On Spatial Security Outage Probability Derivation of Exposure Region Based Beamforming with Randomly Located Eavesdroppers

Yuanrui Zhang*, Youngwook Ko*, Roger Woods*, Alan Marshall§, Joe Cavallaro‡, Kaipeng Li‡,
* ECIT, Queen's University Belfast
Belfast, Northern Ireland, UK
Email: {yzhang31,y.ko,r.woods}@qub.ac.uk
§ Electrical Engineering and Electronics, University of Liverpool
Liverpool, England, UK
Email: Alan.Marshall@liverpool.ac.uk
† Department of Electrical and Computer Engineering, Houston, Texas, USA
Email: {cavallar, kaipeng.li}@rice.edu

***Abstract*—This paper presents the close-form expression of the spatial security outage probability, which is a novel performance metric that measures the security level of the legitimate transmission from the spatial aspect in the presence of Poisson Point Process distributed eavesdroppers. Beamforming is used to create the exposure region where any randomly located eavesdropper causes secrecy outage, based on which the general expression of the spatial security outage probability is derived. Based on the general expression, the close-form expression is obtained for the circular array, which reveals the impact of the array parameters on the security performance.**

I. Introduction

With the ubiquitous utility of wireless communications, the need to develop higher level security grows stronger. Physical layer security has recently received much attention as a complementary approach to the traditional encryption techniques in the higher layers [1]. Much research work is based on Wyner's wiretap channel model [2] and has extended to various channel models (see [3] and references therein). However, the large-scale path loss is not much considered due to the fact that the users are often randomly distributed, until recently, with the aid of the stochastic geometry theory, the distribution of the random users' locations can be modeled, e.g., via Poission point process (PPP) [4], [5].

Users' locations provide intrinsic distinction for the related channels because the large-scale path loss is related to users' distances to the transmitter. In Wyner's wiretap channel model, the legitimate user should have better channel than the eavesdropper. Therefore, user's location should be taken into account when considering a secure transmission to a legitimate user in presence of eavesdroppers. In this paper, we consider the classic model of Alice, Bob and Eve(s), where Alice is equipped with uniform circular array (UCA) and wishes to transmit to Bob in presence of PPP distributed Eves. Bob and Eves have a single antenna. Beamforming is performed to create the exposure region (ER) where any Eve inside causes secrecy outage to the legitimate transmission.

There has been work that considers the physical region related to secure transmissions [5]–[9]. However, in [6], [7], the physical region is not based on the information-theoretic parameters, thus is not subject to information-theoretic security analysis. In [5], [8], [9], the physical region is based on the secrecy outage probability. However, the array parameters are overlooked. Since beamforming is performed via antenna arrays, the ER created by using beamforming is highly related to the array parameters and can be controlled via changing the array parameters.

In this paper, the ER based beamforming is proposed to investigate the physical layer security from the spatial aspect. To this end, a novel performance metric, i.e., the spatial secrecy outage probability (SSOP), is derived to measure the security level of the legitimate transmission, which allows the analysis of the impact of the array parameters on the security performance. The SSOP can be applied to conduct information-theoretic analysis for previous work [6], [7] and can extend the work in [5], [8], [9] by analyzing the security performance with respect to the array parameters.

II. Definitions of ER and SSOP

Consider a secure transmission from Alice to Bob in presence of randomly located Eves. Alice has a UCA with N elements that are equally located on a circle with radius R. Bob and Eves are equipped with a single antenna. For convenience, both Bob and Eves are simply referred to as a 'general user' or a 'user', unless otherwise stated. Users are assumed to be distributed by a homogeneous PPP $\Phi_e$with density λ_e.

Without loss of generality, Alice is located at the origin point in polar coordinates, which is shown in Fig. 1; a general user's coordinates are denoted by $z = (d, \theta)$. Thus, Bob's coordinates are denoted by $z_B = (d_B, \theta_B)$; the k-th eavesdropper's coordinates are $z_{Ek} = (d_{Ek}, \theta_{Ek}), k \in \mathbb{N}^+$. We use the subscript '$B$' and '$E$' for Bob and Eves hereinafter.

We assume that Bob's channel state information (CSI) is known by Alice, e.g., via a separate feedback channel. So, beamforming can be performed according to Bob's CSI. However, Eves' CSI is not known by Alice.

978-1-5386-3954-2/16/$31.00 ©2016 IEEE

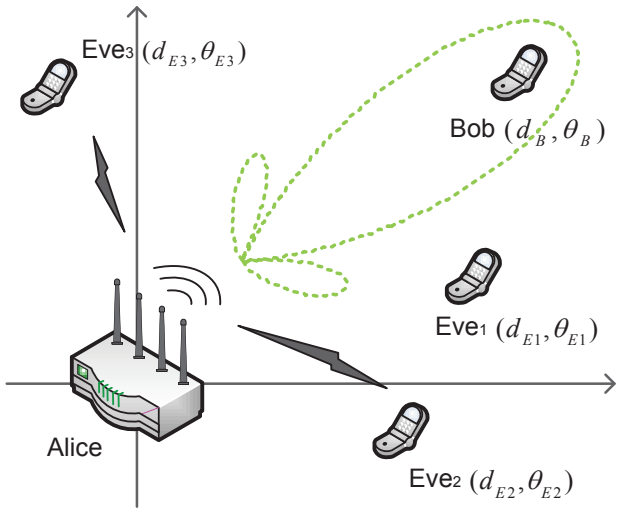

Fig. 1. An example of a dense communications system with Alice, Bob and Eves

Considering the large-scale path loss, the received signal power is related to user's coordinates z, and thus is denoted by $P_r(z)$. The channel capacity of the user located at z, denoted by $C(z)$, can be calculated by

$$C(z) = \log_2\left(1 + \frac{P_r(z)}{\sigma_n^2}\right), \tag{1}$$

where σ_n^2 is the variance of additive white Gaussian noise with zero mean.

In this paper, we adopt the definition of secrecy outage in [10] with two rates: the rate of the transmitted codewords R_B and the rate of the confidential information R_s. Due to the randomness of $C(z_{Ek})$, it is possible that $C(z_{Ek}) > R_B - R_s$. In this case, it is said that secrecy outage occurs.

The ER, denoted by Θ, is the geometric region where we face the secrecy outage if and only if $z_{Ek}, \exists k$ randomly appears in Θ. That is, we have $C(z) > R_B - R_s, \exists z = (d, \theta) \in \Theta$. Accordingly, Θ can be represented by

$$\Theta = \{z : \ C(z) > R_B - R_s\} \tag{2}$$

The SSOP, denoted by p_{SSOP}, is the probability that any Eve is located inside Θ. For PPP distributed Eves, the probability that m Eves are located inside Θ is given by

$$\text{Prob}\{m \text{ Eves in } \Theta\} = \frac{(\lambda_e A)^m}{m!} e^{-\lambda_e A} \tag{3}$$

Then, p_{SSOP} can be formulated by referring to the 'no secrecy outage' event that no Eves are located inside Θ.

$$p_{SSOP} = 1 - \text{Prob}\{0 \text{ Eve in } \Theta\} = 1 - e^{-\lambda_e A}, \tag{4}$$

where A is the measure of the size of Θ. It is noticed from (4) that p_{SSOP} increases along with A.

III. Rest of Paper

According to (4), the general expression of p_{SSOP} mainly consists of A, which will be further derived for PPP distributed Eves, based on which the close-form expression for the UCA will be derived in the form of summation of Bessel functions. p_{SSOP} includes A that is related to the array parameters, which enables the analysis of the security performance with respect to the array parameters.

References

[1] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge: Cambridge University Press, 2011.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, pp. 1550–1573, Jan. 2014.

[4] 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. (ICC)*, Kyoto, Japan, Jun. 2011, pp. 1–5.

[5] T.-X. Zheng, H.-M. Wang, and Q. Yin, "On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers," *IEEE Commun. Lett.*, vol. 18, no. 8, pp. 1299–1302, 2014.

[6] S. Lakshmanan, C. Tsao, R. Sivakumar, and K. Sundaresan, "Securing wireless data networks against eavesdropping using smart antennas," in *Proc. IEEE 28th Int. Conf. on Distributed Computing Syst. (ICDCS)*, Beijing, China, Jun. 2008, pp. 19–27.

[7] A. Sheth, S. Seshan, and D. Wetherall, "Geo-fencing: Confining Wi-Fi coverage to physical boundaries," in *Proc. IEEE 7th Int. Conf. on Pervasive Comput.*, Nara, Japan, May 2009, pp. 274–290.

[8] H. Li, X. Wang, and W. Hou, "Security enhancement in cooperative jamming using compromised secrecy region minimization," in *Proc. IEEE 13th Canadian Workshop on Inform. Theory (CWIT)*, Toronto, Canada, Jun. 2013, pp. 214–218.

[9] J. Wang, J. Lee, F. Wang, and T. Q. Quek, "Jamming-aided secure communication in massive MIMO Rician channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 6854–6868, 2015.

[10] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, pp. 302–304, Mar. 2011.