On Ergodic Secrecy Rate for MISO Wiretap Broadcast Channels with Opportunistic Scheduling

Minyan Pei, A. Lee Swindlehurst, *Fellow, IEEE*, Dongtang Ma, and Jibo Wei

Abstract—In this letter, we study *on-off* opportunistic beamforming for the multiuser downlink channel with a passive eavesdropper. Two opportunistic scheduling schemes exploiting multiuser diversity are investigated which require limited feedback of the effective signal-to-noise ratio (SNR) from the legitimate users. For the two scheduling schemes, we derive new closed-form expressions for the ergodic secrecy rate with *on-off* beamforming over Rayleigh fading channels. Numerical results are provided to verify our analytical results and illustrate the impact of multiuser diversity on the secrecy performance.

Index Terms—Opportunistic beamforming, multiuser scheduling, multiuser diversity, physical layer security.

I. INTRODUCTION

THE problem of broadcasting secret information over wireless links under an information-theoretic secrecy constraint has recently been considered in [1]–[3]. The work of [1] was among the first to consider the impact of multiuser diversity on secrecy systems, and proposed an opportunistic scheme that selects the user with the strongest channel at each time slot. It was shown that this approach achieves the sum capacity when the number of users is large. In [4], several user selection strategies were proposed for multiuser multiple-input multiple-output (MIMO) systems without any eavesdropper information. The use of random beamforming and opportunistic scheduling to improve secrecy was studied in [5] for the special case of a base station simultaneously serving multiple users, each associated with a separate eavesdropper.

In this work, we study the secrecy implications of opportunistic beamforming for the multiple-input single-output (MISO) broadcast channel. We consider an extension of the model in [1], where a multiple-antenna base station (BS) communicates with a large number of single-antenna users in the presence of a passive multiple-antenna eavesdropper. Assuming the BS has only statistical channel state information (CSI) for the eavesdropper channel, we investigate the ergodic secrecy rate for two opportunistic scheduling policies: 1) the user with maximal instantaneous channel quality is scheduled for communication, and 2) the proportional fair scheduling (PFS) approach [6] is applied, which serves the user whose

instantaneous-to-average channel quality is largest. We derive closed-form expressions for the ergodic secrecy rate of both policies assuming *on-off* beamforming over Rayleigh fading channels, and we analyze the asymptotic behavior of the algorithms' performance. We show that the derived analytical results exactly match the simulation results.

II. SYSTEM MODEL AND ASSUMPTIONS

We consider a MISO wiretap broadcast channel with M antennas at the BS, K mobile users each with one antenna, and an eavesdropper equipped with N antennas. We assume that the BS communicates with only a single user at a given time, and that the BS has knowledge of only the instantaneous SNR (but not the channels) of all legitimate users, and only statistical information about the eavesdropper channel. We further assume that the channels to the legitimate users are slow block Rayleigh fading, and the eavesdropper channel is stationary and ergodic within one fading block of the main channels. This modeling approach has been used by a number of authors to characterize secrecy when instantaneous information about the legitimate user's SNR is available, but only statistical CSI is present for the eavesdropper [7].

Since we assume a very limited feedback scenario with only SNR available from the legitimate users and uncorrelated Rayleigh fading at the eavesdropper, an optimized or structured transmit beamforming design is not possible. Instead, we assume the BS employs an opportunistic beamforming technique, in which during the n th block, the BS randomly chooses $\tilde{\mathbf{w}}(n)$, an $M \times 1$ vector of zero-mean unit-variance complex Gaussian random variables, which will be used to form the unit-norm transmit beamformer $\mathbf{w}(n) = \tilde{\mathbf{w}}(n)/\|\tilde{\mathbf{w}}(n)\|$. The individual users only measure their SNR, and are unaware of the actual value of $\mathbf{w}(n)$.

Thus, at time t during block n , the received signal at the k th user and the eavesdropper can be written, respectively, as follows

$$y_k(n, t) = \mathbf{h}_k(n)\mathbf{w}(n)s(t) + n_k(t), \quad (1)$$

$$\mathbf{y}_e(n, t) = \mathbf{H}_e(n, t)\mathbf{w}(n)s(t) + \mathbf{n}_e(t), \quad (2)$$

where $s(t)$ is the transmitted signal with $\mathbb{E}\{|s(t)|^2\} \leq P$, $n_k(t)$ and $\mathbf{n}_e(t)$ represent circularly symmetric zero-mean and unit-variance Gaussian noise at the k th user and eavesdropper, respectively. The channel vector between the BS and the k th user is denoted by $\mathbf{h}_k(n) \in \mathbb{C}^{1 \times M}$, whose elements are assumed to be independent and identically distributed (i.i.d.) complex Gaussian random variables with variance σ_b^2 , i.e., $\mathbf{h}_k(n) \sim \mathcal{CN}(\mathbf{0}, \sigma_b^2 \mathbf{I})$. The channels for different users are assumed to be mutually independent. $\mathbf{H}_e(n, t) \in \mathbb{C}^{N \times M}$ is

Manuscript received August 23, 2013. The associate editor coordinating the review of this letter and approving it for publication was M. Wigger.

M. Pei, D. Ma, and J. Wei are with the College of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China (e-mail: {mypei86, dongtangma, wjbhw}@nudt.edu.cn). D. Ma is the corresponding author.

A. L. Swindlehurst is with the University of California, Irvine, CA (e-mail: swindle@uci.edu).

This work was supported in part by the National Nature Science Foundation of China (NSFC) under grant 61372099 and in part by the NSFC under grant 61101098.

Digital Object Identifier 10.1109/LCOMM.2013.112513.131926

the eavesdropper's channel which is stationary and ergodic during block n with i.i.d. entries distributed as $\mathcal{CN}(0, \sigma_e^2)$.

Since $\mathbf{n}_e(t)$ is spatially white, the optimal beamformer for the eavesdropper in terms of both SNR and MMSE is maximal ratio combining (MRC) [9], and the corresponding instantaneous SNR at the eavesdropper is given by

$$\bar{\gamma}_e(n, t) = \gamma_e(n, t)P, \quad (3)$$

where $\gamma_e(n, t) = \|\mathbf{H}_e(n, t)\mathbf{w}(n)\|^2$, whose CDF is given by

$$F_{\gamma_e}(\gamma_e) = 1 - e^{-\frac{\gamma_e}{\sigma_e^2}} \sum_{i=0}^{N-1} \frac{\gamma_e^i}{i! \sigma_e^{2i}}. \quad (4)$$

We note that the BS is only aware of the statistics of the eavesdropper's channel (σ_e^2), and not its actual channel coefficients $\mathbf{H}_e(n, t)$ or instantaneous SNR $\bar{\gamma}_e(n, t)$.

At the beginning of each block n , after the BS has chosen the transmit beamformer $\mathbf{w}(n)$, the BS schedules one of the users for transmission during the block. We will study the secrecy performance of the following two scheduling policies:

1) *Maximum instantaneous SNR scheduling*: In this approach, the user with the highest instantaneous SNR is scheduled by the BS. According to (1), the instantaneous SNR of the k th user's channel is given by $\bar{\gamma}_k(n) = \gamma_k(n)P$, where $\gamma_k(n) = |\mathbf{h}_k(n)\mathbf{w}(n)|^2$. Each user needs only to measure its SNR and feed it back to the BS; neither the channel $\mathbf{h}_k(n)$ nor the beamformer $\mathbf{w}(n)$ need be known to the users. We will refer to the maximum instantaneous SNR user scheduling criterion as *M-SNR*, as defined by

$$k_1^* = \arg \max_{k=1, \dots, K} \bar{\gamma}_k(n) = \arg \max_{k=1, \dots, K} \gamma_k(n). \quad (5)$$

2) *Approximate proportional fair scheduling*: The PFS scheme [6] schedules a user when its ratio of instantaneous-to-average data rate is largest among all users. It has been shown in [8] that PFS can be approximately simplified to scheduling the user whose ratio of instantaneous-to-peak received SNR is largest. This approximation is especially good at low SNRs. Define the random variable $m_k(n)$ as the ratio of instantaneous-to-peak received SNR for user k during the n th block:

$$m_k(n) = \frac{\gamma_k(n)}{\tilde{\gamma}_k(n)}, \quad (6)$$

where $\tilde{\gamma}_k(n) = \mathbf{h}_k(n)\mathbf{h}_k^H(n)$. We will refer to this quantity as the normalized SNR for user k . This approach requires each user to be aware of its own channel $\mathbf{h}_k(n)$, which can be estimated using some training symbols at the beginning of the block. However, the users still feed back only the scalar quantity $m_k(n)$ to the BS and they do not need to know $\mathbf{w}(n)$. Under this approach, which we refer to as the *A-PFS* criterion, the user k_2^* with the largest normalized SNR is scheduled:

$$m_{k_2^*}(n) = \max_{k \in \{1, \dots, K\}} m_k(n). \quad (7)$$

III. SECRECY PERFORMANCE ANALYSIS

In this section, we derive analytical expressions for the ergodic secrecy rate of both of the above multiuser scheduling schemes over Rayleigh fading channels.

A. Preliminaries

For a given n , $\gamma_k(n)$ has the same statistics for all users, and follows an exponential distribution, i.e.,

$$f_{\gamma_k}(\gamma_k) = \frac{1}{\sigma_b^2} e^{-\frac{\gamma_k}{\sigma_b^2}}. \quad (8)$$

According to the M-SNR scheduler, the selected user's SNR $\gamma_{k_1^*}$ is the maximum of K independent identically distributed exponential random variables. Denoting $\gamma_{k_1^*}$ by γ_1 for simplicity, the CDF of the scheduled user's SNR γ_1 is given by

$$F_{\gamma_1}(\gamma_1) = (F_{\gamma_k}(\gamma_1))^K = \left(1 - e^{-\frac{\gamma_1}{\sigma_b^2}}\right)^K. \quad (9)$$

Under the A-PFS scheme, $m_k(n)$ has the same statistics for all users, and the PDF of m_k is given by [8]

$$f_{m_k}(m_k) = (M-1)(1-m_k)^{M-2} \quad (10)$$

for $0 \leq m_k \leq 1$, which is a beta distribution with parameters 1 and $M-1$, and is independent of $\mathbf{h}_k$. Since $m_{k_2^*}$ is the maximum of K dependent identically distributed random variables, the CDF of $m_{k_2^*}$ can be found to be [8]

$$F_{m_{k_2^*}}(m_{k_2^*}) = \left(1 - (1-m_{k_2^*})^{M-1}\right)^K. \quad (11)$$

Moreover, $\tilde{\gamma}_k$ is a chi-squared random variable with PDF

$$f_{\tilde{\gamma}_k}(\tilde{\gamma}_k) = \frac{\tilde{\gamma}_k^{M-1}}{\sigma_b^2 M (M-1)!} e^{-\frac{\tilde{\gamma}_k}{\sigma_b^2}}. \quad (12)$$

Since the PDFs are independent of the time and user indices, hereafter we omit reference to these indices and denote the selected user's normalized SNR $m_{k_2^*}$ by m , the selected user's peak SNR $\tilde{\gamma}_{k_2^*}$ by $\tilde{\gamma}$ and the selected user's SNR $\gamma_{k_2^*}$ by γ_2 . Thus, the CDF of the selected user's SNR γ_2 is

$$\begin{aligned} F_{\gamma_2}(\gamma_2) &= \int_{\gamma_2}^{\infty} F_m\left(\frac{\gamma_2}{\tilde{\gamma}}\right) f_{\tilde{\gamma}}(\tilde{\gamma}) d\tilde{\gamma} + F_{\gamma_2}(\gamma_2) \\ &= \sum_{k=0}^K \sum_{j=0}^{(M-1)k} (-1)^{k+j} \binom{K}{k} \binom{(M-1)k}{j} \frac{1}{(M-1)!} \\ &\quad \cdot \left(\frac{\gamma_2}{\sigma_b^2}\right)^j \Gamma\left(M-j, \frac{\gamma_2}{\sigma_b^2}\right) + 1 - e^{-\frac{\gamma_2}{\sigma_b^2}} \sum_{i=0}^{M-1} \frac{\gamma_2^i}{i! \sigma_b^{2i}}, \end{aligned} \quad (13)$$

where we apply the binomial expansion and use

$$\int_b^{\infty} x^m e^{-ax} dx = a^{-(m+1)} \Gamma(m+1, ab), \quad (14)$$

and

$$\begin{aligned} &\Gamma(m+1, ab) \\ &= \begin{cases} m! e^{-ab} \sum_{i=0}^m \frac{(ab)^i}{i!}, & m \geq 0 \\ E_1(ab), & m = -1 \\ \frac{(-1)^{-m+1}}{(-m-1)!} \left(E_1(ab) - e^{-ab} \sum_{i=0}^{-m-2} \frac{(-1)^i i!}{(ab)^{i+1}} \right), & m \leq -2 \end{cases} \end{aligned} \quad (15)$$

where $E_1(x)$ is the exponential integral of first order [10].

B. Ergodic Secrecy Rate Analysis

For each block, the main channel after user scheduling is constant while the eavesdropper's channel is fading, and thus the achievable secrecy rate is given by [11, eq. (7)]

$$R_s^{(m)} = \max_{0 \leq \lambda_m \leq 1} \underbrace{\{\log_2(1 + \lambda_m P \gamma_m) - \mathbb{E}_{\gamma_e}[\log_2(1 + \lambda_m P \gamma_e)]\}}_{R_s(\lambda_m)} \quad (16)$$

where $\gamma_m \in \{\gamma_1, \gamma_2\}$. It follows from [11, Theorem 1] that the optimal λ_m results in an *on-off* power allocation:

$$\lambda_m^* = \begin{cases} 1, & \gamma_m \geq \zeta \\ 0, & \text{otherwise} \end{cases} \quad (17)$$

with the threshold

$$\zeta = \frac{1}{P} \left[\exp \left\{ e^{\frac{1}{P\sigma_e^2}} \sum_{n=1}^N E_n \left(\frac{1}{P\sigma_e^2} \right) \right\} - 1 \right] \quad (18)$$

where $E_n(z) = \int_1^\infty e^{-zx} x^{-n} dx$, $n = 0, 1, \dots$, $\Re(z) > 0$, is the exponential integral function of order n [10]. We will let $\langle R_s^{(m)} \rangle_\zeta$ denote the secrecy rate (16) averaged over the users' channel realizations assuming the on-off threshold ζ .

Remark 1: The on-off approach can reduce the amount of required feedback since the users only need to transmit their channel gain to the transmitter when it is greater than the threshold ζ . The threshold ζ is deliberately devised so that the scheduled user can achieve a positive secrecy rate, and has the following asymptotic expression in the limit $P \rightarrow \infty$:

$$\zeta_{inf} = \lim_{P \rightarrow \infty} \zeta = \sigma_e^2 \exp \left(-\gamma + \sum_{n=1}^{N-1} \frac{1}{n} \right), \quad (19)$$

where $\gamma \approx 0.577216$ is Euler's constant. The asymptotic on-off threshold ζ_{inf} increases with σ_e^2 and N , but does not depend on the number of transmit antennas M .

Theorem 1: The ergodic secrecy rate of the MISO Rayleigh-fading wiretap broadcast channel achieved by opportunistic beamforming under the M-SNR scheduling policy with the on-off power allocation λ_1^* is given by

$$\langle R_s^{(1)} \rangle_\zeta = \log_2(e) \sum_{k=1}^K \binom{K}{k} (-1)^{k-1} e^{\frac{k}{P\sigma_b^2}} E_1 \left(\frac{(1+P\zeta)k}{P\sigma_b^2} \right). \quad (20)$$

Proof: See Appendix A. ■

Remark 2: Let $\sigma_e^2 = \alpha \sigma_b^2$. The ergodic secrecy rate under the M-SNR scheduling policy is independent of $M \geq 1$, it decreases with increasing N and α , and converges to a constant in the limit as $P \rightarrow \infty$:

$$\begin{aligned} \lim_{P \rightarrow \infty} \langle R_s^{(1)} \rangle_\zeta &= \log_2(e) \sum_{k=1}^K \binom{K}{k} (-1)^{k-1} E_1 \left(\frac{\zeta_{inf}}{\sigma_b^2} k \right) \\ &= \log_2(e) \sum_{k=1}^K \binom{K}{k} (-1)^{k-1} E_1 \left(k \cdot \alpha \exp \left(-\gamma + \sum_{n=1}^{N-1} \frac{1}{n} \right) \right). \end{aligned} \quad (21)$$

Theorem 2: The ergodic secrecy rate of the MISO Rayleigh-fading wiretap broadcast channel achieved by opportunistic beamforming under the A-PFS policy with the on-off power allocation λ_2^* is given by

Fig. 1. Average achievable secrecy rate versus the number of users with $M = 4$, $N = 1$, for different values of transmit power.

$$\begin{aligned} \langle R_s^{(2)} \rangle_\zeta &= \log_2(e) \left[\sum_{i=0}^{M-1} \frac{1}{i! P^i \sigma_b^{2i}} \int_{P\zeta}^\infty \frac{x^i e^{-x/(P\sigma_b^2)}}{1+x} dx \right. \\ &\quad - \sum_{k=0}^K \sum_{j=0}^{(M-1)k} (-1)^{k+j} \binom{K}{k} \binom{(M-1)k}{j} \\ &\quad \cdot \left. \frac{1}{(M-1)!(P\sigma_b^2)^j} \int_{P\zeta}^\infty \frac{x^j \Gamma(M-j, x/(P\sigma_b^2))}{1+x} dx \right], \end{aligned} \quad (22)$$

where

$$\begin{aligned} &\int_{P\zeta}^\infty \frac{x^i e^{-x/(P\sigma_b^2)}}{1+x} dx \\ &= e^{\frac{1}{P\sigma_b^2}} \sum_{i_k=0}^i \binom{i}{i_k} (-1)^{i-i_k} (P\sigma_b^2)^{i_k} \Gamma \left(i_k, \frac{P\zeta+1}{P\sigma_b^2} \right), \\ &\int_{P\zeta}^\infty \frac{x^j \Gamma(M-j, x/(P\sigma_b^2))}{1+x} dx \\ &= \sum_{i=0}^j \sum_{l=0}^{i-1} \binom{j}{i} \binom{i-1}{l} (-1)^{j-i} \int_{P\zeta}^\infty x^l \Gamma \left(M-j, \frac{x}{P\sigma_b^2} \right) dx. \end{aligned} \quad (23)$$

Proof: The proof is similar to that for Theorem 1, and is omitted due to space limitations. Details regarding evaluation of the integrals in Theorem 2 are given in Appendix B. ■

Remark 3: Unlike the M-SNR scheduling policy, the ergodic secrecy rate for A-PFS increases with the number of transmit antennas M , and decreases with N and $\alpha = \sigma_e^2/\sigma_b^2$. It is worth noting that as M increases, A-PFS will approach the performance of the M-SNR scheduling policy. This is due to the fact that for large M , there is little difference in the value of $\tilde{\gamma}_k$ for different users, and the two scheduling policies will both typically select the same user.

IV. NUMERICAL RESULTS

In this section, numerical results are presented to examine the impact of the number of antennas, the number of users and the average SNR on the secrecy performance. In all the figures, the solid and dashed lines represent the derived analytical expressions and the symbols show the simulation results. Each result is obtained by averaging over 10000 independent blocks.

Fig. 2. Average achievable secrecy rate as a function of transmit power P for the M-SNR scheduler with $M = 4$, $K = 40$, and $\sigma_e^2 = \alpha \sigma_b^2$, $\sigma_b^2 = 1$.

In Fig. 1, we plot the achieved average secrecy rate under both user scheduling policies versus the number of users with $M = 4$, $N = 1$ and $\sigma_e^2 = \sigma_b^2 = 1$. We see that the ergodic secrecy rate increases with the number of users K and the transmit power P . This result illustrates that scheduling algorithms optimized for conventional multiuser diversity systems can still be effective in achieving secrecy constraints. Note that the M-SNR scheme always achieves a higher average secrecy rate than A-PFS, since A-PFS ensures scheduling fairness at the cost of throughput loss.

Fig. 2 shows the achieved average secrecy rate R_s as a function of transmit power P under the M-SNR scheduling policy with $M = 4$, $K = 40$ and $\sigma_e^2 = \alpha \sigma_b^2$ for $\alpha = 0$ (no eavesdropper), 0.4 and $N = 1, 2, 3, 4$. The case without eavesdropping is used as a reference. The dotted lines are obtained using the asymptotic expression in (21). We see that the ergodic secrecy rate decreases with increasing N and α , and that the secrecy rate converges at high transmit power P to the constant value derived in Remark 2.

V. CONCLUSION

We investigated the use of multiuser scheduling on the secrecy performance of MISO downlink wiretap channels in the presence of a passive multi-antenna eavesdropper. Two opportunistic scheduling schemes were investigated; the M-SNR scheme maximizes the instantaneous SNR without considering fairness, while the A-PFS scheme ensures fairness and schedules the user with the largest normalized SNR. We analyzed the ergodic secrecy rate performance of both methods assuming an on-off power allocation policy and Rayleigh fading channels. Our derivations indicate that the ergodic secrecy rate of the M-SNR scheme is independent of the number of BS antennas M , while the performance of A-PFS improves with M and ultimately approaches that of M-SNR. While M-SNR provides a better secrecy rate than A-PFS, it does so at the price of user fairness. Our simulation examples illustrate that despite the simplicity of its implementation, opportunistic scheduling is effective in providing substantial security at the physical layer.

APPENDIX A PROOF OF THEOREM 1

Using the identity [10, eq.(3.352)], it follows from (9), (16) and (17) that

$$\begin{aligned} < R_s^{(1)} >_{\zeta} = \mathbb{E}\{R_s(1)|\gamma_1 \geq \zeta\} Pr\{\gamma_1 \geq \zeta\} \\ &= \log_2(e) \int_{\zeta}^{\infty} \ln\left(\frac{1+Px}{1+P\zeta}\right) dF_{\gamma_1}(x) \\ &= \log_2(e) \sum_{k=1}^K \binom{K}{k} (-1)^{k-1} e^{-\frac{k}{P\sigma_b^2}} E_1\left(\frac{(1+P\zeta)k}{P\sigma_b^2}\right). \end{aligned} \quad (25)$$

APPENDIX B DETAILS FOR THEOREM 2

We denote the integral in (24) by

$$I_0 = \int_{P\zeta}^{\infty} x^l \Gamma\left(M-j, \frac{x}{P\sigma_b^2}\right) dx. \quad (26)$$

Substituting (15) into (26), and using (14) and the identities [10, eq.(5.221.4), eq.(6.223)], we have that when $j \leq M-1$,

$$I_0 = (M-j-1)!(P\sigma_b^2)^{l+1} \sum_{i=0}^{M-j-1} \frac{1}{i!} \Gamma\left(i+l+1, \frac{\zeta}{\sigma_b^2}\right),$$

when $j = M$,

$$I_0 = \frac{l!(P\sigma_b^2)^{l+1}}{l+1} e^{-\frac{\zeta}{\sigma_b^2}} \sum_{k=0}^l \frac{\zeta^k}{k! \sigma_b^{2k}} - \frac{(P\zeta)^{l+1}}{l+1} E_1\left(\frac{\zeta}{\sigma_b^2}\right),$$

and when $j \geq M+1$,

$$\begin{aligned} I_0 &= \frac{(-1)^{j-M}}{(j-M)!} \int_{P\zeta}^{\infty} x^l E_1\left(\frac{x}{P\sigma_b^2}\right) dx \\ &\quad - \frac{(-1)^{j-M}}{(j-M)!} (P\sigma_b^2)^{l+1} \sum_{i=0}^{j-M-1} (-1)^i i! \Gamma\left(l-i, \frac{\zeta}{\sigma_b^2}\right). \end{aligned}$$

REFERENCES

- [1] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting with multiuser diversity," in *Proc. 2006 Allerton Conf. Commun. Contr. Computing*.
- [2] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.
- [3] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "On multiuser secrecy rate in flat fading channel," in *Proc. 2009 Military Commun. Conf.*
- [4] A. Mukherjee and A. Swindlehurst, "User selection in multiuser MIMO systems with secrecy considerations," in *Proc. 2009 Asilomar Conf. on Signals, Systems and Computers*, pp. 1479–1482.
- [5] I. Krikidis and B. Ottersten, "Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling," *IEEE Signal Process. Lett.*, vol. 20, no. 2, pp. 141–144, Feb. 2013.
- [6] P. Viswanath, D. N. C. Tse, and R. Laroia, "Opportunistic beamforming using dumb antennas," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1277–1294, Jun. 2002.
- [7] Z. Li, R. Yates, and W. Trappe, "Achieving secret communication for fast Rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 9, pp. 2792–2799, Sept. 2010.
- [8] N. Sharma and L. Ozarow, "A study of opportunism for multiple-antenna systems," *IEEE Trans. Inf. Theory*, vol. 51, no. 5, pp. 1804–1814, May 2005.
- [9] D. Bliss and S. Govindasamy, *Adaptive Wireless Communications: MIMO Channels and Networks*. Cambridge University Press, 2013.
- [10] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Academic Press, 2007.
- [11] T. V. Nguyen and H. Shin, "Power allocation and achievable secrecy rate in MISOME wiretap channels," *IEEE Commun. Lett.*, vol. 15, no. 11, pp. 1196–1198, Nov. 2011.