Secure Wireless Network Connectivity with Multi-Antenna Transmission

Xiangyun Zhou, *Member, IEEE*, Radha Krishna Ganti, *Member, IEEE*,
and Jeffrey G. Andrews, *Senior Member, IEEE*

***Abstract*—Information-theoretic security constraints reduce the connectivity of wireless networks in the presence of eavesdroppers, which motivates better modeling of such networks and the development of techniques that are robust to eavesdropping. In this letter, we are concerned with the existence of secure connections from a typical transmitter to the legitimate receiver(s) over fading channels, where the legitimate nodes and eavesdroppers are all randomly located. We consider non-colluding and colluding eavesdroppers, and derive the network secure connectivity for both eavesdropper strategies. We mathematically show how nodes with multiple transmit antenna elements can improve secure connectivity by forming a directional antenna or using eigen-beamforming. Compared with single antenna transmission, a large connectivity improvement can be achieved by both multi-antenna transmission techniques even with a small number of antennas.**

***Index Terms*—Network connectivity, physical-layer security, colluding eavesdroppers, directional antenna, beamforming.**

I. Introduction

SECURITY is a pervasive concern in wireless networks due to the broadcast nature of the wireless medium. Recently, information-theoretic security as a physical-layer approach has been widely investigated as a means to provide secure communication. Many studies on information-theoretic security focus on a point-to-point link with single or multiple antennas, *e.g.*, [1–6]. However, few results have been obtained on information-theoretic security in large-scale wireless networks.

Unlike point-to-point communications, security in wireless networks strongly depends on the spatial distribution of both the legitimate nodes and the eavesdroppers. Initial works on network information-theoretic security mainly considered random networks where the legitimate nodes and the eavesdroppers are randomly distributed, and studied the secrecy rate behavior and connectivity properties [7–13]. In particular, the scaling laws of the secrecy rate in static and mobile ad hoc networks were studied in [7] and [8], respectively. A probabilistic characterization of the maximum secrecy rate was given in [9] for the worst-case colluding eavesdroppers. From a network connectivity viewpoint, the node degree under security constraints was studied with and without knowledge of the eavesdroppers' locations in [10–13].

In this letter, we study secure connectivity of wireless random networks with multi-antenna transmission in Rayleigh fading channels. From a theoretical point of view, we aim to statistically characterize the existence of secure connections between a typical node of interest and other legitimate nodes. Two types of eavesdroppers are considered, namely non-colluding eavesdroppers and colluding eavesdroppers. From the viewpoint of secure transmission design, we consider two antenna array techniques for improving secure connectivity by forming a directional antenna or using eigen-beamforming, and quantify the connectivity improvement over single antenna transmission.

II. System Model

The legitimate nodes are distributed on a two-dimensional plane according to a Poisson point process (PPP) Φ_l with density λ_l. The eavesdroppers are distributed according to another independent PPP Φ_e with density λ_e. We define the ratio of densities of Φ_l and Φ_e as $\eta = \lambda_l/\lambda_e$. A typical node o located at the origin wants to transmit confidential messages to one or multiple nodes in Φ_l in the presence of the eavesdroppers in Φ_e. From the viewpoint of secure transmission design, we consider that the typical node o uses M antennas ($M \geq 1$) for transmission, while all the legitimate receivers and eavesdroppers use a single antenna each for reception. We focus on this single-ended multi-antenna transmission scheme since it provides much simpler results and analysis, compared to the case where multi-antenna reception is also used at the receivers and eavesdroppers. We consider both non-colluding and colluding eavesdroppers. In the non-colluding case, the eavesdroppers individually overhear the communication without centralized processing. In the colluding eavesdroppers case, all eavesdroppers are able to jointly process their received message at a central data processing unit. Note that the authors in [12] also studied eavesdropper collusion and focused on single antenna transmission over path loss channels, while we consider two multi-antenna transmission techniques over Rayleigh fading channels.

A. Signal Model

Considering the typical node o at the origin as the transmitter, the received signal power at a legitimate receiver l is given by

$$\mathcal{P}_{rl} = \mathcal{P}_{tl} h_l d_l^{-\alpha}, \tag{1}$$

where $\mathcal{P}_{tl}$ is the transmit power for l, d_l is the distance between o and l, α is the path loss exponent, and h_l is the fading effect of the wireless channel from o to l. We consider

Manuscript received June 9, 2010; revised September 10, 2010; accepted November 4, 2010. The associate editor coordinating the review of this letter and approving it for publication was M. Gursoy.

X. Zhou is with UNIK - University Graduate Center, the University of Oslo, Norway (e-mail: xiangyun@unik.no).

R. K. Ganti and J. G. Andrews are with the Department of Electrical and Computer Engineering, the University of Texas at Austin, Austin, TX 78712, USA (e-mail: rganti@austin.utexas.edu, jandrews@ece.utexas.edu).

R. K. Ganti and J. G. Andrews were supported by the DARPA IT-MANET project.

Digital Object Identifier 10.1109/TWC.2010.112310.101008

Rayleigh fading channels and hence, h_l follows an exponential distribution.

The total received signal power available for eavesdropping depends on whether the eavesdroppers collude. For non-colluding eavesdroppers, the received signal power at eavesdropper e is given by

$$\mathcal{P}_{re} = \mathcal{P}_{te} h_e d_e^{-\alpha}, \tag{2}$$

where $\mathcal{P}_{te}$ is the transmit power for e. For colluding eavesdroppers, the combined received signal power at the eavesdroppers after centralized processing is given by

$$\mathcal{P}_{re} = \sum_{e \in \Phi_e} \mathcal{P}_{te} h_e d_e^{-\alpha}. \tag{3}$$

B. Secure Connection

Physical-layer security is commonly characterized by achievable secrecy rates. For transmission from the typical node o to a legitimate receiver l in the presence of eavesdropper(s) e, a supremum of the secrecy rates is given by the difference in the maximum data rate of the channel between o and l and that between o and e [6, 14]. From a connectivity point of view, a secure connection from the transmitter o to a legitimate receiver l is possible if the secrecy rate is positive [11], *i.e.*,

$$\log_2\left(1 + \frac{\mathcal{P}_{rl}}{\sigma_l^2}\right) - \log_2\left(1 + \frac{\mathcal{P}_{re}}{\sigma_e^2}\right) > 0, \tag{4}$$

where σ_l^2 and σ_e^2 are the noise variance at l and e, respectively. We can rewrite (4) as

$$\frac{\mathcal{P}_{rl}}{\mathcal{P}_{re}} > \beta, \tag{5}$$

where $\beta = \sigma_l^2/\sigma_e^2$. Note that if the secrecy rate is required to be above some positive value R instead of zero, the expression in (5) is still valid in the high signal-to-noise ratio (SNR) regime, *i.e.*, $\frac{\mathcal{P}_{rl}}{\sigma_l^2} \gg 1$ and $\frac{\mathcal{P}_{re}}{\sigma_e^2} \gg 1$, in which case we have $\beta \approx 2^R \sigma_l^2/\sigma_e^2$.

C. Secure Connectivity Metrics

We focus on local connectivity of the network, which is concerned with the connectivity from the viewpoint of the typical node. The following metrics will be used in the analysis.

- $P_{\text{c}}(d_l)$: Probability of a secure connection from o to l with distance d_l.
- P_{n}: Probability of a secure connection from o to the nearest node in Φ_l.
- N_{avg}: The average number of secure connections from o to the nodes in Φ_l.

These metrics are concerned with statistical measures on the existence of secure connection, which are based on an outage formulation. The transmitter only requires the channel state information (CSI) of the legitimate receiver and doe not need the CSI of the eavesdroppers to realize a certain secrecy outage probability or probability of secure connection [14]. This is in contrast to the case of achieving a target secrecy rate, where the CSI of both the legitimate receiver and the eavesdroppers is necessary. Note that N_{avg} is concerned with the secure connection to multiple nodes in Φ_l, where transmission can be either in the form of message broadcasting or time-division multiplexing (TDM).

The metric $P_{\text{c}}(d_l)$ describes the probability of the event in (5) happening with a given distance d_l. It can be seen that P_{n} is related to $P_{\text{c}}(d_l)$ as

$$P_{\text{n}} = \int_0^\infty P_{\text{c}}(d_l) f(d_l)\, \mathrm{d}d_l, \tag{6}$$

where $f(d_l)$ is the distribution of the distance of the node in Φ_l that is closest to the origin, given by $f(d_l) = 2\lambda_l \pi d_l \exp(-\lambda_l \pi d_l^2)$ in [15]. Also, N_{avg} is given by

$$\begin{aligned} N_{\text{avg}} &= E_{\Phi_l,\Phi_e}\Big\{\sum_{l\in\Phi_l} 1(l,\Phi_e)\Big\} \\ &= E_{\Phi_l}\Big\{\sum_{l\in\Phi_l} P_{\text{c}}(d_l)\Big\} \\ &= 2\pi\lambda_l \int_0^\infty P_{\text{c}}(d_l) d_l\, \mathrm{d}d_l, \end{aligned} \tag{7}$$

where $1(l, \Phi_e)$ is an indicator function of secure connection from o to l in the presence of Φ_e, and (7) is obtained using Campbell's theorem [16] and by changing to polar coordinates.

III. Directional Antenna Transmission

By introducing different phase shifts in each antenna element, the antenna array can concentrate its transmit power into the direction of the intended receiver. We consider a simplified model for directional antennas, which is widely used for performance analysis [17]. The antenna beam pattern has a main-lobe of gain M and angle of spread $2\pi\omega$, and a side-lobe of gain νM and angle of spread $2\pi(1-\omega)$, where ν is the side-lobe attenuation factor. The values of ω and ν are determined by preserving the first- and second-order moments of the beam pattern of a practical antenna array, such as uniform circular array (UCA) and uniform linear array (ULA) [17]. Our study on the use of a directional antenna aims to show how the number of antenna elements and the type of antenna array affect the secure connectivity, which is different from the case of independently sectorized transmissions considered in [12].

With this antenna beam model, the eavesdroppers can be classified as in the main-lobe or side-lobe direction. Let us denote the set of main-lobe eavesdroppers as Φ_{e1} and the set of side-lobe eavesdroppers as Φ_{e2}. Clearly, Φ_{e1} and Φ_{e2} are independent PPPs. The received signal power at l is given by $\mathcal{P}_{rl} = \mathcal{P} M h_l d_l^{-\alpha}$, where $\mathcal{P}$ is the transmit power of a single antenna. The received signal power at the main-lobe eavesdroppers is given by $\mathcal{P}_{re} = \mathcal{P} M h_e d_e^{-\alpha}$, while the received signal power at the side-lobe eavesdroppers is given by $\mathcal{P}_{re} = \mathcal{P} \nu M h_e d_e^{-\alpha}$.

A. Non-colluding Eavesdroppers

In the case of non-colluding eavesdroppers, a secure connection is possible if the requirement in (5) is met for every single eavesdropper in Φ_e.

Lemma 1: In the case of non-colluding eavesdroppers, the probability of secure connection at distance d_l *with directional antenna transmission is given by*

$$P_c(d_l)=E_h\{\exp[-\lambda_e\pi d_l^2\beta^\delta\Gamma(1+\delta)h^{-\delta}(\omega+\nu^\delta-\omega\nu^\delta)]\}, \quad (8)$$

where h *has an exponential distribution with rate parameter equal to 1, and* $\delta=2/\alpha$*.*

Proof: For non-colluding eavesdroppers, $P_\mathrm{c}(d_l)$ is given by

$$\begin{aligned}P_\mathrm{c}(d_l) = E_{h_l,\Phi_{e1},\Phi_{e2}}\Big\{ &\prod_{e_i\in\Phi_{e1}} P\Big(\frac{h_l\, d_l^{-\alpha}}{h_{e_i} d_{e_i}^{-\alpha}}>\beta\,\Big|\, e_i,h_l\Big)\\ &\prod_{e_j\in\Phi_{e2}} P\Big(\frac{h_l\, d_l^{-\alpha}}{\nu h_{e_j} d_{e_j}^{-\alpha}}>\beta\,\Big|\, e_j,h_l\Big)\Big\}.\end{aligned}$$

For a PPP Φ, the generating functional is given by [16]

$$E_\Phi\Big\{\prod_{z\in\Phi} f(z)\Big\}=\exp\Big[-\int_{\mathbb{R}^2}\Big(1-f(z)\Big)\lambda(z)\mathrm{d}z\Big],$$

where $\lambda(z)$ is the density function of the PPP. Applying the generating functional for Φ_{e1} and Φ_{e2}, and changing to polar coordinates, we have

$$\begin{aligned}P_\mathrm{c}(d_l) = E_{h_l}\Big\{ &\exp\Big[-2\pi\omega\lambda_e\int_0^\infty P\Big(h_e\geq\frac{h_l q^\alpha}{\beta d_l^\alpha}\,\Big|\, h_l\Big)q\mathrm{d}q\\ &-2\pi(1-\omega)\lambda_e\int_0^\infty P\Big(h_e\geq\frac{h_l q^\alpha}{\nu\beta d_l^\alpha}\,\Big|\, h_l\Big)q\mathrm{d}q\Big]\Big\},\end{aligned}$$

Using $t=\frac{h_l q^\alpha}{\beta d_l^\alpha}$ in the first integral and $t=\frac{h_l q^\alpha}{\nu\beta d_l^\alpha}$ in the second integral, we have

$$\begin{aligned}P_\mathrm{c}(d_l) &= E_{h_l}\Big\{\exp\Big[-\lambda_e\pi d_l^2\beta^\delta h_l^{-\delta}(\omega+\nu^\delta-\omega\nu^\delta)\\ &\qquad\times\delta\int_0^\infty P(h_e\geq t|\, h_l)t^{\delta-1}\mathrm{d}t\Big]\Big\},\\ &= E_{h_l}\Big\{\exp\Big[-\lambda_e\pi d_l^2\beta^\delta h_l^{-\delta}(\omega+\nu^\delta-\omega\nu^\delta)E\{h_e^\delta\}\Big]\Big\},\end{aligned}$$

where $E\{h_e^\delta\}=\Gamma(1+\delta)$ as h_e is exponentially distributed. ■

Using (6) and (7), we obtain the following results.

Corollary 1: In the case of non-colluding eavesdroppers, the probability of secure connection to the nearest legitimate node with directional antenna transmission is given by

$$P_n=E_h\Big\{\frac{1}{1+\eta^{-1}\beta^\delta\Gamma(1+\delta)h^{-\delta}(\omega+\nu^\delta-\omega\nu^\delta)}\Big\}, \quad (9)$$

where h *has an exponential distribution with rate parameter equal to 1.*

Corollary 2: In the case of non-colluding eavesdroppers, the average number of secure connections to the legitimate nodes with directional antenna transmission is given by

$$N_{avg}=\frac{\eta}{\beta^\delta(\omega+\nu^\delta-\omega\nu^\delta)}. \quad (10)$$

In the special case of single antenna transmission, we have $\omega=1$ and $\nu=1$, and hence

$$P_\mathrm{n} = E_h\Big\{\frac{1}{1+\eta^{-1}\beta^\delta\Gamma(1+\delta)h^{-\delta}}\Big\}, \quad (11)$$

$$N_\mathrm{avg} = \frac{\eta}{\beta^\delta}. \quad (12)$$

We see that the use of a directional antenna improves the connectivity by the factor $(\omega+\nu^\delta-\omega\nu^\delta)^{-1}$. Hence, this factor allows the designer to carry out a quick assessment on the secure connectivity implications of different antenna arrays.

B. Colluding Eavesdroppers

The colluding eavesdroppers case represents a worst case scenario from the secure communication viewpoint, while it gives the best possible performance from the eavesdropper design viewpoint.

Lemma 2: In the presence of colluding eavesdroppers, the probability of secure connection at distance d_l *with directional antenna transmission is given by*

$$P_c(d_l)=\exp[-\lambda_e\pi d_l^2\beta^\delta\Gamma(1+\delta)\Gamma(1-\delta)(\omega+\nu^\delta-\omega\nu^\delta)]. \quad (13)$$

Proof: With colluding eavesdroppers, $P_\mathrm{c}(d_l)$ is given by

$$P_\mathrm{c}(d_l)=P\Big(\frac{h_l d_l^{-\alpha}}{\sum_{e_i\in\Phi_{e1}} h_{e_i}d_{e_i}^{-\alpha}+\sum_{e_j\in\Phi_{e2}}\nu h_{e_j}d_{e_j}^{-\alpha}}>\beta\Big). \quad (14)$$

We let $I_1=\sum_{e_i\in\Phi_{e1}} h_{e_i}d_{e_i}^{-\alpha}$ and $I_2=\sum_{e_j\in\Phi_{e2}}\nu h_{e_j}d_{e_j}^{-\alpha}$, which are two shot noise processes. Following the derivation of the Laplace transform of shot noise process in [18, 19], we obtain

$$\begin{aligned}\mathcal{L}_{I_1}(\zeta) &= \exp[-\omega\lambda_e\pi\zeta^\delta\Gamma(1+\delta)\Gamma(1-\delta)],\\ \mathcal{L}_{I_2}(\zeta) &= \exp[-(1-\omega)\nu^\delta\lambda_e\pi\zeta^\delta\Gamma(1+\delta)\Gamma(1-\delta)].\end{aligned}$$

Since Φ_{e1} and Φ_{e2} are independent PPPs, I_1 and I_2 are independent shot noise processes. Hence, the Laplace transform of I_1+I_2 equals the product of the Laplace transforms of I_1 and I_2.

We rewrite (14) as

$$\begin{aligned}P_\mathrm{c}(d_l) &= P\Big(h_l>\beta d_l^\alpha(I_1+I_2)\Big)\\ &= \int_0^\infty P(h_l>\beta d_l^\alpha y)f_{I_1+I_2}(y)\mathrm{d}y\\ &= \int_0^\infty \exp[-\beta d_l^\alpha y]f_{I_1+I_2}(y)\mathrm{d}y,\end{aligned}$$

which is the Laplace transform of I_1+I_2 evaluated at βd_l^α. And (13) is readily obtained. ■

Using (6) and (7), we obtain the following results.

Corollary 3: In the presence of colluding eavesdroppers, the probability of secure connection to the nearest legitimate node with directional antenna transmission is given by

$$P_n=\frac{1}{1+\eta^{-1}\beta^\delta\Gamma(1+\delta)\Gamma(1-\delta)(\omega+\nu^\delta-\omega\nu^\delta)}. \quad (15)$$

Corollary 4: In the presence of colluding eavesdroppers, the average number of secure connections to the legitimate nodes with directional antenna transmission is given by

$$N_{avg}=\frac{\eta}{\beta^\delta\Gamma(1+\delta)\Gamma(1-\delta)(\omega+\nu^\delta-\omega\nu^\delta)}. \quad (16)$$

In the special case of single antenna transmission, we have $\omega=1$ and $\nu=1$, and hence

$$P_\mathrm{n} = \frac{1}{1+\eta^{-1}\beta^\delta\Gamma(1+\delta)\Gamma(1-\delta)}, \quad (17)$$

$$N_\mathrm{avg} = \frac{\eta}{\beta^\delta\Gamma(1+\delta)\Gamma(1-\delta)}. \quad (18)$$

Note that N_{avg} in (18) stays the same for non-fading path loss channels, which was derived in [12]. Again we see that the factor $(\omega + \nu^{\delta} - \omega\nu^{\delta})^{-1}$ characterizes the connectivity improvement from using a directional antenna for transmission.

IV. Eigen-Beamforming

Knowing the CSI of the intended receiver, the transmitter can use eigen-beamforming to maximize the signal strength to the intended receiver. This is done by transmitting linearly weighted copies of the same information signal on each antenna, where the weights are designed to maximize the SNR at the receiver. For simplicity, we assume that the channels are spatially uncorrelated. With eigen-beamforming, the signal power at the legitimate receiver has a Gamma distribution, while the signal power at the eavesdroppers is still exponentially distributed. In the following, we present results for both non-colluding and colluding eavesdroppers.

A. Non-colluding Eavesdroppers

Lemma 3: In the presence of non-colluding eavesdroppers, the probability of secure connection at distance d_l with eigen-beamforming is given by

$$P_c(d_l) = E_h\{\exp[-\lambda_e \pi d_l^2 \beta^{\delta}\Gamma(1+\delta)h^{-\delta}]\}, \tag{19}$$

where h has a Gamma distribution with parameters $(M, 1)$.

Proof: The signal model with eigen-beamforming is the same as that with single antenna transmission, except that h_l now has a Gamma distribution with parameters $(M, 1)$. Therefore, $P_{\text{c}}(d_l)$ is given by the same expression as in (8) with $\omega = 1$, $\nu = 1$ and h follows a Gamma distribution. ■

Using (6) and (7), we obtain the following results.

Corollary 5: In the presence of non-colluding eavesdroppers, the probability of secure connection to the nearest legitimate node with eigen-beamforming is given by

$$P_n = E_h\Big\{\frac{1}{1+\eta^{-1}\beta^{\delta}\Gamma(1+\delta)h^{-\delta}}\Big\}, \tag{20}$$

where h has a Gamma distribution with parameters $(M, 1)$.

Corollary 6: In the presence of non-colluding eavesdroppers, the average number of secure connections to the legitimate nodes with eigen-beamforming is given by

$$N_{avg} = \frac{\eta}{\beta^{\delta}}\frac{\Gamma(M+\delta)}{\Gamma(1+\delta)\Gamma(M)}. \tag{21}$$

Comparing N_{avg} with single antenna transmission and eigen-beamforming in (12) and (21), respectively, the improvement from beamforming is characterized by the factor $\frac{\Gamma(M+\delta)}{\Gamma(1+\delta)\Gamma(M)}$. For example, with $M = 2$ and $\alpha = 4$, this factor equals 1.5. This implies that eigen-beamforming can significantly improve secure connectivity even with a small number of transmit antennas.

B. Colluding Eavesdroppers

Lemma 4: In the presence of colluding eavesdroppers, the probability of secure connection at distance d_l with eigen-beamforming is given by

$$\begin{aligned} P_c(d_l) &= \exp[-\pi\lambda_e\beta^{\delta}d_l^2\Gamma(1{+}\delta)\Gamma(1{-}\delta)] \\ &\quad\times\Big(1{+}\sum_{k=1}^{M-1}\sum_{p=1}^{k}\frac{1}{k!}[-\delta\pi\lambda_e\beta^{\delta}d_l^2\Gamma(1{+}\delta)\Gamma(1{-}\delta)]^p\Upsilon_{k,p}\Big), \end{aligned} \tag{22}$$

where $\Upsilon_{k,p}$ is a constant defined as

$$\begin{aligned} \Upsilon_{k,p} \;=\; &\sum_{\epsilon_j\in comb\binom{k-1}{k-p}}\;\prod_{n_{ij}\in\epsilon_j}\Big(\delta(n_{ij}-i+1)-n_{ij}\Big), \\ &i=1,2,...,|\epsilon_j|,\; j=1,2,...,\binom{k-1}{k-p}, \end{aligned}$$

where $comb\binom{x}{y}$ is the set of all subsets of the natural numbers $\{1,2,...,x\}$ of cardinality y with distinct elements. Note that $\Upsilon_{k,k} = (-1)^k$.

Proof: For colluding eavesdroppers, we have

$$P_{\text{c}}(d_l) = P\left(\frac{h_l d_l^{-\alpha}}{\sum_{e\in\Phi_e} h_e d_e^{-\alpha}} > \beta\right), \tag{23}$$

where the complementary cumulative distribution function (CCDF) of the Gamma distributed random variable h_l with parameter $(M, 1)$ is given by

$$F_{h_l}^{c}(z) = \sum_{k=0}^{M-1}\frac{z^k}{k!}\exp[-z].$$

Using Theorem 1 in [20], (23) can be expressed as

$$P_{\text{c}}(d_l) = \sum_{k=0}^{M-1}\frac{1}{k!}(-\zeta)^k\frac{\mathrm{d}^k}{\mathrm{d}\zeta^k}\mathcal{L}_I(\zeta), \tag{24}$$

where $\zeta = \beta d_l^{\alpha}$ and $I = \sum_{e\in\Phi_e} h_e d_e^{-\alpha}$. The Laplace transform of I is given as

$$\mathcal{L}_I(\zeta) = \exp[-\lambda_e\pi\zeta^{\delta}\Gamma(1+\delta)\Gamma(1-\delta)].$$

Following [20], the derivative of $\mathcal{L}_I(\zeta)$ can be computed as

$$\begin{aligned} \frac{\mathrm{d}^k}{\mathrm{d}\zeta^k}\mathcal{L}_I(\zeta) &= \frac{\exp[-\pi\lambda_e\Gamma(1+\delta)\Gamma(1-\delta)\zeta^{\delta}]}{(-\zeta)^k} \\ &\qquad\times\sum_{p=1}^{k}\Big(-\delta\pi\lambda_e\Gamma(1{+}\delta)\Gamma(1{-}\delta)\zeta^{\delta}\Big)^p\Upsilon_{k,p}. \end{aligned} \tag{25}$$

Substituting (25) into (24), we obtain the result in (22). ■

Using (6) and (7), we obtain our final results.

Corollary 7: In the presence of colluding eavesdroppers, the probability of secure connection to the nearest legitimate node with eigen-beamforming is given by

$$\begin{aligned} P_n \;=\; &\frac{1}{1+\eta^{-1}\beta^{\delta}\Gamma(1+\delta)\Gamma(1-\delta)} \\ &\times\;\Big(1{+}\sum_{k=1}^{M-1}\sum_{p=1}^{k}\frac{p!}{k!}\Big[-\frac{\delta\beta^{\delta}\Gamma(1{+}\delta)\Gamma(1{-}\delta)}{\eta{+}\beta^{\delta}\Gamma(1{+}\delta)\Gamma(1{-}\delta)}\Big]^p\Upsilon_{k,p}\Big). \end{aligned} \tag{26}$$

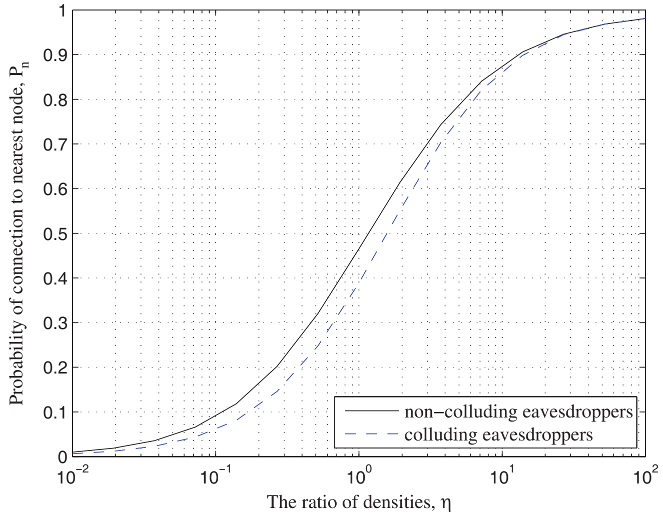

Fig. 1. P_{n} vs. ratio of densities with single antenna transmission in the presence of either non-colluding or colluding eavesdroppers. The path loss exponent of $\alpha = 4$ is used and $\beta = 1$ is chosen.

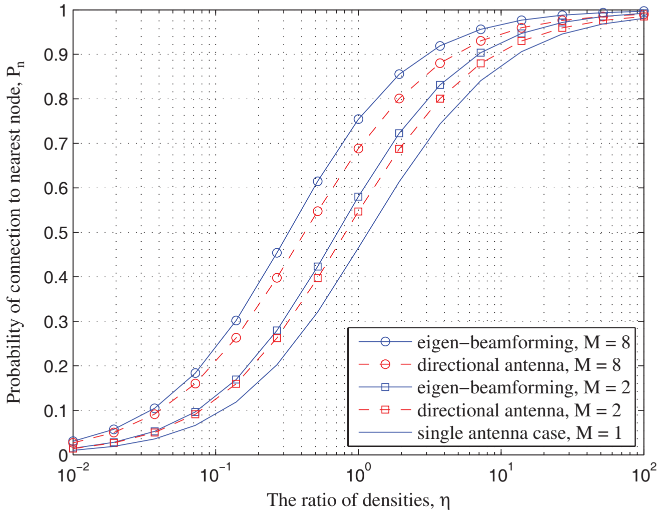

Fig. 2. P_{n} vs. ratio of densities in the presence of non-colluding eavesdroppers. The path loss exponent of $\alpha = 4$ is used and $\beta = 1$ is chosen. For directional antennas, the parameters of the simplified antenna beam model, ω and ν, are determined by preserving the first- and second-order moments of the beam pattern of a UCA. $\omega = 1$ and $\nu = 1$ for $M = 1$. $\omega \approx 0.39$ and $\nu \approx 0.26$ for $M = 2$. $\omega \approx 0.06$ and $\nu \approx 0.10$ for $M = 8$.

Corollary 8: In the presence of colluding eavesdroppers, the average number of secure connections to the legitimate nodes with eigen-beamforming is given by

$$N_{avg} = \frac{\eta}{\beta^{\delta}\Gamma(1+\delta)\Gamma(1-\delta)}\left(1+\sum_{k=1}^{M-1}\sum_{p=1}^{k}\frac{p!}{k!}[-\delta]^{p}\Upsilon_{k,p}\right). \quad (27)$$

Comparing N_{avg} with single antenna transmission and beamforming in (18) and (27), respectively, the improvement from beamforming is characterized by the factor $(1+\sum_{k=1}^{M-1}\sum_{p=1}^{k}\frac{p!}{k!}[-\delta]^{p}\Upsilon_{k,p})$. Indeed, one can numerically check that this factor is exactly the same as $\frac{\Gamma(M+\delta)}{\Gamma(1+\delta)\Gamma(M)}$.

V. Numerical Results

In this section, we present numerical results to investigate the impact of eavesdropper collusion on secure connectivity as well as the connectivity improvement from multi-antenna transmissions.

Fig. 1 compares P_{n} for both non-colluding eavesdroppers and colluding eavesdroppers with single antenna transmission. We see that the effect of collusion is significant at low connectivity. For example, the required eavesdropper density with colluding eavesdroppers is 65% of the required eavesdropper density with non-colluding eavesdroppers for a target $P_{\mathrm{n}} = 0.1$. Therefore, for the eavesdropper design targeting a low level of connectivity, having colluding eavesdroppers significantly reduces the required number of eavesdroppers. We have observed the same trend for multi-antenna transmission and hence the result is omitted for brevity. Furthermore, comparing N_{avg} in (12) and (18), we see that N_{avg} in the colluding case is a factor of $\Gamma(1+\delta)\Gamma(1-\delta)$ smaller than that in the non-colluding case. For example, this factor equals 1.57 for path loss exponent of $\alpha = 4$.

Fig. 2 shows the improvement in P_{n} from multi-antenna transmissions in the presence of non-colluding eavesdroppers. For directional antennas, the parameters of the simplified antenna beam model, ω and ν, are determined by preserving the first- and second-order moments of the beam pattern of a UCA. We see that the use of multiple transmit antennas significantly improves the connectivity even with $M = 2$. For example, when the design of secure network targets a high connectivity level of $P_{\mathrm{n}} = 0.9$, the use of a directional antenna and eigen-beamforming with $M = 2$ require 26% and 45% fewer legitimate nodes, respectively, compared to single antenna transmission. When M increases to 8, the reductions in the number of required nodes are 64% and 77%.

VI. Conclusion

This letter studied the local connectivity of wireless networks with physical-layer security constraints in fading channels. We demonstrated a significant connectivity improvement from multi-antenna transmission even with only two antennas. Furthermore, we quantified the connectivity degradation from eavesdropper collusion and showed that it is significant in the low connectivity regime. Future work could extend these results from local to global connectivity.

References

[1] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. 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] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 41st Annual Conf. on Inform. Sciences and Syst. (CISS)*, Baltimore, MD, Mar. 2007, pp. 905–910.

[4] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Nice, France, June 2007, pp. 2466–2470.

[5] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Toronto, Canada, July 2008, pp. 524–528.

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

[7] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," submitted. Available at http://arxiv.org/abs/0908.0898.

[8] Y. Liang, H. V. Poor, and L. Ying, "Secrecy throughput of MANETs with malicious nodes," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Seoul, Korea, June 2009, pp. 1189–1193.

[9] P. C. Pinto, J. Barros, and M. Z. Win, "Wireless physical-layer security: the case of colluding eavesdroppers," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Seoul, Korea, June 2009, pp. 2442–2446.

[10] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Toronto, Canada, July 2008, pp. 539–543.

[11] P. C. Pinto, J. Barros, and M. Z. Win, "Physical-layer security in stochastic wireless networks," in *Proc. IEEE Int. Conf. Commun. Syst. (ICCS)*, Guangzhou, China, Nov. 2008, pp. 974–979.

[12] ——, "Secure communication in stochastic wireless networks," submitted. Available at http://arxiv.org/abs/1001.3697.

[13] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank, "Modeling location uncertainty for eavesdroppers: a secrecy graph approach," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Austin, TX, June 2010.

[14] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[15] M. Haenggi, "On distances in uniformly random networks," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3584–3586, 2003.

[16] D. Stoyan, W. Kendall, and J. Mecke, *Stochastic Geometry and its Applications*, 2nd edition. John Wiley and Sons, 1996.

[17] J. Yu, Y. D. Yao, A. Molisch, and J. Zhang, "Performance evaluation of CDMA reverse links with imperfect beamforming in a multicell environment using a simplified beamforming model," *IEEE Trans. Veh. Technol.*, vol. 55, no. 3, pp. 1019–1031, 2006.

[18] F. Baccelli, B. Błaszczyszyn, and P. Mühlethaler, "An ALOHA protocol for multihop mobile wireless networks," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 421–436, Feb. 2006.

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

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