Secrecy Sum-Rate for Orthogonal Random Beamforming With Opportunistic Scheduling

Ioannis Krikidis, *Senior Member, IEEE*, and Björn Ottersten, *Fellow, IEEE*

***Abstract*—In this letter, we employ orthogonal random beamforming (ORBF) for the worst-case multi-user downlink scenario where each user is wiretapped by one eavesdropper. Two opportunistic scheduling techniques that ensure confidentiality by exploiting multi-user diversity are investigated; the first technique (optimal) requires limited feedback of the effective signal-to-interference ratio (SIR) from all the users and the eavesdroppers while the second technique (suboptimal) incorporates SIR knowledge from only the legitimate users. By using extreme value theory, we derive the achievable SIR-based secrecy sum-rate and the associated scaling laws for both scheduling techniques.**

***Index Terms*—Beamforming, extreme value theory, physical layer security, scaling law, secrecy rate.**

I. Introduction

THE downlink of a multiuser system, where a multiple-antenna base station (BS) serves multiple single-antenna users, is a fundamental network structure. In the seminal work of [1], the authors proved that the sum capacity of this network is achieved using dirty paper coding (DPC) which is a multi-user encoding strategy. Due to the high complexity of DPC, the investigation of efficient linear precoders was an active research area over several years. For example, the authors in [2] investigated a zero-forcing beamforming (ZFBF) that achieves the same asymptotic sum rate with DPC; in order to reduce the required feedback, an orthogonal random beamforming (ORBF) where the BS generates orthogonal random beams and schedules the users with the strongest channels for each beam, is proposed in [3]. The ORBF achieves the same sum-rate growth with the DPC and is attractive for practical implementations. The sum-rate performance of ORBF for different receiver designs is discussed in [4], using tools from the extreme value theory (EVT) [5].

On the other hand, ensuring confidentiality of the users' messages is a critical issue in the modern wireless networks. Traditionally, security is considered at the higher layers by cryptographic means; however this approach is limited by the computational capabilities of the eavesdroppers. Currently there is a particular interest to employ secrecy at the physical (PHY) layer by exploiting the randomness of the wireless channels [6]. PHY layer security is an information-theoretic approach and achieves security by using channel codes and signal processing; it has been studied in the literature for several network topologies i.e., [7], [8]. In order to tackle both interuser interference and PHY layer secrecy, linear precoders/beamformers designed for eavesdropper-free multiuser environments should be re-examined. In [9] the authors apply a ZFBF scheme for a communication system with individual secrecy rate constraints while the work in [10] investigates the optimal regularized channel inversion precoding and derives the achievable secrecy sum-rate. However, the employment of the ORBF for a network with secrecy constraints has not yet reported in the literature.

In this letter, we study the use of the ORBF scheme to a downlink system with secrecy issues. We focus on a worst-case secrecy scenario where each user is attacked by an unauthorized user and we study the scheduling problem; assignment of the available transmitted beams to a subset of users. In this case, opportunistic scheduling provides a natural protection of the users' data through the spatial multiuser diversity. We investigate two main opportunistic scheduling techniques: a) an optimal approach that requires signal-to-interference (SIR) feedback from all authorized/unauthorized users and schedules the users with the most secure channels and b) a suboptimal approach that incorporates a SIR feedback only from the legitimate users. By using EVT [4], we derive the achievable SIR-based secrecy sum-rate for both scheduling schemes as well as the associated scaling laws. We show that the suboptimal scheme is an efficient scheduling solution when feedback from the eavesdroppers is not available.

Notation: We use lowercase boldface for vectors and $(\bullet)^T$ denotes matrix transpose; the Euclidean norm of a vector is indicated by $\| \bullet \|$, $\mathbb{E}\{\bullet\}$ stands for the expectation operator and we define $[\bullet]^+ \triangleq \max(\bullet, 0)$.

II. System Model

We consider the downlink of a multi-user multiple-input multiple-output (MIMO) system consisting of one base station (BS), K legitimate users u_k (with $k = 1, \ldots, K$) and K eavesdroppers (unauthorized users) e_k. We assume a worst-case scenario where the k-th user is wiretapped by the k-th eavesdropper. The BS is equipped with $M < K$ antennas while both the users and the eavesdroppers have a single antenna. Fig. 1 schematically presents the system model. The BS applies an ORBF strategy and in each time slot it serves M selected users; to do that, it generates a random matrix $\mathbf{W} = [\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_M]$, where $\mathbf{w}_i \in \mathbb{C}^{M \times 1}$, $i = 1, \ldots, M$ are isotropic distributed random orthonormal vectors and represent the beams that are used in order to transmit the M information streams [3]. The total transmitted power is equal to P and a symmetric power allocation is assumed. The received signal at the k-th user and the k-th eavesdropper is written, respectively, as

$$y_k = \sqrt{\frac{P}{M}} \mathbf{h}_k^T \mathbf{W} \mathbf{s} + n_k,$$
$$y_{ek} = \sqrt{\frac{P}{M}} \mathbf{h}_{ek}^T \mathbf{W} \mathbf{s} + n_{ek}, \quad k = 1, \ldots, K, \tag{1}$$

Manuscript received November 03, 2012; accepted December 06, 2012. Date of publication December 20, 2012; date of current version January 04, 2013. This work was supported by the CORE project CO2SAT. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Chandra Ramabhadra Murthy.

I. Krikidis is with the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, L-1359 Luxembourg, and also with the Department of Electrical and Computer Engineering, University of Cyprus, Cyprus (e-mail: ioannis.krikidis@uni.lu).

B. Ottersten is with the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, L-1359 Luxembourg (e-mail: bjorn.ottersten@uni.lu).

Digital Object Identifier 10.1109/LSP.2012.2234109

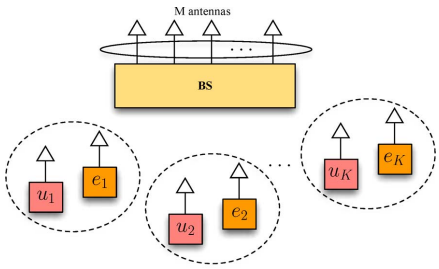

Fig. 1. MIMO downlink with M transmit antennas, $K > M$ single-antenna users and K associated single-antenna eavesdroppers.

where $\mathbf{s} \in \mathbb{C}^{M\times 1}$ is the transmitted symbol vector from the BS's antennas with $\mathbb{E}\{\|\mathbf{s}\|^2\} \leq P$; $\mathbf{h}_k, \mathbf{h}_{ek} \in \mathbb{C}^{M\times 1}$ denote the channel gain vectors to the k-th user and the k-th eavesdropper, respectively; n_k, n_{ek} denote the additive white Gaussian noise (AWGN) at the k-the user and the k-th eavesdropper, respectively. The entries of $\mathbf{h}_k, \mathbf{h}_{ek}$ as well as the noise components n_k, n_{ek} are assumed to be independent and identically distributed (i.i.d.) drawn from a complex Gaussian distribution with zero mean and unit variance (homogeneous network in terms of users' average channels [2]). We assume perfect (local) channel state information (CSI) at the users/eavesdropper but not at the BS's side. If the k-th user decodes the m-th information stream, the signal to interference plus noise ratio (SINR)/SIR at the k-th user and the associated eavesdropper can be written as

$$\Gamma_{k,m} = \frac{\left|\mathbf{h}_k^T \mathbf{w}_m\right|^2}{M/P + \sum_{i\neq m}^{M} \left|\mathbf{h}_k^T \mathbf{w}_i\right|^2} \approx \frac{\left|\mathbf{h}_k^T \mathbf{w}_m\right|^2}{\sum_{i\neq m}^{M} \left|\mathbf{h}_k^T \mathbf{w}_i\right|^2} \ (P\to\infty),$$
$$\Gamma_{ek,m} = \frac{\left|\mathbf{h}_{ek}^T \mathbf{w}_m\right|^2}{M/P + \sum_{i\neq m}^{M} \left|\mathbf{h}_{ek}^T \mathbf{w}_i\right|^2} \approx \frac{\left|\mathbf{h}_{ek}^T \mathbf{w}_m\right|^2}{\sum_{i\neq m}^{M} \left|\mathbf{h}_{ek}^T \mathbf{w}_i\right|^2} \ (P\to\infty), \tag{2}$$

where the above approximation refers to the interference limited case. The achievable secrecy rate for the k-th user decoding the m-th data stream is given by

$$\mathcal{R}_{k,m} = [\log_2(1+\Gamma_{k,m}) - \log_2(1+\Gamma_{ek,m})]^+. \tag{3}$$

For each time slot, the BS schedules M users and assigns their data to the M transmitted beams; subset beam selection and scenarios where the BS serves less than M users are beyond the scope of this paper [11]. A scheduling policy π is defined to be a mapping from each beam to a unique user with $\pi(m) = k$, if the k-th user is served by the m-th beam. The achievable secrecy sum-rate is written as

$$\mathcal{R}_s \triangleq \sum_{m=1}^{M} \mathcal{R}_{\pi(m),m}. \tag{4}$$

Given that the focus of the scheduling schemes is the achievable secrecy sum-rate and the network configuration is homogeneous, fairness issues are not discussed in this work.

III. Opportunistic Scheduling Policies

In this section, we present two scheduling policies for the problem considered with different feedback requirements.

A. Optimal Scheduling

The optimal scheduler requires feedback from all users and eavesdroppers and achieves the maximum secrecy sum-rate; it serves as a benchmark on the achievable secrecy sum-rate. At the beginning of each time slot (training period), the BS transmits a pilot sequence and each user and eavesdropper evaluate the effective SINR for each beam and report this information to the BS via feedback channels. This procedure requires that the eavesdroppers are registered (but not authorized) on the network and therefore are obligated to feed their SINRs to the BS. Based on the feedback, the BS calculates the secrecy rate for each beam at each user and assigns the m-th beam to the user with the highest secrecy rate $R_{k,m}$ according to

$$\pi_{\mathrm{OP}}(m) = \arg \max_{k\in\{1,2,\ldots,K\}} \Phi_{k,m}, \tag{5}$$

where $\Phi_{k,m} \triangleq (1+\Gamma_{k,m})/(1+\Gamma_{ek,m})$. The optimal scheduling requires $2KM$ feedback channels and therefore corresponds to a high complexity (e.g., in practice, each terminal transmits one feedback channel with M SINR indicators). It is worth noting that the probability to allocate multiple beams to the same user is small as the number of users grows and therefore the BS serves M users for large K.

B. Suboptimal Scheduling

The suboptimal scheduler selects the M served users without any information about the eavesdroppers' channels. More specifically, we assume that only the legitimate users report their SINR to the BS during the training period, while the eavesdroppers do not feed any information; the eavesdroppers may be malicious users or not registered on the network. In this case, the scheduler operates in a conventional way and assigns the m-th beam to the user with the highest SINR according to

$$\pi_{\mathrm{SO}}(m) = \arg \max_{k\in\{1,2,\ldots,K\}} \Gamma_{k,m}. \tag{6}$$

Although the above policy is optimal for conventional scenarios without eavesdropping, it becomes suboptimal for the problem under consideration. It is worth noting that each legitimate user feeds to the BS the highest SINR corresponding to its desired beam, therefore the feedback overhead is reduced to K channels [3].

IV. SIR-Based Analysis and Scaling Laws

In this section, we analyze the performance of the scheduling schemes considered in terms of average secrecy sum-rate. Particularly, we focus on the asymptotic performance for large K and P and we derive the corresponding scaling laws by using EVT.

A. Optimal Scheduling

By using high order statistics and based on Appendix A, the CDF of the random variable $\max_k \Phi_{k,m}$ is written as

$$F_{\Phi_{(K)}}(x) = [F_{\Phi}(x)]^K = \left[\frac{2x^{M-1}-1}{2x^{M-1}}\right]^K. \tag{7}$$

We know from EVT that for large K the above distribution converges to one of three distinct asymptotic distributions, the

Gumbel distribution, the Fréchet distribution, or the Weibull distribution [5]. Given that the parent distribution $F_\Phi(\cdot)$ is of the Pareto type and satisfies the condition [4]

$$\lim_{x\to\infty}\frac{1-F_\Phi(x)}{1-F_\Phi(\lambda x)}=\lambda^{M-1}\quad\text{with }\lambda>0, \tag{8}$$

the distribution $F_{\Phi_{(K)}}(\cdot)$ converges to the Fréchet distribution with a CDF given by [5]

$$\hat{F}_{\Phi_{(K)}}(\delta_K x)=\begin{cases}0, & x\le 0\\ \exp\left(-x^{-(M-1)}\right), & x>0\end{cases} \tag{9}$$

where δ_K is the solution to

$$F_\Phi(\delta_K)=1-\frac{1}{K}\Rightarrow\delta_K=\sqrt[M-1]{\frac{K}{2}}. \tag{10}$$

Therefore the corresponding Fréchet asymptotic distribution for $x>0$ is written as

$$\begin{aligned}\hat{F}_{\Phi_{(K)}}(x)&=\exp\left(-\delta_K^{M-1}x^{-(M-1)}\right)\\&=\exp\left(-\frac{K}{2}x^{-(M-1)}\right).\end{aligned} \tag{11}$$

By using the above Fréchet distribution, the average secrecy sum-rate achieved by the optimal scheduler is given by

$$\begin{aligned}\mathbb{E}\{\mathcal{R}_s^{\mathrm{OP}}\}&=\mathbb{E}\left\{\sum_{m=1}^{M}\log_2\left(\frac{1+\Gamma_{\pi_{\mathrm{OP}}(m),m}}{1+\Gamma_{e\pi_{\mathrm{OP}}(m),m}}\right)\right\}\\&=M\int_1^\infty\log_2(x)d\hat{F}_{\Phi_{(K)}}(x)\\&=\frac{M}{\ln(2)}\int_0^\infty\frac{1-\exp\left(-\frac{K}{2(x+1)^{M-1}}\right)}{x+1}dx\\&=\frac{M}{(M-1)\ln(2)}\left[\gamma+\ln\left(\frac{K}{2}\right)-E_i\left(-\frac{K}{2}\right)\right],\end{aligned} \tag{12}$$

where γ denotes the Euler's constant and $E_i(x)\triangleq\int_{-\infty}^{x}\exp(t)/t\,dt$ is the exponential integral. In the limit of large K, the average secrecy sum-rate satisfies the following scaling law

$$\mathbb{E}\{\mathcal{R}_s^{\mathrm{OP}}\}\sim\frac{M}{M-1}\log_2\left(\frac{K}{2}\right), \tag{13}$$

where $x\sim y$ indicates that $\lim_{K\to\infty}x/y=1$.

B. Suboptimal Scheduling

In the suboptimal scheduling, each selected user holds the strongest link between K links and its effective SIR (for high P) follows a CDF equal to $[F_X(x)]^K$, where $F_X(x)$ is given in Appendix A. On the other hand, a selected criterion is not applied to the eavesdroppers' links and therefore each eavesdropper (corresponding to a selected user), it has an SIR with CDF given by $F_X(x)$.

By using similar analytical steps with the optimal scheduling, we can show that for large K, the distribution $F_{X_{(K)}}(x)=[F_X(x)]^K$ asymptotically converges to a Fréchet distribution with a CDF

$$\hat{F}_{X_{(K)}}(x)=\exp\left(-[\sqrt[M-1]{K}-1]^{M-1}x^{-(M-1)}\right). \tag{14}$$

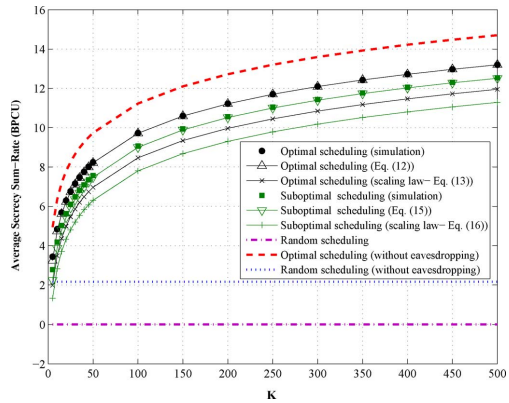

Fig. 2. Average secrecy sum-rate for the investigated opportunistic scheduling schemes versus the number of users; $M=3$ antennas and $P\to\infty$.

The average secrecy sum-rate for the suboptimal scheduling is written as

$$\begin{aligned}&\mathbb{E}\{\mathcal{R}_s^{\mathrm{SB}}\}\\&=\mathbb{E}\left\{\sum_{m=1}^{M}\log_2\left(1+\Gamma_{\pi_{\mathrm{SB}}(m),m}\right)\right\}\\&\quad-\mathbb{E}\left\{\sum_{m=1}^{M}\log_2\left(1+\Gamma_{e\pi_{\mathrm{SB}}(m),m}\right)\right\}\\&=M\int_0^\infty\log_2(1+x)d\hat{F}_{X_{(K)}}(x)\\&\quad-M\int_0^\infty\log_2(1+x)dF_X(x)\\&=\frac{M}{\ln(2)}\int_0^\infty\frac{1-\exp\left(-\frac{[\sqrt[M-1]{K}-1]^{M-1}}{x^{M-1}}\right)}{1+x}dx\\&\quad-\frac{M}{(M-1)\ln(2)}.\end{aligned} \tag{15}$$

A closed-form expression of the above integral is not trivial and therefore we evaluate it numerically (however, we note that closed-form expressions for specific values of M are available). In the limit of large K, the average secrecy sum-rate satisfies the following scaling law

$$\mathbb{E}\left\{\mathcal{R}_s^{\mathrm{SB}}\right\}\sim\frac{M}{M-1}\log_2(K)-\frac{M}{(M-1)\ln(2)}, \tag{16}$$

where the proof of the above expression is given in Appendix B.

V. Numerical Results

Computer simulations are carried out in order to evaluate the SIR performance of the investigated schemes. In Fig. 2 we plot the achieved average secrecy sum-rate in terms of bits per channel use (BPCU) for both the optimal and the suboptimal scheduling policies versus the number of users. The simulation setup follows the system model in Section II with $M=3$ antennas and $P\to\infty$ (interference limited case); the random scheduling policy as well as the case without eavesdropping (sum-rate) are used as reference curves. The first main observation is that eavesdropping reduces the achievable secrecy sum-rate; we observe a performance difference of about 1.5 BPCU for the optimal scheme with/without eavesdropping (the random selection results in a zero secrecy sum-rate due to the considered homogeneous network). On the other hand, the optimal scheme outperforms the suboptimal scheme with a gain almost equal to

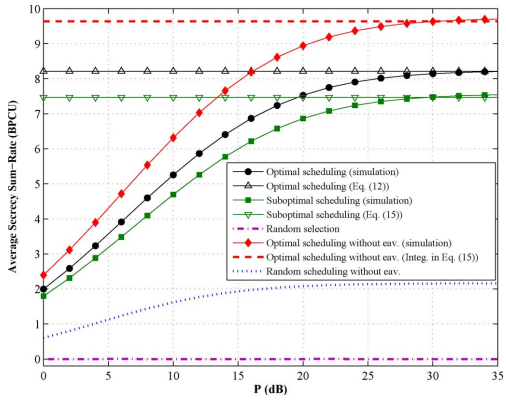

Fig. 3. Average secrecy sum-rate for the investigated opportunistic scheduling schemes versus the transmitted power P; $M = 3$ antennas and $K = 50$ users.

0.7 BPCU for large K; this limited gain introduces the suboptimal scheme as an efficient solution when feedback from the eavesdroppers is not available. As for our mathematical derivations, we can see that the expressions given in (12) and (15) match with the simulation results and therefore agree with our analysis. In addition, Fig. 2 depicts the scaling laws provided in (13) and (16); a comparison with the exact results shows that the proposed scaling laws efficiently approximate the slope of the curves.

In Fig. 3, we plot the average secrecy sum-rate versus the transmitted power P for a case with $M = 3$ antennas and $K = 50$ users. As it can be seen, the proposed SIR-based analysis perfectly matches with the simulation results for high P, while it becomes an efficient approximation for intermediate values of P.

VI. Conclusion

This letter has studied the application of the ORBF scheme to a worst-case secrecy downlink scenario where each user is attacked by one eavesdropper. Two scheduling schemes that allocate the transmitted beams to the users in an opportunistic way have been investigated; the first one is optimal and requires full SIR feedback while the second one does not have any knowledge on the eavesdroppers' links. The SIR-based achievable secrecy sum-rate and the associated scaling laws have been derived in closed form for both scheduling policies using EVT tools. We have shown that the suboptimal scheme efficiently approximates the optimal one and thus is introduced as a useful practical solution.

Appendix A
CDF of the Random Variable $\Phi_{k,m}$

Let $X_1 = \Gamma_{k,m}$, $X_2 = \Gamma_{ek,m}$, $Y_1 = 1+X_1$ and $Y_2 = 1+X_2$; for high signal-to-noise ratios ($P \to \infty$), the random variables X_1, X_2 are i.i.d. with a CDF [3]

$$F_X(x) = 1 - \frac{1}{(1+x)^{M-1}}, \tag{17}$$

and therefore the random variables Y_1, Y_2 are i.i.d. with a CDF and a PDF written as

$$F_Y(y) = F_X(y-1) = 1 - \frac{1}{y^{M-1}} \text{ with } y \geq 1, \tag{18}$$

$$f_Y(y) = \frac{M-1}{y^M}. \tag{19}$$

The CDF of the random variable $\Phi_{k,m} \triangleq Y_1/Y_2$ can be computed as

$$F_\Phi(x) = \Pr\left\{\frac{Y_1}{Y_2} \leq x\right\} = \int_1^\infty F_Y(xy) f_Y(y) dy = \frac{2x^{M-1}-1}{2x^{M-1}}. \tag{20}$$

Appendix B
Scaling Law for the Suboptimal Scheduling

By using the approximation $1 - \exp(-\beta) \approx 1$ with $\beta \geq 4$, the integral in (15) can be simplified as

$$\begin{aligned}
&\frac{M}{\ln(2)} \int_0^\infty \frac{1 - \exp\left(-\frac{[\sqrt[M-1]{K}-1]^{M-1}}{x^{M-1}}\right)}{1+x} dx \\
&\approx \frac{M}{\ln(2)} \int_0^\infty \frac{1 - \exp\left(-\frac{K}{x^{M-1}}\right)}{1+x} dx \quad \text{(for large } K\text{)} \\
&= \frac{M}{\ln(2)} \left[\int_0^{\sqrt[M-1]{\frac{K}{4}}} \frac{1}{1+x} dx \right. \\
&\quad \left. + \int_{\sqrt[M-1]{\frac{K}{4}}}^\infty \frac{1 - \exp\left(-\frac{K}{x^{M-1}}\right)}{1+x} dx \right] \qquad (21) \\
&\to \frac{M}{M-1} \log_2(K), \qquad (22)
\end{aligned}$$

where the second term in (21) becomes zero for $K \to \infty$.

References

[1] G. Caire and S. Shamai, "On the achievable throughput of a multiantenna Gaussian broadcast channel," *IEEE Trans. Inf. Theory*, vol. 49, pp. 1691–1706, Jul. 2003.

[2] T. Yoo and A. Goldsmith, "On the optimality of multiantenna broadcast scheduling using zero-forcing beamforming," *IEEE J. Sel. Areas Commun.*, vol. 24, pp. 528–541, Mar. 2006.

[3] M. Sharif and B. Hassibi, "On the capacity of MIMO broadcast channels with partial side information," *IEEE Trans. Inf. Theory*, vol. 51, pp. 506–522, Feb. 2005.

[4] M.-O. Pun, V. Koivunen, and H. V. Poor, "Performance analysis of joint opportunistic scheduling and receiver design for MIMO-SDMA Downlink systems," *IEEE Trans. Commun.*, vol. 59, pp. 268–280, Jan. 2011.

[5] E. J. Gumbel, *Stastics of Extremes*. New York: Columbia Univ. Press, 1968.

[6] M. Bloch and J. Barros, *Physical Layer Security From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge University Press, Oct. 2011.

[7] J. Li and A. P. Petropulu, "On ergodic secrecy rate for Gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, pp. 1176–1187, Apr. 2011.

[8] Z. Ding, M. Peng, and H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," *IEEE Trans. Commun.*, vol. 60, pp. 3461–3471, Nov. 2012.

[9] J. Lei, Z. Han, M. A. V. Castro, and A. Hjorungnes, "Secure satellite communications systems design with individual secrecy rate constraints," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, pp. 661–671, Sept. 2011.

[10] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. Collings, "Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding," *IEEE Trans. Commun.*, vol. 60, pp. 3472–3482, Nov. 2012.

[11] J. L. Vicario, R. Bosisio, and U. Spagnolini, "Beam selection strategies for orthogonal random beamforming in sparse networks," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 3385–3396, Sep. 2008.