Achieving Secrecy Without Knowing the Number of Eavesdropper Antennas

Biao He, *Student Member, IEEE*, Xiangyun Zhou, *Member, IEEE*, and Thushara D. Abhayapala, *Senior Member, IEEE*

***Abstract*—The existing research on physical layer security commonly assumes the number of eavesdropper antennas to be known. Although this assumption allows one to easily compute the achievable secrecy rate, it can hardly be realized in practice. In this paper, we provide an innovative approach to studying secure communication systems without knowing the number of eavesdropper antennas by introducing the concept of spatial constraint into physical layer security. Specifically, the eavesdropper is assumed to have a limited spatial region to place (possibly an infinite number of) antennas. From a practical point of view, knowing the spatial constraint of the eavesdropper is much easier than knowing the number of eavesdropper antennas. We derive the achievable secrecy rates of the spatially-constrained system with and without friendly jamming. We show that a non-zero secrecy rate is achievable with the help of a friendly jammer, even if the eavesdropper places an infinite number of antennas in its spatial region. Furthermore, we find that the achievable secrecy rate does not monotonically increase with the jamming power, and hence, we obtain the closed-form solution of the optimal jamming power that maximizes the secrecy rate.**

***Index Terms*—Physical layer security, secrecy capacity, friendly jamming, spatial constraints.**

I. Introduction

A. Background and Motivation

DUE to the rapid adoption of wireless technologies in modern life, an unprecedented amount of private information is transmitted in wireless medium. Consequently, communication security has become a critical issue due to the unalterable open nature of wireless channels. As a complement to the traditional cryptographic technique, physical layer security has been extensively studied [1], [2] to secure wireless communications by exploiting the characteristics of wireless channels. Wyner introduced the wiretap-channel system as a framework for the physical layer security in his seminal work [3], and defined the secrecy capacity as the maximum rate at which messages can be reliably sent to the intended receiver without being eavesdropped. This result was then generalized to the broadcast channel with confidential messages by Csiszár and Körner [4] and the Gaussian wiretap channel by Leung-Yan-Cheong and Hellman [5]. In recent years, the fast development of multi-input multi-output (MIMO) techniques has triggered a considerable amount of attention on physical layer security in multi-antenna systems, where the transmitter, the receiver and/or the eavesdropper are equipped with multiple antennas. For example, the secrecy capacity of the multi-antenna system was analyzed in [6]–[8] and signal processing techniques with multiple antennas for improving the secrecy performance were proposed in [9]–[13].

Despite a significant amount of work has been done on physical layer security, most research in this area is theoretically oriented due to the idealized and impractical assumptions. For instance, many existing articles assumed that the transmitter has perfect channel state information (CSI) for the channels to the intended receiver and the eavesdropper. In practice, an external eavesdropper naturally does not cooperate with the transmitter to send CSI feedback, and hence, it is very difficult for the transmitter to obtain the CSI of the eavesdropper. Although the intended receiver may cooperate to send CSI feedback, reliable uplink channels for the feedback cannot always be guaranteed. This leads to an increasing amount of recent work focusing on the scenario where the transmitter does not have perfect CSI of the channel to the intended receiver and/or the eavesdropper, e.g., [14]–[18] and references within.

Apart from the assumption of perfect CSI knowledge, another idealized assumption is often adopted in the existing literature on physical layer security in multi-antenna systems, i.e., the assumption of knowing the number of eavesdropper antennas or setting an upper bound on the number of eavesdropper antennas. If the number of eavesdropper antennas is unknown, we have to assume that the eavesdropper has an infinite number of antennas as a worst-case consideration, and then the secrecy rate would always go to zero intuitively. To the best of the authors' knowledge, no existing literature has studied the scenario where the number of eavesdropper antennas is totally unknown. In practice, an external eavesdropper naturally does not inform the legitimate side about the number of antennas to expose its ability. As a weak justification, the upper bound on the number of eavesdropper antennas could be estimated from the eavesdropper's device size. However, such a weak justification, probably valid in the past, can no longer hold with the current development of large-scale antenna array technologies which allow a fast growing number of antennas be placed within a limited space. Thus, how to characterize the performance of physical layer security without knowing the number of eavesdropper antennas is a challenging but important problem.

Manuscript received February 11, 2015; revised June 4, 2015; accepted July 24, 2015. Date of publication August 3, 2015; date of current version December 8, 2015. This work was supported by the Australian Research Council under Discovery Project Grant DP150103905. The associate editor coordinating the review of this paper and approving it for publication was J. Lee.

The authors are with the Research School of Engineering, Australian National University, Canberra, ACT 0200, Australia (e-mail: biao.he@anu.edu.au; xiangyun.zhou@anu.edu.au; thushara.abhayapala@anu.edu.au).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2015.2463818

B. Our Approach and Contributions

In this work, we provide an innovative solution to the challenging problem by introducing the concept of spatial constraint[1] into physical layer security. In practice, knowing the eavesdropper's spatial constraint for placing antennas is much easier than knowing the exact number of the eavesdropper antennas. For example, we may know the size of the eavesdropper's device, but it is difficult to know how many antennas are installed on the device. We may know that the eavesdropper hides in a room, but it is difficult to known how many antennas are placed inside the room. In addition, considering a spatial constraint instead of an exact location of the eavesdropper allows certain degrees of uncertainty in eavesdropper's location.

We focus on the effects of spatial constraints at the receiver side. Specifically, we consider the scenario where the transmitter has a large number of antennas without spatial constraint while both the intended receiver and the eavesdropper have spatial constraints to place the receive antennas. This is a valid assumption given less geometrical size restriction for the base station to place a large number of transmit antennas, while the size of receiving device in the downlink is often relatively small [19]. Importantly, the number of receive antennas at the eavesdropper may not be known. We consider a simple and practical CSI assumption that the instantaneous CSI is known at the receiver end (the intended receiver and the eavesdropper) but not at the transmitter. Under these assumptions and considerations, we derive the secrecy capacity of the spatially-constrained multi-antenna system, and study the potential benefits brought by two widely-adopted friendly-jamming techniques. The two friendly-jamming techniques studied are the basic jamming technique and the artificial noise (AN) jamming technique: the former degrades both the intended receiver and the eavesdropper's channels, while the latter degrades only the eavesdropper's channel but does not affect the intended receiver's channel. We find that a non-zero secrecy capacity is achievable for the spatially-constrained system with the help of friendly-jamming signals, even if the number of eavesdropper antennas is unknown and considered to be infinity as a worst case.

The primary contributions of this paper are summarized as follows.

1) We introduce spatial constraints into physical layer security. To this end, we propose a framework to study physical layer security in multi-antenna systems with spatial constraints at the receiver side (both the intended receiver and the eavesdropper). We derive the secrecy capacity, and analyze the impact of spatial constraints on the secrecy capacity.
2) For the first time, our proposed framework allows one to analyze physical layer security without the knowledge of the number of eavesdropper antennas. It relaxes the requirement on the knowledge of eavesdropper from knowing the number of antennas to knowing the spatial constraint. We show that a non-zero secrecy capacity is achievable even if the eavesdropper is assumed to have an infinite number of antennas. This is easily achieved by applying the basic friendly-jamming technique where the jammer sends random noise signals.
3) We further study the impact of jamming power on the secrecy capacity of the spatially-constrained jammer-assisted systems. For the basic jammer-assisted system, we find that the secrecy capacity does not monotonically increase with the jamming power, and we obtain the closed-form solution of the optimal jamming power that maximizes the secrecy capacity. The optimality of the obtained solution is confirmed by the numerical result.

[1]Here the spatial constraint means the limited size of the spatial region for placing antennas at the communication node.

The remainder of this paper is organized as follows. Section II describes system models for studying physical layer security with spatial constraints at the receiver side. In Section III, we first give the secrecy capacity of the proposed systems with the knowledge of the number of eavesdropper antennas. The important case of not knowing the number of eavesdropper antennas is studied in Section IV, where the eavesdropper's receiver is assumed to be noise free and allowed to have infinitely many antennas for the worst-case consideration. Finally, Section V concludes the paper and discusses possible future research directions.

Throughout the paper, we adopt the following notations: Scalars, vectors and matrices are denoted by lowercase/uppercase letters, boldface lowercase letters and boldface uppercase letters, respectively, the circularly symmetric complex Gaussian vector with mean $\boldsymbol{\mu}$ and covariance matrix $\mathbf{C}$ is denoted by $\mathcal{CN}(\boldsymbol{\mu}, \mathbf{C})$, $\mathbf{I}_N$ denotes the $N \times N$ identity matrix, $()^H$ denotes the conjugate transpose of a vector or a matrix, $|\mathbf{X}|$ denotes the determinant of matrix $\mathbf{X}$, $\mathbb{E}\{\cdot\}$ denotes the expectation operator, $\lceil\cdot\rceil$ and $\lfloor\cdot\rfloor$ denote the ceiling operator and the floor operator, respectively, $[x]^+ = \max(x, 0)$.

II. System Model

In this paper, we study physical layer security in multi-antenna systems with spatial constraints at the receiver side. We assume that all communication nodes are equipped with multiple antennas and there exist spatial constraints at both the intended receiver and the eavesdropper. That is, the intended receiver and the eavesdropper have limited sizes of spatial regions for placing the receive antennas. To focus on the impact of spatial constraints at the receiver side, we adopt the following two assumptions as briefly mentioned in Section I. Firstly, we assume that there is no spatial constraint at the transmitter side for placing transmit antennas. Secondly, we assume that the transmitter has a large number of transmit antennas, and hence the capacity of the channel from the transmitter to the receiver is mainly restricted by the receiver side. Note that the number of antennas at the base station is often predicted to be in the hundreds for the next generation wireless systems [20], [21]. These two assumptions were often adopted in the literature investigating the impact of spatial constraints at the receiver side on multi-antenna systems without secrecy considerations, e.g., [19], [22]–[24] studying the channel capacity and [25]–[28] studying the spatial degrees of freedom. We specifically investigate two different secure communication systems, which are the wiretap-channel system and the jammer-assisted system. For

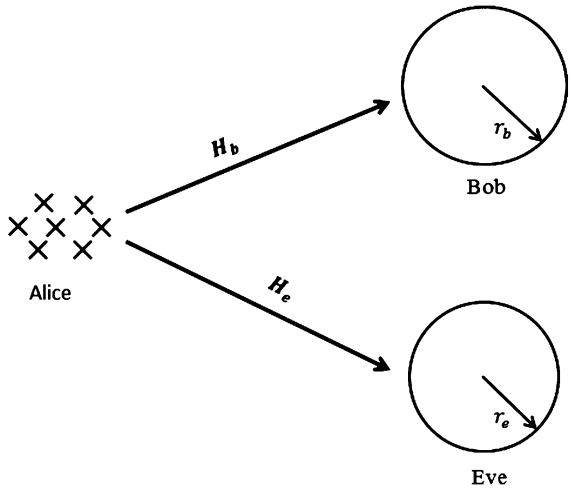


Fig. 1. 2D model for the wiretap-channel system.

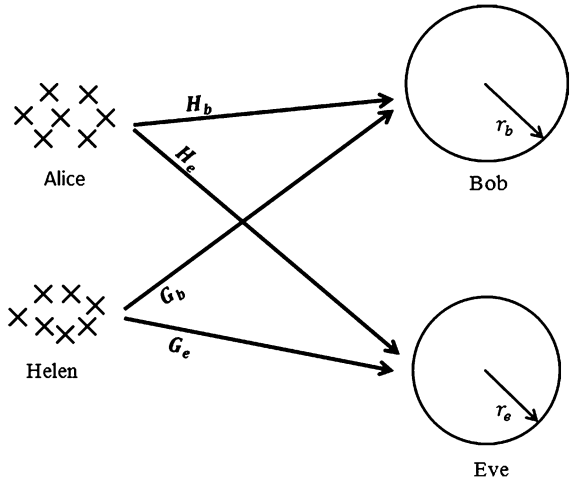


Fig. 2. 2D model for the jammer-assisted system.

the jammer-assisted system, we further consider two different cases depending on the adopted jamming technique, namely basic jammer-assisted system and AN jammer-assisted system. The details of the system models are given in the following subsections.

A. Wiretap-Channel System

The wiretap-channel system consists of a transmitter, an intended receiver and an eavesdropper, with N_t, N_b and N_e antennas, respectively. The transmitter, Alice, sends confidential messages to the intended receiver, Bob, in the presence of the eavesdropper, Eve. The receive antennas at Bob and Eve are both spatially constrained. Alice is assumed to be a base station with a large number of antennas ($N_t \to \infty$) without a spatial constraint. For the 2D analysis, Bob and Eve are assumed to be spatially constrained by circular apertures with radii r_b and r_e, respectively. For the 3D analysis, Bob and Eve are assumed to be spatially constrained by spherical apertures with radii r_b and r_e, respectively. The 2D model of the wiretap-channel system is depicted in Fig. 1.

The received signal vector at Bob or Eve is given by

$$\mathbf{y}_i = \sqrt{\alpha_i}\mathbf{H}_i\mathbf{x} + \mathbf{n}_i \quad i = b \text{ or } e, \tag{1}$$

where the subscripts b and e denote the parameters for Bob and Eve, respectively, $\mathbf{x}$ denotes the transmitted signal vector from Alice with an average power of P_t, i.e., $\mathbb{E}\{\mathbf{x}^H\mathbf{x}\} = P_t$. In addition, $\mathbf{n}_i \sim \mathcal{CN}(\mathbf{0}, \sigma_i^2\mathbf{I})$ denotes the additive white Gaussian noise (AWGN) vector at Bob or Eve, $\mathbf{H}_i = [\mathbf{h}_{i1}\mathbf{h}_{i2}\cdots\mathbf{h}_{iN_t}]$ denotes the $N_i \times N_t$ normalized channel matrix from Alice to Bob or Eve with $\mathbf{h}_{ik}$ ($k \in \{1, 2, \cdots, N_t\}$) representing the $N_i \times 1$ complex zero-mean Gaussian vector of the channel gains corresponding to the kth transmit antenna at Alice. Moreover, α_i denotes the average channel gain from Alice to Bob or Eve, which is often determined by the distance between the transmitter and the receiver. Besides, we assume that Bob and Eve perfectly know their CSI, while Alice does not know either Bob or Eve's instantaneous CSI.

The correlation matrix at the receiver is defined as

$$\mathbf{R}_i = \mathbb{E}\left\{\mathbf{h}_{it}\mathbf{h}_{it}^H\right\}, \tag{2}$$

where the expectation is over all transmit antennas and channel realizations. We can also write

$$\mathbf{R}_i = \begin{bmatrix} \rho_{i,11} & \rho_{i,12} & & \rho_{i,1N_i} \\ \rho_{i,21} & \rho_{i,22} & & \\ \vdots & & \ddots & \vdots \\ \rho_{i,N_i1} & & \cdots & \rho_{i,N_iN_i} \end{bmatrix}, \tag{3}$$

with elements $\rho_{i,kk'}$ corresponding to the spatial correlation between two sensors k and k' at the receiver. The spatial correlation between sensors is mainly determined by the distance between the sensors. The spatial correlation increases as the distance between sensors decreases. Within a fixed space, the distance between the antennas decreases as the number of antennas increases, and hence, the spatial correlation increases as the number of antennas increases.

B. Jammer-Assisted System

The jammer-assisted system consists of a transmitter, a helper, an intended receiver and an eavesdropper, with N_t, N_j, N_b and N_e antennas, respectively. With the aid of the helper, Helen, the transmitter, Alice, sends confidential messages to the intended receiver, Bob, in the presence of the eavesdropper, Eve. Helen helps Alice by broadcasting friendly jamming signals. The receive antennas at Bob and Eve are both spatially constrained. Alice and Helen are assumed to be base stations with a large number of transmit antennas ($N_t, N_j \to \infty$) without the spatial constraint. The detailed assumptions of the spatial constraints on Bob and Eve are the same as those given in Section II-A. The 2D model of the jammer-assisted system is depicted in Fig. 2.

We assume that Bob and Eve perfectly know their CSI, and Alice does not know either Bob or Eve's instantaneous CSI. We further assume that Helen does not know Eve's instantaneous CSI, since the passive eavesdropper does not feed back the CSI

to the helper. Moreover, for Helen's knowledge about Bob's channel, we consider two different cases in order to study two widely-adopted friendly-jamming techniques, as will be detailed next.

1) Case 1—Basic Jammer-Assisted System: In the first case, we assume that Helen does not know Bob's instantaneous CSI. This happens when there is no reliable uplink channel from Bob to Helen for CSI feedback. In this case, Helen broadcasts basic jamming signals that degrade both Bob and Eve's channels.

The received signal vector at Bob or Eve is given by

$$\mathbf{y}_i = \sqrt{\alpha_i}\mathbf{H}_i\mathbf{x} + \sqrt{\beta_i}\mathbf{G}_i\mathbf{w}_1 + \mathbf{n}_i, \quad i = b \text{ or } e, \tag{4}$$

where $\mathbf{x}, \alpha_i, \mathbf{H}_i, \mathbf{n}_i$ and the subscripts b, e follow (1). In addition, $\mathbf{w}_1$ denotes the basic jamming signal vector transmitted from Helen with an average power of P_j, i.e., $\mathbb{E}\{\mathbf{w}_1^H\mathbf{w}_1\} = P_j$, and $\mathbf{G}_i = [\mathbf{g}_{i1}\mathbf{g}_{i2}\cdots\mathbf{g}_{iN_j}]$ denotes the normalized channel matrix from Helen to Bob or Eve with $\mathbf{g}_{ik}$ ($k \in \{1, 2, \cdots, N_j\}$) representing the $N_i \times 1$ complex zero-mean Gaussian vector of the channel gains corresponding to the kth transmit antenna at Helen. Moreover, β_i denotes the average channel gain from Helen to Bob or Eve.

2) Case 2—AN Jammer-Assisted System: In the second case, we assume that Helen perfectly knows the instantaneous CSI from herself to Bob. This happens when there exists a reliable uplink channel from Bob to Helen for CSI feedback. In such a case, Helen broadcasts AN jamming signals that degrade Eve's channel but do not affect Bob's channel. The AN jamming technique was proposed in [9], which is often applied in secure communication networks where the jammer has the CSI to the intended receiver. Specifically, the AN jamming signal vector from Helen, denoted by $\mathbf{w}_2$, is chosen to lie in the null space of the channel to the intended receiver, $\mathbf{G}_b$. That is $\mathbf{G}_b\mathbf{w}_2 = \mathbf{0}$. In particular, $\mathbf{w}_2$ can be constructed by

$$\mathbf{w}_2 = \mathbf{Z}\mathbf{v}, \tag{5}$$

where $\mathbf{v}$ is an independent and identically distributed (i.i.d.) complex Gaussian random variable vector, the $N_j \times (N_j - N_b)$ matrix $\mathbf{Z}$ denotes the orthonormal basis of the null space of $\mathbf{G}_b$ with $\mathbf{Z}^H\mathbf{Z} = \mathbf{I}$.

With the AN jamming signals, the received signal vectors at Bob and Eve are given by

$$\mathbf{y}_b = \sqrt{\alpha_b}\mathbf{H}_b\mathbf{x} + \sqrt{\beta_b}\mathbf{G}_b\mathbf{w}_2 + \mathbf{n}_b = \sqrt{\alpha_b}\mathbf{H}_b\mathbf{x} + \mathbf{n}_b \tag{6}$$

and

$$\begin{aligned}\mathbf{y}_e &= \sqrt{\alpha_e}\mathbf{H}_e\mathbf{x} + \sqrt{\beta_e}\mathbf{G}_e\mathbf{w}_2 + \mathbf{n}_e \\ &= \sqrt{\alpha_e}\mathbf{H}_e\mathbf{x} + \sqrt{\beta_e}\mathbf{G}_e\mathbf{Z}\mathbf{v} + \mathbf{n}_e,\end{aligned} \tag{7}$$

respectively, where, once again, $\mathbf{x}, \alpha_b, \alpha_e, \mathbf{H}_b, \mathbf{H}_e, \mathbf{n}_b, \mathbf{n}_e$ follow (1) and $\beta_b, \beta_e, \mathbf{G}_b, \mathbf{G}_e$ follow (4). Besides, the average transmit power at Helen is still given by P_j, i.e., $\mathbb{E}\{\mathbf{w}_2^H\mathbf{w}_2\} = P_j$.

Remark 1: We highlight that the analysis for the AN jammer-assisted system is mainly motivated by its importance from the theoretical point of view. The basic jamming and the AN jamming are the two most widely-studied physical-layer techniques to improve the secrecy performance of multi-antenna systems. In this work, we study the wireless physical layer security with spatial constraints at the receiver side. It is of significant importance to investigate the benefits brought by both of the jamming techniques in the spatially-constrained systems. The AN jamming technique is often studied in the scenario where both Alice and Helen have the legitimate CSI in the literature. The legitimate CSI available at Alice enables not only the injection of AN jamming signals but also the transmit beamforming, and the secrecy capacity will go to infinity under the assumption of infinitely large number of transmit antennas. This will be shown later in Section III. In order to investigate the capacity improvement solely brought by AN jamming, we assume that Alice does not know the instantaneous CSI to Bob, but Helen knows the instantaneous CSI to Bob. Besides, the practical value of the AN jammer-assisted system studied in this paper can be seen from the following scenario as an example: We can consider that Alice is a base station owned by company A to serve a mobile user, Bob. Helen is another base station owned by company B. Due to particular reasons, e.g., location or surrounding environment, the CSI feedback link from Bob to Alice is bad, while the CSI feedback link from Bob to Helen is good. Then, Alice asks Helen to help the secrecy transmission by broadcasting AN jamming signals. For the secrecy concern, company A does not intend to share the confidential information with company B, and hence Alice does not share the messages to transmit with Helen.

III. Introducing Spatial Constraints Into Secrecy Capacity Calculation

In this section, we derive the secrecy capacity of the systems with spatial constraints at the receiver side as described in Section II. The secrecy capacity characterizes the maximum rate at which messages can be reliably transmitted to Bob while Eve obtains zero information. It is mathematically defined by [5]

$$C_s = [C_b - C_e]^+, \tag{8}$$

where C_b and C_e denote Bob and Eve's channel capacities, respectively.

For the multi-antenna systems with spatial constraint at the receiver, the channel capacity is limited by the rank and the eigenvalues of the spatial correlation matrix at the receiver. As the number of antennas increases in a fixed space, the correlation between antennas increases. The increase in spatial correlation will limit the number of significant eigenvalues of the spatial correlation matrix. As more antennas are placed in the fixed space, they will be highly correlated with other antennas. As a result, the growth of channel capacity with respect to the number of receive antennas reduces from linear to logarithmic. The number of receive antennas at which the capacity scaling is reduced to logarithmic is approximated by the saturation number of receive antennas. The saturation number of receive antennas is given by [19, Chapters 3.3]

$$N_{0i} = \begin{cases} 2\lceil \pi e r_i/\lambda \rceil + 1, & \text{for 2D analysis} \\ (\lceil \pi e r_i/\lambda \rceil + 1)^2, & \text{for 3D analysis,} \end{cases} \tag{9}$$

where λ denotes the wavelength, e denotes Euler's number, and subscript i denotes the parameters for Bob or Eve.[2] As pointed out in [19], the growth of channel capacity (C_b or C_e) with respect to the number of *optimally-placed* receive antennas (N_b or N_e) reduces from linear to logarithmic when the number of receive antennas increases beyond the saturation number (N_{0b} or N_{0e}). Note that similar "saturation" effects on the growth of channel capacity with respect to the number of antennas at the spatially-constrained receiver have also been pointed out in, e.g., [29]–[32].

It is worth mentioning that the capacity results in this paper are approximations based on (9) and the assumption of infinitely large number of transmit antennas. The accuracy of the approximations are verified in Appendices. In the rest of the paper, we simply refer to the approximated capacity result as the capacity.

A. Secrecy Capacity of Wiretap-Channel System

Proposition 1: The secrecy capacity of the wiretap-channel system with spatial constraints at the receiver side is given by $C_s = [C_b - C_e]^+$ where[3]

$$C_b = \begin{cases} N_b \log\left(1 + \frac{\alpha_b P_t}{\sigma_b^2}\right), & \text{if } N_b \le N_{0b} \\ N_{0b} \log\left(1 + \frac{N_b}{N_{0b}} \frac{\alpha_b P_t}{\sigma_b^2}\right), & \text{otherwise,} \end{cases} \tag{10}$$

$$C_e = \begin{cases} N_e \log\left(1 + \frac{\alpha_e P_t}{\sigma_e^2}\right), & \text{if } N_e \le N_{0e} \\ N_{0e} \log\left(1 + \frac{N_e}{N_{0e}} \frac{\alpha_e P_t}{\sigma_e^2}\right), & \text{otherwise.} \end{cases} \tag{11}$$

Proof: The capacities of the channels to the spatially-constrained Bob and Eve follow easily from [19, Chapters 2 and 3]. The details are given in Appendix A. □

Proposition 1 gives the secrecy capacity of the wiretap-channel system taking spatial constraints at the receiver side into account. From Proposition 1, we note that the growth of secrecy capacity with N_b reduces from linear to logarithmic once N_b reaches N_{0b}. Also, the decrease of secrecy capacity with N_e reduces from linear to logarithmic once N_e reaches N_{0e}. Differently, the secrecy capacity without spatial constraint always increases linearly with N_b and decreases linearly with N_e. This verifies that the secrecy performances of the networks with and without spatial considerations are different.

B. Secrecy Capacity of Basic Jammer-Assisted System

Theorem 1: The secrecy capacity of the basic jammer-assisted system with spatial constraints at the receiver side is given by $C_s = [C_b - C_e]^+$ where

$$C_b = \begin{cases} N_b \log\left(1 + \frac{\alpha_b P_t}{\beta_b P_j + \sigma_b^2}\right), & \text{if } N_b \le N_{0b} \\ N_{0b} \log\left(1 + \frac{\frac{N_b}{N_{0b}} \alpha_b P_t}{\frac{N_b}{N_{0b}} \beta_b P_j + \sigma_b^2}\right), & \text{otherwise,} \end{cases} \tag{12}$$

$$C_e = \begin{cases} N_e \log\left(1 + \frac{\alpha_e P_t}{\beta_e P_j + \sigma_e^2}\right), & \text{if } N_e \le N_{0e} \\ N_{0e} \log\left(1 + \frac{\frac{N_e}{N_{0e}} \alpha_e P_t}{\frac{N_e}{N_{0e}} \beta_e P_j + \sigma_e^2}\right), & \text{otherwise.} \end{cases} \tag{13}$$

Proof: See Appendix B. □

Theorem 1 gives the secrecy capacity of the basic jammer-assisted system taking spatial constraints at the receiver side into account. Similar to the result for the wiretap channel, we note that the secrecy capacity grows in linear with N_b when $N_b \le N_{0b}$. Also, the secrecy capacity decreases in linear with N_e when $N_e \le N_{0e}$. However, as N_i increases beyond N_{0i}, the change of secrecy capacity with respect to N_i becomes slower and slower. The secrecy capacity approaches an upper bound as $N_b \to \infty$, and a (possible) non-zero lower bound as $N_e \to \infty$, since

$$\lim_{N_b \to \infty} C_b = N_{0b} \log\left(1 + \frac{\alpha_b P_t}{\beta_b P_j}\right) \tag{14}$$

and

$$\lim_{N_e \to \infty} C_e = N_{0e} \log\left(1 + \frac{\alpha_e P_t}{\beta_e P_j}\right). \tag{15}$$

C. Secrecy Capacity of AN Jammer-Assisted System

Theorem 2: The secrecy capacity of the AN jammer-assisted system with spatial constraints at the receiver side is given by $C_s = [C_b - C_e]^+$ where

$$C_b = \begin{cases} N_b \log\left(1 + \frac{\alpha_b P_t}{\sigma_b^2}\right), & \text{if } N_b \le N_{0b} \\ N_{0b} \log\left(1 + \frac{N_b}{N_{0b}} \frac{\alpha_b P_t}{\sigma_b^2}\right), & \text{otherwise,} \end{cases} \tag{16}$$

$$C_e = \begin{cases} N_e \log\left(1 + \frac{\alpha_e P_t}{\beta_e P_j + \sigma_e^2}\right), & \text{if } N_e \le N_{0e} \\ N_{0e} \log\left(1 + \frac{\frac{N_e}{N_{0e}} \alpha_e P_t}{\frac{N_e}{N_{0e}} \beta_e P_j + \sigma_e^2}\right), & \text{otherwise.} \end{cases} \tag{17}$$

Proof: The capacity of Bob's channel is the same as that for the wiretap-channel system, since the AN jamming signals do not affect Bob's channel. We then derive the capacity of Eve's channel subject to the AN jamming signals. The details are given in Appendix C. □

Theorem 2 gives the secrecy capacity of the AN jammer-assisted system taking spatial constraints at the receiver side into account. We note that the growth of secrecy capacity with N_b reduces from linear to logarithmic once N_b reaches N_{0b}. The decrease of secrecy capacity with N_e is in linear when $N_e \le N_{0e}$, and becomes slower and slower when $N_e > N_{0e}$. The secrecy capacity approaches a (possible) non-zero lower bound as $N_e \to \infty$.

[2]The detailed derivation of the saturation number of antennas closely follows [19, Chapters 2.1 and 3].

[3]Throughout the paper logarithms are to base two, and the capacity is therefore in bits/s/Hz.

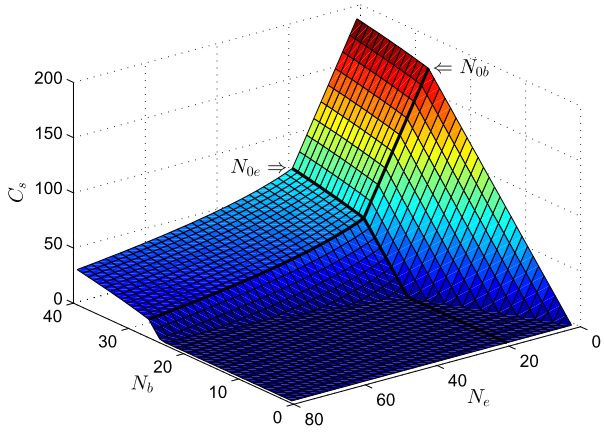


Fig. 3. Wiretap-channel system: Secrecy capacity versus the number of Bob's antennas and the number of Eve's antennas. Bob and Eve are spatially constrained by circular apertures with radii $r_b = 1.5\lambda$ and $r_e = 1\lambda$, respectively.

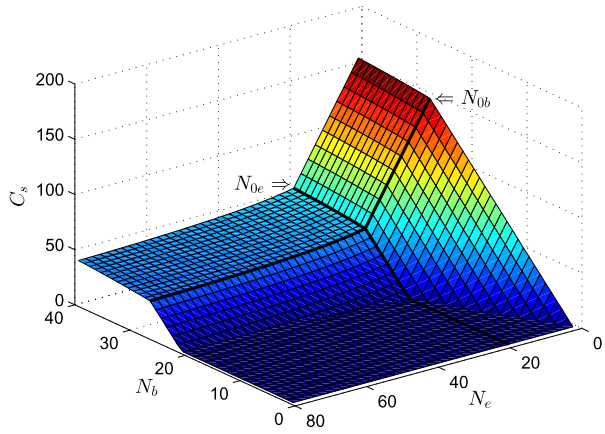


Fig. 4. Basic jammer-assisted system: Secrecy capacity versus the number of Bob's antennas and the number of Eve's antennas. Bob and Eve are spatially constrained by circular apertures with radii $r_b = 1.5\lambda$ and $r_e = 1\lambda$, respectively.

D. Secrecy Capacity With Legitimate CSI Available at Alice

In this paper, we consider a simple and practical CSI assumption that the instantaneous CSI of Bob is not available at Alice. In fact, it is also possible in practice that Bob's CSI is available at Alice. In this subsection, we provide the analysis on the secrecy capacity of the scenario where both Alice and Helen have Bob's CSI. Note that for the scenario without the friendly jammer, Alice can use a portion of the transmit antennas for sending information signals and the rest for broadcasting AN jamming signals. Under the assumption of $N_t \to \infty$, the scenario without the jammer Helen can be regarded as the scenario having both Helen and Alice at the same location.

When Bob's CSI is available at Alice, Alice can design the transmit signals accordingly to enhance Bob's channel capacity. At the same time, Helen can still transmit the AN jamming signals that degrade Eve's channel but do not affect Bob's channel. An infinitely large rate at Bob can be achieved by adopting a simple single-stream beamforming at Alice, under the assumption that the transmitter has an infinitely large number of antennas without the spatial constraint, while Eve does not benefit from the transmit beamforming. Hence, the secrecy capacity is equal to infinity in such a scenario with Bob's CSI available at Alice. It is worth mentioning that the secrecy capacity would be finite in a practical system with spatial constraints at both the transmitter side and the receiver side, due to the finite degrees of freedom in the spatially-constraint channel. The derivation of secrecy capacity in systems with spatial constraints at both the transmitter side and the receiver side is non-trivial and beyond the scope of this paper.

E. Numerical Results

In this subsection, we demonstrate the secrecy capacity versus the number of Bob's antennas and the number of Eve's antennas for different systems. Specifically, the network parameters are $P_t = 20$ dB, $P_j = 0$ dB, $\alpha_b = 1$, $\alpha_e = 1$, $\beta_b = 1$, $\beta_e = 1$, $\sigma_b^2 = 1$, $\sigma_e^2 = 1$, $r_b = 1.5\lambda$ and $r_e = 1\lambda$. We adopt the 2D analysis to characterize the spatial constraints at the receiver side. That is, Bob and Eve are assumed to be spatially constrained by circular apertures. According to (9), the saturation numbers of receive antennas for Bob and Eve are $N_{0b} = 2\lceil \pi e r_b/\lambda \rceil + 1 = 27$ and $N_{0e} = 2\lceil \pi e r_e/\lambda \rceil + 1 = 19$, respectively.

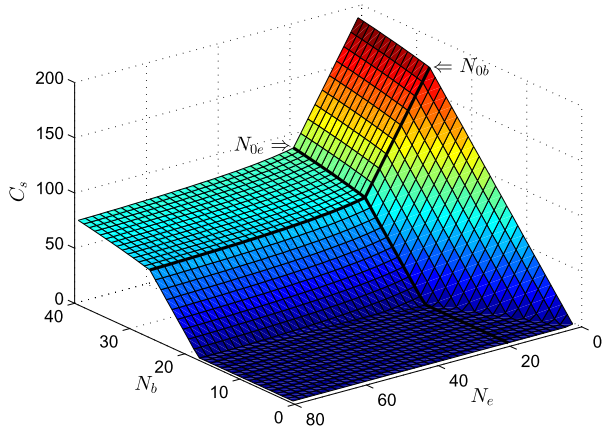


Fig. 5. AN jammer-assisted system: Secrecy capacity versus the number of Bob's antennas and the number of Eve's antennas. Bob and Eve are spatially constrained by circular apertures with radii $r_b = 1.5\lambda$ and $r_e = 1\lambda$, respectively.

Figs. 3, 4, and 5 plot C_s versus N_b and N_e for the wiretap-channel system, the basic jammer-assisted system and the AN jammer-assisted system, respectively. As shown in the figures, C_s increases with N_b and decreases with N_e. The increase of C_s with N_b slows down once $N_b > N_{0b}$ due to the effect of spatial constraint at Bob. Similarly, the decrease of C_s with N_e slows down once $N_e > N_{0e}$ due to the effect of spatial constraint at Eve. Besides, we note that the achieved secrecy capacities for different systems are different.

To make a clear comparison between the achieved secrecy capacities for different systems, we present Fig. 6 plotting C_s versus N_e with a given value of $N_b = 35$. As shown in the figure, the secrecy capacity of the wiretap-channel system decreases fast as the number of Eve's antennas increases. We find

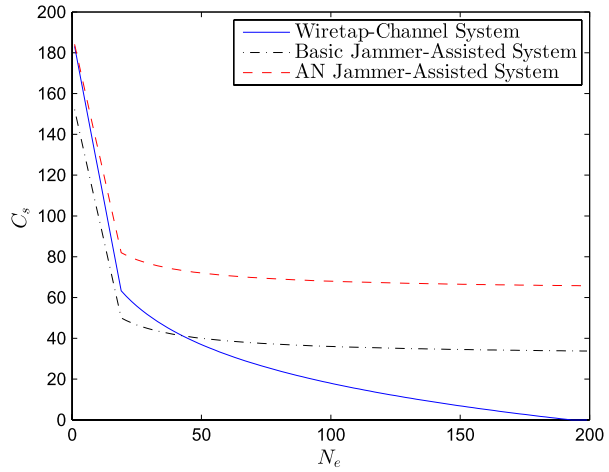


Fig. 6. Secrecy capacity versus the number of eavesdropper antennas with $N_b = 35$. Bob and Eve are spatially constrained by circular apertures with radii $r_b = 1.5\lambda$ and $r_e = 1\lambda$, respectively.

that the secrecy capacity of the wiretap-channel system goes to zero as the number of Eve's antennas continues to increase. Comparing the wiretap-channel system and the basic jammer-assisted system, we note that introducing the basic jamming signals effectively slows down the decrease of C_s when $N_e > N_{0e}$. Thus, the basic jammer-assisted system achieves a higher secrecy capacity compared with the wiretap-channel system when the number of Eve's antennas is large. In addition, as analyzed in Section III-B, the secrecy capacity of the basic jammer-assisted system can approach a non-zero lower bound as $N_e \to \infty$. Besides, we observe from the figure that the secrecy capacity achieved by the basic jammer-assisted system is less than that achieved by the wiretap-channel system when N_e is small. This is actually because the jamming power has not been optimally designed for the results in the figure. Comparing the wiretap-channel system and the AN jammer-assisted system, we find that the AN jammer-assisted system always obtains a higher secrecy capacity than that of the wiretap-channel system. This is because the AN jamming signals degrade Eve's channel only, but do not affect Bob's channel. However, we should note that broadcasting the AN jamming signals requires the helper to know the instantaneous CSI of the intended receiver, which is not always possible in practice.

IV. Worst-Case Analysis for Jammer-Assisted Systems

The previous section provides the basic analysis on the secure communication systems with spatial constraints at the receiver side. However, to evaluate the system performance by the capacity results given in *Proposition 1*, *Theorems 1* and *2*, we require very good knowledge on Eve, including N_e and σ_e^2. In practice, it is desirable to be able to investigate the secrecy performance of a system without the knowledge of N_e and σ_e^2. To this end, we consider a "worst-case eavesdropper" (from the legitimate users' perspective) as in this section.

For such a worst-case eavesdropper, we assume that the number of receive antennas at the eavesdropper approaches infinity and the noise variance at the eavesdropper approaches zero, i.e, $N_e \to \infty$ and $\sigma_e^2 \to 0$. Then, the secrecy capacity with the worst-case consideration is given by

$$C_s^w = \lim_{N_e \to \infty, \sigma_e^2 \to 0} C_s, \tag{18}$$

where C_s is the secrecy capacity of systems with perfect knowledge of N_e and σ_e^2, i.e, the secrecy capacity derived in the previous section. In addition, we refer to C_s^w as the worst-case secrecy capacity.

The worst-case scenario is motivated by the fact that the eavesdropper's ability is difficult to be known or controlled by the legitimate side. As such, in the design of secure communications, we assume the worst-case scenario where the eavesdropper can deploy infinite number of antennas with arbitrarily small noise variance. If we assume that the eavesdropper has a given number of antennas, the designed secure communications would be vulnerable to eavesdropping caused by a larger number of antennas at the eavesdropper in practice. Therefore, the weaker assumption of knowing a finite number of antennas at the eavesdropper cannot lead to the true guarantee of security, and thus it is of critical significance to take into consideration the worst-case scenario with infinite number of eavesdropper antennas.

A. Wiretap-Channel System

Based on *Proposition 1* and (18), the worst-case secrecy capacity of the wiretap-channel system is given by

$$C_s^w = 0. \tag{19}$$

We note that a non-zero worst-case secrecy capacity is not achievable under any condition for the wiretap-channel system, because the capacity of Eve's channel always goes to infinity with $N_e \to \infty$ or $\sigma_e^2 \to 0$.

B. Basic Jammer-Assisted System

1) Worst-Case Secrecy Capacity: Based on *Theorem 1* and (18), the worst-case secrecy capacity of the basic jammer-assisted system is given by

$$C_s^w = \begin{cases} \left[N_b \log\left(1+\frac{\alpha_b P_t}{\beta_b P_j + \sigma_b^2}\right) - N_{0e} \log\left(1+\frac{\alpha_e P_t}{\beta_e P_j}\right)\right]^+, \\ \text{if } N_b \le N_{0b} \\ \left[N_{0b} \log\left(1+\frac{\frac{N_b}{N_{0b}}\alpha_b P_t}{\frac{N_b}{N_{0b}}\beta_b P_j + \sigma_b^2}\right) - N_{0e} \log\left(1+\frac{\alpha_e P_t}{\beta_e P_j}\right)\right]^+, \\ \text{otherwise.} \end{cases} \tag{20}$$

From (20), we note that a non-zero worst-case secrecy capacity sometimes is achievable for the basic jammer-assisted system depending on the system parameters, such as transmit power, average channel gains, the spatial constraint at Bob and the number of antennas at Bob. This result shows for the first time that a non-zero secrecy rate can be achieved even if the eavesdropper's receiver itself is noise free and allowed

to have infinitely many antennas. Moreover, this is achieved by simply asking a friendly-jamming node to send random jamming signals.

To further study the condition for having a non-zero worst-case secrecy capacity, we consider the scenario where the number of antennas at Bob, N_b, is controllable and the other system parameters,[4] i.e., N_{0b}, N_{0e}, α_b, β_b, α_e, β_e, P_t and P_j, are fixed. From (20), we find that a non-zero worst-case secrecy capacity is always achievable by having "enough" receive antennas at Bob when $N_{0b}\log\left(1+\frac{\alpha_b P_t}{\beta_b P_j}\right) > N_{0e}\log\left(1+\frac{\alpha_e P_t}{\beta_e P_j}\right)$. However, the secrecy capacity is always equal to zero when

$$N_{0b}\log\left(1+\frac{\alpha_b P_t}{\beta_b P_j}\right) \le N_{0e}\log\left(1+\frac{\alpha_e P_t}{\beta_e P_j}\right), \tag{21}$$

because $C_b < N_{0b}\log\left(1+\frac{\alpha_b P_t}{\beta_b P_j}\right)$ always holds for any finite value of N_b. In addition, when $N_{0b}\log\left(1+\frac{\alpha_b P_t}{\beta_b P_j}\right) > N_{0e}\log\left(1+\frac{\alpha_e P_t}{\beta_e P_j}\right)$, we can further derive the minimum N_b to ensure a non-zero worst-case secrecy capacity as

$$N_{b,\min} = \begin{cases} \left\lfloor \frac{N_{0e}\log\left(1+\frac{\alpha_e P_t}{\beta_e P_j}\right)}{\log\left(1+\frac{\alpha_b P_t}{\beta_b P_j+\sigma_b^2}\right)} \right\rfloor + 1, \\ \text{if } N_{0b}\log\left(1+\frac{\alpha_b P_t}{\beta_b P_j+\sigma_b^2}\right) \ge N_{0e}\log\left(1+\frac{\alpha_e P_t}{\beta_e P_j}\right) \\ \left\lfloor \frac{N_{0b}\ \sigma_b^2\left(\left(1+\frac{\alpha_e P_t}{\beta_e P_j}\right)^{\frac{N_{0e}}{N_{0b}}}-1\right)}{\alpha_b P_t+\beta_b P_j-\beta_b P_j\left(1+\frac{\alpha_e P_t}{\beta_e P_j}\right)^{\frac{N_{0e}}{N_{0b}}}} \right\rfloor + 1, \\ \text{otherwise.} \end{cases} \tag{22}$$

2) Optimal Jamming Power: From (20), we note that the worst-case secrecy capacity is not a monotonically increasing function of the jamming power. This is because the increase of P_j degrades not only Eve's channel but also Bob's channel, and there arises a tradeoff between maintaining the capacity of Bob's channel and decreasing the capacity of Eve's channel. In the following, we determine the optimal jamming power that maximizes the worst-case secrecy capacity, i.e., $P_j^o = \arg\max_{P_j} C_s^w$.

Proposition 2: The optimal jamming power that maximizes the worst-case secrecy capacity of the basic jammer-assisted system is given by

$$P_j^o = \begin{cases} x_1, & \text{if } N_b \le N_{0b}, f_1(x_1) > 0, x_1 \text{ is real and positive} \\ x_2, & \text{if } N_b \le N_{0b}, f_1(x_2) > 0, x_2 \text{ is real and positive} \\ x_3, & \text{if } N_b \le N_{0b}, f_2(x_3) > 0, x_3 \text{ is real and positive} \\ x_4, & \text{if } N_b \le N_{0b}, f_2(x_4) > 0, x_4 \text{ is real and positive} \\ \text{n/a}, & \text{otherwise,} \end{cases} \tag{23}$$

[4]Here the other system parameters depend on the spatial constraint, the location of communication node and the transmit power.

where

$$f_1(x) = N_b\log\left(1+\frac{\alpha_b P_t}{\beta_b x+\sigma_b^2}\right) - N_{0e}\log\left(1+\frac{\alpha_e P_t}{\beta_e x}\right),$$

$$f_2(x) = N_{0b}\log\left(1+\frac{\frac{N_b}{N_{0b}}\alpha_b P_t}{\frac{N_b}{N_{0b}}\beta_b x+\sigma_b^2}\right) - N_{0e}\log\left(1+\frac{\alpha_e P_t}{\beta_e x}\right),$$

$$x_1 = \frac{2N_{0e}\alpha_e\sigma_b^2 - P_t\alpha_b\alpha_e(N_b-N_{0e})}{2\left(N_b\alpha_b\beta_e - N_{0e}\alpha_e\beta_b\right)} + \frac{\sqrt{\alpha_b^2\alpha_e^2\beta_b^2\ P_t^2\ (N_b-N_{0e})^2+\phi_1}}{2\beta_b\left(N_b\alpha_b\beta_e - N_{0e}\alpha_e\beta_b\right)},$$

$$x_2 = \frac{2N_{0e}\alpha_e\sigma_b^2 - P_t\alpha_b\alpha_e(N_b-N_{0e})}{2(N_b\alpha_b\beta_e - N_{0e}\alpha_e\beta_b)} - \frac{\sqrt{\alpha_b^2\alpha_e^2\beta_b^2\ P_t^2(N_b-N_{0e})^2+\phi_1}}{2\beta_b(N_b\alpha_b\beta_e - N_{0e}\alpha_e\beta_b)},$$

$$x_3 = \frac{2N_{0e}N_{0b}\alpha_e\sigma_b^2 - N_bP_t\alpha_b\alpha_e(N_{0b}-N_{0e})}{2N_b\left(N_{0b}\alpha_b\beta_e - N_{0e}\alpha_e\beta_b\right)} + \frac{\sqrt{\alpha_b^2\alpha_e^2\beta_b^2P_t^2N_b^2(N_{0b}-N_{0e})^2+\phi_2}}{2N_b\beta_b(N_{0b}\alpha_b\beta_e - N_{0e}\alpha_e\beta_b)},$$

$$x_4 = \frac{2N_{0e}N_{0b}\alpha_e\sigma_b^2 - N_bP_t\alpha_b\alpha_e(N_{0b}-N_{0e})}{2N_b(N_{0b}\alpha_b\beta_e - N_{0e}\alpha_e\beta_b)} - \frac{\sqrt{\alpha_b^2\alpha_e^2\beta_b^2P_t^2N_b^2(N_{0b}-N_{0e})^2+\phi_2}}{2N_b\beta_b(N_{0b}\alpha_b\beta_e - N_{0e}\alpha_e\beta_b)},$$

with

$$\phi_1 = 4N_bN_{0e}\alpha_b\alpha_e\beta_b\sigma_b^2\left(P_t\alpha_b\beta_e - P_t\alpha_e\beta_b + \beta_e\sigma_b^2\right),$$

$$\phi_2 = 4N_{0b}^2N_{0e}\alpha_b\alpha_e\beta_b\sigma_b^2\left(N_bP_t\alpha_b\beta_e - N_bP_t\alpha_e\beta_b + N_{0b}\beta_e\sigma_b^2\right).$$

Proof: See Appendix D. □

Remark 2: Proposition 2 provides the optimal jamming power that maximizes the worst-case secrecy capacity of the basic jammer-assisted system. If there is no power constraint at the jammer, we can simply set the jamming power as P_j^o to achieve the best secrecy performance. If there exists a power constraint at the jammer, say $P_j \le P_{j,\max}$, we should first check the feasibility of achieving the non-zero worst-case secrecy capacity, and then set the jamming power as $\min(P_j^o, P_{j,\max})$ if the non-zero worst-case secrecy capacity is achievable.

C. AN Jammer-Assisted System

Based on *Theorem 2* and (18), the worst-case secrecy capacity of the AN jammer-assisted system is given by

$$C_s^w = \begin{cases} \left[N_b\log\left(1+\frac{\alpha_b P_t}{\sigma_b^2}\right) - N_{0e}\log\left(1+\frac{\alpha_e P_t}{\beta_e P_j}\right)\right]^+, \\ \text{if } N_b \le N_{0b} \\ \left[N_{0b}\log\left(1+\frac{N_b}{N_{0b}}\frac{\alpha_b P_t}{\sigma_b^2}\right) - N_{0e}\log\left(1+\frac{\alpha_e P_t}{\beta_e P_j}\right)\right]^+, \\ \text{otherwise.} \end{cases} \tag{24}$$

Similar to the case of basic jammer-assisted system, we note that a non-zero worst-case secrecy capacity sometimes is achievable for the AN jammer-assisted system, depending on the system parameters, such as transmit power, average channel gains, the spatial constraint at Bob and the number of antennas at Bob. Consider the scenario where the number of antennas at Bob, N_b, is controllable and the other system parameters, i.e., N_{0b}, N_{0e}, α_b, β_b, α_e, β_e, P_t, and P_j, are fixed. From (24), we find that a non-zero worst-case secrecy capacity is always achievable by having "enough" receive antennas at Bob, and the minimum N_b to ensure a non-zero worst-case secrecy capacity is given by

$$N_{b,\min} = \begin{cases} \left\lfloor \frac{N_{0e}\log\left(1+\frac{\alpha_e P_t}{\beta_e P_j}\right)}{\log\left(1+\frac{\alpha_b P_t}{\sigma_b^2}\right)} \right\rfloor + 1, \\ \text{if } N_{0b}\log\left(1+\frac{\alpha_b P_t}{\sigma_b^2}\right) \geq N_{0e}\log\left(1+\frac{\alpha_e P_t}{\beta_e P_j}\right) \\ \left\lfloor \frac{N_{0b}\sigma_b^2}{\alpha_b P_t}\left(\left(1+\frac{\alpha_e P_t}{\beta_e P_j}\right)^{\frac{N_{0e}}{N_{0b}}} - 1\right) \right\rfloor + 1, \\ \text{otherwise.} \end{cases} \tag{25}$$

In terms of the optimal jammer power that maximizes the worst-case secrecy capacity, it is wise to have P_j as large as possible, since the increase of P_j only degrades the capacity of Eve's channel but does not affect the capacity of Bob's channel. Mathematically, we give the following proof for that the worst-case secrecy capacity of the AN jammer-assisted system is a monotonically increasing function of the jamming power.

Proof: We first rewrite (24) as

$$C_s^w = \begin{cases} [f_1(P_j)]^+, & \text{if } N_b \leq N_{0b} \\ [f_2(P_j)]^+, & \text{otherwise.} \end{cases} \tag{26}$$

Then, we find that

$$\frac{\partial f_1(P_j)}{\partial P_j} = \frac{\partial f_2(P_j)}{\partial P_j} = \frac{N_{0e}P_t\alpha_e}{\left(1+\frac{\alpha_e P_t}{\beta_e P_j}\right)\ln 2\beta_e P_j^2} > 0 \tag{27}$$

always holds for any positive value of P_j. Thus, the secrecy capacity of the AN jammer-assisted system is a monotonically increasing function of the jamming power. □

D. Numerical Results

In this subsection, we present the numerical results based on the worst-case analysis. Since the worst-case secrecy capacity of the wiretap-channel system is always equal to zero, we do not present the numerical results for the wiretap-channel system in this subsection but focus on the basic jammer-assisted system and the AN jammer-assisted system. Besides, we still adopt the 2D analysis to characterize the spatial constraints at the receiver side, such that Bob and Eve are spatially constrained by circular apertures.

We first compare the minimum numbers of Bob's antennas to achieve a non-zero worst-case secrecy capacity of the basic jammer-assisted system and the AN jammer-assisted system.

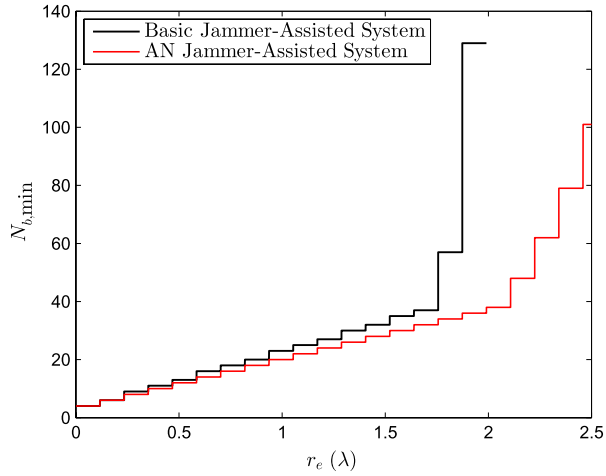


Fig. 7. The minimum number of Bob's antennas for achieving a non-zero worst-case secrecy capacity versus the radius of Eve's spatial constraint. The other system parameters are $P_t = 20$ dB, $P_j = 0$ dB, $\alpha_b = 1$, $\alpha_e = 1$, $\beta_b = 1$, $\beta_e = 1$, $\sigma_b^2 = 1$, and $r_b = 2\lambda$.

Fig. 7 plots $N_{b,\min}$ versus r_e based on (22) and (25). As shown in the figure, $N_{b,\min}$ increases with r_e for both systems, which indicates that we need more antennas at Bob to ensure a non-zero worst-case secrecy capacity as the radius of Eve's spatial constraint increases. In addition, we note that the increase of $N_{b,\min}$ with respect to r_e is slow when r_e is small, but it becomes fast when r_e is large. Such an observation is more clear for the basic jammer-assisted system compared with that for the AN jammer-assisted system. Hence, the cost of antennas at Bob to ensure a non-zero worst-case secrecy capacity is very large when the radius of Eve's spatial constraint is large, especially for the basic jammer-assisted system. When r_e is very large, i.e., $r_e > r_b = 2\lambda$ in the figure, the basic jammer-assisted system cannot achieve a non-zero worst-case secrecy capacity no matter how many antennas are equipped at Bob. The condition under which the basic jammer-assisted system always cannot achieve the non-zero worst-case secrecy capacity is given by (21). In contrast, the AN jammer-assisted system can always ensure a non-zero worst-case secrecy capacity by increasing the number of Bob's antennas, as long as Eve has a finite spatial constraint.

It is worth pointing out that the minimum number of receive antennas to ensure a non-zero worst-case secrecy capacity is determined by not only the spatial constraint at the eavesdropper but also many other system parameters, such as the spatial constraint at the legitimate receiver, transmit power, jamming power, average channel gains and the noise variance at the receiver. Thus, the result in Fig. 7 can be only regarded as an example to illustrate the required values of $N_{b,\min}$ for different values of r_e. The required $N_{b,\min}$ is not necessary to be extremely large for a very large value of r_e. For example, the required $N_{b,\min}$ is equal to 116 for $r_e = 10\lambda$ in an AN jammer-assisted system with $r_b = 8\lambda$, $\alpha_b = 10$, $\alpha_e = 10$, $\beta_b = 10$, and $\beta_e = 10$.

Now, we depict the worst-case secrecy capacity for different spatial constraints at Eve. Fig. 8 plots C_s^w versus r_e for the basic jammer-assisted system and the AN jammer-assisted system according to (20) and (24), respectively. The number of Bob's

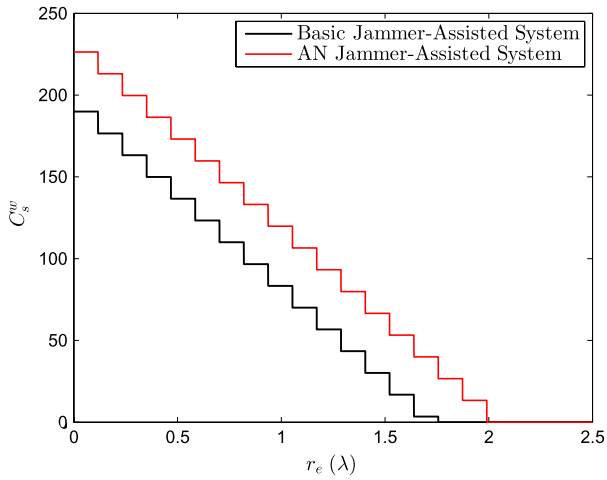


Fig. 8. The worst-case secrecy capacity versus the radius of Eve's spatial constraint. The other system parameters are $P_t = 20$ dB, $P_j = 0$ dB, $\alpha_b = 1$, $\alpha_e = 1$, $\beta_b = 1$, $\beta_e = 1$, $\sigma_b^2 = 1$, $r_b = 2\lambda$, and $N_b = N_{0b} = 37$.

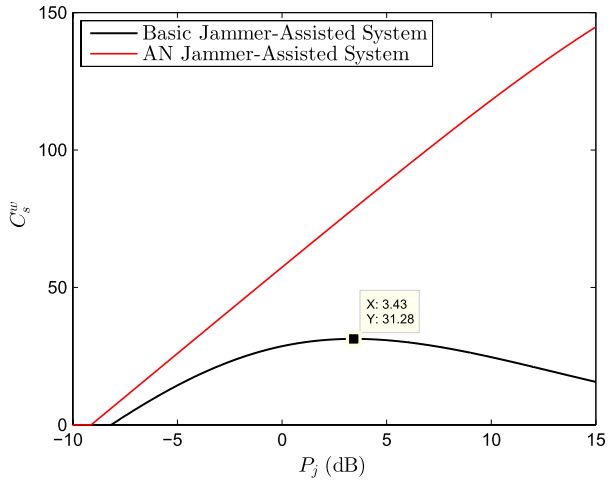


Fig. 9. The worst-case secrecy capacity versus the jamming power. The other system parameters are $P_t = 20$ dB, $\alpha_b = 1$, $\alpha_e = 1$, $\beta_b = 1$, $\beta_e = 1$, $\sigma_b^2 = 1$, $r_b = 1.5\lambda$, $r_e = 1\lambda$, and $N_b = 30$.

antennas is chosen equal to the saturation number of receive antennas at Bob, i.e., $N_b = N_{0b} = 37$. As the figure shows, C_s^w decreases with r_e for both systems. Comparing the two curves, we note that the worst-case secrecy capacity of the basic jammer-assisted system is always smaller than that for the AN jammer-assisted system. In addition, the difference of C_s^w between the two systems keeps the same for different values of r_e. This can be explained as follows. The basic jamming signals and the AN jamming signals have the same effect on Eve's channel while different effects on Bob's channel. Hence, the difference of C_s^w between the two systems is actually due to the difference of the capacity of Bob's channel subject to different jamming techniques, and it is not related to Eve's channel condition or spatial constraint. Therefore, the difference of C_s^w between the two curves in the figure keeps the same for different values of r_e.

Finally, we illustrate the impact of jamming power on the worst-case secrecy capacity. Fig. 9 plots C_s^w versus P_j for both the basic jammer-assisted system and the AN jammer-assisted system. As shown in the figure, the value of C_s^w for the basic jammer-assisted system increases with P_j when P_j is small, but it decreases with P_j when P_j goes large. There exists an optimal value of P_j that maximizes C_s^w for the basic jammer-assisted system, i.e., $P_j = 3.43$ dB in the figure. By using the analytical results given in *Proposition 2*, we also obtain that P_j^o for the given scenario is equal to 3.43 dB. This verifies the optimality of P_j^o obtained in our analytical results. In contrast, the value of C_s^w for the AN jammer-assisted system always increases with P_j, which is also consistent with our analytical results. Moreover, comparing the basic jammer-assisted system and the AN jammer-assisted system, we note that the difference of C_s^w between the two curves increases with P_j all the time.

V. Conclusion and Future Work

In this work, we introduced the spatial constraint into physical layer security for multi-antenna systems, which provides an approach to study the secrecy capacity without knowing the number of eavesdropper antennas. We considered basic secure communication systems with spatial constraints at the receiver side. Specifically, we studied the wiretap-channel system, the basic jammer-assisted system and the AN jammer-assisted system, and derived the expressions for secrecy capacity of each system. We found that a non-zero worst-case secrecy capacity is achievable with the assist of jamming signals, even if the eavesdropper is equipped with infinite number of antennas. Moreover, the optimal jamming power that maximizes the worst-case secrecy capacity was obtained. We highlight that the major contribution of this paper is to address the practically important problem of how to study secure communications without knowing the number of eavesdropper antennas, and hope this work can be a good inspiration for future researchers to design novel physical layer techniques to efficiently secure wireless communications without the information of eavesdropper antennas.

As a first step of studying the effects of spatial constraints on physical layer security, this work considered a simple scenario with spatial constraints at the receiver side only. A natural future work is to extend the study by investigating the effects of spatial constraints at both the transmitter and the receiver sides. To this end, a limited number of transmit antennas with the spatial constraint at the transmitter should be considered. However, it is worth mentioning that the extension is non-trivial, since the secrecy capacity would depend on instantaneous channel realizations even if the number of transmit antennas goes to infinity. In the scenario with spatial constraints at both the transmitter and the receiver sides, the study of having legitimate CSI available at the transmitter side is also of great interest, while this paper assumed the legitimate CSI available only at the receiver side. With the legitimate CSI available at the transmitter, how to optimally design the transmit precoding is an interesting problem to investigate. Another future work direction is to evaluate the achievable secrecy capacity for different antenna array configurations from a signal-processing perspective. Note that the results in this paper were mainly obtained from an information-theoretic perspective by assuming the optimal antenna placement at the receiver side.

APPENDIX A
PROOF OF PROPOSITION 1

The capacity of Bob or Eve's channel can be written as

$$C_i = \log \left| \mathbf{I}_{N_i} + \frac{\alpha_i \mathbf{H}_i \mathbf{Q}_x \mathbf{H}_i^H}{\sigma_i^2} \right|, \tag{28}$$

where $\mathbf{Q}_x$ denotes the covariance matrix of $\mathbf{x}$, i.e., $\mathbf{Q}_x = \mathbb{E}\{\mathbf{x}\mathbf{x}^H\}$. Since Alice has no instantaneous CSI of Bob and there is sufficient space at Alice for independent transmit antenna allocation, the best transmission strategy is to have the transmit signal vector composed of statistically independent equal power components, each with a Gaussian distribution. Then, the covariance matrix of $\mathbf{x}$ is equal to $\mathbf{Q}_x = \frac{P_t}{N_t}\mathbf{I}_{N_t}$, and the channel capacity becomes to

$$C_i = \log \left| \mathbf{I}_{N_i} + \frac{\alpha_i P_t}{\sigma_i^2 N_t} \mathbf{H}_i \mathbf{H}_i^H \right|, \tag{29}$$

where

$$\mathbf{H}_i \mathbf{H}_i^H = \sum_{t=1}^{N_t} \mathbf{h}_{it} \mathbf{h}_{it}^H. \tag{30}$$

Considering a large number of transmit antennas ($N_t \to \infty$) and sufficient space for placing transmit antennas (independent $\mathbf{h}_{it}$), the correlation matrix at the receiver in (2) becomes to

$$\mathbf{R}_i \to \frac{1}{N_t} \sum_{t=1}^{N_t} \mathbf{h}_{it} \mathbf{h}_{it}^H. \tag{31}$$

Note that there is no expectation over channel realizations in (31), since $\frac{1}{N_t}\sum_{t=1}^{N_t} \mathbf{h}_{it}\mathbf{h}_{it}^H = \mathbb{E}\left\{\frac{1}{N_t}\sum_{t=1}^{N_t} \mathbf{h}_{it}\mathbf{h}_{it}^H\right\}$ when $N_t \to \infty$. Then, the channel capacity with a large number of sufficiently separated transmit antennas is approximated by

$$C_i \approx \log \left| \mathbf{I}_{N_i} + \frac{\alpha_i P_t}{\sigma_i^2} \mathbf{R}_i \right|. \tag{32}$$

We highlight that the approximation by (32) provides good accuracy even if the number of transmit antennas is finite. To examine the accuracy of the approximation by (32), we compare the true value of C_i obtained by (29) and the approximation obtain by (32) for given receive antenna array configurations. The simulation result is presented by Fig. 10. The number of transmit antennas is set as a large but finite number, $N_t = 100$. The number of receive antennas is in the range of $1 \le N_i \le N_t = 100$. We consider two different antenna array configurations, which are the uniform linear array (ULA) and the uniform circular array (UCA), in a fixed circular aperture at the receiver with $r_i = 1\lambda$. Since the number of transmit antennas is set as a finitely large number but not infinity, the capacity result by (29) would depend on the instantaneous channel realization. Thus, the "true value" in Fig. 10 is the average value of C_i obtained by (29) over different channel realizations. It is evident from Fig. 10 that the difference between the true value and the approximation is very small for the whole range of N_i,

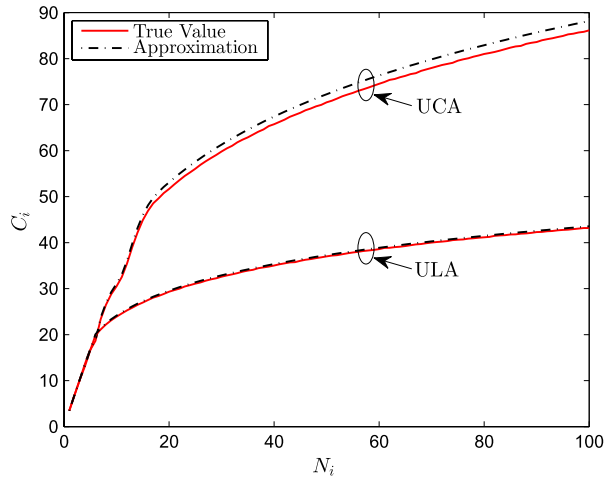


Fig. 10. Without jamming signals: C_i versus N_i. The other system parameters are $N_t = 100$, $r_i = 1\lambda$, $P_t = 10$ dB, $\alpha_i = 1$, $\sigma_i^2 = 1$.

which indicates that the approximation by (32) provides good accuracy even if the transmitter has a finite number of antennas.

For the receiver with N_i optimally-placed antennas in a fixed aperture region, the channel capacity in (32) can be further approximated by [19, Chapter 3],

$$C_i \approx \begin{cases} N_i \log\left(1 + \frac{\alpha_i P_t}{\sigma_i^2}\right), & \text{if } N_i \le N_{0i} \\ N_{0i} \log\left(1 + \frac{N_i}{N_{0i}} \frac{\alpha_i P_t}{\sigma_i^2}\right), & \text{otherwise,} \end{cases} \tag{33}$$

where the expression of N_{0i} for a 2D circular aperture or a 3D spherical aperture is given by (9). The C_i in (33) is derived with the approximation that $J_m\left(\frac{2\pi}{\lambda} r_i\right) \to 0$ for $m \ge \lceil \pi e r_i/\lambda \rceil + 1$, where $J_m(\cdot)$ denotes the Bessel function of order m. Such an approximation is shown to be very accurate in [19].

Finally, substituting (33) into (8) completes the proof of Proposition 1.

APPENDIX B
PROOF OF THEOREM 1

The capacity of Bob or Eve's channel subject to the basic jamming signals is written as [33, Section 3.1]

$$C_i = \log \left| \mathbf{I}_{N_i} + \alpha_i \mathbf{H}_i \mathbf{Q}_x \mathbf{H}_i^H \left(\beta_i \mathbf{G}_i \mathbf{Q}_w \mathbf{G}_i^H + \sigma_i^2 \mathbf{I}_{N_i}\right)^{-1} \right|, \tag{34}$$

where $\mathbf{Q}_x$ and $\mathbf{Q}_w$ denote the covariance matrices of $\mathbf{x}$ and $\mathbf{w}_1$, respectively, i.e., $\mathbf{Q}_x = \mathbb{E}\{\mathbf{x}\mathbf{x}^H\}$ and $\mathbf{Q}_w = \mathbb{E}\{\mathbf{w}_1\mathbf{w}_1^H\}$. Since neither Alice nor Helen has the instantaneous CSI to Bob or Eve, the equal power allocation at the transmit antennas is adopted at both Alice and Helen, and the covariance matrices of $\mathbf{x}$ and $\mathbf{w}_1$ are equal to $\mathbf{Q}_x = \frac{P_t}{N_t}\mathbf{I}_{N_t}$ and $\mathbf{Q}_w = \frac{P_j}{N_j}\mathbf{I}_{N_j}$, respectively. Then, the channel capacity becomes to

$$C_i = \log \left| \mathbf{I}_{N_i} + \frac{\alpha_i P_t}{N_t} \mathbf{H}_i \mathbf{H}_i^H \left(\frac{\beta_i P_j}{N_j} \mathbf{G}_i \mathbf{G}_i^H + \sigma_i^2 \mathbf{I}_{N_i}\right)^{-1} \right|. \tag{35}$$

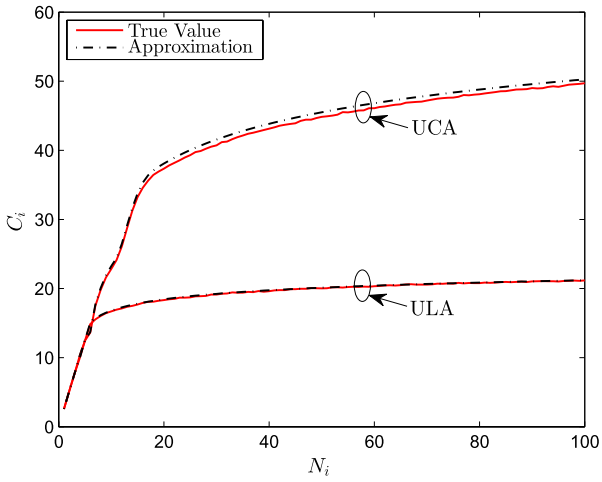


Fig. 11. With jamming signals: C_i versus N_i. The other system parameters are $N_t = N_j = 100$, $r_i = 1\lambda$, $P_t = 10$ dB, $P_j = 0$ dB $\alpha_i = 1$, $\beta_i = 1$, $\sigma_i^2 = 1$.

Considering the large number of transmit antennas ($N_t \to \infty, N_j \to \infty$) and sufficient space for placing transmit antennas (independent $\mathbf{h}_{it}$ and independent $\mathbf{g}_{it}$), we have

$$\frac{1}{N_t}\sum_{t=1}^{N_t}\mathbf{h}_{it}\mathbf{h}_{it}^H = \frac{1}{N_j}\sum_{t=1}^{N_j}\mathbf{g}_{it}\mathbf{g}_{it}^H = \mathbf{R}_i, \tag{36}$$

where $\mathbf{R}_i$ is the correlation matrix at the receiver side. Note that $\mathbf{R}_i$ is determined by the receive antenna correlations.

Therefore, the channel capacity can be approximated by

$$\begin{aligned} C_i &\approx \log\left|\mathbf{I}_{N_i} + \alpha_i P_t \mathbf{R}_i \left(\beta_i P_j \mathbf{R}_i + \sigma_i^2 \mathbf{I}_{N_i}\right)^{-1}\right| \\ &= \log\left|\mathbf{I}_{N_i} + \left(\frac{\alpha_i P_t}{\sigma_i^2} + \frac{\beta_i P_j}{\sigma_i^2}\right)\mathbf{R}_i\right| \\ &\quad - \log\left|\mathbf{I}_{N_i} + \frac{\beta_i P_j}{\sigma_i^2}\mathbf{R}_i\right|. \end{aligned} \tag{37}$$

We highlight that the approximation by (37) provides good accuracy even if the number of transmit antennas and the number of jamming antennas are finite. To examine the accuracy of the approximation by (37), we compare the true value of C_i obtained by (35) and the approximation obtain by (37) for given receive antenna array configurations. The simulation result is presented by Fig. 11. The number of transmit antennas and the number of jamming antennas are set as $N_t = N_j = 100$. The number of receive antennas is in the range of $1 \le N_i \le N_t = N_j = 100$. We still consider two different antenna array configurations, i.e., the ULA and the UCA, in a fixed circular aperture at the receiver with $r_i = 1\lambda$. It is evident from Fig. 11 that the difference between the true value and the approximation is very small for the whole range of N_i. This confirms that the approximation by (37) provides good accuracy even if the transmitter and the jammer have finite numbers of antennas.

For the receiver with N_i optimally-placed antennas in a fixed aperture region, the channel capacity in (37) can be further approximated by

$$C_i \approx \begin{cases} N_i \log\left(1 + \frac{\alpha_i P_t}{\beta_i P_j + \sigma_i^2}\right), & \text{if } N_i \le N_{0i} \\ N_{0i} \log\left(1 + \frac{\frac{N_i}{N_{0i}}\alpha_i P_t}{\frac{N_i}{N_{0i}}\beta_i P_j + \sigma_i^2}\right), & \text{otherwise.} \end{cases} \tag{38}$$

Still, the C_i in (38) is derived with the approximation that $J_m\left(\frac{2\pi}{\lambda} r_i\right) \to 0$ for $m \ge \lceil \pi e r_i/\lambda \rceil + 1$.

Finally, substituting (38) into (8) completes the proof of Theorem 1.

Appendix C
Proof of Theorem 2

Since the AN jamming signals do not degrade Bob's channel, we derive the capacity of Bob's channel directly from (33), which is given by

$$C_b \approx \begin{cases} N_b \log\left(1 + \frac{\alpha_b P_t}{\sigma_b^2}\right), & \text{if } N_b \le N_{0b} \\ N_{0b} \log\left(1 + \frac{N_b}{N_{0b}}\frac{\alpha_b P_t}{\sigma_b^2}\right), & \text{otherwise.} \end{cases} \tag{39}$$

Now, we derive the capacity of Eve's channel subject to the AN jamming signals. The received signal vector at Eve is written as

$$\mathbf{y}_e = \sqrt{\alpha_e}\mathbf{H}_e\mathbf{x} + \sqrt{\beta_e}\mathbf{K}\mathbf{v} + \mathbf{n}_e, \tag{40}$$

where $\mathbf{K} = \mathbf{G}_e\mathbf{Z}$ represents the equivalent channel for the vector $\mathbf{v}$ to Eve. Due to the orthonormality of $\mathbf{Z}$, the $N_e \times (N_j - N_b)$ matrix $\mathbf{K}$ has circularly symmetric i.i.d. complex Gaussian distributed elements. Then, the capacity of Eve's channel is written as

$$C_e = \log\left|\mathbf{I}_{N_e} + \alpha_e \mathbf{H}_e \mathbf{Q}_x \mathbf{H}_e^H \left(\beta_e \mathbf{K}\mathbf{Q}_v\mathbf{K}^H + \sigma_e^2\mathbf{I}_{N_e}\right)^{-1}\right|, \tag{41}$$

where $\mathbf{Q}_x$ and $\mathbf{Q}_v$ denote the covariance matrices of $\mathbf{x}$ and $\mathbf{v}$, respectively, i.e., $\mathbf{Q}_x = \mathbb{E}\{\mathbf{x}\mathbf{x}^H\}$ and $\mathbf{Q}_v = \mathbb{E}\{\mathbf{v}\mathbf{v}^H\}$. With the equal power allocation at Alice, we have $\mathbf{Q}_x = \frac{P_t}{N_t}\mathbf{I}_{N_t}$. Also, since $\mathbf{v}$ is chosen as i.i.d. complex Gaussian random variables, we have $\mathbf{Q}_v = \frac{P_j}{N_j - N_b}\mathbf{I}_{N_j - N_b}$. Then, the capacity of Eve's channel becomes to

$$C_e = \log\left|\mathbf{I}_{N_e} + \alpha_e P_t \mathbf{R}_e \left(\frac{\beta_e P_j}{N_j - N_b}\mathbf{K}\mathbf{K}^H + \sigma_e^2\mathbf{I}_{N_e}\right)^{-1}\right|, \tag{42}$$

where $\mathbf{R}_e$ is the correlation matrix at Eve, and is determined by the receive antenna correlations at Eve. Define $\mathbf{K} = [\mathbf{k}_1 \cdots \mathbf{k}_i \cdots \mathbf{k}_{N_j - N_b}]$, $\mathbf{Z} = [\mathbf{z}_1 \cdots \mathbf{z}_i \cdots \mathbf{z}_{N_j - N_b}]$, and hence $\mathbf{k}_i = \mathbf{H}_e\mathbf{z}_i$.

If we can prove that $\mathbf{k}_i$ *are independent*, the correlation matrix would converge to $\mathbf{R} \to \frac{1}{N_j - N_b}\mathbf{K}\mathbf{K}^H$ as $(N_j - N_b) \to \infty$, and the capacity of Eve's channel could be written as

$$C_e = \log\left|\mathbf{I}_{N_e} + \alpha_e P_t \mathbf{R}_e \left(\beta_e P_j \mathbf{R}_e + \sigma_e^2 \mathbf{I}_{N_e}\right)^{-1}\right|. \tag{43}$$

Having (43), we can derive the channel capacity of spatially-constrained Eve which is the same as (38).

Therefore, in the following, we need only to prove that $\mathbf{k}_i$ are independent to complete the proof of Theorem 2. For any $\mathbf{k}_m$ and $\mathbf{k}_n$ where $m \neq n$, we have

$$[\mathbf{k}_m - \mathbb{E}\{\mathbf{k}_m\}]^H [\mathbf{k}_n - \mathbb{E}\{\mathbf{k}_n\}] = \mathbf{z}_m^H \mathbf{H}_e^H \mathbf{H}_e \mathbf{z}_n \overset{(a)}{=} \mathbf{z}_m^H \mathbf{z}_n \overset{(b)}{=} 0, \tag{44}$$

where (a) is because of the independence between transmit antennas and (b) is because of the orthogonality of $\mathbf{Z}$. Thus, $\mathbf{k}_i$ are pairwise uncorrelated. In addition, multivariate normality and no correlation implies independence. Multivariate normality and pairwise independence implies mutual independence. Since $\mathbf{k}_i$ are multivariate normally distributed, $\mathbf{k}_i$ are mutually independent. This completes the proof of Theorem 2.

Appendix D
Proof of Proposition 2

We first rewrite (20) as

$$C_s^w = \begin{cases} \left[f_1(x = P_j)\right]^+, & \text{if } N_b \leq N_{0b} \\ \left[f_2(x = P_j)\right]^+, & \text{otherwise.} \end{cases} \tag{45}$$

If $N_b \leq N_{0b}$, we can obtain two possible stationary points of $f_1(x)$, i.e., x_1 and x_2, by taking the derivative of $f_1(x)$ with respect to x and equating it to zero. If C_s^w is not always equal to zero, P_j^o should exist and be equal to one of the stationary points, since $\lim_{x\to 0} f(x) \to -\infty$ and $\lim_{x\to\infty} f(x) \to 0$. Then, we determine P_j^o by examining the values of x_1 and x_2. When neither x_1 nor x_2 is real and positive, it is not applicable to determine the optimal value of P_j, because the stationary point for $f_1(x)$ does not exist, and C_s^w is always equal to zero for any value of P_j. Similarly, if $N_b > N_{0b}$, we can obtain two possible stationary points of $f_2(x)$, i.e., x_3 and x_4, by taking the derivative of $f_2(x)$ with respect to x and equating it to zero. Then, we determine P_j^o by examining the values of x_3 and x_4. When neither x_3 nor x_4 is real and positive, it is not applicable to determine the optimal value of P_j, because C_s^w is always equal to zero for any value of P_j. This completes the proof of Proposition 2.

References

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

[2] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. Boca Raton, FL, USA: CRC Press, 2013.

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

[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[5] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[6] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[7] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[8] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[9] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 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.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[11] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425–430, Feb. 2011.

[12] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[13] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[14] B. He and X. Zhou, "Secure on-off transmission design with channel estimation errors," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1923–1936, Dec. 2013.

[15] B. He, X. Zhou, and T. D. Abhayapala, "Wireless physical layer security with imperfect channel state information: A survey," *ZTE Commun.*, vol. 11, no. 3, pp. 11–19, Sep. 2013.

[16] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 63, no. 4, pp. 1678–1690, May 2014.

[17] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. L. Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.

[18] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. L. Goff, "Robust outage secrecy rate optimizations for a MIMO secrecy channel," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 86–89, Feb. 2015.

[19] T. S. Pollock, "On Limits of Multi-Antenna Wireless Communications in Spatially Selective Channels," Ph.D. dissertation, Dept. Telecommun. Eng., Australian Nat. Univ., Canberra, ACT, Australia, Jul. 2003. [Online]. Available: http://hdl.handle.net/1885/47999

[20] E. G. Larsson, O. Edfors, F. Tufvesson, and T. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, Feb. 2014.

[21] J. G. Andrews *et al.*, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[22] T. S. Pollock, T. D. Abhayapala, and R. A. Kennedy, "Introducing space into MIMO capacity calculations," *J. Telecommun. Syst.*, vol. 24, no. 2, pp. 415–436, Oct. 2003.

[23] T. D. Abhayapala, R. A. Kennedy, and J. T. Y. Ho, "On capacity of multi-antenna wireless channels: Effects of antenna separation and spatial correlation," in *Proc. IEEE AusCTW*, Canberra, ACT, Australia, Feb. 2002, pp. 4–5.

[24] T. S. Pollock, T. D. Abhayapala, and R. A. Kennedy, "Introducing "space" into space-time MIMO capacity calculations: A new closed form upper bound," in *Proc. ICT*, Feb. 2003, vol. 2, pp. 1536–1541.

[25] R. A. Kennedy, P. Sadeghi, T. D. Abhayapala, and H. M. Jones, "Intrinsic limits of dimensionality and richness in random multipath fields," *IEEE Trans. Signal Process.*, vol. 55, no. 6, pp. 2542–2556, Jun. 2007.

[26] F. Bashar and T. D. Abhayapala, "Degrees of freedom of band limited signals measured over space," in *Proc. ISCIT*, Oct. 2012, pp. 735–740.

[27] F. Bashar, S. M. A. Salehin, and T. D. Abhayapala, "Analysis of degrees of freedom of wideband random multipath fields observed over time and space windows," in *Proc. IEEE Workshop SSP*, Jun. 2014, pp. 45–48.

[28] F. Bashar, S. M. A. Salehin, and T. D. Abhayapala, "Band limited signals observed over finite spatial and temporal windows: An upper bound to signal degrees of freedom," *IEEE Trans. Signal Process.*, submitted for publication. [Online]. Available: http://arxiv.org/abs/1405.2163

[29] D. Gesbert, T. Ekman, and N. Christophersen, "Capacity limits of dense palm-sized MIMO arrays," in *Proc. IEEE GLOBECOM*, Nov. 2002, vol. 2, pp. 1187–1191.

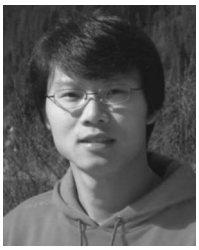
[30] L. Hanlen and M. Fu, "Capacity of MIMO wireless systems with spatially correlated receive elements," in *Proc. WITSP*, Wollongong, NSW, Australia, Dec. 2002, pp. 1–6.

[31] T. S. Pollock, T. D. Abhayapala, and R. A. Kennedy, "Antenna saturation effects on MIMO capacity," in *Proc. IEEE ICC*, May 2003, vol. 4, pp. 2301–2305.

[32] Y. Wu and Z. Nie, "On the MIMO channel capacity saturation for spatially constrained receive region," *J. Syst. Eng. Electron.*, vol. 18, no. 3, pp. 437–442, Sep. 2007.

[33] A. Bayesteh, M. Ansari, and A. K. Khandani, "Effect of jamming on the capacity of MIMO channels," in *Proc. Allerton Conf. Commun.*, Oct. 2004, pp. 401–410.

Biao He (S'13) received both the B.E. (hons.) degree in electronic and communication systems from the Australian National University (ANU), Canberra, ACT, Australia, and the B.E. degree in information engineering from Beijing Institute of Technology (BIT) in 2012. Currently, he is pursuing the Ph.D. degree with the Research School of Engineering, ANU. His research interests include physical layer security, wireless communications, and information theory.



Xiangyun Zhou (M'11) received the B.E. (hons.) degree in electronics and telecommunications engineering and the Ph.D. degree in telecommunications engineering from the Australian National University, Canberra, ACT, Australia, in 2007 and 2010, respectively. From 2010 to 2011, he worked as a Postdoctoral Fellow at UNIK - University Graduate Center, University of Oslo, Oslo, Norway. He joined the Australian National University in 2011 and currently works as a Senior Lecturer. His research interests are in the fields of communication theory and wireless networks.

Dr. Zhou currently serves on the editorial board of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and *IEEE Communications Letters*. He also served as a guest editor for *IEEE Communications Magazine's* feature topic on wireless physical layer security in 2015 and *EURASIP Journal on Wireless Communications and Networking's* special issue on energy harvesting wireless communications in 2014. He was a co-chair of the ICC workshop on wireless physical layer security at ICC'14 and ICC'15. He was the chair of the ACT Chapter of the IEEE Communications Society and Signal Processing Society from 2013 to 2014. He is a recipient of the Best Paper Award at ICC'11.

Thushara D. Abhayapala (M'00–SM'08) received the B.E. degree (with Honors) in engineering in 1994 and the Ph.D. degree in telecommunications engineering in 1999, both from the Australian National University (ANU), Canberra, ACT, Australia. He is a Professor at ANU. He was the Director of the Research School of Engineering at ANU from January 2010 to October 2014 and the Leader of the Wireless Signal Processing (WSP) Program at the National ICT Australia (NICTA) from November 2005 to June 2007. His research interests are in the areas of spatial audio and acoustic signal processing, space-time signal processing for wireless communication systems, and array signal processing. He has supervised over 30 research students and coauthored over 200 peer reviewed papers. He is an Associate Editor of IEEE/ACM TRANSACTIONS ON AUDIO, SPEECH, AND LANGUAGE PROCESSING. He is also a Member of the Audio and Acoustic Signal Processing Technical Committee (2011–2015) of the IEEE Signal Processing Society. He is a Fellow of the Engineers Australia (IEAust).