Enhancing Secrecy with Sectorized Transmission in Decentralized Wireless Networks

Xi Zhang*, Xiangyun Zhou†, Matthew R. McKay*
*Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology, Hong Kong
†Research School of Engineering, Australian National University, Australia

Abstract—**In this paper, we combine sectorized transmission with artificial noise to establish secrecy in decentralized wireless networks. The locations of the legitimate nodes and the eavesdroppers are both modeled by homogeneous Poisson point processes. Using sectorized antennas, each legitimate transmitter sends an information signal in the sector which contains its intended receiver, while simultaneously emitting artificial noise in other sectors, in order to provide secrecy against the eavesdroppers. We first separately characterize the reliability performance of the legitimate link and the secrecy performance against malicious eavesdropping. Then, we derive the secrecy transmission capacity to measure the networkwide secrecy throughput. To facilitate the practical system design, we provide a sufficient condition, in terms of the system parameters and constraints, under which a positive secrecy transmission capacity is achievable. The optimal transmit power allocation between the information signal and the artificial noise for achieving the maximal secrecy transmission capacity is also investigated. Our analysis indicates that sectorized transmission provides significant secrecy enhancements in decentralized wireless networks.**

I. Introduction

Nowadays, the task of ensuring privacy and security of the data transmitted in wireless networks is becoming increasingly important. The continuing development of computing devices has undermined the traditional cryptographic security mechanisms. The recently emerged physical-layer security techniques [1, 2] offer enhanced data security, regardless of the eavesdroppers' computational capability, and it has been introduced into decentralized wireless networks to provide improved secrecy performance [3–8].

Much of the literature on secrecy in decentralized networks can be classified into three categories based on the used performance metric and the modeling of the eavesdroppers. For the first category, the secure connectivity performance was inspected in the absence of interference (e.g., [3, 4]). For the second category, the secrecy throughput performance was investigated and the interference from other transmitting nodes was taken into consideration. The eavesdroppers therein were assumed to be incapable of resolving concurrent transmissions, hence simply treating them as interference (e.g., [5]). This assumption is often too optimistic and the designed system might be vulnerable if eavesdroppers with multi-user decodability (such as successive interference cancellation) are trying to intercept. As a more robust approach, in the last category, the secrecy rate/throughput performance was studied under a worst-case assumption that the eavesdroppers are capable of multi-user decoding (e.g., [6–8]).

In decentralized networks, if the eavesdroppers are capable of multi-user decoding, the interference caused by concurrent transmissions of information signals can potentially be resolved by the eavesdroppers. To provide secrecy in this challenging scenario, the aforementioned studies [6–8] introduced artificial noise [9] and jamming signals [10, 11] into decentralized networks, creating non-resolvable interference to the eavesdroppers. Specifically, in [6], the legitimate users which are far away from the intended receiver are selected to emit artificial noise; in [7], a certain percentage of legitimate users are randomly chosen to radiate jamming signals. Note that with single antenna transmission, as in [6, 7], some legitimate users have to stop their own message transmission, in order to deliver artificial noise or jamming signals.

With sectorized antennas [12, 13], independent signals can be transmitted in different sectors simultaneously. Here, as a means of conquering eavesdroppers with multi-user decodability, we propose to use sectorized transmission such that each transmitter sends an information signal in the sector containing its intended receiver, while simultaneously radiating artificial noise in other sectors to help provide secrecy for the entire network. In this way, no legitimate users need to sacrifice their own message transmission, which is a considerable advantage over the case of single antenna transmission [6, 7].

In this paper, we study the proposed artificial-noise-aided sectorized transmission in decentralized wireless networks. We start by characterizing the probability of connection outage on the legitimate link and the possibility of secrecy outage against malicious eavesdropping. Then, we derive the secrecy transmission capacity to measure the networkwide throughput of secure transmissions. After that, we provide a sufficient condition on the system parameters and constraints, under which a positive secrecy transmission capacity is achievable. Finally, we optimize the power allocation between the information signal and the artificial noise to maximize the secrecy transmission capacity. Our analysis clearly shows that sectorized transmission provides significant secrecy enhancements in decentralized wireless networks.

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).

978-1-4673-5577-3/13/$31.00 ©2013 IEEE

II. System Model

We consider a decentralized wireless network, with nodes randomly distributed on a 2-dimensional plane $\mathbb{R}^2$. The legitimate transmitters and the malicious eavesdroppers are modeled by two independent homogeneous Poisson point processes (PPPs) Φ_L and Φ_E with densities[1] λ_l and λ_e, respectively. Following the commonly-used network model [14], we assume that each transmitter has an intended receiver at distance r in a random direction. Each transmitter is equipped with N directional transmit antennas, while each receiver (both legitimate and malicious) has only one omnidirectional receive antenna. In addition to Rayleigh fading, the distance attenuation is modeled by a path-loss exponent $\alpha > 2$. We further assume that each legitimate receiver has perfect knowledge of the channel to the associated transmitter, while the malicious eavesdroppers have the channel knowledge to any transmitter they wish to intercept. Compared with the aggregated interference, the local thermal noise is assumed to be negligible and thus the signal-to-interference ratio (SIR) will be used to measure the system performance.

A. Sectorized Transmission with Artificial Noise

With N directional antennas, the transmitters are capable of sending independent signals in N disjoint sectors, each of these covering $\frac{2\pi}{N}$ radians with an antenna gain G. The antenna gain usually increases as the spread angle decreases. As done in [4], we assume that the sidelobes are suppressed sufficiently and thus can be omitted in later analysis. This sectorized transmission has been widely used to improve the connectivity performance in decentralized wireless networks [12, 13].

As discussed in Section I, we consider the following scheme to combine sectorized transmission with artificial noise: 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 this transmission scheme requires to know the direction of the intended receiver and this information can be obtained through discovery mechanisms, such as those developed in [13].

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 $P_T = P\phi$, while the power allocated to the artificial noise is $P_J = P\left(1-\phi\right)$. With the antenna gain, in the intended sector, information signal is transmitted with power GP_T, while in each of the other $N-1$ sectors, artificial noise is radiated with power $\frac{GP_J}{N-1}$.

We assume that the legitimate receivers are just common receivers and do not apply any 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 [6–8], 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.

B. Wiretap Coding and Outage Definition

Before transmission, the data are encoded using the wiretap code [1]. The codeword rate and the message rate are denoted as R_b and R_s, respectively. The rate redundancy $R_e := R_b - R_s$ is intentionally added to provide secrecy. More discussions on code construction can be found in [15].

If the channel from the transmitter to the intended receiver cannot support the codeword rate R_b, then the receiver may not be able to decode the message correctly, and 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 introduced rate redundancy R_e, this transmission fails to achieve perfect secrecy and a secrecy outage is deemed to occur [7].

III. Outage Performance Analysis

In this section, we investigate the outage performance of the legitimate link and the eavesdropping link, by deriving and inspecting the connection outage probability and the secrecy outage probability, respectively.

A. Connection Outage Probability

Here, we drive the connection outage probability p_{co} to measure the probability that the intended link cannot support the selected codeword rate. To this end, we focus on a typical transmitter-receiver pair and put the receiver at the origin of the coordinate system. From Slivnyak's theorem [16], 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, the interfering nodes can be classified into two classes: i) interferers transmitting information signals toward the origin; ii) interferers sending artificial noise toward the origin. With such a classification, the transmitters in Φ_L can be divided into two independent homogeneous PPPs, which are denoted by Φ_T and Φ_J with densities $\frac{1}{N}\lambda_l$ and $\frac{N-1}{N}\lambda_l$, respectively [16].

[1] Note that the density of the eavesdroppers is assumed to be known. This is an assumption made on behalf of the designer: If the target is to separate the network from a known one (e.g., hide a military network from a civilian one), the designer should have access to the density of the known network. Meanwhile, our analysis is still valid if the actual density of the eavesdroppers is not available: If a high security level is demanded, the designer may assume a large value for the eavesdroppers' density. This assumption is commonly adopted in the literature [3–8].

978-1-4673-5577-3/13/$31.00 ©2013 IEEE

For the typical receiver, the aggregated interference from the transmitters in Φ_T and Φ_J is given by

$$I_T = GP_T \sum_{x\in\Phi_T} S_{xo} D_{xo}^{-\alpha} \ , \quad I_J = \frac{GP_J}{N-1} \sum_{x\in\Phi_J} S_{xo} D_{xo}^{-\alpha} \ ,$$

where S_{xo} and D_{xo} represent the channel gain resulting from Rayleigh fading and the distance from the transmitter at x to the typical receiver at o (the origin), respectively. The channel gain from Rayleigh fading S_{xo} is exponentially distributed with unit mean, i.e., $S_{xo} \sim \mathrm{Exp}\,(1)$.

The total interference seen by the typical receiver is $I_T + I_J$. Since I_T and I_J are two independent shot noise processes, by [14], the Laplace transform of the probability density function (p.d.f.) of $I_T + I_J$ is given by

$$\mathcal{L}_{I_T+I_J}(\zeta) = \exp\left(-\frac{\lambda_l C_\alpha G^{\frac{2}{\alpha}}}{N}\left(P_T^{\frac{2}{\alpha}} + (N-1)^{1-\frac{2}{\alpha}}\, P_J^{\frac{2}{\alpha}}\right)\zeta^{\frac{2}{\alpha}}\right) ,$$

where

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

with $\Gamma(\cdot)$ denote the gamma function.

The channel gain resulting from Rayleigh fading between the typical transmitter and the typical receiver is denoted as $S_o \sim \mathrm{Exp}\,(1)$. The SIR at the typical receiver is given by

$$\mathrm{SIR}_o = GP_T S_o r^{-\alpha} \left(I_T + I_J\right)^{-1} \ .$$

For a given codeword rate R_b, a threshold SIR value for connection outage is defined as $\beta_b = 2^{R_b} - 1$. The connection outage probability is then given by

$$\begin{aligned} p_{\mathrm{co}} &= \Pr\left(\mathrm{SIR}_o \le \beta_b\right) \qquad (1)\\ &= 1 - \Pr\left(S_o \ge \frac{\beta_b r^\alpha}{GP_T}\left(I_T + I_J\right)\right)\\ &= 1 - \mathcal{L}_{I_T+I_J}\left(\frac{\beta_b r^\alpha}{GP_T}\right)\\ &= 1 - \exp\left(-\frac{\beta_b^{\frac{2}{\alpha}}\lambda_l C_\alpha r^2}{N}\left(1 + (N-1)^{1-\frac{2}{\alpha}}\left(\phi^{-1}-1\right)^{\frac{2}{\alpha}}\right)\right) . \end{aligned}$$

Remark: For a given power allocation ratio, it can be mathematically shown that with a reasonable path-loss exponent, i.e., $\alpha = 2 \sim 4$, the connection outage probability decreases when extra transmit sectors are added. The improvement comes from two aspects: i) the intended sectors shrink and thus the legitimate receivers are interfered by less information signals; ii) 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 derive the secrecy outage probability p_{so} to measure the possibility that the transmitted message is not perfectly secure against the eavesdroppers. To this end, we focus on a typical transmitter-receiver pair and put the transmitter at the origin. According to the assumption made in Section II-A, the interference at the eavesdroppers consists of the artificial noise only. The transmitters which are radiating artificial noise toward the eavesdropper at z form a homogeneous PPP Φ_J with density $\frac{N-1}{N}\lambda_l$ [16]. The interference seen by the eavesdropper at z is given by

$$I_J = \frac{GP_J}{N-1} \sum_{x\in\Phi_J} S_{xz} D_{xz}^{-\alpha} \ ,$$

where $S_{xz} \sim \mathrm{Exp}\,(1)$ and D_{xz} represent the channel gain resulting from Rayleigh fading and the distance from the transmitter at x to the eavesdropper at z, respectively.

By [14], the Laplace transform of p.d.f. of I_J is given by

$$\mathcal{L}_{I_J}(\zeta) = \exp\left(-\frac{\lambda_l C_\alpha G^{\frac{2}{\alpha}}}{N}\,(N-1)^{1-\frac{2}{\alpha}}\, P_J^{\frac{2}{\alpha}} \zeta^{\frac{2}{\alpha}}\right) .$$

With wiretap coding, the message from the typical transmitter is not perfectly secure against the eavesdropper at z if the channel from the typical transmitter to the eavesdropper at z can support a data rate larger than the added rate redundancy, i.e., $\log_2(1+\mathrm{SIR}_z) > R_e$, where SIR_z denotes the SIR received by the eavesdropper at z. With sectorized transmission, only the eavesdroppers inside the intended sector of the typical transmitter may cause secrecy outage. Though those eavesdroppers form a fan-shaped PPP, by Mapping Theorem [16], they can be mapped as a homogeneous PPP on the whole plane, which is denoted as Φ_Z with density $\frac{1}{N}\lambda_e$.

The SIR received by the eavesdropper at z is given by

$$\mathrm{SIR}_z = GP_T S_{oz} D_{oz}^{-\alpha} I_J^{-1} \ ,$$

where $S_{oz} \sim \mathrm{Exp}\,(1)$ and D_{oz} represent the channel gain resulting from Rayleigh fading and the distance from the typical transmitter at o (the origin) to the eavesdropper at z.

For a given rate redundancy R_e, a threshold SIR value for secrecy outage is defined as $\beta_e = 2^{R_e} - 1$. By taking the complement of the probability that the transmitted message is perfectly secure against all eavesdroppers, the secrecy outage probability can be expressed as

$$\begin{aligned} p_{\mathrm{so}} &= 1 - \mathbb{E}_{\Phi_J}\left\{\mathbb{E}_{\Phi_Z}\left\{\prod_{z\in\Phi_Z} \Pr\left(\mathrm{SIR}_z < \beta_e | \Phi_J\right)\right\}\right\} \qquad (2)\\ &= 1 - \mathbb{E}_{\Phi_J}\left\{\exp\left(-\frac{\lambda_e}{N}\int_{\mathbb{R}^2} \Pr\left(\mathrm{SIR}_z > \beta_e | \Phi_J\right) \mathrm{d}z\right)\right\} , \end{aligned}$$

where the 2nd line is obtained by applying the probability generating functional of a PPP (see Definition A.5 in [16]).

While a closed-form expression seems not available, we invoke the bounding technique used in [5], i.e., applying Jensen's inequality, to give the following upper bound:

$$\begin{aligned} p_{\mathrm{so}} &\le 1 - \exp\left(-\frac{\lambda_e}{N}\int_{\mathbb{R}^2} \Pr\left(\mathrm{SIR}_z > \beta_e\right) \mathrm{d}z\right)\\ &= 1 - \exp\left(-\frac{\lambda_e}{N}\int_{\mathbb{R}^2} \mathcal{L}_{I_J}\left(\frac{\beta_e D_{oz}^\alpha}{GP_T}\right) \mathrm{d}z\right)\\ &= 1 - \exp\left(-\frac{\frac{\pi}{C_\alpha}\frac{\lambda_e}{\lambda_l}}{\beta_e^{\frac{2}{\alpha}}\,(N-1)^{1-\frac{2}{\alpha}}\left(\phi^{-1}-1\right)^{\frac{2}{\alpha}}}\right)\\ &= p_{\mathrm{so}}^{\mathrm{UB}} \ . \qquad (3) \end{aligned}$$

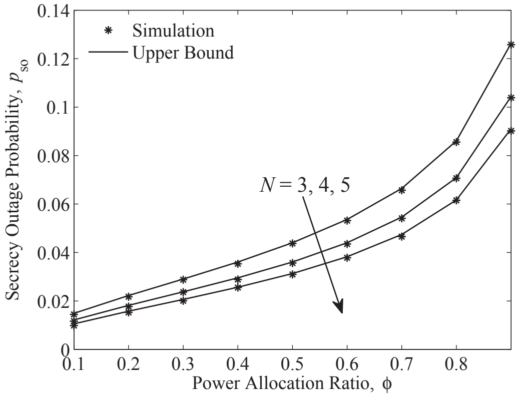

Fig. 1. The secrecy outage probability versus the power allocation ratio for different numbers of transmit sectors. Results are shown for the case where $\alpha = 4$, $\lambda_l = 0.01$, $\lambda_e = 0.001$, $R_e = 1$ and $\beta_e = 1$.

As shown in Fig. 1, the upper bound in (3) gives a very accurate approximation for the actual secrecy outage probability. From (3), we made the following observations:

Remark: For a given power allocation ratio, the secrecy outage probability can be reduced by adding extra transmit sectors. This result follows the intuition that by adding transmit sectors: i) the intended sector shrinks and thus less eavesdroppers may cause secrecy outage; ii) the artificial noise from other transmitters covers a larger region and thus more eavesdroppers are degraded. Moreover, as we may expect, the secrecy outage probability decreases if more legitimate transmitter-receiver pairs are deployed, since the reception at the eavesdroppers are degraded more severely.

IV. Secrecy Throughput Analysis

In this section, we study the networkwide throughput in terms of the secrecy transmission capacity, which measures the maximal achievable rate of successful transmission of confidential messages per unit area [5].

For a given pair of outage constraints, $p_{\mathrm{co}} = \sigma$ and $p_{\mathrm{so}} = \epsilon$, the secrecy transmission capacity is defined as

$$\begin{aligned} C &= (1-\sigma)\,\lambda_l R_s \\ &= (1-\sigma)\,\lambda_l \left[R_b - R_e\right]^+ \ , \end{aligned} \tag{4}$$

where $[x]^+ = \max\{0, x\}$, σ determines R_b, while ϵ determines R_e.

From (1), letting $p_{\mathrm{co}} = \sigma$ and recalling that $\beta_b = 2^{R_b} - 1$, the supported codeword rate R_b is

$$R_b = \log_2\left[1 + \left(\frac{\frac{N}{\lambda_l C_\alpha r^2}\ln\left(\frac{1}{1-\sigma}\right)}{1+(N-1)^{1-\frac{2}{\alpha}}\left(\phi^{-1}-1\right)^{\frac{2}{\alpha}}}\right)^{\frac{\alpha}{2}}\right] . \tag{5}$$

From (3), letting $p_{\mathrm{so}}^{\mathrm{UB}} = \epsilon$ and recalling that $\beta_e = 2^{R_e} - 1$, an upper bound to the required rate redundancy R_e can be found as

$$R_e^{\mathrm{UB}} = \log_2\left[1 + \left(\frac{\frac{\pi}{C_\alpha}\frac{\lambda_e}{\lambda_l}}{\ln\left(\frac{1}{1-\epsilon}\right)(N-1)^{1-\frac{2}{\alpha}}\left(\phi^{-1}-1\right)^{\frac{2}{\alpha}}}\right)^{\frac{\alpha}{2}}\right] . \tag{6}$$

With (5) and (6), a lower bound to the secrecy transmission capacity in (4) is obtained as follows:

$$\begin{aligned} C_{\mathrm{LB}} &= (1-\sigma)\,\lambda_l\left[R_b - R_e^{\mathrm{UB}}\right]^+ \\ &= (1-\sigma)\,\lambda_l \qquad\qquad (7) \\ &\times\left[\log_2\left(\frac{1+\left(\frac{\frac{N}{\lambda_l C_\alpha r^2}\ln\left(\frac{1}{1-\sigma}\right)}{1+(N-1)^{1-\frac{2}{\alpha}}(\phi^{-1}-1)^{\frac{2}{\alpha}}}\right)^{\frac{\alpha}{2}}}{1+\left(\frac{\frac{\pi}{C_\alpha}\frac{\lambda_e}{\lambda_l}}{\ln\left(\frac{1}{1-\epsilon}\right)(N-1)^{1-\frac{2}{\alpha}}(\phi^{-1}-1)^{\frac{2}{\alpha}}}\right)^{\frac{\alpha}{2}}}\right)\right]^+ . \end{aligned}$$

Since the upper bound in (3) tracks the exact secrecy outage probability very closely, the lower bound in (7) provides a very tight approximation to the actual secrecy transmission capacity. From (7), we made the following observations:

Remark: The secrecy transmission capacity increases logarithmically as the number of transmit sectors goes large. This result comes from fact that under the outage constraints, as the number of transmit sectors goes large, the supported codeword rate in (5) increases logarithmically, while the required rate redundancy in (6) diminishes.

A. Condition for Positive Secrecy Transmission Capacity

Here, we derive a sufficient condition, in terms of the system parameters and outage constraints, under which a positive secrecy transmission capacity is achievable.

From (7), a positive secrecy transmission capacity is achieved if:

$$\ln\!\left(\frac{1}{1-\sigma}\right)\ln\!\left(\frac{1}{1-\epsilon}\right) > \frac{\pi\lambda_e r^2}{N}\left(1+\frac{1}{(N-1)^{1-\frac{2}{\alpha}}\left(\phi^{-1}-1\right)^{\frac{2}{\alpha}}}\right) . \tag{8}$$

Since the power allocation ratio ϕ satisfies $0 \leq \phi \leq 1$, if the following inequality stands:

$$\ln\left(\frac{1}{1-\sigma}\right)\ln\left(\frac{1}{1-\epsilon}\right) > \frac{\pi\lambda_e r^2}{N} \ , \tag{9}$$

then ϕ may always be adjusted such that the condition in (8) is met. In other words, if the condition in (9) is satisfied, a positive secrecy transmission capacity can always be achieved by using a proper power allocation ratio.

Remark: Interestingly, as can be seen from the left-hand-side of (9), the feasible region formed by pairs of (σ, ϵ), with which a positive secrecy transmission capacity is achievable, is a symmetric function of the two outage constraints, σ and ϵ. From the right-hand-side of (9), we know that adding extra transmit sectors is an effective method to enlarge the feasible region. Compared with the results in Corollary 1 of [5], the artificial-noise-aided sectorized transmission proposed in this paper expands the feasible region by a factor of the number of transmit sectors N, even under a more stringent assumption that the eavesdroppers can perform multi-user decoding.

B. Power Allocation Optimization

In this subsection, we optimize the power allocation between the information signal and the artificial noise to maximize the secrecy transmission capacity.

978-1-4673-5577-3/13/$31.00 ©2013 IEEE

Remark: By properly factorizing the derivative of the secrecy transmission capacity lower bound C_{LB} in (7) w.r.t. the power allocation ratio ϕ, it can be shown that by increasing ϕ, the derivative is first positive and then negative. Hence, the optimal power allocation ratio ϕ^*, which maximizes C_{LB}, is unique and can be found by solving the derivative, even if the objective function is non-concave, as can be shown from (7).

For the case where $\alpha = 4$, setting the derivative of C_{LB} w.r.t. ϕ to zero gives a cubic equation and solving it provides a closed-form expression for ϕ^*. Here, we skip the details for space limitation and present the results directly.

Define:

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

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

The optimal power allocation ratio for $\alpha = 4$ is given by

$$\phi^*_{\alpha=4} = \left(1 + \frac{\varsigma^{\frac{2}{3}}\left(2^{\frac{2}{3}}\varrho^{\frac{4}{3}}\varsigma^{\frac{1}{3}}\kappa^{\frac{2}{3}} + 2^{\frac{4}{3}}\varrho^2\varsigma + 2\varrho^{\frac{2}{3}}\varsigma^{\frac{5}{3}}\kappa^{\frac{1}{3}}\right)^2}{4\left(N-1\right)\varrho^{\frac{4}{3}}\kappa^{\frac{2}{3}}\left(\varrho^2 - \varsigma^2\right)^2}\right)^{-1}.$$

Remark: As $N \to \infty$, we see that $\phi^*_{\alpha=4} = 1 - \mathcal{O}\left(N^{-1}\right)$, and similar asymptotic behavior can be observed when $\sigma \to 1$. In other words, the optimal power allocation ratio increases as the number of transmit sectors goes large or as the connection outage constraint becomes loose. The former observation can be explained by noting that adding extra transmit sectors allows the transmitter to concentrate more on the transmission toward the intended receiver, and thus 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.

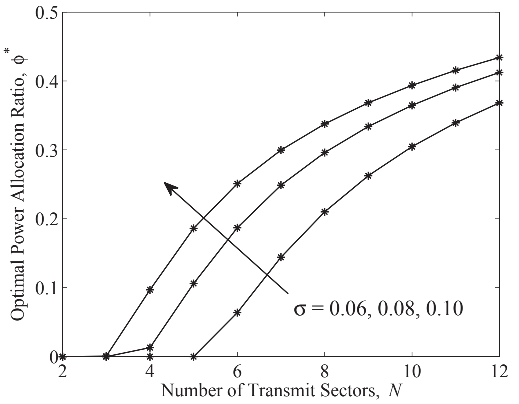

Fig. 2. Optimal power allocation ratio versus the number of transmit sectors for different connection outage constraints. Results are shown for the case where $\alpha = 3$, $r = 1$, $\epsilon = 0.01$, $\lambda_l = 0.01$ and $\lambda_e = 0.001$.

Fig. 2 depicts the optimal power allocation ratio versus the number of transmit sectors with $\alpha = 3$. As can be seen, the observations made from the case $\alpha = 4$ holds more generally. Numerical results also indicate that with optimal power allocation, the secrecy transmission capacity increases logarithmically as the number of transmit sectors goes large, which agrees with our earlier observation made from (7).

V. Conclusion and Future Work

In this paper, we combined sectorized transmission with artificial noise to enhance the secrecy performance in decentralized wireless networks. After characterizing the secrecy transmission capacity, we provided a sufficient condition for achieving a positive secrecy transmission capacity and investigated the optimal power allocation for maximizing the secrecy transmission capacity. The analytical results indicates that with sectorized transmission, significant secrecy enhancements can be achieved. Note that sectorized transmission only requires to know the direction of the intended receiver. If the channel knowledge of the intended receiver is available at the transmitter, artificial-noise-aided beamforming [9] can be employed to exploit the benefits of having multiple transmit antennas, and it is currently under investigation.

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] 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.

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

[5] 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.

[6] S. Vasudevan, D. Goeckel, and D. Towsley, "Security-capacity trade-off in large wireless networks using keyless secrecy," in *Proc. 11th ACM Int. Sympos. Mobile Ad Hoc Network. Comput.*, Chicago, America, 2010, pp. 21–30.

[7] 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.

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

[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. 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.

[11] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 256–266, Jun. 2011.

[12] L. Bao and J. J. Garcia-Luna-Aceves, "Transmission scheduling in ad hoc networks with directional antennas," in *Proc. 8th Ann. Int. Conf. Mobile Comput. Network.*, Atlanta, America, Sep. 2002, pp. 48–58.

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

[14] 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. Selected Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, Sep. 2009.

[15] 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.

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