PHYSICAL-LAYER SECRECY OF MIMO COMMUNICATIONS IN THE PRESENCE OF A POISSON RANDOM FIELD OF EAVESDROPPERS

Mounir Ghogho

University of Leeds, United Kingdom
International University of Rabat, Morocco
m.ghogho@ieee.org

Ananthram Swami

Army Research Lab, USA

a.swami@ieee.org

ABSTRACT

This paper presents a probabilistic framework for physical layer secrecy of MIMO communications when the eavesdroppers channels and locations are unknown and modeled by Rayleigh fading and a Poisson point process, respectively. We first quantify the gain in probability of secrecy when using beamforming. Then, we study the case where, in addition to beamforming, artificial noise generation is employed to confuse the eavesdroppers.

I. INTRODUCTION

There has been increasing interest in secrecy guarantees offered by exploiting characteristics of the physical layer, as an alternative to or an augmentation of the traditional, but computationally demanding, cryptography-based security. Security or secrecy in a wireless channel is a harder problem than in the wired case due to the lack of specific ingress and egress points. If the state of the channel to the eavesdroppers is known, then secrecy can be guaranteed in an information-theoretic sense if the communication rate is below the so-called *secrecy capacity*, which essentially is non-zero if the received signal-to-noise ratios (SNR) at the eavesdroppers are lower than that at the legitimate receiver [1]. Secrecy has been improved through beamforming in MIMO systems [2] and artificial noise generation [3], [4]. Multiuser diversity has also been used for noise generation [5]. Stochastic geometry tools have been exploited to study the secrecy of large random networks [6], [7], where the *secrecy graph* was defined and connectivity was studied. In most of the above approaches, the locations or the channel state information of the eavesdroppers are assumed known, which is not realistic in the case of purely passive eavesdroppers. In this paper, we use stochastic geometry tools to develop a statistical framework for secrecy when the locations and channels state information of the eavesdroppers are random and unknown, and when both legitimate users and eavesdroppers may have multiple antennas.

II. NETWORK AND SIGNAL MODELS

In this section, we first present the models for the legitime and eavesdroppers nodes. Then, we present the model for the received signal-to-noise ratio in the presence of transmit beamforming at the legitimate transmitters and receive beamforming at both legitimate receivers and eavesdroppers. Finally, we introduce a probabilistic framework for secrecy. We focus on two-dimensional networks; extensions to higher-dimensions are possible.

II-A. Poisson random field of eavesdroppers

Let $\psi = \{e_i\}_{i=1}^{\infty} \subset \mathbb{R}^2$ denote the locations of the eavesdroppers. The positions of the eavesdroppers are assumed *unknown* to the legitimate nodes and are thus modeled as randomly distributed according to a Poisson point process (PPP) with density λ_e, i.e., the probability of finding k eavesdroppers in $\mathcal{A} \subset \mathbb{R}^2$ is given by the Poisson distribution

$$\mathbb{P}[k \text{ nodes in } \mathcal{A}] = e^{-\lambda_e |\mathcal{A}|} \frac{(\lambda_e |\mathcal{A}|)^k}{k!}$$

where $|\mathcal{A}|$ denotes the area of $\mathcal{A}$. For example a density λ_e of 0.001 corresponds to an average of 40 eavesdroppers in an area of 200m$\times$200m.

II-B. Wireless propagation and beamforming

We assume that the transmitter and receiver are equipped with N_t and N_r antennas, respectively, and the eavesdroppers with N_e antennas. Let $\mathbf{s}$ denote the transmitted signal and $\mathbf{u}$ and $\mathbf{v}_k$ the signal received at the legitimate receiver and the kth eavesdropper respectively, which are modeled as

$$\mathbf{u} = \mathbf{H}\mathbf{s} + \mathbf{n} \quad (1)$$

$$\mathbf{v}_k = \mathbf{H}_k\mathbf{s} + \mathbf{n}_k \quad (2)$$

where $\mathbf{H}$ and $\mathbf{H}_k$ are $(N_r \times N_t)$ and $(N_e \times N_t)$ channel matrices, and $\mathbf{n}$ and $\mathbf{n}_k$ are mutually independent zero-mean complex Gaussian noise vectors with covariances $\sigma^2\mathbf{I}$ and $\sigma_e^2\mathbf{I}$, respectively. To include geometric information, we model these matrices as

$$\mathbf{H} = r^{-\frac{\alpha}{2}}\tilde{\mathbf{H}} \quad (3)$$

$$\mathbf{H}_k = r_k^{-\frac{\alpha}{2}}\tilde{\mathbf{H}}_k \quad (4)$$

where α is the path loss exponent ($\alpha \geq 2$), r (resp. r_k) is the distance between the legitimate transmitter and receiver

978-1-61284-955-3/11/$26.00 ©2011 IEEE

(resp. kth eavesdropper), and $\tilde{\mathbf{H}}$ and $\tilde{\mathbf{H}}_k$ are fading channel matrices which are independent of the communication range.

Let $\mathbf{C}_s = \mathbb{E}\left\{\mathbf{s}\mathbf{s}^H\right\}$ denote the covariance matrix of $\mathbf{s}$ and let P denote the transmit power, i.e., $\mathrm{Tr}\left\{\mathbf{C}_s\right\} = P$. Consider beamforming of a single data stream, [1] and assuming that a fraction of P is used to transmit artificial noise to confuse the eavesdroppers [3], [4], we model $\mathbf{s}$ as

$$\mathbf{s} = \sqrt{(1-\epsilon)P}\ \mathbf{t}\ d + \sqrt{\epsilon P}\ \boldsymbol{\eta} \tag{5}$$

where $0 \leq \epsilon < 1$, $\mathbf{t}$ is a $(N_t \times 1)$ beamforming vector ($\|\mathbf{t}\| = 1$), d is the scalar information symbol ($\mathbb{E}\left\{|d|^2\right\} = 1$), $\boldsymbol{\eta}$ is an $(N_t \times 1)$ noise vector which is orthogonal to $\mathbf{t}$, i.e., $\mathbf{t}^H\boldsymbol{\eta} = 0$, with covariance matrix $\mathbf{C}_\eta$ such that $\mathrm{Tr}\left\{\mathbf{C}_\eta\right\} = 1$.

The optimum transmit beamforming vector $\mathbf{t}$, in the sense of maximizing the receive SNR, is the principal eigenvector $\mathbf{t}_1$ of $\mathbf{H}^H\mathbf{H}$, i.e., the eigenvector corresponding to the largest eigenvalue. The legitimate receiver should set its beamforming vector to $\mathbf{w} = \mathbf{H}\mathbf{t}_1$, in order to estimate d. Hence, the SNR of the legitimate link is

$$\mathrm{SNR} = \frac{(1-\epsilon)P\ \nu_1}{\sigma^2} \tag{6}$$

where ν_1 is the largest eigenvalue of $\mathbf{H}^H\mathbf{H}$, which is also equal to $\tilde{\nu}_1 r^{-\alpha}$ with $\tilde{\nu}_1$ being the largest eigenvalue of $\tilde{\mathbf{H}}^H\tilde{\mathbf{H}}$.

Orthogonality of $\boldsymbol{\eta}$ and $\mathbf{t}_1$ implies $\boldsymbol{\eta}$ should be a linear combination of the eigenvectors vectors of $\mathbf{H}^H\mathbf{H}$ except for $\mathbf{t}_1$. Since the CSI corresponding to the eavesdroppers are not known to the transmitter, the power ϵP should be distributed equally among these eigenvectors, i.e.,

$$\boldsymbol{\eta} = \sqrt{\frac{1}{N_t - 1}} \sum_{i=2}^{N_t} \mathbf{t}_i\ \eta \tag{7}$$

where $\mathbf{t}_i$ is the ith eigenvector of $\mathbf{H}^H\mathbf{H}$, and η is a random scalar with unit variance[2]. Hence, we have that

$$\mathbf{C}_\eta = \frac{1}{N_t - 1} \sum_{i,j=2}^{N_t-1} \mathbf{t}_i\mathbf{t}_j^H \tag{8}$$

We assume the worst case scenario where the eavesdroppers know ϵ, $\mathbf{C}_\eta$ and $\mathbf{t}_1$; in order to maximize their receive SNR, the eavesdroppers should set their beamforming vectors to

$$\mathbf{w}_k = \left[(1-\epsilon)P\mathbf{H}_k\mathbf{C}_\eta\mathbf{H}_k^H + \sigma_e^2\mathbf{I}\right]^{-1}\mathbf{H}_k\mathbf{t}_1 \tag{9}$$

Hence, the receive SNR at the kth eavesdropper is

$$\mathrm{SNR}_k = (1-\epsilon)P\ \mathbf{t}_1^H\ \mathbf{H}_k^H\left[\epsilon P\mathbf{H}_k\mathbf{C}_\eta\mathbf{H}_k^H + \sigma_e^2\mathbf{I}\right]^{-1}\mathbf{H}_k\ \mathbf{t}_1 \tag{10}$$

which can also be expressed as (useful later)

$$\mathrm{SNR}_k = (1-\epsilon)P\ \mathbf{t}_1^H\ \tilde{\mathbf{H}}_k^H\left[\epsilon P\tilde{\mathbf{H}}_k\mathbf{C}_\eta\tilde{\mathbf{H}}_k^H + \sigma_e^2 r_k^\alpha\mathbf{I}\right]^{-1}\tilde{\mathbf{H}}_k\ \mathbf{t}_1 \tag{11}$$

[1] Beamforming was shown to be the optimum transmit processing for MISO channels but may not be so for MIMO channels, from the secrecy capacity point of view; see [8].

[2] η could be set to one

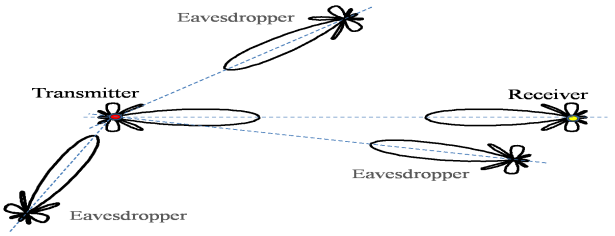

Fig. 1. Beamforming

II-C. Physical-layer secrecy

Since the CSI of the eavesdroppers are unknown, the legitimate transmitter cannot evaluate the secrecy capacity (defined in [1]) of the links. Thus, here, instead of secrecy capacity, we define the probability of secure communications (PSC) between a given transmitter and receiver.

We assume that the transmitter uses the minimum transmit power to achieve the minimum SNR required to successfully transmit the stream of information symbols to the receiver, i.e. $(1-\epsilon)P = (\sigma^2\overline{\mathrm{SNR}}/\nu_1)$. All eavesdroppers with receive SNR smaller than $\overline{\mathrm{SNR}}$ will not be able to decode the transmitted information. We therefore define the probability of secrecy of the communication link as the probability that the receive SNRs at all eavesdroppers in the network are smaller than $\overline{\mathrm{SNR}}$, i.e.

$$\mathbb{P}[\mathrm{SNR} > \mathrm{SNR}_k,\ \forall e_k \in \psi] \tag{12}$$

In the above expression, the random variables are SNR_k whose realizations change with the realizations of the Poisson point process of the eavesdroppers, ψ, and the fading channels.

An alternative approach would be to evaluate the probability that a certain data rate, c, can be transmitted securely, i.e.

$$\mathbb{P}[\log(1+\mathrm{SNR}) - \log(1+\mathrm{SNR}_e) > c] \tag{13}$$

where $\mathrm{SNR}_e = \max_{e_k\in\psi}\mathrm{SNR}_k$. If $c = 0$, the above probability of secrecy is equivalent to the one in (12). In this paper, we use the definition in (12) to simplify the analysis.

III. PROBABILISTIC FRAMEWORK OF SECRECY

Here, we will first address the case where $\epsilon = 0$, i.e. no noise generation. Then we will study the analytically more challenging $\epsilon > 0$ case. We model the H_k's as mutually independent; we also assume that their rows are mutually independent but each row is a zero-mean complex Gaussian vector with covariance $\mathbf{C}_h$. This allows for modeling of correlation between antennas at the transmitter but not at the eavesdroppers, which may be justified since the eavesdroppers want to maximize their beamforming gain. Correlation at the transmitter may be required when the transmitter is a highly elevated base station due to limited angular spread.

Since the PPP of the eavesdroppers is homogeneous and the corresponding fading coefficients are independent, the PSC for a link will only be a function of the Euclidean distances r_k, the spatial correlations of the fading channels, r and the channel realization of the legitimate link. Hence, in what follows, we use the notation $p_s(r, g)$ to denote the probability of secrecy of the legitimate link, where g is the beamforming gain which will be defined later.

III-A. Beamforming without noise generation

In this subsection, we consider the case where $\epsilon = 0$. The more general case of $\epsilon > 0$ will be addressed in the following subsection.

Proposition 1 The probability that a given transmitter can communicate securely with a given receiver, located at distance r, in the presence of a Poisson point process of eavesdroppers with density λ_e, is given by

$$p_s(r, g) = \exp\left(-\pi\ \lambda_e\ r^2\ \xi_\alpha\ \left[\frac{\sigma^2}{g\ \sigma_e^2}\right]^{\frac{2}{\alpha}}\right) \qquad (14)$$

where $\mathbf{C}_h$ is the correlation of the channel coefficients at the transmitter side,

$$g = \frac{\tilde{\nu}_1}{\mathbf{t}_1^H \mathbf{C}_h \mathbf{t}_1}$$

and

$$\xi_\alpha = \frac{2}{\alpha} \sum_{i=0}^{N_e-1} \frac{\Gamma\left(i + \frac{2}{\alpha}\right)}{i!}$$

where $\Gamma(.)$ is the Gamma function.

Proof: The kth eavesdropper will be unable to decode information if $\mathrm{SNR}_k < \mathrm{SNR}$, i.e. $\mathbf{t}_1^H \tilde{\mathbf{H}}_k^H \tilde{\mathbf{H}}_k \mathbf{t}_1 < c_k$ where $c_k = \nu_1(\sigma_e^2/\sigma^2) r_k^\alpha$. Since the rows are assumed uncorrelated, $\mathbf{t}_1^H \tilde{\mathbf{H}}_k^H \tilde{\mathbf{H}}_k$ is distributed as $(\mathbf{t}_1^H \mathbf{C}_h \mathbf{t}_1/2)\ \chi_{2N_e}$. Thus, PSC with respect to the kth eavesdropper is $1 - \Gamma(N_e, a r_k^\alpha)/\Gamma(N_e)$ where $a = g(\sigma_e^2/\sigma^2) r^{-\alpha}$, and $\Gamma(.,.)$ is the upper incomplete Gamma function, which can be expressed

$$\Gamma(N_e, a r_k^\alpha) = (N_e - 1)! e^{-a r_k^\alpha} \sum_{i=0}^{N_e-1} \frac{[a r_k^\alpha]^i}{i!}$$

The overall PSC is $\prod_{e_k \in \psi} \mathbb{P}\{\mathrm{SNR}_k < \mathrm{SNR}\}$. Since the locations of the eavesdroppers are also random, the average probability is $\mathbb{E}\left\{\prod_{e_k \in \psi} \mathbb{P}\{\mathrm{SNR}_k < \mathrm{SNR}\}\right\}$. Using the above results, this can be expressed as

$$p_s(r, g) = \mathbb{E}\left\{\prod_{e_k \in \psi} \left(1 - e^{-a r_k^\alpha} \sum_{i=0}^{N_e-1} \frac{[a r_k^\alpha]^i}{i!}\right)\right\}$$

Using Campbell' theorem, we have that

$$p_s(r, g) = \exp\left(-\lambda_e \sum_{i=0}^{N_e-1} \frac{a^i}{i!} \int_0^\infty e^{-a\rho^\alpha} \rho^{i\alpha} \Lambda_e(d\rho)\right)$$

where $\Lambda_e(d\rho) = 2\pi\rho d\rho$. Now, using the result $\int_0^\infty \rho^{m-1} \exp(-a\rho) = \Gamma(m)/a^m$, for $m > 0$, and substituting for a lead to the final result.□

The PSC expression in (14) has a nice interpretation as the probability that there are no eavesdroppers in the disc centered at the transmitter and with an effective radius $\tilde{r}$ given by

$$\tilde{r} = r \times \left[\frac{\sigma^2}{\sigma_e^2}\right]^{\frac{1}{\alpha}} \times \left[\frac{\mathbf{t}_1^H \mathbf{C}_h \mathbf{t}_1}{\tilde{\nu}_1}\right]^{\frac{1}{\alpha}} \times \left[\frac{2}{\alpha} \sum_{i=0}^{N_e-1} \frac{\Gamma\left(i + \frac{2}{\alpha}\right)}{i!}\right]^{\frac{1}{2}}.$$

Equivalently it can be written in terms of an effective eavesdropper density. The expression for $\tilde{r}$ is a product of four terms. The third-term is a measure of MIMO benefit of the legitimate link; on average, it decreases with N_t and N_r. It increases with α for values of ν_1 larger than one. The fourth term increases monotonically with the number of antennas at the eavesdropper; it counteracts the benefits of MIMO in the legitimate link. The fourth term decreases with α; the impact of increasing antennas diminishes with path loss exponent, as the exposed range decreases. With $N_e = 10$ and $\alpha = 4$, this term is less than two.

Since g/r^α is known to the transmitter[3], it can decide to transmit only when $\mathbf{H}$ is such that the PSC is higher than a certain value, say, β. It is therefore instructive to evaluate the probability of outage associated with secrecy. For $\mathbf{C}_h = \mathbf{I}$, this probability is given by

$$p_{\mathrm{out}}(\beta; r) = \mathcal{F}\left(N_e \frac{\sigma^2}{\sigma_e^2} \left[\frac{\pi \lambda_e \xi_\alpha\ r^2}{-\log \beta}\right]^{\frac{\alpha}{2}}\right)$$

where $\mathcal{F}(x)$ is the cumulative distribution function of the maximum eigenvalue of the complex Wishart matrix $\tilde{\mathbf{H}}^H \tilde{\mathbf{H}}$, which can be found in [9], [10] For single input single output (SISO) transmissions for the legitimate link, but $N_e \geq 1$, the above CDF becomes $\mathcal{F}(x) = 1 - \exp(-x)$. Figure 2 displays the outage probabilities for $\beta = 0.9$ when $\alpha = 2$. It is seen that the benefits of MIMO almost vanish if the eavesdroppers too are equipped with multiple antennas. The probability of outage when $\alpha = 4$ is displayed in Figure 3. We conclude that the secrecy performance significantly decreases with α.

III-B. Beamforming with noise generation

In this section we limit our study to the case where $N_t > N_e$. The $N_t \leq N_e$ can be analyzed along the same lines; it is omitted here because of page limitation.

Proposition 2. The probability that a given transmitter can communicate securely with a given receiver, located at distance r, in the presence of a Poisson point process of

[3]Only $\mathbf{H}$, which encompasses both path loss and fading, is needed at the transmitter. The location of the receiver is not required but it can help the transmitter set its outage probability

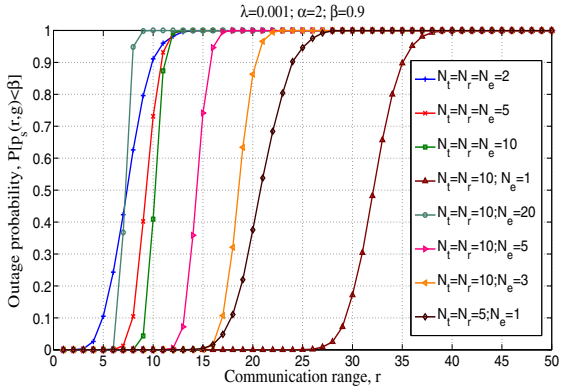

Fig. 2. Outage probability vs. r for different values of N_t, N_t and N_e, when $\lambda_e = 0.001$, $\beta = 0.9$ and $\alpha = 2$.

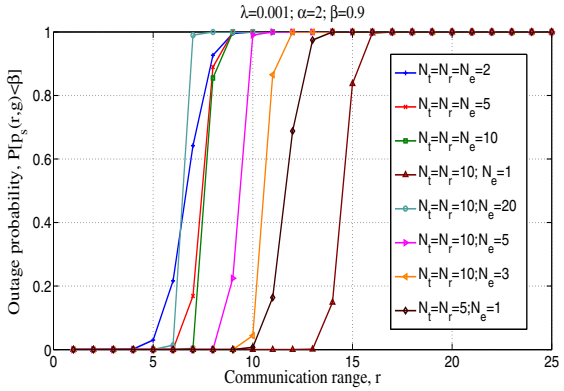

Fig. 3. Outage probability vs. r for different values of N_t, N_t and N_e, when $\lambda_e = 0.001$, $\beta = 0.9$ and $\alpha = 4$.

eavesdroppers with density λ_e, when the power of artificial noise is ϵP and $N_t > N_e$, is given by

$$p_s(r, \tilde{\nu}_1, \epsilon) = \exp\left(-\lambda_e \pi \mathbb{E}_{\tilde{\boldsymbol{\delta}}}\left\{\sum_{i=1}^{N_e} \frac{2e^{-\tilde{\delta}_i \breve{a}\ r^2}}{\alpha \breve{b}^{\frac{2}{\alpha}}} \sum_{m=0}^{N_e-1} \frac{\kappa_{i,m}^{(\tilde{\boldsymbol{\delta}})} \Gamma\left(m+\frac{2}{\alpha}\right)}{(r^2\breve{a})^{m+\frac{2}{\alpha}}}\right\}\right) \quad (15)$$

where $\breve{a} = (\epsilon P)^2 \tilde{\nu}_1/((N_t-1)\sigma^2)$, $\breve{b} = (N_t-1)\sigma_e^2/(\epsilon P)^2$, $\tilde{\boldsymbol{\delta}} = [\tilde{\delta}_1, \cdots, \tilde{\delta}_{N_e}]$ are the eigenvalues of a normalized $(N_e \times N_e)$ complex Wishart matrix with $N_t - 1$ degrees of freedom, $\mathcal{W}_{N_e}(N_t-1, \mathbf{I})$, and

$$\kappa_{i,m}^{(\tilde{\boldsymbol{\delta}})} = \frac{\bar{\kappa}_{i,m}^{(\tilde{\boldsymbol{\delta}})}}{\prod_{j \neq i}(\tilde{\delta}_j - \tilde{\delta}_i)}$$

with $\bar{\kappa}_{i,m}^{(\tilde{\boldsymbol{\delta}})}$ being the coefficient associated with x^m in the polynomial $\prod_{j=1; j\neq i}^{N_e}(\tilde{\delta}_j + x)$.

Proof: the one page proof is omitted here because of lack of space.

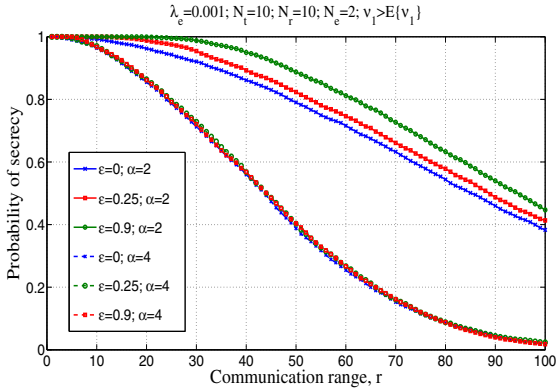

Fig. 4. PSC vs. r for different values of ϵ and α when $\lambda_e = 0.001$, $N_t = 10$, $N_r = 10$ and $N_e = 2$.

Remark 1 Although deriving the expectation wrt $\tilde{\delta}$ in Proposition 2 is intractable, it can be evaluated efficiently via simple simulations. Thus, the expression for the PSC is useful to predict performance without running Monte-Carlo simulations where a large Poisson point process is simulated and BF is performed for each eavesdropper in the network. The derived expression can be useful to optimize network parameters.

Remark 2 In the case where $N_t \leq N_e$, the last $N_t - 1 - N_e$ elements of δ are equal since the last $N_t - 1 - N_e$ elements of $\tilde{\delta}$ are zero. In this case, the expression of the CDF of the generalized χ^2 random variable $\sum_{i=1}^{N_e} \delta_i^{-1} |\tilde{y}_k(i)|^2$ is available but is rather messy; we therefore omit the results for this case due to lack of space.

Figure 4 displays the PSC versus the communications range r for different values of ϵ and α when communication takes place only when ν_1 exceeds its average value. It is seen that communication is secure with high probability (practically one) within a disc centered at the transmitter and with a radius which depends on network and signal parameters. In our example, this radius is 10m, 16m and 26m for $\epsilon = 0$, $\epsilon = 0.25$ and $\epsilon = 0.9$, respectively, when $\alpha = 2$. It is worth pointing out that the secrecy benefit of adding artificial noise decreases with α.

IV. EXTENSIONS TO FREQUENCY-SELECTIVE CHANNELS

In this section, we see how frequency-selectivity can improve secrecy. We consider a multicarrier system such as OFDM. Let M denote the number of subcarriers. Let $\mathbf{h}_{i,j} = [h_{i,j}(0), \cdots, h_{i,j}(L-1)]^T$ denote the impulse response of the channel between the ith receive antenna and jth transmit antenna, and let $\mathbf{H}(m)$ be the frequency response of the channels at the mth subcarrier. Let the channels for the eavesdroppers $\mathbf{H}_k(m)$ be similarly defined.

The SNR for each subcarrier is given by

$$\begin{aligned}\mathrm{SNR}(m) &= \frac{(1-\epsilon)P_m\ \nu_1(m)}{\sigma^2}\\ \mathrm{SNR}_k(m) &= (1-\epsilon)P_m\ \mathbf{t}_1^H(m)\ \tilde{\mathbf{H}}_k^H(m)\left[\epsilon P_m\tilde{\mathbf{H}}_k(m)\right.\\ &\quad \left.\mathbf{C}_\eta(m)\tilde{\mathbf{H}}_k^H(m)+\sigma_e^2 r_k^\alpha\mathbf{I}\right]^{-1}\tilde{\mathbf{H}}_k(m)\ \mathbf{t}_1(m)\end{aligned}$$

where P_m is the power allocated to the mth subcarrier.

Since channel state information is assumed available at the transmitter, we assume that the latter performs adaptive bit loading or adaptive power control. Without specifying the algorithm used for this, let us just assume that the best M_a subcarriers are activated and a power distribution is associated with them. The message to be transmitted is split between the activated subcarriers according to the available SNR at each subcarrier. We assume that the entire message can be decoded *if and only if* all the segments of the message transmitted over the activated subcarriers are successfully decoded. Hence, an eavesdropper will successfully detect the message iff the SNR at *all* subcarriers are at least equal to their counterparts in the legitimate link, i.e., the PSC is defined as

$$p_s(r,\mathbf{g}) = 1-\mathbb{P}[\exists e_k\,|\,\mathrm{SNR}(m)<\mathrm{SNR}_k(m);\forall\ m\in\mathcal{N}] \quad (16)$$

where $\mathcal{N}$ denotes the M_a-element set of activated subcarriers, and $\mathbf{g}$ is the corresponding beamforming gain vector.

The exact PSC in the case of frequency-selective fading channels is difficult to obtain in closed-form. Hence, we use numerical techniques to evaluate them. In our simulations, we assume that the channel taps are independent zero-mean complex Gaussian variables with variances $\sigma_\ell^2 = \mathbb{E}(|h_{i,j}(\ell)|)^2$. Figure 5 displays the averaged (over the legitimate channels) PSC when $M=64$, $\mathcal{N}$ is the set of the best $M_a=32$ subcarriers and $L=8$, for different values of N_e and ϵ. It is seen that a large gain in secrecy is obtained with frequency-selectivity if the eavesdroppers have a single antenna. This gain however rapidly decreases when $N_e>1$. This can be ascribed to the fact that the 'aggregate' channels between the transmitter and eavesdroppers and thus the SNRs at the eavesdroppers become less frequency selective when N_e increases.

V. CONCLUSIONS

In the presence of a network of eavesdroppers with unknown and random locations and channels, the secrecy benefits of MIMO may be significant only when the eavesdroppers are not equipped with multiple antennas. The benefits of generating artificial noise to confuse eavesdroppers may not be significant when the path-loss exponent is large. Frequency-selectivity improves secrecy but the gain in secrecy rapidly decreases when the eavesdroppers have multiple antennas.

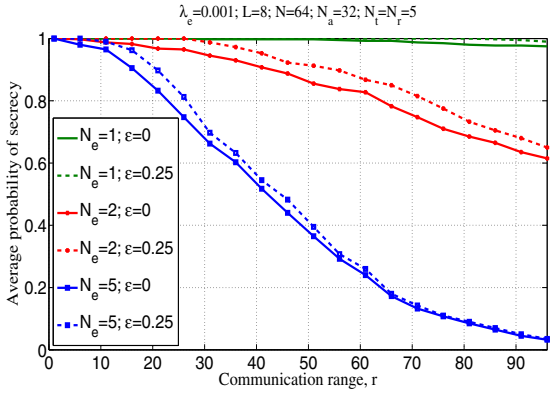

Fig. 5. PSC vs. r for different values of ϵ and N_e when $\lambda_e=0.001$, $N_t=N_r=5$, $L=8$, $M=64$ and $M_a=32$.

VI. REFERENCES

[1] A. D. Wyner, The wire-tap channel, *The Bell System Technical Journal*, vol. 54, pp. 1355-1387, 1975.

[2] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, On the Gaussian MIMO wiretap channel, in *Proc. IEEE Int. Symp. Information Theory*, Nice, France, June 2007.

[3] S. Goel and R. Negi, Guaranteeing secrecy using artificial noise, IEEE Trans. Wireless Commun., vol. 7, no. 6, pp. 2180-2189, June 2008.

[4] X. Zhou and M. R. McKay, Physical layer security with artificial noise: Secrecy capacity and optimal power allocation, Proc. Int. Conf. on Sig. Proc. and Commun. Syst., Omaha, NE, Sept. 2009.

[5] S. Vasudevan, S. Adams, D. Goeckel, Z. Ding, D. Towsley, and K. Leung. Multi-user diversity for secrecy in wireless networks. *Information Theory and Applications Workshop*, 2009.

[6] M. Haenggi, The Secrecy Graph and Some of its Properties, *IEEE International Symposium on Information Theory (ISIT'08)*, Toronto, Canada, July 2008.

[7] P. C. Pinto, J. O. Barros, and M. Z. Win, Physical-layer security in stochastic wireless networks, in *Proc. IEEE Int. Conf. on Commun. Systems*, Guangzhou, China, Nov. 2008.

[8] S. Shafiee and S. Ulukus, Achievable rates in Gaussian MISO channels with secrecy constraints, in *Proc. IEEE Int. Symp. Information Theory*, Nice, France, June 2007.

[9] A. J. Grant, Performance analysis of transmit beamforming, *IEEE Trans. Commun.*, vol. 53, no. 4, pp. 738744, Apr 2005.

[10] M. R. McKay, A. J. Grant and I. B. Collings, "Largest eigenvalue statistics of double-correlated complex Wishart matrices and MIMO-MRC," *Proc. ICASSP'06*, Toulouse, May 2006.