,q} = 1$ if user $k \in A_i$ and A_i selected in chunk q; otherwise $\rho_{k,i,q} = 0$ for all $k = 1,2,...,K$; $i = 1,2,...,I$,

$q = 1,2,...,Q$. In the same way, Then the capacity of Eve is

$$c_{Eve,q} = \frac{B}{Q} log\left(1 + \frac{\left\|G_q b_q\right\|_2^2 \alpha_q P_q}{\left\|G_q w_q\right\|_2^2 \left(\frac{1-\alpha_q}{M-1}\right) P_q + \sigma_{Eve,q}^2}\right) \quad (10)$$

The problem of the maximization of the total capacity with Q chunks can be defined as:

$$R = \sum_{k=1}^{K}\sum_{q=1}^{Q}\sum_{i=1}^{I} c_{k,i,q} - \sum_{q=1}^{Q} c_{Eve,q} \quad (11)$$

The problem above (10) is an non-deterministic polynomialtime hard combinatorial optimization problem with non-linear constraints. So the solution can be obtained by exhaustive search of all possible user allocation for optimization. The complexity is given by I^Q, which is extremely complicated for even small K, Q. Hence, In the following section, a fast resource allocation algorithm is proposed based on array redundancy and spatial correlation between different users [1][3].

III. User Selection And Resource Allocation

The effect of the spatial correlation between different users on resource allocation can be analyzed as follows. For user k, which belongs to A_i, $\tilde{\mathbf{H}}_\mathbf{q}(A_i)\mathbf{w}_{k,q} = \left(0,\cdots,\left\|\mathbf{h}_{k,q}\right\|,\cdots,0\right)^T$. To achieve this, $w_{k,q}$ must lie in the null space of $\tilde{\mathbf{H}}_\mathbf{q}(A_i \setminus k)$, where $A_i \setminus k$ is defined as all of selected users excluding k. For $rank\left(\tilde{\mathbf{H}}_\mathbf{q}(\mathbf{A_i} \setminus \mathbf{k})\right) < M-1$, $\tilde{\mathbf{H}}_\mathbf{q}(\mathbf{A_i} \setminus \mathbf{k})$ can be expressed as

$$\tilde{\mathbf{H}}_\mathbf{q}(A_i \setminus k) = \mathbf{U}_{q,A_i \setminus k} \mathbf{\Sigma}_{q,A_i \setminus k} \left[\mathbf{V}^1_{q,A_i \setminus k} \mathbf{V}^0_{q,A_i \setminus k}\right]^H \quad (12)$$

using singular value decomposition, where $V^0_{q,A_i \setminus k}$ holds the last $M - rank\left(H_q\left(A_i \setminus k\right)\right)$ right singular vectors. So $V^0_{q,A_i \setminus k}$ forms an orthogonal basis for the null space of $\tilde{\mathbf{H}}_\mathbf{q}(\mathbf{A_i} \setminus \mathbf{k})$. Hence, $w_{k,q}$ can be generally posed as

$$w_{k,q} = V^0_{q,A_i \setminus k} P_{k,q} \quad (13)$$

where $P_{k,q}$ is a power vector. Applying the Cauchy-Schwarz inequality, (10) can be written as

$$\left\|h_{k,q}\right\| \le \left\|h_{k,q} V^0_{q,A_i \setminus k}\right\| \left\|P_{k,q}\right\| \quad (14)$$

The value of $\left\|h_{k,q} V^0_{q,A_i \setminus k}\right\|$ is decreased with increasing correlation between user k and user $A_i \setminus K$. So, $\| P_{k,q} \|$ must be sufficiently large according to (11), which leads to the less channel capacity. The proposed algorithm comprises the following steps:

1)Step 1:

Set $\rho_{k,i,q} = 0$, $\forall k,i,q$, $SC = \{1,...,Q\}$

2)Step 2: While $SC \neq \phi$

①Select a user randomly.

②Find subcarrier chunk $q = arg\ max\{h_{k,s}\}$, $\forall s \in SC$.

③Set $U = \{1,...,K\} \setminus k$; $A_i = \phi$; $t = 2$; $\rho_{k,i,q} = 1$; $A_i(t) = \{k\}$, where $A_i(t)$ is defined as the allocation result of the step.

④While $2 \le t \le M-1$

- For each $l \in A_i(t-1)$ and $m \in U$, compute $\eta_{l,m,q}$, which denotes the spatial correlation between user l and user m in subcarrier chunk q.
- Let $Cor_{m,A_i(t-1),q} = \frac{\sum_{l \in A_i(t-1)} \eta_{l,m,q}}{\left|A_i(t-1)\right|}$ be the average correlation between m and $A_i(t-1)$.
- Form a group, $\hat{A}$, of candidates that contains users with the above value of $Cor_{m,A_i(t-1),q}$ sorted from the lowest one to the highest one.
- Set $\rho_{k,i,q} = 1$; $A_i(t) = A_i(t-1) \cup s_t$; $U = U \setminus s_t$.
- Set $SC = SC \setminus q$.

3)Output:

- $A_{i,q}$.

During the first iteration, the user with the largest channel plus should be selected. Then subcarrier chunk that maximizes the channel capacity of the user should be chosen. The following iterations are divided into two parts. Before meeting all of users, additional users are admitted to the subcarrier based on two criteria: 1) total transmitted power must be lower than the most transmitted power of each subcarrier, and 2) the total assigned received power must not be larger than the total one . Initialization step of the proposed algorithm is constant time, then in the loop, which runs for every chunk of set S, the best user among K for Q chunks is found. The operation requires O (KL). Then at most T−1 other users are found for chunk q. It is easily observed that the proposed algorithm has a larger reduction in complexity than the exhaustive search. Hence, chunk-based allocation proposed in the paper is very available in practical application.

IV. Simulation Results

In this section, we evaluate the performance using matlab simulation. A cell with 1 BS and 1024 subcarriers, the number of chunks is 8 and bandwidth is 100MHz. Users are placed uniformly to the cell area. In the DAS, one of the antennas is placed at the center and the others on the vertices o fa homocentric cell. All results are averaged over 2000 simulation runs. The channel is modeled as frequency-

selective channel comprising of 6 independent Rayleigh multipath components with each multipath component modeled by Clarke's flat fading model. Each data packet comprises 200 OFDM symbols. The QPSK modulated symbols are transmitted in the presence of additive complex Gaussian noise with zero mean and unit variance in each simulation.

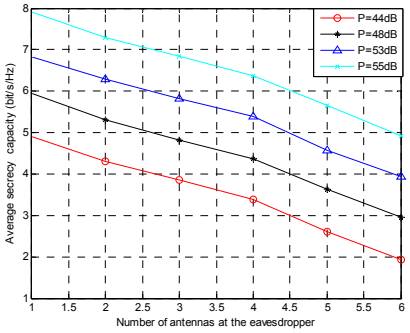

Figure 2. Average secrecy capacity versus the number of antennas employed at eavesdropper for different transmit powers and M = 8 antennas at the base station

Figure 2 depicts the average secrecy capacity versus the number of receive antenna employed at the eavesdropper for several transmit power levels. There are 8 antenna at the BS. It can be observed that the secrecy capacity decreases as the number of receive antenna increases, since more of the transmit power has to be allocated to the artificial noise for degrading the receive signal of Eve. On the other hand, we can get that one non-zero secrecy capacity can be achieved as long as the number of BS is larger than that of Eve.

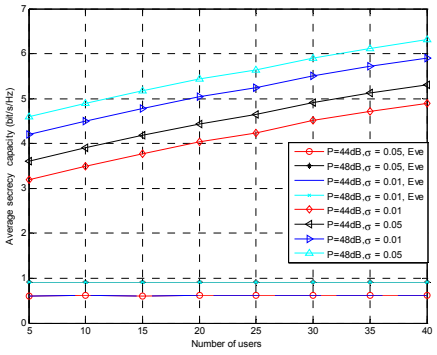

Figure 3. Average secrecy capacity versus the number of users.

Figure 3 depicts the average secrecy capacity versus the number of users for different transmit powers. It can be observed that the secrecy capacity grows with the users since the proposed resource allocation algorithm is able to exploit multiuser diversity with the existence of the eavesdropper. On the other hand, as shown in Figure 3, a more stringent secrecy probability will be introduce more artificial noise to interfere Eve, which decreases the average capacity.

V. CONCLUSION

A resource allocation algorithm for the distributed secure MISO-OFDMA downlink has been introduced. In the algorithm, chunk is the resource allocation unit to reduce the complexity. So the complexity of the algorithm is smaller than the complexity of other previously proposed methods with the same security performance, as was verified through simulations.

ACKNOWLEDGMENT

The authors would like to thank Jianming Fu of Wuhan university for simulation data and references.

REFERENCES

[1] V. D. Papoutsis, I. G. Fraimis, and S. A. Kotsopoulos,"User Selection and Resource Allocation Algorithm with Fairness in MISO-OFDMA,"IEEE Communicaitons Letters, vol. 14, NO. 5, pp.411-413. May. 2010.

[2] H. Zhu, S. Karachontzitis, and D. Toumpakaris, "Low-complexity resource allocation and its application to distributed antenna systems," IEEE Wireless Commun., vol. 17, no. 3, pp. 44-50, June 2010.

[3] Vasileios D. Papoutsis, Stavros A. Kotsopoulos, "Chunk-Based Resource Allocation in Distributed MISO-OFDMA Systems with Fairness Guarantee," IEEE COMMUNICATIONS LETTERS, vol. 3(3), pp. 2-23, 2011.

[4] H. Weingarten, Y. Steinberg, and S. Shamai, "The capacity region of the Gaussian MIMO broadcast channel," IEEE Trans. Inf. Theory, vol. 52, no. 9, pp. 3936-3964, Sep. 2006.

[5] G. 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.

[6] P. W. C. Chan and R. S. Cheng, "Capacity maximization for zeroforcing MIMO-OFDMA downlink systems with multiuser diversity," IEEE Trans. Wireless Commun., vol. 6, no. 5, pp. 1880-1889, May 2007.

[7] M. Shen, G. Li, and H. Liu,"Effect of traffic channel configuration on the orthogonal frequency division multiple access downlink performance," IEEE Trans. Wireless Commun., vol. 4, no. 4, pp. 1901-1913, July 2005.

[8] H. Zhu and J. Wang, "Chunk-based resource allocation in OFDMA systemsCpart I: chunk allocation," IEEE Trans. Commun., vol. 57, no. 9, pp. 2734-2744, Sep. 2009.

[9] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," IEEE Trans. Wireless Commun., vol. 7, pp. 2180 C 2189, June 2008.

[10] X. Zhou and M. R. McKay, "Secure Transmission with Artificial Noise over Fading Channels: Achievable Rate and Optimal Power Allocation," IEEE Trans. Veh. Technol., pp. 3831 C 3842, July 2010.

[11] Z. Li, R. Yates, and W. Trappe, "Secrecy Capacity of Independent Parallel Channels," in Proc. 44th Annu. Allerton Conf. Commun., Control and Computing, Sep 2006, pp. 841C848.

[12] A. D. Wyner, "The Wire-Tap Channel," Tech. Rep., Oct 1975.

[13] Derrick Wing Kwan Ng and Robert Schober,"Resource Allocation for Secure OFDMA Communication Systems",AusCTW 2011.

[14] E. A. Jorswieck and A. Wolf, "Resource Allocation for the Wire-Tap Multi-Carrier Broadcast Channel," in Proc. International Conf. On Telecommun., June 2008, pp. 1 C 6.

[15] Z. Li, R. Yates, and W. Trappe, "Secrecy Capacity of Independent Parallel Channels," in Proc. 44th Annu. Allerton Conf. Commun., Control and Computing, Sep 2006, pp. 841C848.