Turkish Journal of Computer and Mathematics Education Vol.11 No.03 (2020), 1199-1205
Research Article

Design and Performance Analysis of Interference cancellation inHeterogeneous networks With Multi-Antenna Arrays

Fathima Zaheera[1], I. V. Prakash[2]

[1]Assistant Professor,[2]Associate Professor, [1,2]Department of ECE

[1,2]Gandhi Institute for Technology (GIFT), Bhubaneswar, India

---

Abstract

To improve national security, government agencies have long been committed to enforcing powerful surveillance measures on suspicious individuals or communications. In this paper, we consider a wireless legitimate surveillance system, where a full-duplex multi-antenna legitimate monitor aims to eavesdrop on a dubious communication link between a suspicious pair via proactive jamming. Massive Multiple-Input Multiple-Output (MIMO), small cell, and full-duplex are promising techniques for future 5G communication systems, where interference has become the most challenging issue to be coped with. In this paper, we provide an interference coordination framework for a two-tier heterogeneous network (HetNet) that consists of a massive-MIMO enabled macro-cell base station (MBS) and a number of full-duplex small-cell base stations (SBSs). For each scenario, the optimal jamming power is derived in closedform and efficient algorithms are obtained for the optimal transmit/receive beamforming vectors. Moreover, low-complexity suboptimal beamforming schemes are proposed for the MIMO case. Our analytical findings demonstrate that by exploiting multiple antennas at the legitimate monitor, the eavesdropping non-outage probability can be significantly improved compared to the single antenna case.

Keywords:OFDM, MIMO systems, interference cancellation.

1.INTRODUCTION

Wireless communications provide an efficient and convenient means for establishing connections between people. However, due to the open and broadcast nature of the wireless medium, wireless communications are particularly susceptible to security breaches, hence establishing reliable and safe connections is a challenging task. Responding to this, physical layer security, as a promising technique to enable secure communications, has attracted considerable attentions in recent years [1]–[15], and various sophisticated techniques such as artificial noise [16], [17] and security-oriented beamforming [18], [19] have been proposed to enhance the secrecy performance. In the physical layer security framework, the eavesdroppers are illegitimate adversaries, who intend to breach the confidentiality of a private conversation. On the other hand, wireless communications also facilitate the collaboration between the criminals or terrorists, thereby posing significant threats on national security.

Therefore, to prevent crimes or terror attacks, there is a strong need for the government agencies to legitimately monitor any suspicious communication links to detect abnormal behaviors, such as communications containing sensitive word combinations, addressing information, or other factors with a frequency that deviates from the average. For wireless communication surveillance, passive eavesdropping, where the legitimate monitor simply listens to the suspicious links, is a straightforward method. However, the legitimate monitor may be in general deployed far away from the suspicious transmitter to avoid getting exposed, as such the quality of the legitimate eavesdropping channel is a degraded version of the suspicious channel, making passive eavesdropping an inefficient approach.

2.LITERATURE SURVEY

Many works on LTE resource allocation are available in the literature [5]. The 10 ms duration of an LTE radio frame typically requires that allocation of resources must be broken into subproblems, favoring low complexity of implementation over better approximations of the optimal solution. Scheduling frequency resources for the LTE uplink is itself a combinatorial optimization problem that can be impractical to solve optimally. [6], [7] and [8] propose several heuristic algorithms for frequency resource scheduling which trade between performance and complexity. LTE power allocation is often treated as a separate problem. [9], [10] and [11] examine power control mechanisms within LTE, considering performance trades between throughput, self-interference, and energy efficiency.

Because LTE generally has exclusive access to the spectrum bands they operate in, a mechanism to preclude interference to another system is not a part of these and other works on LTE resource allocation. An appropriate architecture and adapted algorithms are needed to enable effective LTE-METSAT sharing for the scenario in [4]. The subject of avoiding interference is often treated in the literature under the topic of cognitive radio. [12], [13] and [14] derive results for cognitive radios subject to interference constraints, including identification of frequency and power selection strategies, but only for a single cognitive radio transmitter. This does not lend insight into how resources should be allocated across multiple transmitters within the LTE network. The effect of aggregate interference due to multiple transmitters is included in [15]–[20] and [21], and resource allocation algorithms are developed, but all of these works assume that perfect channel state information is available.

3. SYSTEM MODEL

We consider a three-node point-to-point legitimate surveillance system as shown in Fig. 1, where a legitimate monitor E aims to eavesdrop a dubious communication link between a suspicious pair S and D via jamming. It is assumed that the suspicious transmitter and receiver are equipped with a single antenna each.1 To enable simultaneous eavesdropping and jamming, the legitimate monitor is equipped with two sets of antennas, i.e., Nr antennas for eavesdropping (receiving) and Nt antennas for jamming (transmitting). Quasi-static channel fading is assumed, such that the channel coefficients remain unchanged during each transmission block but vary independently between different blocks.

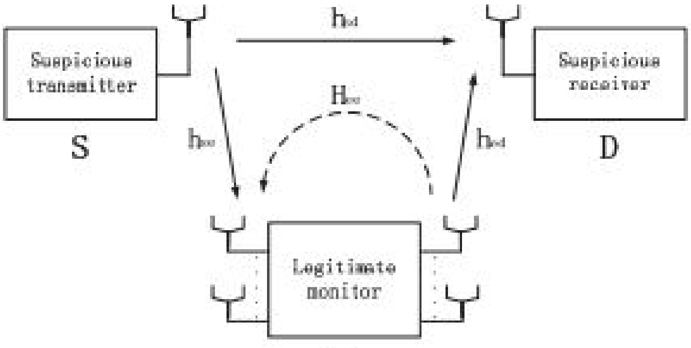

Fig. 1: A point-to-point legitimate surveillance system consisting of one suspicious transmitter S, one suspicious receiver D and one legitimate monitor E.

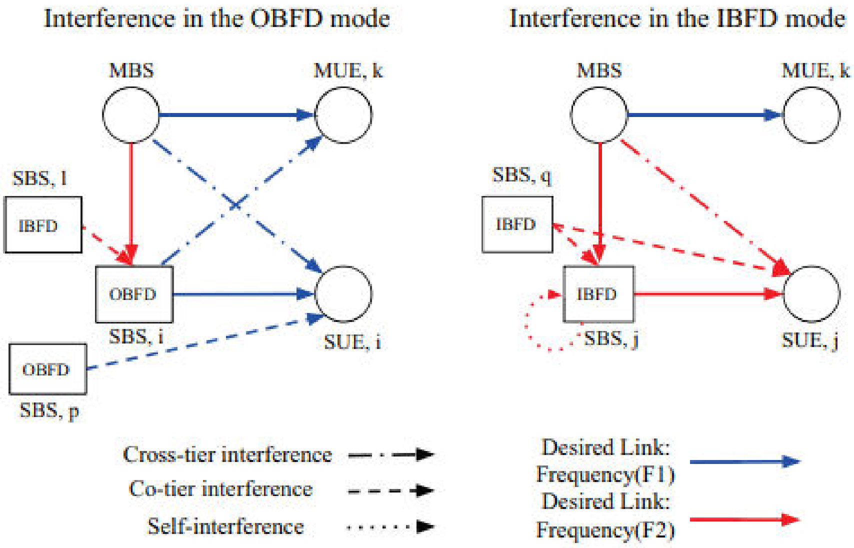

Fig. 2. The full-duplex mode of each SBS determines its interference pattern.

We consider the downlink of a two-tier HetNet as illustrated in Fig. 1, where a MBS comprising N transmit antennas provides services for K single-antenna macro-cell UEs (MUEs). In addition, there exist S SBSs in the cell, and each SBS communicates with the MBS and serves the small-cell UEs (SUE) simultaneously using full-duplex techniques. Massive MIMO is invoked by the MBS, so it is practical that N K and N S. Linear zero-forcing beamforming (LZFBF) with equal power per stream is utilized in MBS's access links to MUEs and wireless backhauls to SBSs.

SBS could operate in two modes as follows.

- Out-of-band Full-duplex Mode (OBFD): access link and backhaul link employ different frequency bands.
- In-band Full-duplex Mode (IBFD): access link and backhaul link are conducted at the same frequency band.

Since the MBS provides services for MUEs and SBSs at the same time, assigning these two links with identical frequency band results in a complicated transmission coordination problem. As such, we divide the total available bandwidth into two equal parts, denoted as F1 and F2, respectively, and assume that the macro-cell access link exploits F1 band while the backhaul link occupies F2. In this setting, the choice between F1 and F2 for small-cell access link directly determines the full-duplex mode of the corresponding SBS. If small-cell access link employs F2, then this SBS is in IBFD mode, and vice versa. For notational convenience, we refer to the set of all IBFD SBSs as SI and that of all OBFD SBSs as SO. The set of all SBSs is denoted as S. From Fig. 2, we see SBSs in different sets experience distinct interference patterns.

Keeping these two interference patterns in mind, we are able to model the considered HetNet in details. Each SBS can operate in two modes for backhaul transmission, i.e.,

- **In-Band Full-Duplex (IBFD) mode:** in which the access link and backhaul link transmissions are conducted in the same frequency band (say F1) of bandwidth B. Thus, the total bandwidth usage of IBFD mode is B.
- **Out-of-Band Full-Duplex (OBFD) mode**: in which the access link and backhaul link transmissions are conducted in different frequency bands F2 and F1, respectively. Note that, in OBFD mode, if we

calculate capacity by considering F1 and F2 each of bandwidth B, then the total bandwidth usage of OBFD mode becomes 2B. This is an unfair setting from the perspective of bandwidth usage and in turn capacity calculation. In order to have a fair comparison, we need to assume that each mode (i.e., IBFD or OBFD) can consume a total bandwidth of B Hz only, i.e., the IBFD mode would use B Hz for both access and backhaul link transmissions. On the other hand, the OBFD mode would have to use 0.5B Hz of F2 for the access link and 0.5B Hz of F1 for the backhaul link.

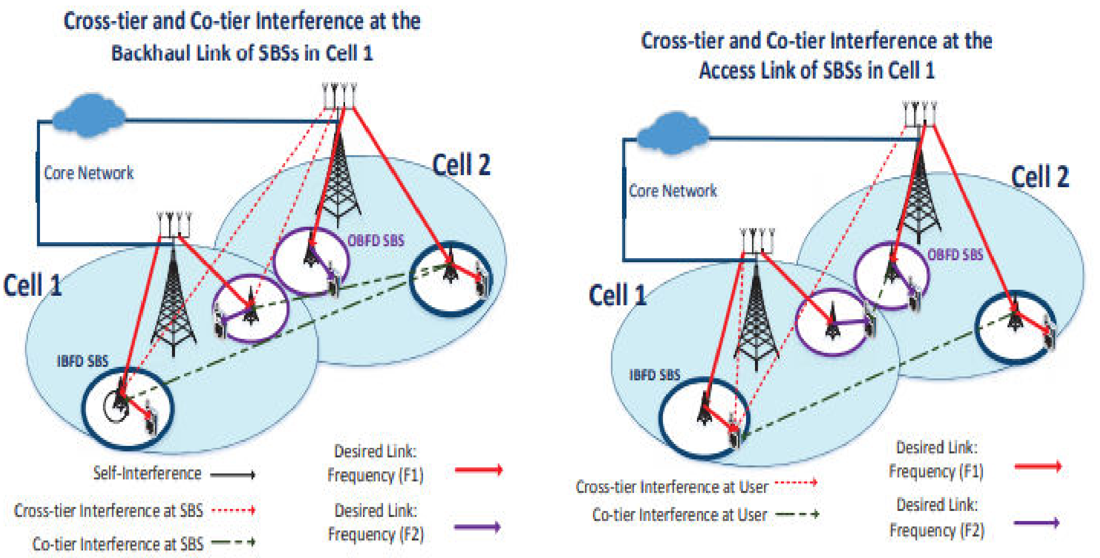

Fig. 3: Graphical illustration of the considered massive MIMO-enabled wireless backhaul network for both in-band and outof-band small cells. Co-tier and cross-tier interferences experienced at the access and backhaul links are illustrated for in-band and out-of-band small cells located in cell 1

For efficient antenna usage, in this paper, FD operation is achieved at the SBS using a shared antenna that separates the transmitting and receiving circuit chains through an ideal circulator. The transmission mode selection for small cells is modeled by independent Bernoulli RVs such that small cells are configured in IBFD and OBFD mode with probability q and $1-q$, respectively, where q is identical for all small cells. With the independent thinning of Φ_s, we can represent the SBSs in IBFD and OBFD modes as two independent PPPs Φ_{sI} and Φ_{sO} with density $q\lambda_s$ and $(1-q)\lambda_s$, respectively Although the feasibility of HD SBSs (referred as out-ofband FD SBSs in this paper) has been investigated for wireless backhauls, there has not been any comprehensive study on the performance and feasibility of FD SBSs (referred as inband FD SBSs in this paper) in wireless backhauled small cell networks. In particular, the use of full-duplex communication in wireless backhauling and the performance gains have not been investigated. With this motivation, this paper provides a framework to understand the performance and significance of full-duplex communication in wireless backhaul networks. While the in-band FD operation can ideally double the spectral efficiency in a link, the network-level gain of exploiting FD transmission in the wireless backhauls remains unclear due to the complicated interference environments, e.g., SI, co-tier, and cross-tier interferences at the backhaul and access links (as illustrated in Fig. 3). Due to the complicated interference environments in full-duplex backhaul transmission scenarios, a theoretical framework is required to characterize the diverse interference issues and to critically analyze the scenarios in which in-band backhauling may be beneficial over out-of-band backhauling. In this context, the contributions of this paper are listed as follows: • Using tools from stochastic geometry, we model the performance of a massive MIMO-enabled wireless backhaul network that supports single-antenna small cells. A hierarchical network structure is considered in which the massive MIMO-enabled wireless backhaul hubs (or connector nodes (CNs)) are deployed to provide simultaneous backhaul to multiple SBSs. Each SBS can be configured either in the in-band or out-of-band FD backhaul mode with a certain probability. Note that the in-band FD backhaul mode leads to three-node full-duplex (TNFD) transmission which involves three nodes, i.e., the CN transmits to an SBS and the SBS transmits to a user2.

- The downlink rate coverage (which is a function of the rate coverage in the access and backhaul links) of a small cell user is derived considering both the in-band and out-of-band FD backhaul modes of a given SBS. Due to the channel hardening effect in massive MIMO, the backhaul links experience long-term channel effects only, whereas the access links experience both the long term and short term channel effects. Thus, unlike traditional Rayleigh fading assumption, the framework captures the heterogeneity of the access and backhaul links.
- Closed-form rate coverage expressions are then provided for specific scenarios. The simplified expressions, under the assumption of perfect backhaul coverage, are then utilized to customize the proportion of in-band and outof-band FD SBSs in a small cell network in closed-form.
- A distributed backhaul interference-aware mode selection mechanism is then discussed to gain insights into selecting the proportion of in-band and out-of-band FD SBSs as a function of network parameters.
- Due to backhaul interference, downlink transmission to a user by an SBS is directly affected by the transmission in the backhaul link to this SBS. We therefore present few remedial solutions that can potentially mitigate the backhaul interference and quantify the enhancements in the performance of in-band FD wireless backhauls.

4.SIMULATION RESULTS

Intuitively, when all SBSs operate in OBFD mode, the system suffers the most serious co-tier and cross-tier interference and the induced throughput can be seen as a lower bound, we take it as a benchmark in our simulations. Besides, two centralized algorithms, i.e., genetic algorithm (GEA) and greedy algorithm (GRA) based on heuristic searching, are compared with the proposed DGCA method. Fig. 4,5,6 and 7 shows that the downlink throughput increases linearly with the number of SBSs. This is intuitive since dense smallcell network leads to better network performance. Also, it can be seen that DGCA, GEA and GRA induce a significant gain compared with the benchmark, which is benefited from the selection of IBFD mode. Although the performance of DGCA is not as good as GRA, it is still very promising due to its capability of reducing MBS's computation overhead.

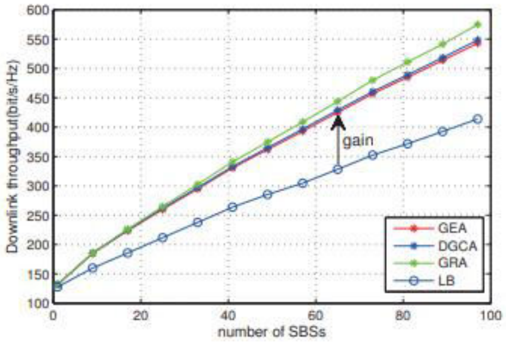

Fig. 4. Downlink capacity versus the number of SBSs when $N = 200$

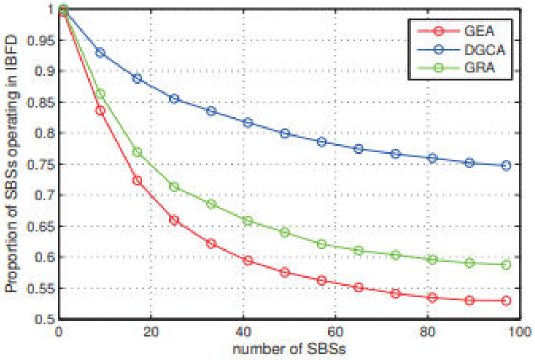

Fig. 5. The selection proportion of IBFD mode versus the number of SBSs

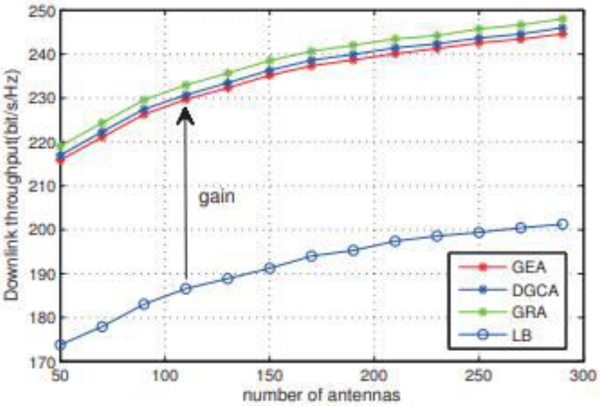

Fig. 6. Downlink capacity versus the number of antennas N when $S = 20$

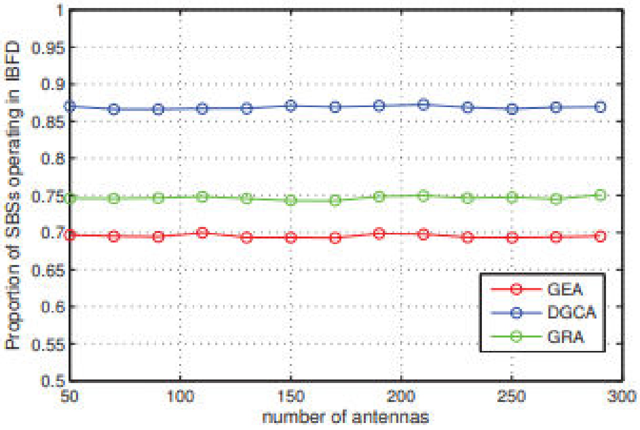

Fig. 7. The selection proportion of IBFD mode versus the number of antennas

5. CONCLUSION

We have investigated the performance of a massive MIMOenabled wireless backhaul network which is composed of a mixture of small cells configured either in the in-band or outof-band FD backhaul mode. The feature of massive MIMO at CNs and shared-antenna based full-duplexing at SBSs can enable the use of the proposed framework in existing LTE-A standards. Downlink coverage probability has been derived for a typical user considering both the IBFD and OBFD modes. It has been shown that selecting a correct proportion of out-ofband small cells in the network and appropriate SI cancellation value is crucial in obtaining a high rate coverage. Few remedial solutions for backhaul interference management have been presented. The framework can be extended to include multiple antennas at SBSs, to consider the possibility of serving users through CNs, i.e., depending on the coverage requirements a user can opportunistically switch between SBSs and CNs. Further extensions to this work could include the effect of opportunistic scheduling on the rate coverage probability

REFERENCES

[1] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, “On the application of cooperative transmission to secrecy communiactions,” IEEE J. Sel. Areas Commun., vol. 30, no. 2, pp. 359–368, Feb. 2012.

[2] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, “Physical layer security of TAS/MRC with antenna correlation,” IEEE Trans. Inf. Foren. Sec., vol. 8, no. 1, pp. 254–259, Jan. 2013.

[3] J. Zhu, R. Schober, and V. K. Bhargava, “Secure transmission in multicell massive MIMO systems,” IEEE Trans. Wireless Commun., vol. 13, no. 9, pp. 4766–4781, Sep. 2014.

[4] F. Zhu, F. Gao, M. Yao, and H. Zou, “Joint information- and jammingbeamforming for physcial layer security with full duplex base station,” IEEE Trans. Signal Process., vol. 62, no. 24, pp. 6391–6401, Dec. 2014.

[5] Y. Zou, J. Zhu, X. Wang, and V. Leung, “Improving physical-layer security in wireless communications using diversity techniques,” IEEE Network, vol. 29, no. 1, pp. 42–48, Jan. 2015.

[6] F. Al-Qahtani, C. Zhong, and H. M. Alnuweiri, “Opportunistic relay selection for secrecy enhancement in cooperative networks,” IEEE Trans. Commun., vol. 63, no. 5, pp. 1756–1770, May 2015.

[7] X. Fang, X. Sha, and L. Mei, “Guaranteeing wireless communication secrecy via a WFRFT-based cooperative system,” China Commun., vol. 12, no. 9, pp. 76–82, Sep. 2015.

[8] J. Zhu, R. Schober, and V. K. Bhargava, “Linear precoding of data and artificial noise in secure massive MIMO systems,” IEEE Trans. Wireless Commun., vol. 15, no. 3, pp. 2245–2261, Mar. 2016.

[9] S. Gong, C. Xing, Z. Fei, and J. Kuang, “Resource allocation for physical layer security in heterogeneous network with hidden eavesdropper,” China Commun., vol. 13, no. 3, pp. 82–95, Mar. 2016.