Multi-antenna Wireless Legitimate Surveillance Systems: Design and Performance Analysis

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

[1]Associate Professor,[2]Assistant 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. Assuming that the legitimate monitor can successfully overhear the suspicious information only when its achievable data rate is no smaller than that of the suspicious receiver, the key objective is to maximize the eavesdropping non-outage probability by joint design of the jamming power, receive and transmit beamformers at the legitimate monitor. Depending on the number of receive/transmit antennas implemented, i.e., single-input single-output, single-input multipleoutput, multiple-input single-output and multiple-input multipleoutput (MIMO), four different scenarios are investigated. 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: full-duplex multi-antenna, multiple-input multiple output (MIMO), low-complexity suboptim.

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 [1-9], and various sophisticated techniques such as artificial noise and security-oriented beamforming 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. The main contributions of this paper are summarized as follows:

- Depending on the number of receive/transmit antennas implemented at the legitimate monitor, i.e., single-input single-output (SISO), single-input multipleoutput (SIMO), multiple-input single-output (MISO) and multiple-input multiple-output (MIMO), four different scenarios are studied. For each case, the optimal jamming power is derived in closed-form. In addition, employing the semidefinite relaxation (SDR) technique, the efficient algorithms are obtained for the optimal transmit/receive beamforming vectors.
- Three low-complexity suboptimal beamforming schemes are proposed, namely, transmit zero-forcing (TZF)/ maximum ratio combing (MRC), maximum ratio transmission (MRT)/ receive zero-forcing (RZF), and MRT/ MRC. Closed-form expressions for the eavesdropping nonoutage probability of TZF/MRC and MRT/RZF schemes are derived. In addition, simple and informative high SNR approximations of all suboptimal schemes are presented.
- The findings of the paper suggest that, deploying multiple antennas is an effective means to enhance the system performance. Also, the optimal joint jamming power and beamforming scheme outperforms the proposed suboptimal schemes, the performance gap is rather insignificant compared with the TZF/MRC scheme, and gradually diminishes when the maximum jamming power becomes large. In addition, full diversity can be achieved by the MRC scheme, while the RZF attains a lower diversity since one degree of freedom is used for self-interference cancellation.

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.Another work [9]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.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 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.

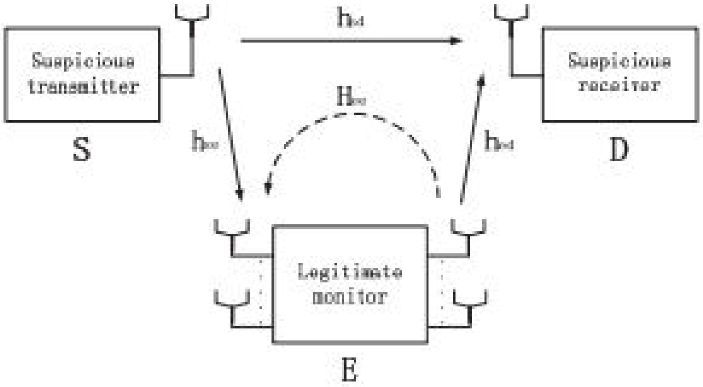


Fig. 1: A point-to-point legitimate surveillance system consisting of one suspicious transmitter S, one suspicious receiver D and one legitimate monitor E.

The received signal at the suspicious receiver D can be expressed as

$$yD = p\ PS\ hsds + hedwtx + nd \qquad (1)$$

where PS denotes the transmit power of the suspicious transmitter, hsd is the channel coefficient of the S → D link which is a zero-mean complex Gaussian random variable with variance λ1. The 1 × Nt vector hed denotes the jamming channel between E and D, whose entries are identically and independently distributed (i.i.d.) zero-mean complex Gaussian random variables with variance λ3 and wt is the transmit beamforming vector at the legitimate monitor with ‖wt‖ = 1.

In addition, s is the information symbol with unit power, while x denotes the jamming symbol with E{|x| 2} = pd satisfying 0 ≤ pd ≤ PJ where PJ denotes the maximum jamming power. Finally, nd is the zero-mean additive white Gaussian noise (AWGN) with variance ND. Similarly, the received signal at the legitimate monitor E is given by

$$yE = p\ PShses + \surd\ \rho Heewtx + ne, \qquad (2)$$

where the Nr ×1 vector hse denotes the channel coefficient of the S → E link with entries being i.i.d. zero-mean complex Gaussian random variables with variance λ2. As the residual self-interference channel is modeled by √ρHee, where the Nr×Nt matrix Hee denotes the fading loop channel with entries being i.i.d. zero-mean complex Gaussian random variables with variance λ4 and ρ (0 ≤ ρ ≤ 1) parameterizes the effect of passive self-interference suppression. Finally, ne is the zero-mean AWGN noise at the legitimate monitor with E{nen † e } = NEINr .

We assume that E employs a linear receiver wr with ||wr|| = 1 for signal detection, as such,

yE = w† ryE = p PSw† rhses + √ ρw† rHeewtx + w† rne. (3)

Therefore, the end-to-end signal-to-interference-plus-noise ratio (SINR) at the suspicious receiver SINRD and the legitimate monitor SINRE can be respectively expressed as

SINRD = PS |hsd| 2 pd|hedwt| 2 + ND and

SINRE = PS|w† rhse| 2 ρpd|w † rHeewt| 2 + NE (4)

We assume that global channel state information (CSI) is available at the legitimate monitor 2, while the suspicious transmitter and receiver only know the CSI of the suspicious link. This assumption is practical since it is difficult for the suspicious transmitter to know the existence of the legitimate monitor. To ensure reliable detection at D, the suspicious transmitter varies the transmission rate according to SINRD. Hence, if SINRE ≥ SINRD, the legitimate monitor can also reliably decode the information. On the other hand, if SINRE < SINRD, it is impossible for the legitimate monitor to decode the information without any error. Therefore, we adopt the following indicator function to denote the event of successful eavesdropping at the legitimate monitor:

X = 1 if SINRE ≥ SINRD, 0 otherwise, (5)

where X = 1 and X = 0 denote eavesdropping nonoutage and outage events, respectively. Note that the indicator function X is irrespective of the transmit power PS at the suspicious transmitter. As in [20], we adopt the eavesdropping non-outage probability as the performance metric. Hence, the main objective is to maximize the eavesdropping non-outage probability E{X} by jointly optimizing the receive and transmit beamforming vector wr, wt and the jamming power pd. Hence, the optimization problem can be formulated as

(P1) : max wr,wt,pd E{X} s.t. 0 ≤ pd ≤ PJ & ||wr|| = ||wt|| = 1 (6)

4.SIMULATION RESULTS

In this section, numerical results are presented to illustrate the performance of the proposed proactive eavesdropping schemes and validate the analytical expressions. Unless otherwise specify, the number of transmit and receive antennas at the legitimate monitor is Nt = Nr = 3, the noise variances at both D and E are normalized such that ND = NE = 1, the self-interference coefficient is ρ = 0.5, the average channel gains λ1, λ2, λ3 and λ4 are set to be 1, 0.1, 0.1 and 1, respectively.

Fig. 2 depicts the eavesdropping non-outage probability for the SISO case. For comparison, the performance of the two benchmark schemes proposed in literature are also plotted, namely, 1) Proactive eavesdropping with constant jamming power, i.e., pd = PJ , 2) Passive eavesdropping, i.e., pd = 0. As expected, the proposed proactive eavesdropping with optimal jamming power substantially outperforms the other two reference schemes. Moreover, we observe that for the proactive constant-power jamming scheme, increasing the jamming power may decrease the eavesdropping non-outage probability due to the potential severe interference inflicted on the legitimate monitor. In contrast, increasing the maximum jamming power is always beneficial for the proposed proactive eavesdropping scheme with optimal jamming power.

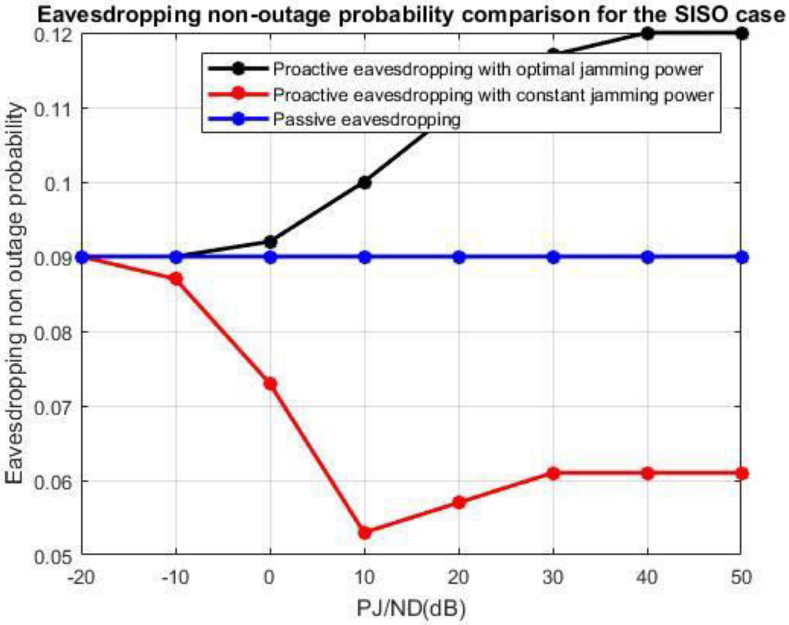


Fig. 2: Eavesdropping non-outage probability comparison for the SISO case.

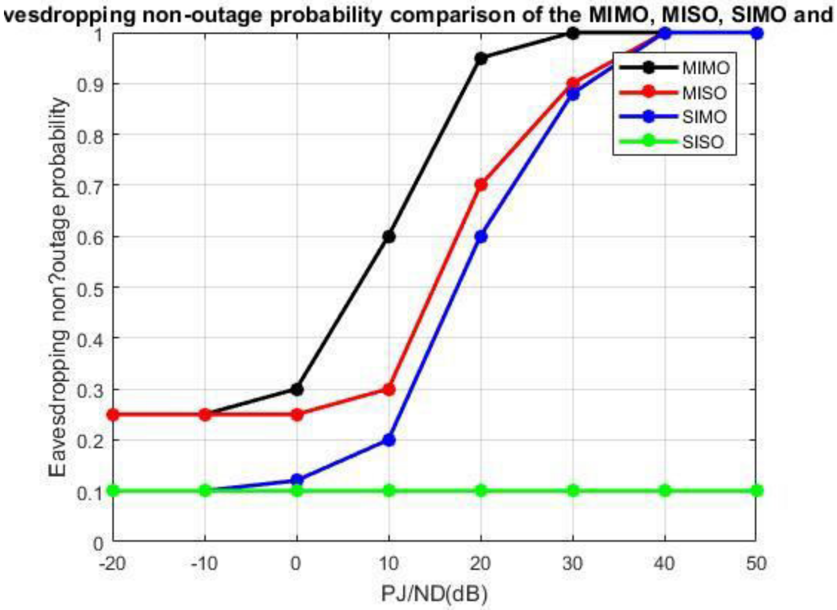


Fig. 3: Eavesdropping non-outage probability comparison of the MIMO, MISO, SIMO and SISO cases.

Fig. 3 compares the achievable eavesdropping non-outage probability of the MIMO, MISO, SIMO and SISO cases. As expected, the MIMO case always yields the best performance, while the SISO case is the worst. Also, the MISO and SIMO cases significantly outperform the SISO case, thereby demonstrating the potential benefit of implementing multiple antennas at the legitimate monitor. In addition, the performance of SIMO case is in general better then the MISO case. When the maximum jamming power is sufficiently large, the eavesdropping non-outage probability of all multiple antenna cases approaches one. However, if the maximum jamming power is small, the benefit of deploying multiple transmit antenna vanishes.

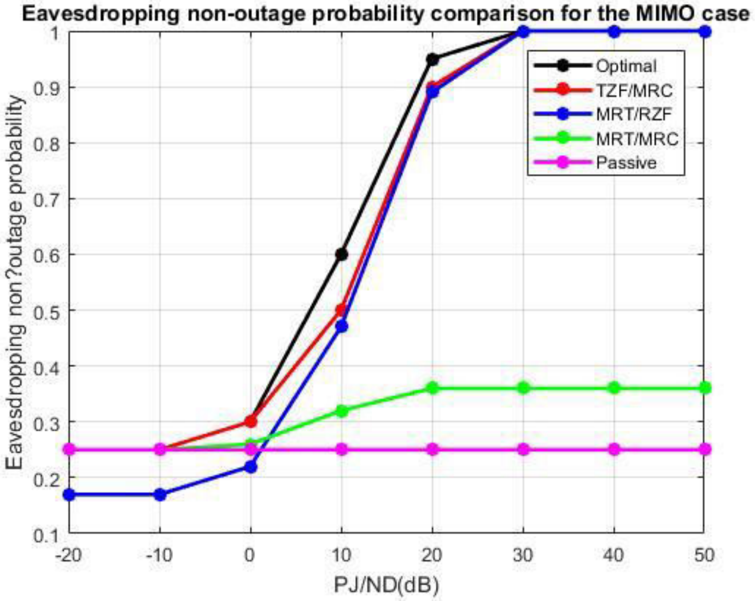


Fig. 4: Eavesdropping non-outage probability of the MIMO case: Optimal design v.s. Suboptimal design.

Fig. 4 illustrates the eavesdropping non-outage probability of the proposed suboptimal schemes. We observe that, among the proposed suboptimal schemes, the TZF/MRC scheme achieves the best performance, and remarkably, it has a similar performance as the optimal scheme. Also, the performance of the MRT/MRC scheme is noticeably worse than that of the TZF/MRC and MRT/RZF schemes with moderate maximum jamming power, which indicates the critical importance of properly handling the self-interference at the legitimate monitor. In addition, the MRC schemes outperform the RZF scheme at low maximum jamming power region, the reason is that in such region, the self-interference is rather insignificant, hence, it is better to utilize all the receive antennas to enhance the quality of the desired signal, instead of sacrificing one degree of freedom for self-interference suppression.

Fig. 5 plots the eavesdropping non-outage probability with different self-interference suppression parameter ρ for the MIMO case. We observe that, regardless of ρ, the optimal scheme achieves the best performance. Also, for the ZF-based schemes, the eavesdropping non-outage probability remains constant, since both schemes can perfectly eliminate selfinterference. While for the MRT/MRC scheme, increasing ρ decreases the eavesdropping non-outage probability, and when ρ is small, the MRT/MRC scheme tends to outperform other suboptimal schemes.

Fig. 6 investigates the eavesdropping non-outage probability with different Nt for the MIMO case when Nt + Nr = 14. From Fig. 6(a) and Fig. 6(b), we see that, for the optimal, TZF/MRC and MRT/RZF schemes, there exists a unique Nt which yields the best performance. However, for the MRT/MRC scheme, the impact of Nt on the achievable performance depends heavily on λ4. With large λ4, i.e., λ4 = 1, which corresponds to the strong self-interference scenario, it is better to deploy more antennas at the receive side as shown in Fig. 6(a). On the other hand, with small λ4, i.e., λ4 = 0.1, which corresponds to the weak self-interference scenario, the number of transmit and receive antenna needs to be balanced.

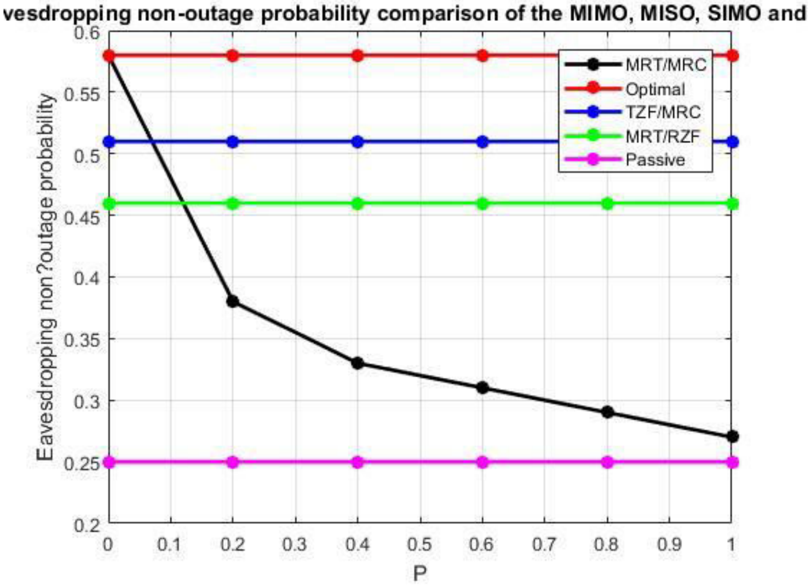
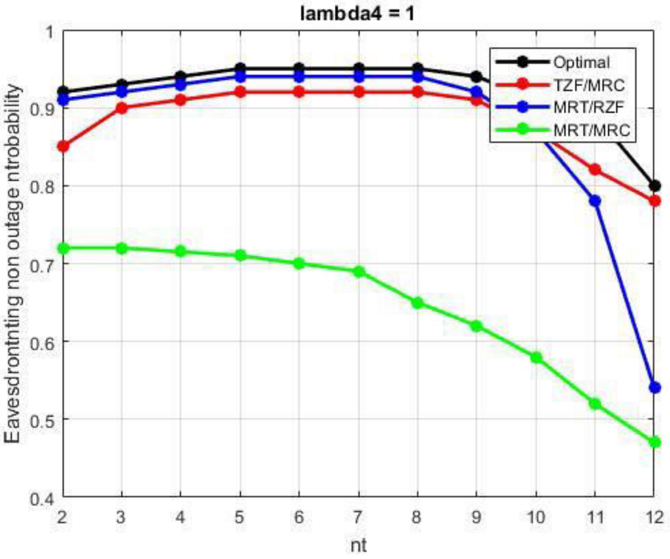
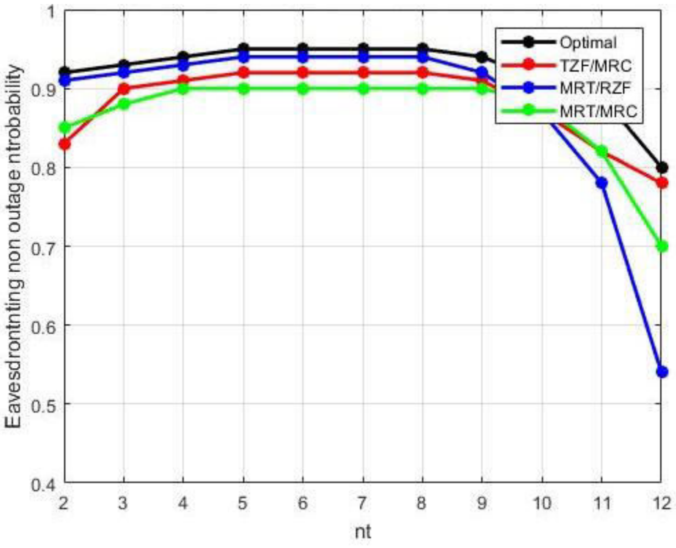


Fig. 5: Eavesdropping non-outage probability versus self-interference suppression parameter ρ for the MIMO case with PJ /ND = 10dB.



(a)



(b)

Fig. 6: Eavesdropping non-outage probability versus Nt for the MIMO case with Nt + Nr = 14 and PJ /ND = 10dB.

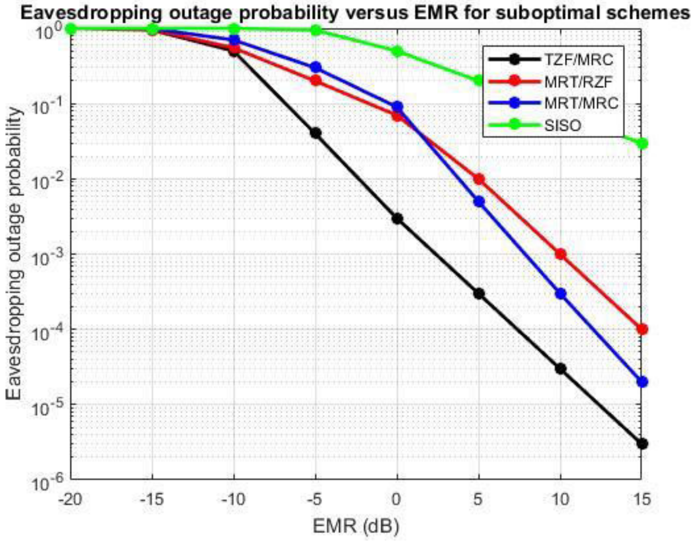


Fig. 7: Eavesdropping outage probability versus EMR for suboptimal schemes with PJ /ND = 10dB

The main reason is that, with strong self-interference, the benefit of deploying more antennas at the receive side to enhance the eavesdropping channel capacity overweights the capacity degradation of the suspicious channel by employing the same number of transmit antennas. Fig. 7 examines the eavesdropping outage probability with different EMR for the proposed suboptimal schemes. We observe that both the TZF/MRC and MRT/MRC schemes achieve a diversity order of Nr, and the MRT/RZF scheme attains a diversity order of Nr − 1, while the SISO scheme only achieves unit diversity order, which is consistent with the analytical results presented in section IV. In addition, the MRT/RZF scheme outperforms the MRT/MRC scheme when the EMR is small, while becomes inferior as the EMR increases.

5. CONCLUSION

We have studied the joint design of jamming power and transmit/receive beamforming vectors at the legitimate monitor to maximize the eavesdropping non-outage probability. Four different scenarios have been considered. For each scenario, the optimal jamming power was characterized in closed-form. Also, efficient algorithms were proposed to obtain the optimal transmit/receive beamforming vectors. Finally, low-complexity suboptimal beamforming schemes were proposed, and analytical expressions were derived for the achievable eavesdropping non-outage probabilities of the suboptimal schemes. The findings suggest that adopting multiple-antenna tremendously improves the performance of the system. Moreover, the suboptimal TZF/MRC scheme attains similar performance as the optimal scheme, hence provides an attractive low-complexity solution for practical implementation.

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.