Enhancing Secrecy with Multi-Antenna Transmission in Wireless Ad Hoc Networks

Xi Zhang, *Student Member, IEEE,* Xiangyun Zhou, *Member, IEEE,*
and Matthew R. McKay, *Senior Member, IEEE*

***Abstract*—We study physical-layer security in wireless ad hoc networks and investigate two types of multi-antenna transmission schemes for providing secrecy enhancements. To establish secure transmission against malicious eavesdroppers, we consider the generation of artificial noise with either sectoring or beamforming. For both approaches, we provide a statistical characterization and tradeoff analysis of the outage performance of the legitimate communication and the eavesdropping links. We then investigate the networkwide secrecy throughput performance of both schemes in terms of the secrecy transmission capacity, and study the optimal power allocation between the information signal and the artificial noise. Our analysis indicates that, under transmit power optimization, the beamforming scheme outperforms the sectoring scheme, except for the case where the number of transmit antennas are sufficiently large. Our study also reveals some interesting differences between the optimal power allocation for the sectoring and beamforming schemes.**

***Index Terms*—Physical-layer security, ad hoc networks, multi-antenna transmission, artificial noise, power allocation, outage probability, throughput optimization.**

I. Introduction

INFORMATION security is a prime concern in emerging wireless networks. Traditional security mechanisms, typically involving cryptographic algorithms, implicitly assume that any potential eavesdroppers have limited computational abilities. Rapid development of computing hardware, however, has meant that there is an ever-increasing susceptibility of such methods to attack. To address this problem and further strengthen existing wireless security technologies, physical-layer security mechanisms [1–3] have recently attracted significant attention. Such mechanisms work by exploiting the physical properties of the wireless medium in order to provide an additional layer of robustness which is "information-theoretically secure". In the past decade, physical-layer security techniques have been proposed in many different communication scenarios; e.g., multi-input multi-output, relay/jammer-assisted, cognitive-radio-enabled, and so on (see e.g., [4–9] and the references therein). Very recently, physical-layer security techniques have also been introduced into large-scale decentralized ad hoc networks, in order to provide enhanced secrecy performance [10–18].

When characterizing the networkwide secrecy throughput of large-scale networks, the interference due to concurrent transmissions plays an important role. On the one hand, from the point of view of the legitimate receivers, interference is a nuisance which leads to unwanted throughput loss; whilst, on the other hand, to the eavesdroppers, interference makes it more difficult to intercept transmissions (thereby providing enhanced security). In decentralized networks, it is reasonable to assume that the legitimate receivers do not have sophisticated multi-user decoding capabilities, and thereby treat interference simply as noise. For the eavesdroppers, however, one should typically not make such strong assumptions, since the capabilities of eavesdroppers are often unknown. This has led researchers to design for a worst-case scenario (see e.g., [15–17]), whereby the eavesdroppers are assumed to be capable of performing multi-user decoding (e.g., successive interference cancellation), allowing the interference created by concurrent transmission of information signals to be potentially resolved.

In order to confuse eavesdroppers with multi-user decodability in ad hoc networks, methods have been introduced in [16, 17] based on generating artificial noise (see [19, 20]) or cooperative jamming (see [21, 22]). In both cases, the aim is to create non-resolvable interference at the eavesdroppers. Specifically, in [16], the legitimate users which are far away from the intended receiver were selected to emit artificial noise; while in [17], a certain percentage of legitimate users were randomly chosen to radiate jamming signals. Note that when the legitimate nodes have only a single antenna, as in [16, 17], some legitimate users must suspend their own message transmission in order to deliver artificial noise or jamming signals. In [18], the authors considered the case where there are many multi-antenna helping jammers, generating artificial interference but zero-forcing to nearby legitimate receivers. The injected jamming signals can also help to deal with eavesdroppers with multi-user decodability. However, in some cases, such a large number of helping jammers may not be obtainable and when this happens, the designed transmission scheme might be vulnerable.

A. Our Approach and Contribution

In this paper, we consider two artificial-noise-aided multi-antenna transmission strategies, based on antenna sectoring

X. Zhang and M. R. McKay are with the Department of Electronic and Computer Engineering, the Hong Kong University of Science and Technology, Hong Kong (e-mails: xizhangx@ust.hk, eemckay@ust.hk).

X. Zhou is with the Research School of Engineering, the Australian National University, Australia (e-mail: xiangyun.zhou@anu.edu.au).

This paper was presented in part at the IEEE International Workshop on Signal Processing Advances for Wireless Communications, Darmstadt, Germany, June 16–19, 2013. The work of X. Zhang and M. R. McKay was supported by the Hong Kong Research Grants Council (Grant No. 616312). The work of X. Zhou was supported by the Australian Research Council's Discovery Projects funding scheme (Project No. DP110102548).

or beamforming, for providing secrecy in wireless ad hoc networks. Knowing the direction of the intended receiver, with antenna sectoring, an information signal is transmitted towards the intended receiver, while artificial noise is simultaneously radiated in other sectors. With the channel state information (CSI) of the intended receiver, through beamforming, artificial noise is injected into the null-space of the intended channel, leaving the intended receiver unaffected. Note that these two transmission schemes do *not* require any instantaneous channel knowledge of the eavesdroppers. With the proposed transmission schemes, non-resolvable interference is created at the potential eavesdroppers by the introduced artificial noise, allowing us to guarantee a target secrecy throughput, which appears difficult without using artificial noise. Moreover, as a major advantage of these schemes, no legitimate users must stop their own message transmission, which is in contrast to the single-antenna transmission approaches [16, 17]. In particular, since the artificial-noise generated interference is created by the legitimate transmitters themselves, the system can work in the absence of helping jammers [18].

Previous studies in [19–30] have clearly shown that smartly injecting artificial interference can achieve secrecy enhancements in point-to-point scenarios. In such cases, the artificial noise generated from multi-antenna beamforming results in interference in some subspaces but no interference in others. Contrarily, in ad hoc networks where transmitters generate artificial noise in a decentralized manner, artificial interference is created collectively in all subspaces over the entire network. In short, the artificial-noise-aided beamforming and sectoring schemes considered in this paper have a *cooperative jamming* effect in ad hoc networks, which ensures that every eavesdropper is subjected to jamming. With these cooperative jamming effects, it is unclear how well the proposed artificial-noise-aided multi-antenna transmission schemes can work in large-scale networks, as a means of jointly providing high communication performance and security. Our main objective is to address this key question.

For both the sectoring and beamforming schemes, we characterize the performance of the legitimate link and the eavesdropping link, by deriving new closed-form expressions for the connection and secrecy outage probabilities respectively. We then illustrate the tradeoff between the connection and secrecy outage performance. Under constraints on the connection and secrecy outage probabilities, we quantify the achievable secrecy throughput performance of both schemes in terms of the secrecy transmission capacity. Finally, we investigate the optimal power allocation between the information signal and the artificial noise which maximizes the secrecy transmission capacity, and compare the corresponding maximum secrecy transmission capacity of both schemes. Our analytical and numerical results suggest that the considered multi-antenna transmission schemes can achieve significant secrecy enhancements in wireless ad hoc networks.

We observe that by adding extra transmit antennas, the optimal ratio of power allocated to the information signal that maximizes the secrecy transmission capacity of the beamforming scheme converges to a certain fraction which is strictly less than one, while that for the sectoring scheme keeps increasing towards one. We show that as the number of transmit antennas grows large, for both the sectoring and beamforming schemes, the optimized secrecy transmission capacity increases logarithmically. Our analysis also indicates that, in terms of the optimized secrecy transmission capacity, the beamforming scheme outperforms the sectoring scheme for a wide range of antenna numbers, at the expense of requiring additional channel knowledge. Nevertheless, as the number of transmit antennas becomes sufficiently large, quite interestingly, the sectoring scheme can achieve a better throughput performance than the beamforming scheme. The performance crossover happens at a larger antenna number if the secrecy outage constraint becomes more stringent.

The rest of the paper is organised as follows. In Section II, we introduce the system model and illustrate the proposed transmission schemes. In Section III, we characterize the outage performance of the sectoring scheme. In Section IV, we study the outage performance of the beamforming scheme. In Section V, we analyze and compare the secrecy throughput performance of the sectoring and beamforming schemes. Finally, in Section VI, we conclude this paper.

II. System Model

The legitimate transmitters and malicious eavesdroppers are modeled by two independent homogeneous Poisson point processes (PPPs) on a two dimensional plane $\mathbb{R}^2$ with densities λ_l and λ_e, respectively. The location sets of the legitimate transmitters and eavesdroppers are denoted by Φ_L and Φ_E, respectively. Following the widely-used bipolar network model [31, 32], we assume that every transmitter has an intended receiver at distance r in a random direction[1]. Each transmitter is equipped with N transmit antennas, while each receiver (both legitimate and malicious) has a single receive antenna. In addition to an exponential path loss with parameter $\alpha > 2$, the wireless channels are assumed to be experiencing independent Rayleigh fading. Since we are studying large-scale networks with uncoordinated concurrent transmissions, the aggregate interference will be dominant, and the local thermal noise is usually negligible. As done in [13, 14, 17], we omit the thermal noise and use the signal-to-interference ratio (SIR) as the main performance metric.

The total transmit power at each transmitter is denoted by P. Define ϕ as the ratio of the power of the information signal to the total transmit power. Thus, the power allocated to the information signal is $P_I = P\phi$, while the power allocated to the artificial noise is $P_A = P(1-\phi)$. In the following, we consider the use of artificial noise in the form of either sectoring or beamforming, for providing secrecy against the malicious eavesdroppers.

[1]This bipolar network model is suitable for modeling the case where the distance from the transmitter to the intended receiver is relatively small, compared with the distances between the transmitters, and it is widely used in the literature (see e.g., [13, 17, 18, 31, 32]). Generalization can be made by setting the distance r as a random variable following a certain distribution, and then averaging the network performance over the distribution of r, as mentioned in [31].

A. Sectoring with Artificial Noise

With N directional antennas, each transmitter can send independent signals in N disjoint sectors, each of these covering $\frac{2\pi}{N}$ radians with an antenna gain G_N. The antenna gain usually increases as the spread angle decreases (i.e., increasing N). As done in [12], we assume that the sidelobes are suppressed sufficiently and thus can be omitted in later analysis[2]. We then consider the following scheme to combine sectoring with artificial noise generation: Each transmitter sends an information signal in the sector containing its intended receiver, while simultaneously emitting artificial noise in all other sectors, creating non-resolvable interference to the malicious eavesdroppers. Note that the transmitter needs to know the direction of the intended receiver and this information can be accurately obtained through the discovery mechanisms, such as the "informed discovery" mechanism in [33], where the feedback from the intended receiver is exploited for a high accuracy. We further assume that the time needed for acquiring and feeding back this directional information is negligible. Note that this sectoring scheme does *not* require the CSI at the transmitter. With the antenna gain, in the intended sector, the information signal is transmitted with power $G_N P_I$, while in each of the other $N-1$ sectors, artificial noise is radiated with power $\frac{G_N P_A}{N-1}$.

B. Beamforming with Artificial Noise

With N omnidirectional antennas, the transmitters can perform artificial-noise-aided beamforming [19, 20]. To do this, the instantaneous CSI of the intended receiver is needed at the associated transmitter. This information can be obtained via pilot training and we assume that the time needed for the training phase is negligible. With the CSI, the transmitter performs maximal ratio transmission towards the intended receiver with power P_I. Meanwhile, to confuse the malicious eavesdroppers, artificial noise with total power P_A is uniformly injected into the null space of the intended channel. To be specific, denoting the intended channel by $\mathbf{h}$, an orthonormal basis is generated at the transmitter as $\left[\frac{\mathbf{h}}{\|\mathbf{h}\|}, \mathbf{W}\right]$, where $\mathbf{W}$ is a $N \times (N-1)$ matrix, the columns of which are mutually orthogonal while also being orthogonal to $\frac{\mathbf{h}}{\|\mathbf{h}\|}$. The message vector to be transmitted will then have the following form:

$$\mathbf{x} = \frac{\mathbf{h}}{\|\mathbf{h}\|} u + \mathbf{W}\mathbf{v} \tag{1}$$

where u is the information signal, assumed to be complex Gaussian distributed with variance P_I; $\mathbf{v}$ is the artificial noise vector, the entries of which are complex Gaussian distributed with zero mean and variance $\sigma_v^2 = \frac{P_A}{N-1}$.

[2]We point out that the analytical results can be generalized to incorporate the sidelobe leakage signals, by accounting for the eavesdroppers outside the main lobe of the intended sector, and carefully evaluating the aggregate artificial noise received by the eavesdroppers. However, the resulting analytical expressions become much more complicated, whilst few new insights can be extracted. In fact, it can be shown that, as long as the leakage signals in the sidelobes are not particularly strong, the resulting performance degradations are insignificant. For simplicity, we focus on the case of perfectly sectorized antennas with negligible sidelobes.

C. Wiretap Coding and Outage Definition

Here we explain the coding scheme and the outage definitions. Before transmission, the data is encoded using the wiretap code [1]. The codeword rate and the secret message rate are denoted by R_b and R_s, respectively. The codeword rate R_b is the actual transmission rate of the codewords, while the secrecy rate R_s is the rate of the embedded message. The rate redundancy $R_e := R_b - R_s$ is intentionally added, in order to provide secrecy against malicious eavesdropping. More discussions on code construction can be found in [34]. If the channel from the transmitter to its intended receiver cannot support the codeword rate R_b, the receiver may not be able to decode the transmitted codeword correctly. We consider this as a *connection outage* event.

There are possibly several eavesdroppers trying to intercept the same transmitter, while the exact number of them is unknown. To minimize the assumption on the eavesdroppers' behavior and design for a worst case, we consider the scenario where all eavesdroppers are trying to decode the message from the transmitter under consideration. Therefore, if the channel from the transmitter to any of the eavesdroppers can support a data rate larger than the embedded rate redundancy R_e, this transmission fails to achieve perfect secrecy and a *secrecy outage* is deemed to occur [35]. As mentioned in [14], this kind of secrecy outage formulation provides a "strong" secrecy performance.

Note that we assume the legitimate receivers do not apply multi-user decoding techniques. Thus, the interference at the legitimate receivers consists of the information signals and the artificial noise. On the other hand, we assume that the eavesdroppers are capable of multi-user decoding, i.e., resolving concurrent transmissions. In order to design the network parameters to achieve the maximum level of secrecy, as done in [15–17], we consider a worst-case assumption to overestimate the eavesdroppers' multi-user decodability: For the signal reception at any eavesdropper, only the artificial noise constitutes the interference, whereas the received information signals are resolvable and hence are not part of the interference.

III. Outage Performance of Sectoring Scheme

In this section, we study the outage performance of the sectoring scheme. We start by deriving the outage probability of the intended links. Then, we characterize the possibility that the transmitted message is not secure against the malicious eavesdroppers.

A. Connection Outage Probability

Here, we derive the connection outage probability p_{co}. A threshold SIR value for connection outage is defined as β_b. We focus on a typical transmitter-receiver pair and place the receiver at the origin of the coordinate system. From Slivnyak's theorem [36], the distribution of all other nodes' locations will not be affected; thus, the obtained statistics can reflect the system performance accurately.

For the typical receiver at the origin, the interfering nodes can be classified into two classes: 1) interferers transmitting

information signals towards the typical receiver; 2) interferers sending artificial noise towards the typical receiver. With such a classification, by [36], the transmitters in Φ_L can be divided into two independent homogeneous PPPs, which are denoted as Φ_I and Φ_A with densities $\frac{1}{N}\lambda_l$ and $\frac{N-1}{N}\lambda_l$, respectively.

Then, the aggregate interference resulting from the transmitters in Φ_I and Φ_A is given by

$$I_I = G_N P_I \sum_{x\in\Phi_I} S_{xo} D_{xo}^{-\alpha}$$
$$I_A = \frac{G_N P_A}{N-1} \sum_{x\in\Phi_A} S_{xo} D_{xo}^{-\alpha} \tag{2}$$

where D_{xo} represents the distance from the transmitter at x to the typical receiver at the origin, and S_{xo} represents the corresponding channel gain. With independent Rayleigh fading, the channel gains S_{xo} are independent and exponentially distributed with unit mean, i.e., $S_{xo} \sim \mathrm{Exp}\,(1)$. The channel gain from the typical transmitter to the typical receiver is denoted by S_o, with $S_o \sim \mathrm{Exp}\,(1)$. The SIR at the typical receiver is given by

$$\mathrm{SIR}_o = G_N P_I S_o r^{-\alpha} \left(I_I + I_A\right)^{-1} \tag{3}$$

and the connection outage probability is given by

$$p_{\mathrm{co}} = \Pr\left(\mathrm{SIR}_o \le \beta_b\right) . \tag{4}$$

This can be derived in closed-form and is presented in the following theorem:

Theorem 1. The connection outage probability of the sectoring scheme in (4) is given by

$$p_{\mathrm{co}} = 1 - \exp\left(-\frac{\beta_b^{\frac{2}{\alpha}} \lambda_l C_{\alpha,2} r^2}{N}\left(1 + (N-1)^{1-\frac{2}{\alpha}} \left(\phi^{-1}-1\right)^{\frac{2}{\alpha}}\right)\right) \tag{5}$$

where

$$C_{\alpha,N} := \pi \frac{\Gamma\left(N-1+\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right)}{\Gamma\left(N-1\right)} \tag{6}$$

and $\Gamma\left(\cdot\right)$ is the gamma function.

Proof: See Appendix A. ∎

From (5), we observe that as the distance between each transmitter-receiver pair r or the density of the transmitters λ_l increases, the connection outage probability increases towards one (as expected), with the rate of increase being exponential in r^2 or λ_l. In the latter case, as λ_l increases, more transmitters "on average" will be closer to any given legitimate receiver, leading to an increased connection outage probability.

From (5), for a given power allocation ratio, it can be shown that with a relatively small path-loss exponent, i.e., $\alpha = 2 \sim 4$, the connection outage probability decreases when extra directional antennas are added. The improvement comes from two aspects: 1) the intended sectors shrink and thus the legitimate receivers are interfered by less information signals; 2) the power allocated to the artificial noise is distributed in more sectors and thus the legitimate receivers are interfered by relatively less artificial noise.

B. Secrecy Outage Probability

Here, we characterize the secrecy outage probability p_{so}. A threshold SIR value for secrecy outage is defined as β_e. As before, we focus on a typical transmitter-receiver pair but shift the coordinate system to put the transmitter at the origin. The message from the typical transmitter is not secure against the eavesdropper at z if $\mathrm{SIR}_z > \beta_e$, where SIR_z denotes the SIR received by the eavesdropper at z. With the sectoring scheme, only the eavesdroppers inside the intended sector of the typical transmitter may cause secrecy outage. Those eavesdroppers form a fan-shaped PPP and by [36, Theorem A.1], they can be mapped as a homogeneous PPP on the whole plane, denoted by Φ_Z with density $\frac{1}{N}\lambda_e$.

As done in [15–17], we design for a worst-case scenario by overestimating the eavesdroppers' multi-user decodability: The aggregate interference at the eavesdropper side consists of the artificial noise only. By [36], the transmitters which are radiating artificial noise towards the eavesdropper at z form a homogeneous PPP Φ_A with density $\frac{N-1}{N}\lambda_l$. Hence, the interference seen by the eavesdropper at z is

$$I_A = \frac{G_N P_A}{N-1} \sum_{x\in\Phi_A} S_{xz} D_{xz}^{-\alpha} \tag{7}$$

where D_{xz} represents the distance from the transmitter at x to the eavesdropper at z, whilst $S_{xz} \sim \mathrm{Exp}\,(1)$ represents the corresponding channel gain.

The SIR received by the eavesdropper at z is given by

$$\mathrm{SIR}_z = G_N P_I S_{oz} D_{oz}^{-\alpha} I_A^{-1} \tag{8}$$

where D_{oz} represents the distance from the typical transmitter to the eavesdropper at z, whilst $S_{oz} \sim \mathrm{Exp}\,(1)$ represents the corresponding channel gain.

By taking the complement of the probability that the transmitted message is secure against all of the eavesdroppers, the secrecy outage probability can be expressed as

$$p_{\mathrm{so}} = 1 - \mathbb{E}_{\Phi_A}\left\{\mathbb{E}_{\Phi_Z}\left\{\prod_{z\in\Phi_Z} \Pr\left(\mathrm{SIR}_z < \beta_e | \Phi_A\right)\right\}\right\} . \tag{9}$$

The following theorem presents closed-form upper and lower bounds for this quantity:

Theorem 2. The secrecy outage probability of the sectoring scheme in (9) satisfies

$$p_{\mathrm{so}}^{\mathrm{LB}} \le p_{\mathrm{so}} \le p_{\mathrm{so}}^{\mathrm{UB}} \tag{10}$$

where

$$p_{\mathrm{so}}^{\mathrm{UB}} = 1 - \exp\left(-\frac{\frac{\pi}{C_{\alpha,2}}\frac{\lambda_e}{\lambda_l}}{\beta_e^{\frac{2}{\alpha}}\left(N-1\right)^{1-\frac{2}{\alpha}}\left(\phi^{-1}-1\right)^{\frac{2}{\alpha}}}\right) \tag{11}$$

and

$$p_{\mathrm{so}}^{\mathrm{LB}} = \frac{\pi\lambda_e}{\pi\lambda_e + \lambda_l C_{\alpha,2}\beta_e^{\frac{2}{\alpha}}\left(N-1\right)^{1-\frac{2}{\alpha}}\left(\phi^{-1}-1\right)^{\frac{2}{\alpha}}} \tag{12}$$

with $C_{\alpha,2}$ defined in (6).

Proof: See Appendix B. ∎

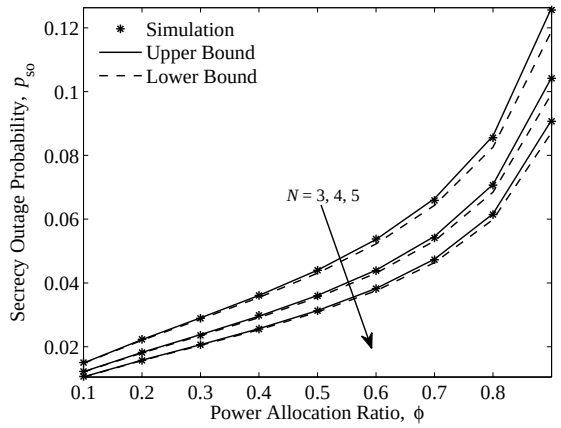


Fig. 1. The secrecy outage probability bounds of the sectoring scheme in (11) and (12) and the simulation results versus the power allocation ratio. Results are shown for the case where $\alpha = 4$, $\lambda_l = 0.01$, $\lambda_e = 0.001$ and $\beta_e = 1$.

In the low outage region (i.e., as $p_{\rm so} \to 0$), the upper bound in (11) and the lower bound in (12) share the same leading order term:

$$p_{\rm so}^{\rm UB} \approx \frac{\frac{\pi}{C_{\alpha,2}}\frac{\lambda_e}{\lambda_l}}{\beta_e^{\frac{2}{\alpha}}\left(N-1\right)^{1-\frac{2}{\alpha}}\left(\phi^{-1}-1\right)^{\frac{2}{\alpha}}} \approx p_{\rm so}^{\rm LB} \qquad (13)$$

implying that they both approach the exact secrecy outage probability as it becomes small. As shown in Fig. 1, the upper bound in (11) gives a very accurate approximation for the entire range of the secrecy outage probabilities shown, while the lower bound in (12) gets asymptotically accurate as the secrecy outage probability becomes small.

From (11), we see that the secrecy outage probability increases with increasing the eavesdroppers' density λ_e. Intuitively, as λ_e increases, more eavesdroppers "on average" will be closer to any given transmitter, which leads to an increased secrecy outage probability. More interestingly, the secrecy outage probability in (11) depends on the densities of the transmitter-receiver pairs and the eavesdroppers solely through their ratio $\frac{\lambda_e}{\lambda_l}$.

From (11), we observe that for a given power allocation ratio, the secrecy outage probability can be reduced by adding extra directional transmit antennas. This result follows the intuition that by adding transmit antennas: 1) the intended sector shrinks and thus less eavesdroppers may cause secrecy outage; 2) the artificial noise from other transmitters covers a larger region and thus more eavesdroppers are degraded.

IV. Outage Performance of Beamforming Scheme

In this section, we characterize the outage performance of the beamforming scheme. As before, we first derive the outage probability of the intended links. Then, we inspect the possibility that the transmitted message is not secure against malicious eavesdropping.

A. Connection Outage Probability

To facilitate our subsequent analysis, we first derive the distribution of the interference power resulting from the beamforming signal in (1).

Lemma 1. For a given realization of the intended channel $\mathbf{h}$, if the transmitted signal $\mathbf{x}$ in (1) is received by a non-intended receiver through an unknown channel $\mathbf{h}_z$, and if $P_I \neq \frac{P_A}{N-1}$ (i.e., $\phi \neq \frac{1}{N}$), then the resulting interference power P_x is distributed according to the following probability density function (p.d.f.):

$$f_{P_x}(z) = \frac{1}{P_I}\left(1-\frac{P_A}{(N-1)P_I}\right)^{1-N} {\rm e}^{-\frac{z}{P_I}} \times \left(1-{\rm e}^{-\left(\frac{N-1}{P_A}-\frac{1}{P_I}\right)z}\sum_{k=0}^{N-2}\frac{\left(\frac{N-1}{P_A}-\frac{1}{P_I}\right)^k z^k}{k!}\right), \ z>0\,. \qquad (14)$$

Meanwhile, if $\phi = \frac{1}{N}$, P_x is gamma distributed with shape parameter N and scale parameter P_I, i.e., $P_x \sim {\rm Gamma}\left(N, P_I\right)$. Note that the distribution of P_x is independent of the intended channel (i.e., $\mathbf{h}$).

Proof: See Appendix C. ∎

With Lemma 1, we now derive the connection outage probability $p_{\rm co}$. A threshold SIR value for connection outage is defined as β_b. As before, we focus on a typical transmitter-receiver pair, and put the typical receiver at the origin to observe the network performance. We denote the interference power from the transmitter at x to the typical receiver by P_{xo}, where the path loss is excluded. Note that P_{xo} admits the p.d.f. in (14). The aggregate interference seen by the typical receiver is given by

$$I_{IA} = \sum_{x\in\Phi_L} P_{xo} D_{xo}^{-\alpha} \qquad (15)$$

where D_{xo} denotes the distance from the transmitter at x to the typical receiver at the origin.

The channel vector from the typical transmitter to the typical receiver is denoted as $\mathbf{h}_o$. With Rayleigh fading, the elements of $\mathbf{h}_o$ are independent complex Gaussian distributed with zero mean and unit variance. With the beamforming strategy in (1), the SIR at the typical receiver is given by

$${\rm SIR}_o = P_I \|\mathbf{h}_o\|^2 r^{-\alpha} I_{IA}^{-1} \qquad (16)$$

and the connection outage probability is then given by

$$p_{\rm co} = \Pr\left({\rm SIR}_o \leq \beta_b\right)\,. \qquad (17)$$

We have the following key theorem:

Theorem 3. The connection outage probability of the beamforming scheme in (17) admits

$$p_{\rm co} = 1 - {\rm e}^{-\beta_b^{\frac{2}{\alpha}}\psi(\phi)} - {\rm e}^{-\beta_b^{\frac{2}{\alpha}}\psi(\phi)}\sum_{p=1}^{N-1}\frac{1}{p!}\sum_{k=1}^{p}\left(\frac{2}{\alpha}\beta_b^{\frac{2}{\alpha}}\psi(\phi)\right)^k \zeta(p,k) \qquad (18)$$

where $\psi\left(\phi\right)$ is defined in (19) and

$$\zeta(p,k) = \sum_{\theta\in{\rm comb}\binom{p-1}{p-k}} \prod_{\substack{l_i\in\theta \\ i=1,\ldots,p-k}} \left(l_i - \frac{2}{\alpha}\left(l_i - i + 1\right)\right). \qquad (20)$$

Here ${\rm comb}\binom{p-1}{p-k}$ is the set of all distinct subsets of the natural numbers $\{1,2,\ldots,p-1\}$ with cardinality $p-k$. For each subset, the elements are arranged in an increasing order and $l_i \in \theta$ is the i-th element of θ. For $p \geq 1$, $\zeta\left(p,p\right) = 1$.

Proof: See Appendix D. ∎

$$\psi(\phi)=\begin{cases}\pi\lambda_l r^2\Gamma\left(1-\frac{2}{\alpha}\right)\left(\frac{N-\phi^{-1}}{N-1}\right)^{1-N}\left(\Gamma\left(1+\frac{2}{\alpha}\right)-\left(\frac{\phi^{-1}-1}{N-1}\right)^{1+\frac{2}{\alpha}}\sum_{k=0}^{N-2}\left(\frac{N-\phi^{-1}}{N-1}\right)^{k}\frac{\Gamma\left(k+1+\frac{2}{\alpha}\right)}{\Gamma(k+1)}\right) & \text{if } \phi\neq\frac{1}{N}\\ \pi\lambda_l r^2\frac{\Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(N+\frac{2}{\alpha}\right)}{\Gamma(N)} & \text{if } \phi=\frac{1}{N}\end{cases} \tag{19}$$

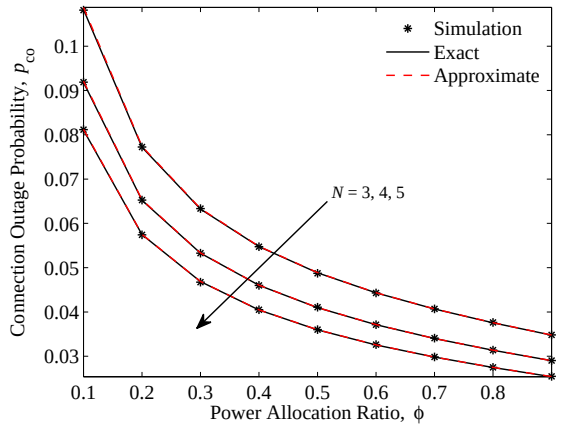


Fig. 2. The connection outage probability of the beamforming scheme in (18), the low outage approximation in (21) and the simulation results versus the power allocation ratio. Results are shown for the case where $\lambda_l = 0.01$, $r = 1$, $\alpha = 4$ and $\beta_b = 3$.

Due to the complexity of the derived expression in (18), observing the effects of varying the key system parameters such as the power allocation ratio ϕ and the number of transmit antennas N seems difficult. Nevertheless, with (18), we may readily evaluate the system performance and thereby avoid large-scale network simulations. In the low outage region, a much simpler approximation can be found as follows:

Corollary 1. In the low outage region (i.e., as $p_{\rm co}\to 0$), the connection outage probability in (18) can be approximated by

$$\tilde{p}_{\rm co}=\beta_b^{\frac{2}{\alpha}}\psi(\phi)K_{\alpha,N} \tag{21}$$

where $\psi(\phi)$ is defined in (19) and

$$K_{\alpha,N}=1-\frac{2}{\alpha}\sum_{p=1}^{N-1}\frac{1}{p!}\prod_{l=1}^{p-1}\left(l-\frac{2}{\alpha}\right)\ . \tag{22}$$

Proof: See Appendix E. ∎

As demonstrated in Fig. 2, for outage probabilities of practical interests, the difference between the exact value and the low outage approximation in (21) can hardly be seen.

B. Secrecy Outage Probability

Here we derive the secrecy outage probability $p_{\rm so}$. A threshold SIR value for secrecy outage is defined as β_e. As before, we focus on a typical transmitter-receiver pair but shift the coordinate system to put the transmitter at the origin.

As done in [15–17], we design for a worst-case scenario by overestimating the eavesdroppers' multi-user decodability: The aggregate interference at the eavesdropper side consists of the artificial noise only. We denote the channel from the transmitter at x to the eavesdropper at z by $\mathbf{h}_{xz}$. For the eavesdropper at z, by (1), the artificial noise received from the transmitter at x is given by $\mathbf{h}_{xz}^H\mathbf{W}_x\mathbf{v}_x$, where $\mathbf{W}_x$ and $\mathbf{v}_x$ constitute the beamforming matrix and the artificial noise vector for the transmitter at x. Define $\mathbf{g}_{xz}:=\mathbf{h}_{xz}^H\mathbf{W}_x$ and note that $\mathbf{g}_{xz}$ is a $N-1$ dimensional row vector. The corresponding interference power is given by $\|\mathbf{g}_{xz}\|^2\sigma_v^2$, where $\sigma_v^2=\frac{P_A}{N-1}$ is the variance of each element of $\mathbf{v}_x$. Then, for the eavesdropper at z, the aggregate interference created by the artificial noise from the transmitters in Φ_L is given by

$$I_A=\frac{P_A}{N-1}\sum_{x\in\Phi_L}\|\mathbf{g}_{xz}\|^2D_{xz}^{-\alpha} \tag{23}$$

where D_{xz} denotes the distance from the transmitter at x to the eavesdropper at z. Since the columns of $\mathbf{W}_x$ are unit-norm and mutually orthogonal, the elements of $\mathbf{g}_{xz}$ are independent complex Gaussian distributed with zero mean and unit variance; thus, we know that $\|\mathbf{g}_{xz}\|^2\sim\text{Gamma}\,(N-1,1)$. Note that the eavesdroppers will also be jammed by the artificial noise from the typical transmitter. Similar to the discussions above, for the eavesdropper at z, the interference power created by the typical transmitter is given by $\frac{P_A}{N-1}\|\mathbf{g}_{oz}\|^2D_{oz}^{-\alpha}$, where $\|\mathbf{g}_{oz}\|^2\sim\text{Gamma}\,(N-1,1)$, and D_{oz} is the distance from the typical transmitter to the eavesdropper at z.

Denote $\mathbf{h}_o$ as the channel from the typical transmitter to the typical receiver, and $\mathbf{h}_{oz}$ as the channel from the typical transmitter to the eavesdropper at z. Then, denote the channel gain resulting from Rayleigh fading from the typical transmitter to the eavesdropper at z by S_{oz}. Due to the fact that the typical transmitter is beamforming towards the typical receiver, the channel gain S_{oz} is given by

$$S_{oz}=\left|\mathbf{h}_{oz}^H\frac{\mathbf{h}_o}{\|\mathbf{h}_o\|}\right|^2\sim\text{Exp}\,(1)\ . \tag{24}$$

The SIR for the eavesdropper at z is then given by

$$\text{SIR}_z=\frac{P_IS_{oz}D_{oz}^{-\alpha}}{\frac{P_A}{N-1}\|\mathbf{g}_{oz}\|^2D_{oz}^{-\alpha}+I_A}\ . \tag{25}$$

By taking the complement of the probability that the transmitted message is secure against all of the eavesdroppers, the secrecy outage probability can be expressed as

$$p_{\rm so}=1-\mathbb{E}_{\Phi_L}\left\{\mathbb{E}_{\Phi_E}\left\{\prod_{z\in\Phi_E}\Pr\left(\text{SIR}_z<\beta_e|\Phi_L\right)\right\}\right\}\ . \tag{26}$$

We can find closed-form upper and lower bounds as follows:

Theorem 4. The secrecy outage probability of the beamforming scheme in (26) satisfies

$$p_{\rm so}^{\rm LB}\le p_{\rm so}\le p_{\rm so}^{\rm UB} \tag{27}$$

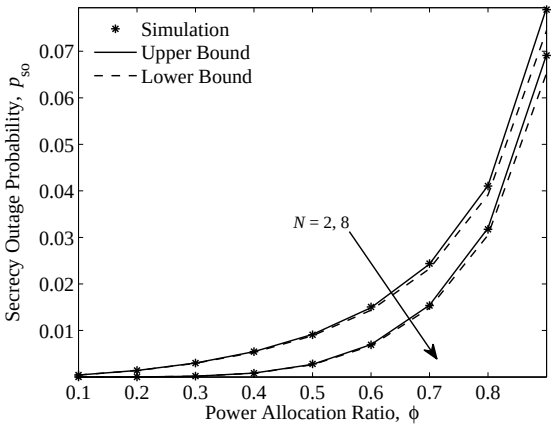


Fig. 3. The secrecy outage probability bounds of the beamforming scheme in (28) and (29) and the simulation results versus the power allocation ratio. Results are shown for the case where $\alpha = 4$, $\lambda_l = 0.01$, $\lambda_e = 0.001$ and $\beta_e = 3$.

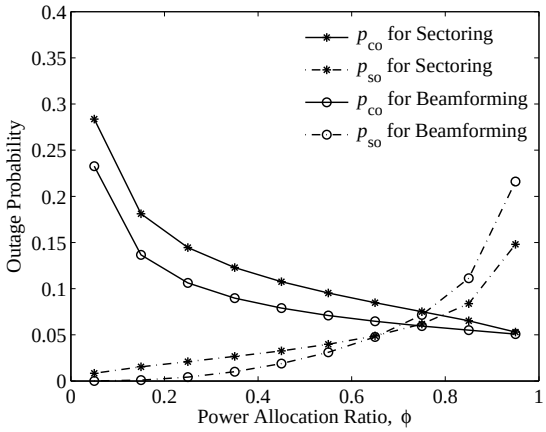


Fig. 4. The outage probabilities of the sectoring and beamforming schemes in (5), (11), (18) and (28) versus the power allocation ratio. Results are shown for the case where $\lambda_l = 0.01$, $\lambda_e = 0.001$, $r = 1$, $\alpha = 4$, $N = 4$, $\beta_b = 10$ and $\beta_e = 1$.

where

$$p_{\rm so}^{\rm UB} = 1 - \exp\left[-\frac{\lambda_e}{\lambda_l}\frac{\pi\left(\beta_e\frac{\phi^{-1}-1}{N-1}+1\right)^{1-N}}{C_{\alpha,N}\left(\beta_e\frac{\phi^{-1}-1}{N-1}\right)^{\frac{2}{\alpha}}}\right] \tag{28}$$

and

$$p_{\rm so}^{\rm LB} = \left(\beta_e\frac{\phi^{-1}-1}{N-1}+1\right)^{1-N}\frac{\pi\lambda_e}{\pi\lambda_e+\lambda_l C_{\alpha,N}\left(\beta_e\frac{\phi^{-1}-1}{N-1}\right)^{\frac{2}{\alpha}}} \tag{29}$$

with $C_{\alpha,N}$ defined in (6).

Proof: See Appendix F. ∎

In the low outage region (i.e., as $p_{\rm so} \to 0$), the upper bound in (28) and the lower bound in (29) share the same leading order term:

$$p_{\rm so}^{\rm UB} \approx p_{\rm so}^{\rm Lead} := \frac{\lambda_e}{\lambda_l}\frac{\pi\left(\beta_e\frac{\phi^{-1}-1}{N-1}+1\right)^{1-N}}{C_{\alpha,N}\left(\beta_e\frac{\phi^{-1}-1}{N-1}\right)^{\frac{2}{\alpha}}} \approx p_{\rm so}^{\rm LB} \tag{30}$$

implying that these two bounds both capture the leading order behavior of the secrecy outage probability as it becomes small. The leading order term $p_{\rm so}^{\rm Lead}$ can serve as an accurate approximation for the secrecy outage probability in the low outage region. As shown in Fig. 3, the upper bound in (28) gives a very accurate approximation for the entire range of the secrecy outage probabilities shown, while the lower bound in (29) gets asymptotically accurate as the secrecy outage probability becomes small.

We point out that with the p.d.f. provided in Lemma 1, following a similar procedure as that used in deriving Theorem 4, it is not difficult to study the case where the eavesdroppers do not have multi-user decodability and simply treat interference as noise. This argument also applies to the sectoring scheme. However, as we mentioned in the introduction, in order to achieve the maximum level of secrecy, assuming eavesdroppers with multi-user decodability is a more robust approach. Therefore, in this paper, we retain our focus on this case.

Connection and Secrecy Outage Tradeoff: As shown in Fig. 4, for both the sectoring and beamforming schemes, when giving more power to the information signal (i.e., increasing the power allocation ratio ϕ), the connection outage probability $p_{\rm co}$ decreases whilst the secrecy outage probability $p_{\rm so}$ increases. Hence, there is a tradeoff between the connection and secrecy outage performance w.r.t. the transmit power allocation.

V. Secrecy Throughput Performance

In this section, based on the outage probability expressions obtained in the last two sections, we investigate the network-wide secrecy throughput performance for the sectoring and beamforming schemes, in terms of the secrecy transmission capacity [13].

The secrecy transmission capacity is defined as the achievable rate of successful transmission of confidential messages per unit area with constraints on both the connection and secrecy outage probabilities. With outage constraints $p_{\rm co} = \sigma$ and $p_{\rm so} = \epsilon$, the corresponding secrecy transmission capacity is given by

$$\begin{aligned} C &= (1-\sigma)\,\lambda_l R_s \\ &= (1-\sigma)\,\lambda_l\,[R_b - R_e]^+ \end{aligned} \tag{31}$$

where $[x]^+ = \max\{0, x\}$. Note that the message rate R_s is a function of σ and ϵ, since $R_b = \log_2(1+\beta_b)$ is determined by the connection outage constraint σ, while $R_e = \log_2(1+\beta_e)$ is determined by the secrecy outage constraint ϵ. Whenever $R_b - R_e$ is negative, the required secrecy and connection outage performance cannot be guaranteed simultaneously, and the message transmission should be suspended. More discussions on the relationship between the transmission rates and the outage events can be found in Section II-C.

A. Sectoring Scheme

Here we characterize the secrecy transmission capacity of the sectoring scheme in the following proposition:

Proposition 1. For the sectoring scheme, a tight lower bound to the secrecy transmission capacity in (31) can be given by

$$C_{\text{Sector}}^{\text{LB}} = (1-\sigma)\lambda_l \times \left[\log_2\left(\frac{1+\left(\frac{\frac{N}{\lambda_l C_{\alpha,2}\, r^2}\ln\left(\frac{1}{1-\sigma}\right)}{1+(N-1)^{1-\frac{2}{\alpha}}(\phi^{-1}-1)^{\frac{2}{\alpha}}}\right)^{\frac{\alpha}{2}}}{1+\left(\frac{\frac{\pi}{C_{\alpha,2}}\frac{\lambda_e}{\lambda_l}}{\ln\left(\frac{1}{1-\epsilon}\right)(N-1)^{1-\frac{2}{\alpha}}(\phi^{-1}-1)^{\frac{2}{\alpha}}}\right)^{\frac{\alpha}{2}}}\right)\right]^{+} \tag{32}$$

with $C_{\alpha,2}$ defined in (6).

Proof: From (5) and (11), we solve $p_{\text{co}} = \sigma$ and $p_{\text{so}}^{\text{UB}} = \epsilon$ w.r.t. $R_b = \log_2(1+\beta_b)$ and $R_e^{\text{UB}} = \log_2(1+\beta_e)$, respectively. Then, plugging the obtained R_b and R_e^{UB} into (31), we have the lower bound in (32). ∎

Note that (32) is derived based on the secrecy outage probability upper bound in (11). Since (11) tracks the exact secrecy outage probability very closely, the lower bound in (32) provides a tight approximation to the actual secrecy transmission capacity. From (32), we observe that the secrecy transmission capacity increases logarithmically as the number of transmit antennas grows large. The underlying reason is that under the outage constraints, as the number of transmit antennas grows large, the supported codeword rate R_b increases logarithmically, while the required rate redundancy R_e diminishes.

By properly adjusting the power allocation ratio ϕ, we can maximize the secrecy transmission capacity. Though a general expression for the optimal ϕ seems not available, we still have the following corollary:

Corollary 2. The optimal power allocation ratio ϕ^* of the sectoring scheme, which maximizes the tight secrecy transmission capacity lower bound $C_{\text{Sector}}^{\text{LB}}$ in (32), is unique and can be found by numerically solving for the root of the first-order derivative of $C_{\text{Sector}}^{\text{LB}}$ w.r.t. ϕ. This is true even if the objective function is generally non-concave.

Proof: See Appendix G. ∎

For the case where $\alpha = 4$, setting the derivative of $C_{\text{Sector}}^{\text{LB}}$ in (32) w.r.t. ϕ to zero gives a cubic equation and solving it provides a closed-form expression for ϕ^*. Define:

$$\varrho = \frac{N}{\lambda_l C_{\alpha,2}\, r^2}\ln\left(\frac{1}{1-\sigma}\right),\ \varsigma = \frac{1}{\ln\left(\frac{1}{1-\epsilon}\right)}\frac{\pi}{C_{\alpha,2}}\frac{\lambda_e}{\lambda_l} \tag{33}$$

$$\kappa = \varrho^2+\varsigma^2+\left(\varrho^2-\varsigma^2+\sqrt{\left((\varrho-\varsigma)^2+1\right)\left((\varrho+\varsigma)^2+1\right)}\right)\left(\varrho^2-\varsigma^2\right).$$

Then, the optimal power allocation ratio for $\alpha = 4$ is

$$\phi_{\text{Sector}}^{\alpha=4} = \left(1+\frac{\varsigma^{\frac{2}{3}}\left(2^{\frac{2}{3}}\varrho^{\frac{4}{3}}\varsigma^{\frac{1}{3}}\kappa^{\frac{2}{3}}+2^{\frac{4}{3}}\varrho^2\varsigma+2\varrho^{\frac{2}{3}}\varsigma^{\frac{5}{3}}\kappa^{\frac{1}{3}}\right)^2}{4(N-1)\varrho^{\frac{4}{3}}\kappa^{\frac{2}{3}}\left(\varrho^2-\varsigma^2\right)^2}\right)^{-1}. \tag{34}$$

We observe that as $N \to \infty$, $\phi_{\text{Sector}}^{\alpha=4} = 1-\mathcal{O}\left(N^{-1}\right)$. In other words, the optimal power allocation ratio increases towards one as the number of transmit antennas grows large. This observation can be explained by noting that adding extra transmit antennas allows the transmitter to concentrate more on the transmission towards the intended receiver, while less and less eavesdroppers may cause secrecy outage. Hence, more transmit power can be given to the information signal to achieve a better throughput performance, while still satisfying the connection and secrecy outage constraints. As can be seen from Fig. 5, the observations made from the case where $\alpha = 4$ holds more generally for $3 \le \alpha \le 5$. The numerical results in Fig. 6 indicate that with optimized power allocation, the secrecy transmission capacity increases logarithmically as the number of transmit antennas grows large, which agrees with our earlier observation made from (32).

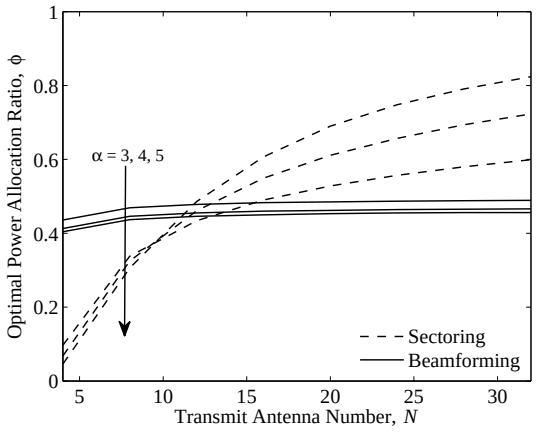


Fig. 5. The optimal power allocation ratio of the sectoring and beamforming schemes versus the number of transmit antennas. Results are shown for the case where $\lambda_l = 0.01$, $\lambda_e = 0.001$, $r = 1$, $\sigma = 0.1$ and $\epsilon = 0.01$.

B. Beamforming Scheme

Now we study the secrecy transmission capacity of the beamforming scheme. Generally speaking, the secrecy transmission capacity can be computed by solving $p_{\text{co}} = \sigma$ w.r.t. $R_b = \log_2(1+\beta_b)$ from (18) and solving $p_{\text{so}} = \epsilon$ w.r.t. $R_e = \log_2(1+\beta_e)$ from (26), and then plugging the obtained results into (31). However, the equation $p_{\text{co}} = \sigma$ seems not analytically solvable due to the existence of multiple summations. Note that the typical value of the connection outage constraint σ is expected to be small (e.g., below 0.1). This allows us to use the low outage approximation provided in (21). Letting $\tilde{p}_{\text{co}} = \sigma$, recalling that $R_b = \log_2(1+\beta_b)$, the supported codeword rate R_b can be approximated by

$$\tilde{R}_b = \log_2\left[1+\left(\frac{\sigma}{\psi(\phi)\, K_{\alpha,N}}\right)^{\frac{\alpha}{2}}\right] \tag{35}$$

where $\psi(\phi)$ and $K_{\alpha,N}$ are defined in (19) and (22), respectively.

Then, we need to solve $p_{\text{so}} = \epsilon$ w.r.t. $R_e = \log_2(1+\beta_e)$. Note that the secrecy outage constraint ϵ is also expected to be small (e.g., below 0.1), this allows us to use the leading-order low outage approximation of the secrecy outage probability in (30). In the special case of $\alpha = 4$ and $N = 2$, by solving $p_{\text{so}}^{\text{Lead}} = \epsilon$, which turns to be a cubic equation, an approximation to the required rate redundancy R_e can be

obtained as follows:

$$\tilde{R}_e=\log_2\left[1+\frac{\phi}{1-\phi}\left(\frac{\left(\frac{108\pi\lambda_e}{\epsilon\lambda_l C_{\alpha,2}}+12\sqrt{\left(\frac{9\pi\lambda_e}{\epsilon\lambda_l C_{\alpha,2}}\right)^2+12}\right)^{\frac{2}{3}}-12}{6\sqrt[3]{\frac{108\pi\lambda_e}{\epsilon\lambda_l C_{\alpha,2}}+12\sqrt{\left(\frac{9\pi\lambda_e}{\epsilon\lambda_l C_{\alpha,2}}\right)^2+12}}}\right)^2\right] \quad (36)$$

where $C_{\alpha,2}$ is defined in (6). Plugging (35) and (36) into (31), we have a closed-form approximation for the secrecy transmission capacity of the beamforming scheme when $\alpha = 4$ and $N = 2$:

$$C_{\text{Beam}}^{\text{Approx}} = (1-\sigma)\,\lambda_l \left[\tilde{R}_b - \tilde{R}_e\right]^+ . \quad (37)$$

Unfortunately, it seems that we cannot extend the analytical results to the case where $N \geq 3$, due to the fact that there is not a general algebraic solution for the quintic (i.e., fifth order) equation and above (see Abel's impossibility theorem in [37], an alternative proof to it written in English can be found in [38]). Hence, for these cases, we study the secrecy transmission capacity numerically. From (30), by solving $p_{\text{so}}^{\text{Lead}} = \epsilon$ w.r.t. $R_e = \log_2(1+\beta_e)$, an approximation to the required rate redundancy can be obtained and we denote it as $\tilde{R}_e$. Then, plugging $\tilde{R}_b$ in (35) and $\tilde{R}_e$ into (31), we have an approximation for the secrecy transmission capacity of the beamforming scheme, which can be written as (37). Note that this approximation is very accurate for small outage constraints (i.e., σ and ϵ), since the outage probability approximations in (21) and (30) are both very accurate in the low outage region. We then numerically optimize the power allocation to maximize the secrecy transmission capacity.

As illustrated in Fig. 5, as the number of transmit antennas N grows large, the optimal power allocation ratio that maximizes the secrecy transmission capacity of the beamforming scheme converges to a certain value, which is strictly less than one. Here we explain why the optimal power allocation ratio does not increase to one. Note that the density of the eavesdroppers which may cause secrecy outage does not change with increasing N. More importantly, as N increases, the power of the emitted artificial noise decreases, and the increments of the artificial interference brought by adding extra transmit antennas will be neutralized. In such cases, giving too much power to the information signal will break the secrecy outage constraint and thus the optimal power allocation ratio will not increase to one. As demonstrated in Fig. 6, with optimized transmit power allocation, as N grows large, the maximum secrecy transmission capacity of the beamforming scheme increases logarithmically, which is similar to the sectoring scheme.

C. Sectoring versus Beamforming

Here we compare the sectoring and beamforming schemes, in terms of the optimal power allocation ratio that maximizes the secrecy transmission capacity and the corresponding maximum secrecy transmission capacity.

Regarding the optimal power allocation ratio:

- As shown in Fig. 5, as the number of transmit antennas N increases, the optimal power allocation ratio for the beamforming scheme converges to a certain value which is less than one, while that for the sectoring scheme keeps increasing towards one. This difference can be explained by noting that for the beamforming scheme, with increasing N, the equivalent density of eavesdroppers which may cause secrecy outage remains the same, while that for the sectoring scheme decreases inversely linearly. Hence, the reduced secrecy outage probability of the sectoring scheme allows the transmitters to give more transmit power to the information signal, while still satisfying the secrecy outage constraint, which is not true for the beamforming scheme.
- As shown in Fig. 5, when the path-loss becomes more severe (i.e., as α increases), the optimal power allocation ratio for the beamforming scheme decreases. More interestingly, with increasing α and N, there is twist in the optimal power allocation ratio of the sectoring scheme. The underlying reason is that with increasing N, the optimal power allocation ratio of the sectoring scheme increases faster in a high path-loss environment.

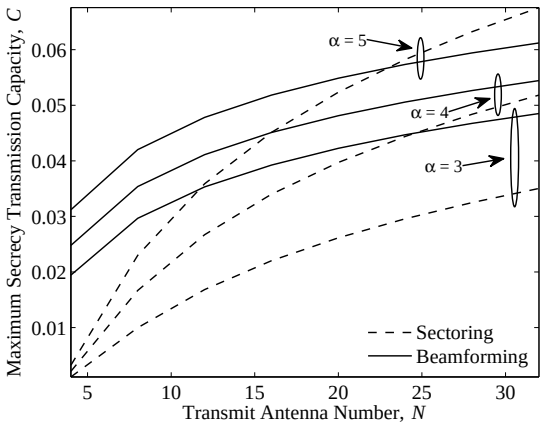


Fig. 6. The maximum secrecy transmission capacity of the sectoring and beamforming schemes versus the number of transmit antennas. Results are shown for the case where $\lambda_l = 0.01$, $\lambda_e = 0.001$, $r = 1$, $\sigma = 0.1$ and $\epsilon = 0.01$.

Regarding the maximum secrecy transmission capacity:

- As shown in Fig. 6, the beamforming scheme outperforms the sectoring scheme for a wide range of antenna numbers, in terms of achieving a larger secrecy transmission capacity. This makes sense because that having more channel knowledge at the transmitters, such that beamforming can be performed, is generally better than having directional transmit antennas, which are needed for the sectoring scheme.
- However, when N becomes sufficiently large, the sectoring scheme can achieve a larger secrecy transmission capacity, compared with the beamforming scheme. The reason behind this is that with increasing N, the transmitter of the sectoring scheme becomes quite capable of concentrating the transmission towards the intended receiver while less and less eavesdroppers may cause secrecy outage. As can be seen from Fig. 5, the corresponding optimal power allocation ratio also increases

with increasing N, giving more transmit power to the information signals to achieve a better throughput performance. In addition, the performance crossover between the sectoring and beamforming schemes happens at a larger N if the secrecy outage constraint becomes more stringent (i.e., reducing ϵ).

VI. Conclusion

In this paper, we studied physical-layer security in wireless ad hoc networks and investigated two types of multi-antenna transmission schemes. In particular, in order to jam the eavesdroppers over the entire network, we combined artificial noise with either sectoring or beamforming. For these two schemes, we provided closed-form expressions for the connection and secrecy outage probabilities and showed the tradeoff between them. We then quantified the secrecy throughput performance for both schemes in terms of the secrecy transmission capacity. Our results indicated that the proposed transmission schemes can provide significant secrecy enhancements over single-antenna methods. Our analysis also shed light on the behavior of the optimal power allocation between the information signal and the artificial noise for achieving the maximum secrecy throughput.

Appendix

A. Proof of Theorem 1

Here we derive the connection outage probability in (5). By (2), the total interference seen by the typical receiver at the origin is $I_I + I_A$. Since I_I and I_A are two independent shot noise processes, by [31, eq. (8)], the Laplace transform of the p.d.f. of $I_I + I_A$ is given by

$$\mathcal{L}_{I_I+I_A}(s)=\exp\left(-\frac{\lambda_l C_{\alpha,2} G_N^{\frac{2}{\alpha}}}{N}\left(P_I^{\frac{2}{\alpha}}+(N-1)^{1-\frac{2}{\alpha}}P_A^{\frac{2}{\alpha}}\right)s^{\frac{2}{\alpha}}\right) \quad (38)$$

where $C_{\alpha,2}$ is defined in (6).

By (3) and (4), we have

$$\begin{aligned} p_{\rm co} &= 1-\Pr\left(S_o \geq \frac{\beta_b r^\alpha}{G_N P_I}\left(I_I+I_A\right)\right) \\ &= 1-\int_0^\infty \exp\left(-\frac{\beta_b r^\alpha}{G_N P_I} z\right) f_{I_I+I_A}(z)\,\mathrm{d}z \\ &= 1-\mathcal{L}_{I_I+I_A}\left(\frac{\beta_b r^\alpha}{G_N P_I}\right) \end{aligned} \quad (39)$$

where $f_{I_I+I_A}(\cdot)$ is the p.d.f. of I_I+I_A and the last line comes from the definition of the Laplace transform. Then, plugging in the Laplace transform in (38) leads to the results in (5).

B. Proof of Theorem 2

We first derive the secrecy outage probability upper bound in (11). By [31, eq. (8)], the Laplace transform of the p.d.f. of the aggregate artificial noise I_A in (7) is given by

$$\mathcal{L}_{I_A}(s)=\exp\left(-\frac{\lambda_l C_{\alpha,2} G_N^{\frac{2}{\alpha}}}{N}(N-1)^{1-\frac{2}{\alpha}}P_A^{\frac{2}{\alpha}}s^{\frac{2}{\alpha}}\right) \quad (40)$$

where $C_{\alpha,2}$ is defined in (6).

By applying the probability generating functional of a PPP (see Definition A.5 in [36]) to the inner expectation of (9), we have

$$p_{\rm so}=1-\mathbb{E}_{\Phi_A}\left\{\exp\left(-\frac{\lambda_e}{N}\int_{\mathbb{R}^2}\Pr(\mathrm{SIR}_z>\beta_e|\Phi_A)\mathrm{d}z\right)\right\}. \quad (41)$$

Invoking the bounding technique used in [13, 39] (i.e., applying Jensen's inequality), we get the following upper bound:

$$\begin{aligned} p_{\rm so} \leq p_{\rm so}^{\rm UB} &:= 1-\exp\left(-\frac{\lambda_e}{N}\int_{\mathbb{R}^2}\Pr\left(\mathrm{SIR}_z>\beta_e\right)\mathrm{d}z\right) \\ &= 1-\exp\left(-\frac{\lambda_e}{N}\int_{\mathbb{R}^2}\mathcal{L}_{I_A}\left(\frac{\beta_e D_{oz}^\alpha}{G_N P_I}\right)\mathrm{d}z\right). \end{aligned} \quad (42)$$

Plugging in (40) and changing to a polar coordinate system to evaluate the integral yields the results in (11).

By considering the nearest eavesdropper only, we now derive the secrecy outage probability lower bound in (12). Denote the location of the nearest eavesdropper by n. By [40, eq. (2)], the distance between the typical transmitter and the nearest eavesdropper in Φ_Z, denoted by D_{on}, is distributed according to the following p.d.f.:

$$f_{D_{on}}(z)=\frac{2\pi\lambda_e}{N}z\,\mathrm{e}^{-\frac{\pi\lambda_e}{N}z^2},\ z>0. \quad (43)$$

The received SIR at this eavesdropper is given by

$$\mathrm{SIR}_n = G_N P_I S_{on} D_{on}^{-\alpha} I_A^{-1} \quad (44)$$

where $S_{on} \sim \mathrm{Exp}(1)$, I_A is the aggregate artificial noise, defined in (7).

By (44), the secrecy outage probability in (9) can be lower bounded by

$$\begin{aligned} p_{\rm so} \geq p_{\rm so}^{\rm LB} &:= \Pr\left(\mathrm{SIR}_n>\beta_e\right) \\ &= \mathbb{E}_{D_{on},I_A}\left[\exp\left(-\frac{\beta_e D_{on}^\alpha}{G_N P_I}I_A\right)\right] \\ &= \mathbb{E}_{D_{on}}\left[\mathcal{L}_{I_A}\left(\frac{\beta_e D_{on}^\alpha}{G_N P_I}\right)\right]. \end{aligned} \quad (45)$$

Using (40) and (43) to evaluate the last expectation yields the results in (12).

C. Proof of Lemma 1

Here we derive the interference distribution in (14). For a given realization of the intended channel $\mathbf{h}$ and with the beamforming strategy in (1), the covariance matrix of the transmitted signal vector $\mathbf{x}$ is

$$\mathbf{C_x} = P_I\frac{\mathbf{h}\mathbf{h}^H}{\|\mathbf{h}\|^2}+\frac{P_A}{N-1}\mathbf{W}\mathbf{W}^H. \quad (46)$$

Noting that $\mathbf{W}\mathbf{W}^H = \mathbf{I}-\frac{\mathbf{h}\mathbf{h}^H}{\|\mathbf{h}\|^2}$, we can rewrite the covariance matrix as

$$\mathbf{C_x} = \frac{P_A}{N-1}\mathbf{I}+\left(P_I-\frac{P_A}{N-1}\right)\frac{\mathbf{h}\mathbf{h}^H}{\|\mathbf{h}\|^2}. \quad (47)$$

If this signal $\mathbf{x}$ is received by a non-intended receiver through an unknown channel $\mathbf{h}_z$, the corresponding interference power is given by

$$P_x = \frac{P_A}{N-1}\|\mathbf{h}_z\|^2+\left(P_I-\frac{P_A}{N-1}\right)\left|\mathbf{h}_z^H\frac{\mathbf{h}}{\|\mathbf{h}\|}\right|^2. \quad (48)$$

For a given $\mathbf{h} \neq \mathbf{0}$ and with a random $\mathbf{h}_z$, the interference power P_x can be interpreted as the weighted sum of the squared magnitude of $\mathbf{h}_z$ and the squared magnitude of the projection of $\mathbf{h}_z$ on the direction of $\mathbf{h}$. Hence, the amplitude of $\mathbf{h}$ is irrelevant and only its direction matters; more importantly, with the ergodicity of $\mathbf{h}_z$ over the symmetric complex space, the statistical distribution of P_x becomes independent of the direction of $\mathbf{h}$. For this reason, we set $\mathbf{h} = [1, 0, \ldots, 0]^T$ to characterize the distribution of P_x. Denote the elements of $\mathbf{h}_z$ as h_{zi} with $i = 1, \ldots, N$. The interference power P_x can be expressed as

$$P_x = P_I \left|h_{z1}\right|^2 + \frac{P_A}{N-1} \sum_{i=2}^{N} \left|h_{zi}\right|^2 \ . \tag{49}$$

We first consider the case where $P_I \neq \frac{P_A}{N-1}$ (i.e., $\phi \neq \frac{1}{N}$). Note that $P_I \left|h_{z1}\right|^2 \sim \mathrm{Exp}\left(\frac{1}{P_I}\right)$ and $\frac{P_A}{N-1} \sum_{i=2}^{N} \left|h_{zi}\right|^2 \sim \mathrm{Gamma}\left(N-1, \frac{P_A}{N-1}\right)$ are mutually independent. The p.d.f. of P_x can be computed as

$$\begin{aligned} f_{P_x}(z) = &\frac{1}{P_I}\left(1 - \frac{P_A}{(N-1)P_I}\right)^{1-N} \mathrm{e}^{-\frac{z}{P_I}} \\ &\times \gamma\left(N-1, \left(\frac{N-1}{P_A} - \frac{1}{P_I}\right) z\right) \ , \ z > 0 \end{aligned} \tag{50}$$

where $\gamma(\cdot,\cdot)$ is the regularized lower incomplete gamma function. Plugging in the series representation of $\gamma(\cdot,\cdot)$ yields the results in (14). Note that the expression above does not hold for $P_I = \frac{P_A}{N-1}$ (i.e., $\phi = \frac{1}{N}$). From (49), it is clear that when $\phi = \frac{1}{N}$, $P_x \sim \mathrm{Gamma}(N, P_I)$.

D. Proof of Theorem 3

Here we derive the connection outage probability in (18). By [31, eq. (8)], the Laplace transform of the p.d.f. of the aggregate interference I_{IA} in (15) is given by

$$\mathcal{L}_{I_{IA}}(s) = \exp\left(-\lambda_l \pi \mathbb{E}\left[P_x^{\frac{2}{\alpha}}\right] \Gamma\left(1 - \frac{2}{\alpha}\right) s^{\frac{2}{\alpha}}\right) \ . \tag{51}$$

If $P_I \neq \frac{P_A}{N-1}$ (i.e., $\phi \neq \frac{1}{N}$), by (14), $\mathbb{E}\left[P_x^{\frac{2}{\alpha}}\right]$ is given in (52); and if $P_I = \frac{P_A}{N-1}$ (i.e., $\phi = \frac{1}{N}$), we have

$$\mathbb{E}\left[P_x^{\frac{2}{\alpha}}\right] = P_I^{\frac{2}{\alpha}} \frac{\Gamma\left(N + \frac{2}{\alpha}\right)}{\Gamma(N)} \ . \tag{53}$$

In (16), $\|\mathbf{h}_o\|^2 \sim \mathrm{Gamma}(N, 1)$ and its complementary cumulative distribution function takes the form in [41, eq. (9)], with $\mathcal{N} = \{1\}$, $\mathcal{K} = \{1, \ldots, N-1\}$ and $a_{nk} = \frac{1}{k!}$. Hence, with the Laplace transformation obtained in (51), we can invoke [41, Theorem 1] to characterize the connection outage probability as follows:

$$p_{\mathrm{co}} = 1 - \sum_{p=0}^{N-1} \left[\frac{(-s)^p}{p!} \frac{\mathrm{d}^p}{\mathrm{d}s^p} \mathcal{L}_{I_{IA}}(s)\right]_{s=\frac{\beta_b r^\alpha}{P_I}} \ . \tag{54}$$

By convention, the zero-th order derivative denotes the function itself. Plugging (51) into (54), we have the results in (18).

E. Proof of Corollary 1

Here we derive a low outage approximation for the connection outage probability in (18). From (18) and (19), it is clear that when $\psi(\phi) \to 0$, the connection outage probability $p_{\mathrm{co}} \to 0$. Note that the quantity $\psi(\phi)$ couples many system parameters like r and λ_l, and more importantly, ϕ and N. By making $\psi(\phi)$ small, we are effectively studying all cases of system parameters that may lead to a small p_{co}, including but not limited to the asymptotic regions where $r \to 0$ or $\lambda_l \to 0$. We expand (18) around $\psi(\phi) = 0$ as follows:

$$\begin{aligned} p_{\mathrm{co}} &= \beta_b^{\frac{2}{\alpha}} \psi(\phi) - \mathrm{e}^{-\beta_b^{\frac{2}{\alpha}} \psi(\phi)} \beta_b^{\frac{2}{\alpha}} \psi(\phi) \frac{2}{\alpha} \sum_{p=1}^{N-1} \frac{1}{p!} \zeta(p, 1) + \mathcal{O}\left(\psi(\phi)^2\right) \\ &= \beta_b^{\frac{2}{\alpha}} \psi(\phi) - \beta_b^{\frac{2}{\alpha}} \psi(\phi) \frac{2}{\alpha} \sum_{p=1}^{N-1} \frac{1}{p!} \prod_{l=1}^{p-1} \left(l - \frac{2}{\alpha}\right) + \mathcal{O}\left(\psi(\phi)^2\right) \end{aligned} \tag{55}$$

where $\zeta(\cdot,\cdot)$ is defined in (20). Ignoring the high order terms gives the results in (21).

F. Proof of Theorem 4

We first derive the secrecy outage probability upper bound in (28). By [31, eq. (8)], the Laplace transform of the p.d.f. of the aggregate artificial noise I_A in (23) is given by

$$\mathcal{L}_{I_A}(s) = \exp\left(-\lambda_l C_{\alpha,N} \left(\frac{P_A}{N-1}\right)^{\frac{2}{\alpha}} s^{\frac{2}{\alpha}}\right) \tag{56}$$

where $C_{\alpha,N}$ was defined in (6).

Using the generating functional of a PPP (see Definition A.5 in [36]), by (26), we have

$$\begin{aligned} p_{\mathrm{so}} &= 1 - \mathbb{E}_{\Phi_L}\left\{\exp\left[-\lambda_e \int_{\mathbb{R}^2} \Pr\left(\mathrm{SIR}_z > \beta_e | \Phi_L\right) \mathrm{d}z\right]\right\} \\ &\leq 1 - \exp\left[-\lambda_e \int_{\mathbb{R}^2} \Pr\left(\mathrm{SIR}_z > \beta_e\right) \mathrm{d}z\right] \end{aligned} \tag{57}$$

where the second line is obtained by applying Jensen's inequality. By (25), the probability inside the integral can be evaluated as

$$\begin{aligned} &\Pr\left(\mathrm{SIR}_z > \beta_e\right) \\ &= \mathbb{E}_{\|\mathbf{g}_{oz}\|^2, I_A}\left\{\exp\left(-\frac{\beta_e D_{oz}^\alpha}{P_I}\left(\frac{P_A}{N-1}\|\mathbf{g}_{oz}\|^2 D_{oz}^{-\alpha} + I_A\right)\right)\right\} \\ &= \left(\beta_e \frac{\phi^{-1} - 1}{N-1} + 1\right)^{1-N} \mathcal{L}_{I_A}\left(\frac{\beta_e D_{oz}^\alpha}{P_I}\right) \\ &= \left(\beta_e \frac{\phi^{-1} - 1}{N-1} + 1\right)^{1-N} \exp\left(-\beta_e^{\frac{2}{\alpha}} D_{oz}^2 \lambda_l C_{\alpha,N} \left(\frac{\phi^{-1} - 1}{N-1}\right)^{\frac{2}{\alpha}}\right) . \end{aligned} \tag{58}$$

Plugging (58) into (57), after changing to a polar coordinate system, evaluating the integral gives the results in (28).

By considering the nearest eavesdropper only, we now derive the secrecy outage probability lower bound in (29). Denote the location of the nearest eavesdropper by n. By [40, eq. (2)], the distance between the typical transmitter and the nearest eavesdropper in Φ_E, denoted by D_{on}, is distributed according to the following p.d.f.:

$$f_{D_{on}}(z) = 2\pi\lambda_e z \, \mathrm{e}^{-\pi\lambda_e z^2} \ , \ z > 0 \ . \tag{59}$$

The received SIR at this eavesdropper is given by

$$\mathrm{SIR}_n = \frac{P_I S_{on} D_{on}^{-\alpha}}{\frac{P_A}{N-1}\|\mathbf{g}_{on}\|^2 D_{on}^{-\alpha} + I_A} \tag{60}$$

$$\mathbb{E}\left[P_x^{\frac{2}{\alpha}}\right]=\frac{1}{P_I}\left(1-\frac{P_A}{(N-1)\,P_I}\right)^{1-N}\left(P_I^{1+\frac{2}{\alpha}}\Gamma\left(1+\frac{2}{\alpha}\right)-\left(\frac{P_A}{N-1}\right)^{1+\frac{2}{\alpha}}\sum_{k=0}^{N-2}\left(1-\frac{P_A}{(N-1)\,P_I}\right)^{k}\frac{\Gamma\left(k+1+\frac{2}{\alpha}\right)}{\Gamma\left(k+1\right)}\right) \quad (52)$$

where $S_{on}\sim\mathrm{Exp}\left(1\right)$, $\|\mathbf{g}_{on}\|^2\sim\mathrm{Gamma}\left(N-1,1\right)$ and I_A is the aggregate artificial noise, defined in (23).

Then, the secrecy outage probability in (26) can be lower bounded by

$$\begin{aligned}p_{\mathrm{so}}&\geq p_{\mathrm{so}}^{\mathrm{LB}}\\&:=\mathbb{E}_{D_{on},I_A,\|\mathbf{g}_{on}\|^2}\left[\Pr\left(\mathrm{SIR}_n>\beta_e|D_{on},I_A,\|\mathbf{g}_{on}\|^2\right)\right]\\&=\left(\beta_e\frac{\phi^{-1}-1}{N-1}+1\right)^{1-N}\mathbb{E}_{D_{on},I_A}\left[\exp\left(-\frac{D_{on}^{\alpha}\beta_e}{P_I}I_A\right)\right]\\&=\left(\beta_e\frac{\phi^{-1}-1}{N-1}+1\right)^{1-N}\mathbb{E}_{D_{on}}\left[\mathcal{L}_{I_A}\left(\frac{D_{on}^{\alpha}\beta_e}{P_I}\right)\right]\ . \quad (61)\end{aligned}$$

Plugging in (56) and (59) to evaluate the last expectation leads to the results in (29).

G. Proof of Corollary 2

Here we show that the optimal power allocation ratio that maximizes the secrecy transmission capacity lower bound in (32) is unique. Define the following quantities:

$$\begin{aligned}x&:=(N-1)^{1-\frac{2}{\alpha}}\left(\phi^{-1}-1\right)^{\frac{2}{\alpha}}\\\delta&:=\frac{\alpha}{2}\ .\end{aligned} \quad (62)$$

With the notation defined in (33), the lower bound in (32) can be expressed as

$$C_{\mathrm{Sector}}^{\mathrm{LB}}=(1-\sigma)\lambda_l\left[\log_2\left(\frac{1+\left(\frac{\varrho}{1+x}\right)^{\delta}}{1+\left(\frac{\varsigma}{x}\right)^{\delta}}\right)\right]^{+}\ . \quad (63)$$

We assume that $\varrho>\varsigma$, such that a positive $C_{\mathrm{Sector}}^{\mathrm{LB}}$ can be achieved by choosing x from $\left(\frac{\varsigma}{\varrho-\varsigma},\infty\right)$. More discussions on the feasibility of a positive $C_{\mathrm{Sector}}^{\mathrm{LB}}$ can be found in [42]. Then, by the monotonicity of the logarithm function, maximizing $C_{\mathrm{Sector}}^{\mathrm{LB}}$ is equivalent to maximizing the following function:

$$f\left(x\right)=\left(1+\left(\frac{\varrho}{1+x}\right)^{\delta}\right)\left(1+\left(\frac{\varsigma}{x}\right)^{\delta}\right)^{-1}\ . \quad (64)$$

The derivative of $f\left(x\right)$ w.r.t. x is given by

$$\frac{\mathrm{d}}{\mathrm{d}x}f\left(x\right)=\frac{\varsigma^{\delta}+\frac{\varrho^{\delta}\varsigma^{\delta}}{(1+x)^{\delta+1}}-\varrho^{\delta}\left(\frac{x}{1+x}\right)^{\delta+1}}{\delta^{-1}x^{\delta+1}\left(1+\left(\frac{\varsigma}{x}\right)^{\delta}\right)^{2}} \quad (65)$$

where the denominator is always positive. When increasing x from $\frac{\varsigma}{\varrho-\varsigma}$ to infinity, the first two terms in the numerator decreases from $\varsigma^{\delta}+\varrho^{-1}\varsigma^{\delta}\left(\varrho-\varsigma\right)^{\delta+1}$ to ς^{δ} and the third term increases from $\varrho^{-1}\varsigma^{\delta+1}$ to ϱ^{δ} monotonically. Since $\varrho>\varsigma$, the derivative of $f\left(x\right)$ is first positive and then negative on $x\in\left(\frac{\varsigma}{\varrho-\varsigma},\infty\right)$. When increasing ϕ from zero to one, the value of x decreases from infinity to zero monotonically. This implies that the derivative of $C_{\mathrm{Sector}}^{\mathrm{LB}}$ w.r.t. ϕ is first positive and then negative with increasing ϕ, and thus the optimal value of ϕ is unique.

REFERENCES

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

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

[3] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge Univ. Pr., 2011.

[4] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, Canada, Jul. 2008, pp. 524–528.

[5] H. Wang, L. Lightfoot, and T. Li, "On PHY-layer security of cognitive radio: Collaborative sensing under malicious attacks," in *Proc. Annu. Conf. Inf. Sci. Syst.*, Princeton, America, Mar. 2010, pp. 1–6.

[6] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[7] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, Oct. 2012.

[8] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 82–91, Jan. 2013.

[9] S. Luo, J. Li, and A. P. Petropulu, "Uncoordinated cooperative jamming for secret communications," *IEEE Trans. Inf. Foren. Sec.*, vol. 8, no. 7, pp. 1081–1090, Jul. 2013.

[10] Y. Liang, H. V. Poor, and L. Ying, "Secrecy throughput of MANETs with malicious nodes," in *Proc. IEEE Int. Symp. Inf. Theory*, Seoul, Korea, Jun. 2009, pp. 1189–1193.

[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] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks – Part I: Connectivity," *IEEE Trans. Inf. Foren. Sec.*, vol. 7, no. 1, pp. 125–138, Feb. 2012.

[13] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.

[14] J. Lee, H. Shin, and M. Z. Win, "Secure node packing of large-scale wireless networks," in *Proc. IEEE Int. Conf. Commun.*, Ottawa, Canada, Jun. 2012, pp. 815–819.

[15] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," in *Proc. Inf. Theory Applicat. Workshop*, La Jolla, America, Feb. 2010, pp. 1–4.

[16] S. Vasudevan, D. Goeckel, and D. Towsley, "Security-capacity trade-off in large wireless networks using keyless secrecy," in *Proc. ACM Int. Symp. Mobile Ad Hoc Network. Comput.*, Chicago, America, 2010, pp. 21–30.

[17] X. Zhou, M. Tao, and R. A. Kennedy, "Cooperative jamming for secrecy in decentralized wireless networks," in *Proc. IEEE Int. Conf. Commun.*, Ottawa, Canada, Jun. 2012.

[18] W. Shi and J. A. Ritcey, "Distributed jamming for secure communication in Poisson fields of legitimate nodes and eavesdroppers," in *Proc. Asilomar Conf. Signals, Syst., Comput.*, Pacific Grove, America, Nov. 2012, pp. 1881–1885.

[19] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[20] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *IEEE Int. Conf. Acoust., Speech Signal Process.*, Taipei, China, Apr. 2009, pp. 2437–2440.

[21] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[22] X. He and A. Yener, "Cooperative jamming: The tale of friendly interference for secrecy," in *Securing Wireless Communications at the Physical Layer*. Springer, 2010, pp. 65–88.

[23] 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.

[24] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[25] X. Zhang, X. Zhou, and M. R. McKay, "Benefits of multiple transmit antennas in secure communication: A secrecy outage viewpoint," in *Proc. Asilomar Conf. Signals, Syst., Comput.*, Pacific Grove, America, Nov. 2011, pp. 212–216.

[26] S. C. Lin, T. H. Chang, Y. L. Liang, Y. W. P. Hong, and C. Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 901–915, Mar. 2011.

[27] Q. Li, W. K. Ma, and A. M. C. So, "Safe convex approximation to outage-based MISO secrecy rate optimization under imperfect CSI and with artificial noise," in *Proc. Asilomar Conf. Signals Syst. Comput.*, Pacific Grove, America, Nov. 2011, pp. 207–211.

[28] 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.

[29] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Foren. Sec.*, vol. 7, no. 2, pp. 704–716, Apr. 2012.

[30] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.

[31] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE J. Select. Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, Sep. 2009.

[32] B. Błaszczyszyn and P. Mühlethaler, "Stochastic analysis of non-slotted Aloha in wireless ad-hoc networks," in *Proc. IEEE Int. Conf. Comput. Commun.*, San Diego, America, Mar. 2010, pp. 1–9.

[33] R. Ramanathan, J. Redi, C. Santivanez, D. Wiggins, and S. Polit, "Ad hoc networking with directional antennas: A complete system solution," *IEEE J. Select. Areas Commun.*, vol. 23, no. 3, pp. 496–506, Mar. 2005.

[34] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[35] 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, no. 3, pp. 302–304, Mar. 2011.

[36] M. Haenggi and R. K. Ganti, *Interference in Large Wireless Networks*. Now Publishers Inc., 2009.

[37] N. H. Abel, "Beweis der unmöglichkeit, algebraische gleichungen von höheren graden als dem vierten allgemein aufzulösen," *Journal für die reine und angewandte Mathematik*, vol. 1, pp. 65–84, 1826.

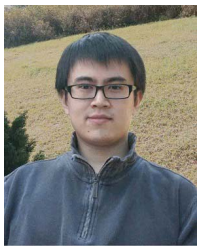
[38] H. Żołądek, "The topological proof of Abel–Ruffini theorem," *J. Juliusz Schauder Center*, vol. 16, pp. 253–265, 2000.

[39] R. K. Ganti and M. Haenggi, "Single-hop connectivity in interference-limited hybrid wireless networks," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 2007, pp. 366–370.

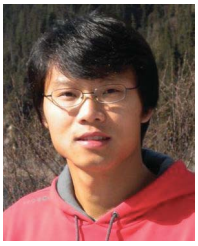
[40] M. Haenggi, "On distances in uniformly random networks," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3584–3586, 2005.

[41] A. M. Hunter, J. Andrews, and S. Weber, "Transmission capacity of ad hoc networks with spatial diversity," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 5058–5071, Dec. 2008.

[42] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing secrecy with sectorized transmission in decentralized wireless networks," in *Proc. IEEE Int. Workshop Signal Process. Advances for Wireless Commun.*, Darmstadt, Germany, Jun. 2013, pp. 1–5.



Xi Zhang (S'11) received the B.E. degree in communication engineering from the University of Electronic Science and Technology of China in 2010. He is currently working toward the Ph.D. degree in electronic and computer engineering at the Hong Kong University of Science and Technology. His research interests are in the fields of wireless communication and signal processing techniques, including physical-layer security, ad hoc networking, and random matrix theory.



Xiangyun Zhou (S'08-M'11) is a lecturer at the Australian National University (ANU), Australia. He received the B.E. (hons.) degree in electronics and telecommunications engineering and the Ph.D. degree in telecommunications engineering from the ANU in 2007 and 2010, respectively. From June 2010 to June 2011, he worked as a postdoctoral fellow at UNIK - University Graduate Center, University of Oslo, Norway. His research interests are in the fields of communication theory and wireless networks.

Dr. Zhou serves on the editorial board of the following journals: IEEE Communications Letters, Security and Communication Networks (Wiley), and Ad Hoc & Sensor Wireless Networks. He has also served as the TPC member of major IEEE conferences. Currently, he is the Chair of the ACT Chapter of the IEEE Communications Society and Signal Processing Society. He is a recipient of the Best Paper Award at the 2011 IEEE International Conference on Communications.

Matthew R. McKay (S'03-M'07-SM'13) received the combined B.E. degree in electrical engineering and the B.IT. degree in computer science from the Queensland University of Technology, Australia, in 2002, and the Ph.D. degree in electrical engineering from the University of Sydney, Australia, in 2007. He then worked as a Research Scientist at the Commonwealth Science and Industrial Research Organization (CSIRO), Sydney, prior to joining the faculty at the Hong Kong University of Science and Technology (HKUST) in 2007, where he is currently the Hari Harilela Associate Professor of Electronic and Computer Engineering. He is also a member of the Center for Wireless Information Technology at HKUST, as well as an affiliated faculty member with the Division of Biomedical Engineering. His research interests include communications and signal processing; in particular the analysis and design of MIMO systems, random matrix theory, information theory, wireless ad-hoc and sensor networks, and physical-layer security.

Dr. McKay was awarded the University Medal upon graduating from the Queensland University of Technology. He and his coauthors have been awarded a Best Student Paper Award at IEEE ICASSP 2006, Best Student Paper Award at IEEE VTC 2006-Spring, Best Paper Award at ACM IWCMC 2010, Best Paper Award at IEEE Globecom 2010, Best Paper Award at IEEE ICC 2011, and was selected as a Finalist for the Best Student Paper Award at the Asilomar Conference on Signals, Systems, and Computers 2011. In addition, he received the 2010 Young Author Best Paper Award by the IEEE Signal Processing Society, the 2011 Stephen O. Rice Prize in the Field of Communication Theory by the IEEE Communication Society, and the 2011 Young Investigator Research Excellence Award by the School of Engineering at HKUST. Dr. McKay serves on the editorial boards of the IEEE Transactions on Wireless Communications and the mathematics journal, Random Matrices: Theory and Applications. In 2011, he served as the Chair of the Hong Kong Chapter of the IEEE Information Theory Society, whilst previously serving as the Vice-Chair and the Secretary. He has also served on the technical program committee for numerous international conferences, as well as the Publications Chair for IEEE SPAWC 2009, Publicity Chair for IEEE SPAWC 2012, and Poster Chair for IEEE CTW 2013.