Channel Correlation Map based Indoor-to-outdoor Artificial Noise Design and Secrecy Analysis

Huijun Li*, Zekai Liang*, Güneş Karabulut Kurt†, Gerd Ascheid*, Guido Dartmann*
*Institute for Communication Technologies and Embedded Systems, RWTH Aachen University
{huijun.li, ascheid, dartmann}@ice.rwth-aachen.de, zekai.liang@rwth-aachen.de
†Wireless Communications Research Laboratory, Istanbul Technical University, Turkey
gkurt@itu.edu.tr

***Abstract*—Generating random artificial noise (AN) in the null space of the legitimate channel is an effective way to achieve secrecy in wireless communication when the locations and channels of eavesdroppers are not known. In this paper, we propose an AN design based on the channel correlation map assuming passive eavesdroppers (Eves) for indoor-to-outdoor scenario. Channel correlation map is a geographical map with overlay knowledge of long-term channel correlation matrices for possible Eves' locations. This knowledge is learned by legitimate users passing through these areas in the past. Different from the existing secrecy analyses with passive Eves, correlated transmit antenna arrays are assumed. Our AN vector is generated by maximizing the secure probability of attaining a pre-determined secrecy level for a certain number of the most dangerous potential Eves, which is found by the correlation map. We give an intuitive view of the secrecy performance for the whole area and show that our strategy enhances the secrecy level of the system when compared to the existing random null space AN method.**

I. Introduction

Secure wireless communication is essential for protecting legitimate users. Today, the security relies on bit-level cryptographic techniques, which are offline analyses and may not perfectly be secure if an eavesdropper has enough time and computing resources to extract the key. Physical layer security was pioneered by Wyner [1] and is a promising complementary solution. In secrecy problems, the legitimate transmitter (Alice) sends signals to the legitimate receiver (Bob) in the presence of the eavesdropper (Eve). Security in physical layer exploits the natural variation of wireless channels to degrade the Eve's signal-to-noise ratio (SNR) while guaranteeing Bob's SNR to be above a certain level.

There are two basic scenarios concerning the status of Eve: 1) Eve is active, so the channel between Alice and Eve is assumed to be available at Alice; 2) Eve is passive, then the position and the channel of Eve are not known. In the literature, the first scenario was considered more often assuming the presence of channel state information (CSI) of all links. Beamforming transmission was found to be the optimal input structure for Gaussian nodes in [2]. The authors in [3] designed beamforming and artificial interference by jointly maximizing the inverse SNR of Eve and the SNR of Bob. In [4], the optimal power allocation was developed to maximize the secrecy rate achievable by beamforming assuming the awareness of Eve's location. However the assumption of available Eve's location or/and CSI knowledge is impractical, as it is more likely to observe the second scenario in practice.

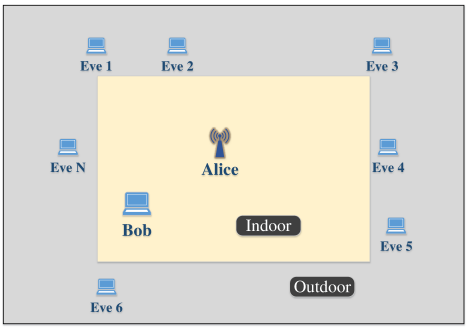

Fig. 1. System outline. Alice and Bob are legitimate transmitter and receiver respectively, that are located indoors. Multiple Eves (N) are located outdoors closely.

This passive eavesdropping case is more challenging. Artificial noise (AN) based method is effective since Eve's CSI is not known. In this method, Alice uses a fraction of her power to send information-bearing signals with a beamforming vector and the rest to generate AN, which is injected into the null-subspace of Bob's channel. The authors in [5] and [6] considered fast fading characteristics of Eve's channel to calculate the outage probability, which is defined as the probability that the instantaneous secrecy capacity falls below a certain secrecy rate. The presence of a Poisson random field of Eves was considered in [7] and [8]. In the above literature, uncorrelated antenna arrays were assumed and the AN vectors were random combinations of all the basis vectors orthogonal to Bob's channel, because the CSI of Eve is not known. In this paper, we consider a scenario where Alice and Bob are in an indoor environment while multiple passive Eves are outside but still within a close proximity. The system outline is shown in Fig. 1. We have no constraint on the number or distribution of Eves. This is a practical scenario for places such as institutes and factories. It is specially of significant importance to cyber-physical system. Here, the secure communication should be guaranteed within the members indoors. We assume correlated antenna arrays. The long-term channel correlation matrices for the whole outdoor neighborhood can be learned through channel feedback by legitimate users passing by these areas. With this knowledge, we introduce a channel correlation map,

which is a geographical map with overlay channel correlation matrices at position samples. Instead of generating random AN vectors orthogonal to Bob's channel, we propose an AN generation approach to maximize the secure probability of having a certain level secrecy capacity for the most dangerous potential Eves (defined in Section III) based on the correlation map. This is different from the assumption of available channel correlation information of Eve as partial knowledge because Alice in this paper has no knowledge about Eves and they might exist on all the location samples. Further we give a method to calculate the probability with correlated Gaussian antenna arrays. Through the correlation map we illustrate the secrecy performances for the whole indoor-to-outdoor area intuitively and show that the proposed approach guarantees a more secure transmission than the random null space AN method.

The rest of the paper is organized as follows. Section II describes the system and signal model for our indoor-to-outdoor scenario. We present the AN design algorithm based on channel correlation map in Section III. In Section IV, the performance of the proposed method is shown. Finally, conclusions are given in Section V.

II. System Model

We consider an indoor wireless network which consists of a single legitimate transmitter Alice, that can be a base station (BS) equipped with N_t correlated elements, a single-antenna legitimate receiver (Bob) and a number of single-antenna passive eavesdroppers (Eves) in the surrounding outdoor area, which is called indoor-to-outdoor area. The channel between Alice and Bob is denoted by $\boldsymbol{h}_b \in \mathbb{C}^{N_t \times 1}$, which is perfectly known by Alice. Eve's channel $\boldsymbol{h}_e$ and position are assumed not known by Alice. Here we model the received signal from one of the Eves in order to maintain notational simplicity. The model will be extended to presence of multiple Eves in the following sections.

The total transmit power is denoted by P. Alice uses a fraction of it to transmit a data signal using beamforming and the rest to transmit artificial noise. Thus, the transmitted signal can be written as:

$$\boldsymbol{x} = \sqrt{\alpha P}\boldsymbol{u}s + \sqrt{(1-\alpha)P}\boldsymbol{z} \tag{1}$$

with $\alpha \in [0,1]$ and $\mathbb{E}\{|s|^2\} = 1$. The signal s is the data information transmitted to Bob. The vector $\boldsymbol{u} \in \mathbb{C}^{N_t \times 1}$ is the normalized beamforming vector with $||\boldsymbol{u}|| = 1$ and $\boldsymbol{z} \in \mathbb{C}^{N_t \times 1}$ is the AN vector with $||\boldsymbol{z}|| = 1$. Thus, the received signals by Bob and Eve are written as follows:

$$y_b = \boldsymbol{h}_b^H \boldsymbol{x} + n_b \tag{2}$$

$$y_e = \boldsymbol{h}_e^H \boldsymbol{x} + n_e \tag{3}$$

where the additive noise terms n_b and n_e are independent complex Gaussian random variables with zero means and variances σ_b^2 and σ_e^2.

In order to suppress Eve's SNR while not decreasing Bob's SNR, Alice sets the beamforming vector to $\boldsymbol{u} = \boldsymbol{h}_b/||\boldsymbol{h}_b||$, which is the eigenvector corresponding to the largest eigenvalue of $\boldsymbol{h}_b\boldsymbol{h}_b^H$ [5] [6]. The artificial noise should meet the condition $\boldsymbol{h}_b^H\boldsymbol{z} = 0$. The SNR of Bob and Eve are given by:

$$\gamma_b = \frac{\alpha P||\boldsymbol{h}_b||^2}{\sigma_b^2} \quad , \tag{4}$$

$$\gamma_e = \frac{\alpha P \boldsymbol{h}_e^H R_{\boldsymbol{u}} \boldsymbol{h}_e}{\sigma_e^2 + (1-\alpha)P\boldsymbol{h}_e^H R_{\boldsymbol{z}} \boldsymbol{h}_e} \tag{5}$$

with $R_{\boldsymbol{u}} = \boldsymbol{u}\boldsymbol{u}^H$ and $R_{\boldsymbol{z}} = \boldsymbol{z}\boldsymbol{z}^H$.

III. Channel Correlation Map based Artificial Noise Design

The aim of the proposed system is to increase the secrecy capacity of the interested area, which is defined as:

$$C = (\log_2(1+\gamma_b) - \log_2(1+\gamma_e))^+ \tag{6}$$

with $x^+ = \max(x, 0)$. It is the maximum achievable rate from Alice to Bob while keeping Eve completely ignorant of the transmitted message [5]. In this section, we first briefly describe the random AN generation by literature and the concept of channel correlation map. Then, the AN design is proposed based on the correlation map to maximize the secure probability of reaching a certain secrecy capacity level.

A. Review of Random AN Generation

Because Eve's channel $\boldsymbol{h}_e$ is not known by Alice, the AN vector $\boldsymbol{z}$ is obtained by the random linear combination of the remaining $N_t - 1$ eigenvectors of $\boldsymbol{h}_b\boldsymbol{h}_b^H$ except the beamforming vector $\boldsymbol{u}$. In this way, the AN vector is always orthogonal to the beamformer. In [6] and [7] the power is distributed equally among these eigenvectors without Eve's CSI knowledge, i.e.,

$$\boldsymbol{z} = \sqrt{\frac{1}{N_t - 1}} \sum_{i=2}^{N_t} \boldsymbol{u}_i v_i \tag{7}$$

where $\boldsymbol{u}_i$ is the ith eigenvector of $\boldsymbol{h}_b\boldsymbol{h}_b^H$ and v_i is a random complex scalar with unit magnitude and uniformly distributed phase.

B. Channel Correlation Map

Long-term channel correlation matrices are determined by large scale position-dependent parameters like path loss, shadowing, local scattering. This knowledge can be learned per location. Although the instantaneous CSIs of Eves are not known, the long-term channel correlation matrices of possible Eves can be learned by channel feedback of legitimate users passing the indoor-to-outdoor area in the history. The correlation matrices are averaged per location samples.

Let $\bar{R}_{\boldsymbol{e}} = \mathbb{E}\{\boldsymbol{h}_e\boldsymbol{h}_e^H\}$ denote the long-term channel covariance matrix of Eve and $\mathbf{tr}\{\cdot\}$ stand for the trace of a matrix. Eve's channel follows a complex Gaussian distribution $\mathcal{CN} \sim (0, \bar{R}_{\boldsymbol{e}})$ where $\varepsilon = \mathbf{tr}\{\bar{R}_{\boldsymbol{e}}\}$ accounts for the path loss and shadowing effects. The map is used to determine the dangerous potential Eves (location samples) and AN design.

C. Proposed AN Design

We assume Bob's SNR γ_b must be above a certain level SNR_b so that he can decode the message with sufficient accuracy. Thus, we guarantee Bob's SNR level and use the rest of the total power to generate the AN. The percentage of signal transmission power is calculated from Eq. (4):

$$\alpha = \frac{\text{SNR}_b \sigma_b^2}{P||\boldsymbol{h}_b||^2} \quad . \tag{8}$$

When we set a secrecy capacity threshold $C_{\text{TH}} > 0$ that denotes secure transmission $C \geq C_{\text{TH}}$, the Eve's SNR should meet $\gamma_e \leq \text{SNR}_e$ with $\text{SNR}_e = 2^{\log_2(1+\text{SNR}_b)-C_{\text{TH}}} - 1$. The secure probability $\mathbb{P}(C \geq C_{\text{TH}})$ can be written as:

$$\begin{aligned}\mathbb{P}(C \geq C_{\text{TH}}) &= \mathbb{P}(\gamma_e \leq \text{SNR}_e) \\ &= \mathbb{P}\Big(\frac{\alpha P \boldsymbol{h}_e^H R_{\boldsymbol{u}} \boldsymbol{h}_e}{\sigma_e^2 + (1-\alpha) P \boldsymbol{h}_e^H R_{\boldsymbol{z}} \boldsymbol{h}_e} \leq \text{SNR}_e\Big) \\ &= \mathbb{P}(\boldsymbol{h}_e^H A \boldsymbol{h}_e \leq \frac{\sigma_e^2}{P})\end{aligned} \tag{9}$$

with $A = \frac{\alpha}{\text{SNR}_e} R_{\boldsymbol{u}} - (1-\alpha) R_{\boldsymbol{z}}$. Then the so called outage probability in [5] and [6] is simply $\epsilon_{\text{out}} = 1 - \mathbb{P}(C \geq C_{\text{TH}})$. Although we do not know the number and the positions of Eves, we can define the dangerous location areas (contain $\tilde{M}$ location samples) where the condition $\{\boldsymbol{u}^H \bar{R}_e \boldsymbol{u} > \epsilon\}$ meets. Since $\tilde{M}$ can be very large, we find the M ($M \leq \tilde{M}$) dangerous location samples which have the M largest values of $\{\boldsymbol{u}^H \bar{R}_e \boldsymbol{u}\}$. Our strategy is to combine artificial noise vectors, which maximize the probabilities of guaranteed secrecy capacities for the M most dangerous potential Eves. For one specific Eve, the index of Eve is ignored for convenience and the problem is stated as:

$$\begin{aligned}\boldsymbol{z}^* = \underset{\boldsymbol{z}}{\text{argmax}}\, &\mathbb{P}(\boldsymbol{h}_e^H A \boldsymbol{h}_e \leq \frac{\sigma_e^2}{P}) \\ s.t. \quad &||\boldsymbol{z}|| = 1 \\ &\boldsymbol{h}_b^H \boldsymbol{z} = 0 \quad .\end{aligned} \tag{10}$$

We provide two approaches to solve this problem.

1) Semidefinite Relaxation: We can relax our problem through semidefinite programming (SDP) [9]. This problem can be reformulated as:

$$\begin{aligned}R_z^* = \underset{R_z}{\text{argmax}}\, &\mathbb{P}(\mathbf{tr}\{A R_{\boldsymbol{e}}\} \leq \frac{\sigma_e^2}{P}) \\ s.t. \quad &\mathbf{tr}\{R_{\boldsymbol{z}}\} = 1 \\ &R_{\boldsymbol{z}} \succeq 0 \\ &\mathbf{tr}\{R_{\boldsymbol{b}} R_{\boldsymbol{z}}\} = 0\end{aligned} \tag{11}$$

where $R_{\boldsymbol{b}} = \boldsymbol{h}_b \boldsymbol{h}_b^H$ and $R_{\boldsymbol{e}} = \boldsymbol{h}_e \boldsymbol{h}_e^H$. Since Eve is passive, the instantaneous correlation $R_{\boldsymbol{e}}$ is not known by the BS. However, from the map we have the long-term channel correlation of all possible Eves. If we relax the problem (12) further and use $\bar{R}_{\boldsymbol{e}}$ instead of $R_{\boldsymbol{e}}$. The problem is now rewritten as:

$$\lambda_1^* = \min_{R_z} \mathbf{tr}\{A \bar{R}_{\boldsymbol{e}}\} \tag{12}$$

$$\begin{aligned}s.t. \quad &\mathbf{tr}\{R_{\boldsymbol{z}}\} = 1 \\ &R_{\boldsymbol{z}} \succeq 0 \\ &\mathbf{tr}\{R_{\boldsymbol{b}} R_{\boldsymbol{z}}\} = 0 \quad .\end{aligned} \tag{13}$$

The optimal R_z^* can be found by a convex solver. The AN vector $\boldsymbol{z}^*$ is the eigenvector corresponding to the largest eigenvalue of R_z^*.

2) Transformation to an eigenvalue problem: The probability in Eq. (9) depends on the quadratic form $\boldsymbol{h}_e^H A \boldsymbol{h}_e$. We can reformulate the problem in Eq. (12) as:

$$\begin{aligned}\boldsymbol{z}^* = \underset{\boldsymbol{z}}{\text{argmin}}\, &\frac{\alpha}{\text{SNR}_e} \boldsymbol{u}^H R_e \boldsymbol{u} - (1-\alpha) \boldsymbol{z}^H R_e \boldsymbol{z} \\ s.t. \quad &||\boldsymbol{z}|| = 1 \\ &\boldsymbol{h}_b^H \boldsymbol{z} = 0 \quad .\end{aligned} \tag{14}$$

We relax the problem to use $\bar{R}_e$ instead of R_e. Since $B = \frac{\alpha}{\text{SNR}_e} \boldsymbol{u}^H R_e \boldsymbol{u}$ is a constant, the problem is equivalent to the following:

$$\begin{aligned}\boldsymbol{z}^* = \underset{\boldsymbol{z}}{\text{argmin}}\, &B - \boldsymbol{z}^H \bar{R}_e \boldsymbol{z} \\ s.t. \quad &||\boldsymbol{z}|| = 1 \\ &\boldsymbol{h}_b^H \boldsymbol{z} = 0 \quad .\end{aligned} \tag{15}$$

Let the matrix $C \in \mathbb{C}^{Nt \times Nt-1}$ contain $N_t - 1$ eigenvectors of $\boldsymbol{h}_b \boldsymbol{h}_b^H$ except the beamformer $\boldsymbol{u}$. According to [10], we can transform this problem by projecting the eigenvalue problem into the constraint space by explicitly constructing a basis for the null space of C. Let $\boldsymbol{z}^* = C\boldsymbol{y}^*$, we thus obtain the equivalent formulation of the problem as:

$$\lambda_2^* = \min_{\boldsymbol{y}} B - \boldsymbol{y}^H (C^H \bar{R}_e C) \boldsymbol{y} \tag{16}$$

$$s.t. \quad ||\boldsymbol{y}|| = 1 \quad .$$

Our problem is transformed to a known eigenvalue problem with a single magnitude constraint. The optimal solution $\boldsymbol{y}^*$ is the eigenvector of $C^H \bar{R}_e C$ corresponding to the largest eigenvalue.

Based on Eq. (12) and (16) we propose the AN generation algorithm summarized in Algorithm 1. The two approaches are noted by (a) and (b). The power for AN is distributed equally against those M potential Eves. The solution of AN design jointly against Eves are under development and is not within the scope of this paper. In order to calculate the probability in Eq. (9) the distribution of $\boldsymbol{h}_e$ should be considered with the optimized AN vector $\boldsymbol{z}^*$. The indefinite quadratic form (IQF) in Eq. (9) after the AN vector optimization becomes:

$$Y = \boldsymbol{h}_e^H A^* \boldsymbol{h}_e \tag{17}$$

Algorithm 1 Artificial Noise Generation

1: Determine the $\tilde{M}$ dangerous location samples $\boldsymbol{u}^H \bar{R}_e \boldsymbol{u} > \epsilon$
2: Choose the M most dangerous potential Eves ($M \leq \tilde{M}$)
$\{\bar{R}_{e1}, \bar{R}_{e2}, ..., \bar{R}_{eM}\} = \text{argmax}_{\text{all}\bar{R}_{ei}} \{\boldsymbol{u}^H \bar{R}_{ei} \boldsymbol{u}\}_{i=1}^{\tilde{M}}$
3: **for** $i = 1$ to M **do**
(a) Get $\boldsymbol{z}_i^* = \text{argmin}_{\boldsymbol{z}_i} \mathbf{tr}\{A \bar{R}_{ei}\}$, s.t. (13) through a convex solver, or
(b) Get the eigenvector $\boldsymbol{y}_i^*$ corresponding to the largest eigenvalue of $C^H \bar{R}_{ei} C$, and then calculate $\boldsymbol{z}_i^* = C\boldsymbol{y}_i^*$
4: AN vector $\boldsymbol{z}^* = \frac{1}{M} \sum_{i=1}^{M} \boldsymbol{z}_i^*$
$R_z^* = \boldsymbol{z}\boldsymbol{z}^*$

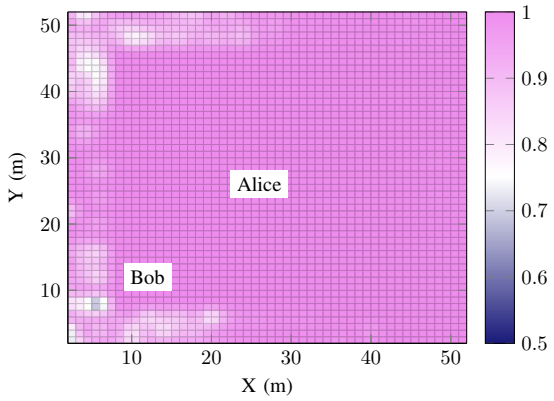

Fig. 2. Expected secure probability map using proposed AN with $M = 50$ (a). (Alice: $N_t = 4$, total power: 10mW)

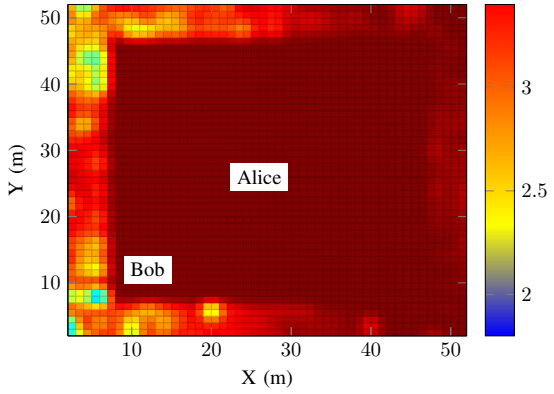

Fig. 3. Expected secrecy capacity map (bit/s/Hz) using proposed AN with $M = 50$ (a). (Alice: $N_t = 4$, total power: 10mW)

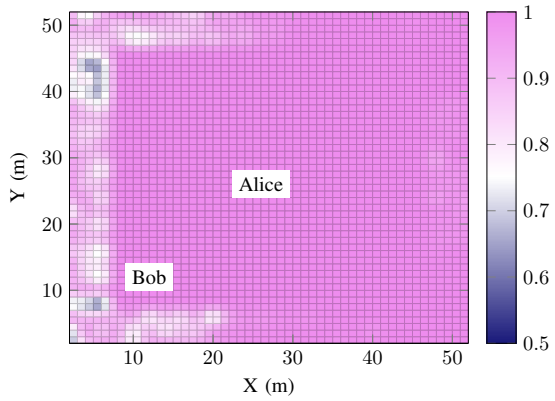

Fig. 4. Expected secure probability map using random AN. (Alice: $N_t = 4$, total power: 10mW)

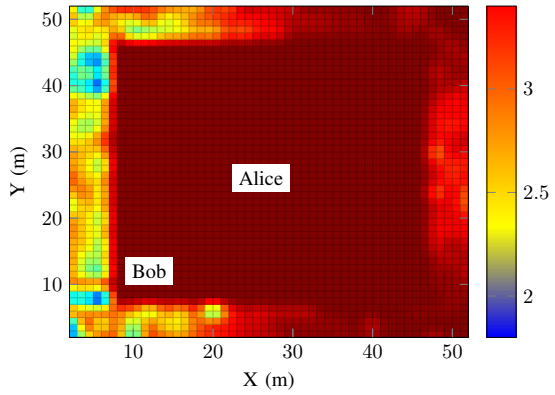

Fig. 5. Expected secrecy capacity map (bit/s/Hz) using random AN. (Alice: $N_t = 4$, total power: 10mW)

where $A^* = \frac{\alpha}{\text{SNR}_e} R_{\boldsymbol{u}} - (1-\alpha) R_{\boldsymbol{z}}^*$ is an $N_t \times N_t$ Hermitian matrix, and $\boldsymbol{h}_e$ is a complex normal random vector with zero mean and covariance matrix $\bar{R}_{\boldsymbol{e}}$. Let the matrix L be any nonsingular factorization of $\bar{R}_{\boldsymbol{e}}$, such that $\bar{R}_{\boldsymbol{e}} = 2L^H L$. The IQF can be rewritten according to [11] as:

$$Y = \boldsymbol{v}^H \Lambda \boldsymbol{v} \tag{18}$$

where $\boldsymbol{v}$ is a complex Gaussian vector with independent components whose real and imaginary parts both have zero mean and a unit variance. The matrix Λ is a diagonal matrix with (λ_1, λ_2, ...,λ_{N_t}) that are the eigenvalues of the matrix LA^*L^H. The CDF of Y can be calculated according to the derivation in [12] as:

$$F_Y(y) = u(y) - \sum_{i=1}^{N_t} \frac{\lambda_i^{N_t}}{\prod_{l \neq i}(\lambda_i - \lambda_l)} \frac{1}{|\lambda_i|} e^{-\frac{y}{\lambda_i}} u\Big(\frac{y}{\lambda_i}\Big) \tag{19}$$

where $u(y)$ is the unit step function. Since $y = \frac{\sigma_e^2}{P} \geq 0$, the probability in Eq. (9) becomes

$$\mathbb{P}(C \geq C_{\text{TH}}) = 1 - \sum_{i=1}^{N_t} \frac{\lambda_i^{N_t}}{\prod_{l \neq i}(\lambda_i - \lambda_l)} \frac{1}{|\lambda_i|} e^{-\frac{\sigma_e^2}{\lambda_i P}} u(\frac{\sigma_e^2}{\lambda_i P})$$

IV. Simulation Results

In this section we present numerical results to illustrate the performance of the proposed AN generation method in terms of average secrecy capacity and secure probability for the whole area with maps.

We evaluate the performance of our proposed algorithm by comparing it with random AN transmission described in III-A. All channel links are generated by using Winner channel model [13]. The channel correlation map is obtained by position sample moving average. The map coverage is 52m $\times$ 52m and the center 40m $\times$ 40m is indoor area and the outer-ring is indoor-to-outdoor area. Alice is transmitting with multiple linear antenna arrays with the antenna spacing the half of the wavelength. Alice is located in the center at the coordinate (26m, 26m) and Bob is located at (12m, 12m). Eve can be anywhere in the indoor-to-outdoor area. We set the noise variances to $\sigma_b^2 = \sigma_e^2 = 5 \times 10^{-6}$. The SNR threshold for Bob is set to $\text{SNR}_b = 10$ dB. The performances are averaged over sufficient channel realizations.

Fig. 2 and Fig. 4 illustrate the expected secure probability maps with the threshold $C_{\text{TH}} = 2.46$ bit/s/Hz using the proposed AN with $M = 50$ (a) and random AN approaches. The total power constraint is $P = 10$ mW and Alice transmits with 4 antenna arrays. The secrecy capacity threshold can be converted to the Eves' SNR constraint of 0 dB (SNR_e). The area between $X = 0$ m and $X = 10$ m is the most dangerous. The proposed AN (a) design offers overall a larger probability

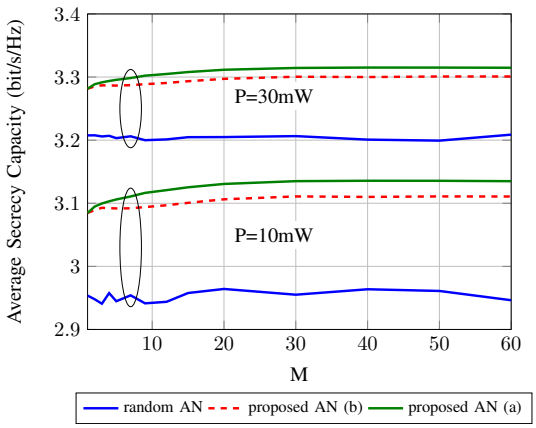

Fig. 6. Expected secrecy capacity of the dangerous area over M for different AN methods with 10mW and 30mW power constraints. (Alice: $N_t = 4$)

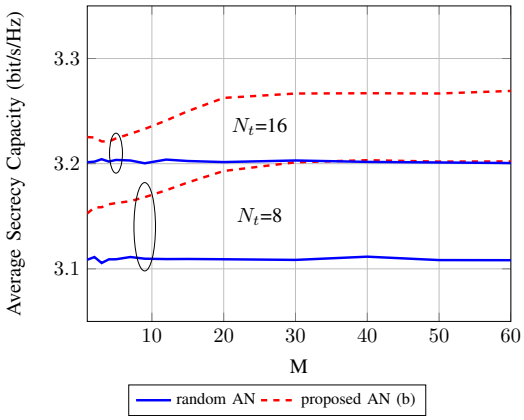

Fig. 7. Expected secrecy capacity of the dangerous area over M for different numbers of transmit antennas with power scaling. (power $P = 40/N_t$ mW)

to reach the secrecy capacity threshold than the random null space AN method. Fig. 3 and Fig. 5 show the average secrecy capacities (bit/s/Hz) of the whole area using the proposed AN approach with $M = 50$ (a) and the random AN method. The secrecy capacity for indoor-to-outdoor area using the proposed AN design is overall improved compared to that of the random AN approach. Fig. 6 compares the average secrecy capacities for the whole dangerous area over $\tilde{M}$ for three different AN generation methods: random AN, the proposed AN using matrix transformation (b) and using a convex solver (a) for two different power constraints. The both proposed methods outperform the random AN method even with $M = 1$. The method (a) achieves a better performance than (b) in the settings considered but at the expense of much higher complexity. The curves converge with the increasing parameter M ($M > 30$). In Fig. 7 we compare the performances of the random and the proposed AN methods for larger numbers of transmit antennas (N_t = 8, 16). We use power scaling to give a fair comparison, i.e. $PN_t = 40$. In this way, the part of the total power transmitting signals α in Eq. (4) would not decrease. Thus the performance gain only relies on the AN increase caused by the larger antenna arrays. Due to the computation complexity, we only show the proposed method (b). The proposed method (b) converges slower for larger antenna arrays due to larger degree of freedom in the channel vector space. For $M > 30$, the proposed method (b) for 8 transmit antennas achieves a comparable performance as the random AN method for 16 antennas.

V. Conclusion

In this paper, we propose a new AN generation method based on channel correlation maps to enhance secure transmission in the presence of passive Eves. A probability approach for correlated multiple-input-multiple-output (MISO) channel arrays are investigated. The AN vector is generated by maximizing the probability of achieving a certain level of secrecy capacity. We offered two methods to solve the problem. They are not limited to the indoor-to-outdoor scenario. Simulation results show that our algorithm guarantees a more secure communication comparing with the existing random null space AN approach. When the secrecy capacity maps such as Fig. 3 are available for all possible locations of Bobs, Alice can instruct Bob to move to a safer position. Finally, the proposed method can be extended to the scenario where multiple legitimate users and passive eavesdroppers exist with multiple antennas.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355 – 1387, Oct. 1975.

[2] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symposium on Inf. Theory*, June 2007, pp. 2466–2470.

[3] G. Dartmann, O. Cepheli, G. K. Kurt, and G. Ascheid, "Beamforming aided interference management with improved secrecy for correlated channels," in *Proc. IEEE Veh. Technol. Conf. (VTC Spring)*, May 2014.

[4] T. V. Nguyen and H. Shin, "Power allocation and achievable secrecy rates in MISOME wiretap channels," *IEEE Commun. Lett.*, vol. 15, no. 11, pp. 1196–1198, November 2011.

[5] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628–1631, October 2012.

[6] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71–74, Feb 2012.

[7] M. Ghogho and A. Swami, "Physical-layer secrecy of MIMO communications in the presence of a poisson random field of eavesdroppers," in *Proc. IEEE Int. Conf. on Commun. Workshops (ICC)*, June 2011, pp. 1–5.

[8] P. Huang and X. Wang, "Secrecy enhancement with artificial noise in decentralized wireless networks: A stochastic geometry perspective," in *Proc. IEEE Wireless Commun. and Networking Conf. (WCNC)*, April 2013, pp. 935–940.

[9] Z.-Q. Luo, W.-K. Ma, A.-C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, May 2010.

[10] G. Golub and C. V. Loan, *Matrix Computations*, 3rd ed. The Johns Hopkins University Press, 1996.

[11] D. Raphaeli, "Distribution of noncentral indefinite quadratic forms in complex normal variables," *IEEE Trans. on Inf. Theory*, vol. 42, no. 3, pp. 1002–1007, May 1996.

[12] T. Al-Naffouri and B. Hassibi, "On the distribution of indefinite quadratic forms in gaussian random variables," in *Proc. IEEE Int. Symposium on Inf. Theory*, June 2009, pp. 1744–1748.

[13] "MATLAB implementation of the WINNER phase II channel model ver1.1 [online]," L. Hentil, P. Kysti, M. Kske, M. Narandzic , and M. Alatossava, Dec 2007. [Online]. Available: https://www.ist-winner.org/phase_2_model.html