Reducing Precoder/Channel Mismatch and Enhancing Secrecy in Practical MIMO Systems Using Artificial Signals

Berker Peköz, *Graduate Student Member, IEEE*, Mohammed Hafez, *Graduate Student Member, IEEE*, Selçuk Köse, *Member, IEEE*, and Hüseyin Arslan, *Fellow, IEEE*

***Abstract*— Practical multiple-input-multiple-output (MIMO) systems depend on a predefined set of precoders to provide spatial multiplexing gain. This limitation on the flexibility of the precoders affects the overall performance. Here, we propose a transmission scheme that can reduce the effect of mismatch between users' channels and precoders. The scheme uses the channel knowledge to generate an artificial signal, which realigns the predefined precoder to the actual channel. Moreover, the scheme can provide an additional level of secrecy for the communication link. The performance of the proposed scheme is evaluated using bit-error rate (BER), error vector magnitude (EVM), and secrecy capacity. The results show a significant improvement for the legitimate user, along with a degradation for the eavesdropper.**

***Index Terms*— Artificial signals, channel mismatch, communication systems, multiple-input-multiple-output (MIMO), precoding, physical-layer-security.**

I. Introduction

Multiple antenna systems have been essential part of almost all current wireless systems, and will be part of any upcoming wireless standard. multiple-input-multiple-output (MIMO) systems introduce additional degrees of freedom (DsoF) that can be utilized to provide diversity, facilitate multiplexing, or enhance secrecy. Thorough investigation proves additional DsoF introduced MIMO systems provide significant capacity gains [1].

With the expected migration towards higher frequency ranges (i.e., mmWave) in the next generation networks, another form of MIMO systems is expected to be adopted, namely, hybrid MIMO. In mmWave a larger number of antennas can be packed into smaller sizes. As promising as that sounds, that large number imposes a huge load on the system in terms of both software and hardware. Hybrid MIMO introduces a cost reduction to the system by reducing the number of used RF chains, where each subset of antennas is derived using a single RF chain [2]. Then, using only a set of phase-shifters, an analog beamformer is applied for that subset of antennas.

On another hand, in a fully digital or hybrid MIMO, signal precoding raises a computational complexity issue. The optimization of the precoders usually involve heavy computational processes. Moreover, the overhead to transfer the precoding information between the transmitter and receiver deems this approach unfeasible. In order to avoid both issues, the current wireless standards rely on codebooks [3]. The predefined codebook reduces complexity by avoiding the computational processes. Also, it reduces the overhead as the index of the used precoder is only information required to be transferred.

A downside of having a predefined codebook is the availability of such information to the public. This availability can help any malicious node in the system to receive the data correctly. This lack of information security goes against the philosophy of next generation networks. The future networks include applications with highly sensitive information (e.g., remote surgery). These applications require additional measures for information security, which brings physical-layer security to the picture. In physical layer security, the unique characteristics of the communications medium (i.e., channel) is used to protect the data from different malicious attacks (e.g., eavesdropping) [4].

To this day, the wireless community has been focusing on the design of precoders in general [5], or codebooks design specifically [6]. Moreover the designed codebooks usually have a single aim either enhanced achievable rate, better energy efficiency, or lower complexity [7]. Beside the precoding design, artificial noise (AN) insertion approaches are used to provide some security measures [8]. AN approaches try to balance the trade-off between performance and security using different noise power allocation algorithms [9].

In this work, we propose two approaches to construct artificial signals (ASs). These ASs are designed to realign the codebook-based precoders to the actual MIMO communication channel. Such a design has the following benefits:

- Easy direct implementation that avoids the power allocation optimization required by AN insertion algorithms.
- Enhanced legitimate user performance by mitigating the mismatch between codebook precoders and the actual channel.

Manuscript received February 17, 2020; revised February 26, 2020; accepted February 28, 2020. Date of publication March 3, 2020; date of current version June 10, 2020. This work was supported in part by the U.S. National Science Foundation under Grant ECCS-1609581. The associate editor coordinating the review of this letter and approving it for publication was G. Zheng. *(Corresponding author: Berker Peköz.)*

Berker Peköz is with the Department of Electrical Engineering, University of South Florida, Tampa, FL 33620 USA (e-mail: pekoz@usf.edu).

Mohammed Hafez is with Intel Corporation, Santa Clara, CA 95054 USA (e-mail: mhafez@mail.usf.edu).

Selçuk Köse is with the Department of Electrical and Computer Engineering, University of Rochester, Rochester, NY 14627 USA (e-mail: selcuk.kose@rochester.edu).

Hüseyin Arslan is with the Department of Electrical Engineering, University of South Florida, Tampa, FL 33620 USA, and also with the Department of Electrical and Electronics Engineering, Istanbul Medipol University, 34810 Istanbul, Turkey (e-mail: arslan@usf.edu).

Digital Object Identifier 10.1109/LCOMM.2020.2978058

- Additional layer of secrecy as the transmitted signal is constructed using the channel of the legitimate user.
- Keeping the same simple feedback structure conserves the adopted reduced overhead.

The rest of this letter is organized as follows: Section II provides the adopted system model. Section III introduces AS construction approaches. Gains are demonstrated in Section IV. Finally, the letter is concluded in Section V.

Notation: Throughout this letter, vectors are represented using lowercase bold-face letters, matrices are uppercase bold-face letters, and non-bold letters are used for scalars. The superscripts $(\cdot)^{\mathsf{H}}$, $(.)^{-1}$ stand for the conjugate-transpose, and inverse operations, respectively. $\mathbb{C}$ represents the complex numbers domain, and $\sim \mathcal{CN}\left(\mu, \sigma^2\right)$ corresponds to complex Gaussian distributed random variable with mean μ and variance σ^2. $\|\cdot\|$ corresponds to the Euclidean norm.

II. System Model

A transmitting device, hereinafter referred to as Alice, wishes to convey information to another device, hereinafter referred to as Bob. Alice transmits the information over N antennae while Bob receives the information over M antennae, where $M \leq N$. The communication channel between each antenna of Alice and Bob is representable in the form of one tap over the utilized bandwidth, and is time-invariant over the transmission interval. The channel coefficient between Alice's nth antenna and Bob's mth antenna is represented in the mth row and nth column of the matrix $\boldsymbol{H} \in \mathbb{C}^{M\times N}$, and all elements are assumed to be known perfectly by Alice. The information symbols that are desired to be conveyed over a transmission interval are denoted by the vector $\boldsymbol{s} \in \mathbb{C}^{M\times 1}$.

Ideally, the mutual information (MI) between the information symbols and their received counterparts is maximized if Alice precodes the symbols with $\boldsymbol{V} \in \mathbb{C}^{N\times M}$, comprising the first M columns of the unitary matrix $\check{\boldsymbol{V}} \in \mathbb{C}^{N\times N}$ and Bob combines the channel outputs with the unitary matrix $\boldsymbol{U}^{\mathsf{H}} \in \mathbb{C}^{M\times M}$, where [10]

$$\boldsymbol{H} = \boldsymbol{U}\boldsymbol{D}\check{\boldsymbol{V}}^{\mathsf{H}} \tag{1}$$

is the singular-value decomposition (SVD) of the channel coefficient matrix $\boldsymbol{H}$ [11, Sec. 3]. The received symbol estimates $\hat{\boldsymbol{s}} \in \mathbb{C}^{M\times 1}$ in the ideal case are modeled as

$$\hat{\boldsymbol{s}} = \boldsymbol{D}^{-1}\boldsymbol{U}^{\mathsf{H}}\left(\boldsymbol{H}\boldsymbol{V}\boldsymbol{s} + \boldsymbol{n}\right), \tag{2}$$

where the parenthesized content is the signal received at Bob's antennae, where elements of $\boldsymbol{n} \in \mathbb{C}^{M\times 1}$ are independent and identically distributed with $\sim \mathcal{CN}\left(0, {}^{1}\!/_{\gamma}\right)$ where γ is the overall signal-to-noise ratio (SNR) of Bob for mean channel gain.

While the scheme described in (2) maximizes capacity and is secure, in practice, precoder-combiner matrix pair $\tilde{\boldsymbol{V}}$ and $\tilde{\boldsymbol{U}}^{\mathsf{H}}$ that are imperfect approximations of the similarly denoted counterparts in 1 may be used due to reasons made clear in I. Let

$$\tilde{\boldsymbol{H}} = \sqrt{\phi}\boldsymbol{H} + \left(1 - \sqrt{\phi}\right)\boldsymbol{W} \tag{3}$$

denote the precoder-combiner induced channel $\tilde{\boldsymbol{H}} \in \mathbb{C}^{M\times N}$ where $0 \leq \phi \leq 1$ denotes the correlation between $\boldsymbol{H}$ and $\tilde{\boldsymbol{H}}$; and $\boldsymbol{W} \in \mathbb{C}^{M\times N}$ is the mismatch between them. Accordingly, (2) will hereinafter be considered as

$$\hat{\boldsymbol{s}} = \boldsymbol{D}^{-1}\tilde{\boldsymbol{U}}^{\mathsf{H}}\left(\boldsymbol{H}\tilde{\boldsymbol{V}}\boldsymbol{s} + \boldsymbol{n}\right). \tag{4}$$

The $\tilde{\boldsymbol{V}}$ and $\tilde{\boldsymbol{U}}^{\mathsf{H}}$ matrix pairs are public knowledge, and are known by a third device with $L > N$ antennae, hereinafter referred to as Eve, that does not respect the confidentiality principle and wishes to unlawfully eavesdrop the information Alice conveys to Bob. Let $\breve{\boldsymbol{H}} \in \mathbb{C}^{L\times N}$ similarly refer to the communication channel between Alice and Eve, known perfectly by Eve, and similarly denoted and sized counterparts of elements in (4) to other modeled properties. Eve estimates the information signals as

$$\breve{\boldsymbol{s}} = \tilde{\boldsymbol{V}}^{\mathsf{H}}\breve{\boldsymbol{H}}^{\dagger}\left(\breve{\boldsymbol{H}}\tilde{\boldsymbol{V}}\boldsymbol{s} + \breve{\boldsymbol{n}}\right), \tag{5}$$

wherein $\breve{\boldsymbol{H}}^{\dagger} = \breve{\boldsymbol{H}}^{\mathsf{T}}\left(\breve{\boldsymbol{H}}\breve{\boldsymbol{H}}^{\mathsf{T}}\right)^{-1}$ is the pseudo-inverse of $\breve{\boldsymbol{H}}$.

III. Artificial Signal Construction

Instead of transmitting the information symbols directly or precoding them with the nonideal precoder, an AS that maximizes the mutual information between $\boldsymbol{s}$ and $\hat{\boldsymbol{s}}$ can be designed. Zero forcing (ZF) the AS such that the least squares (LS) estimates match the information symbols perfectly results in a power-unbounded AS of which power has to be downscaled to meet the transmit power requirements, hence is not an efficient way to approach the problem. The AS minimizing the instantaneous error while efficiently utilizing the transmit power can be formulated as

$$\tilde{\boldsymbol{x}} = \arg\min_{\boldsymbol{\xi}} \left\|\boldsymbol{D}^{-1}\tilde{\boldsymbol{U}}^{\mathsf{H}}\boldsymbol{H}\tilde{\boldsymbol{V}}\boldsymbol{\xi} - \boldsymbol{s}\right\| \tag{6a}$$

$$\text{subject to } \|\boldsymbol{\xi}\| \leq \sqrt{N}, \tag{6b}$$

which is a convex optimization problem that can be solved computationally efficiently without introducing long processing delays [12].

Note that $\tilde{\boldsymbol{x}} \in \mathbb{C}^{M\times 1}$ designed in (6a) takes the precoder into account. This is particularly useful if the precoding operation is performed in the hardware level, such as hybrid beamformers [13] or other mechanical beamformers [14] such as lens array beamformers [15], and these beamformers are not to be removed from the system. Hardware limitations such as the resolutions of the phase shifters, digital to analog converters (DACs) and the analog to digital converters (ADCs) at the receiver (if known) are also reflected in the precoder and combiner matrices [16]. On the other hand, if the transmitter is capable of digital beamforming, a signal design allowing the removal of the precoder from the system is possible. Accordingly, (6a) can be further simplified to

$$\boldsymbol{x} = \arg\min_{\boldsymbol{\xi}} \left\|\boldsymbol{D}^{-1}\tilde{\boldsymbol{U}}^{\mathsf{H}}\boldsymbol{H}\boldsymbol{\xi} - \boldsymbol{s}\right\| \tag{7a}$$

$$\text{subject to } \|\boldsymbol{\xi}\| \leq \sqrt{N}, \tag{7b}$$

which also provides more freedom as $\boldsymbol{x} \in \mathbb{C}^{N\times 1}$.

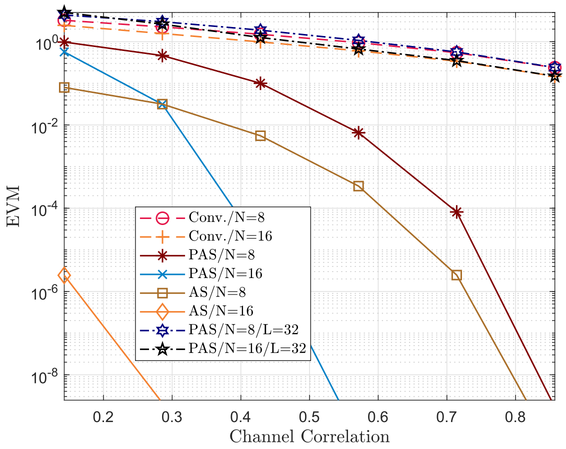

Fig. 1. EVM at various receivers in the absence of noise.

The complexity of the algorithms are not derived, but compared to the prior art, the equations involve lesser number of variables, therefore the complexity is logically expected to be lower than those already found acceptable.

IV. Results

The gains of the proposed technique are numerically verified by comparing the EVMs and uncoded BERs at Bob and Eve as well as the secrecy capacity for conventional codebook transmission, precoded AS (PAS) transmission per (6a) and direct AS transmission per (7a) as a function of ϕ and γ. $M = 4$, $N \in \{8, 16\}$, $L = 32$, $\boldsymbol{W} \sim \mathcal{CN}(0, 1)$ and information symbols comprising $\boldsymbol{s}$ are QPSK modulated regardless of SNR, which ranges from $0\,\text{dB}$ to $10\,\text{dB}$. Both (6a) and (7a) were solved using CVX, a package for specifying and solving convex programs [12], [17]. In the following figures, the curve is observed at Bob if only N is provided, whereas it is observed at Eve if L is also provided. In Fig. 1 and 2, $\phi = 1$ (precoder perfectly aligned to the channel) results are not shown as all schemes abruptly converge as expected, which occurs at a value very different than the rest of the figure.

Fig. 1 demonstrates the change in the precoding-combining quality provided by the proposed technique by comparing the EVM at various receivers in the absence of noise as a function of ϕ. It is seen that the conventional scheme does not yield a waterfall gain unless $\phi \rightarrow 1$, and doubling the number of transmitter antennae reduces EVM by about $1\,\text{dB}$. The proposed algorithms, however, present waterfalling EVM schemes at the legitimate receiver for any channel correlation and greatly outperform the conventional scheme for any nonunitary ϕ. While the number of transmitter antennae is the most significant factor in reducing EVM for both proposed algorithms, AS significantly outperforms PAS due to the increased level of flexibility for lower ϕ values while the difference narrows as ϕ increases. In the meantime, both proposed algorithms (AS not drawn due to overlapping) limit the EVM performance at Eve to that provided by the conventional schemes at the legitimate receiver for $\phi \neq 1$. The EVM at Eve for conventional transmission is mathematically insignificant for all investigated valid number of antennae combinations, hence is not shown.

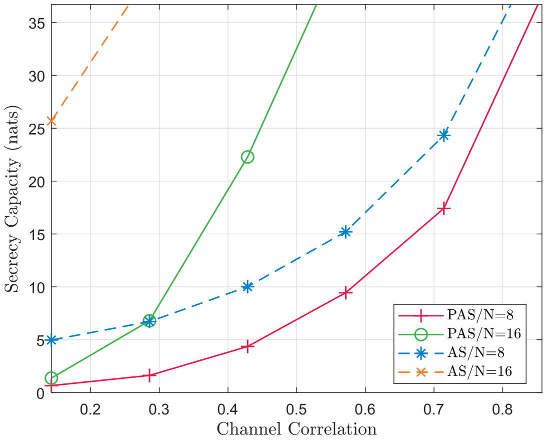

Fig. 2. Secrecy capacity between Bob and Eve.

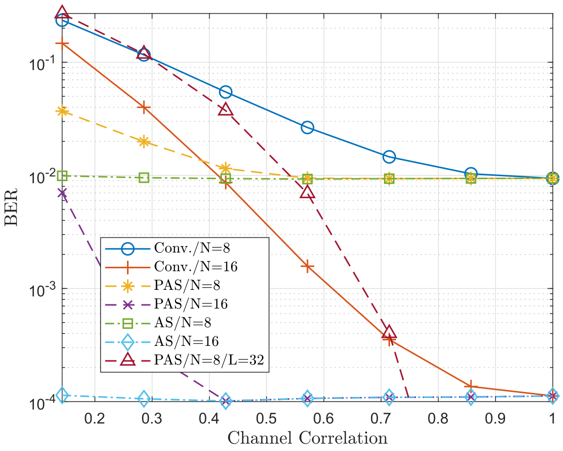

Fig. 3. BER at various receivers for SNR=$3\,\text{dB}$.

Fig. 2 shows the secrecy capacity comprising the difference of capacities between Bob and Eve as a function of ϕ in the absence of noise. The findings of Fig. 1 are confirmed, AS is more secure than PAS at lower ϕ as a result of the additional flexibility, which is later dominated by N as ϕ increases due to additional diversity. The secrecy capacity increases up to $\phi \rightarrow 85\%$ and diminishes to zero beyond higher correlations as Eve's capacity increases. The secrecy capacity of conventional transmission is zero hence is not shown.

Fig. 3 shows the BER as a function of ϕ for $3\,\text{dB}$ SNR. Under noisy reception, the performance of AS becomes independent of ϕ as the introduced flexibility allows matching the exact channel at any ϕ and is dominated by the diversity provided by the number of antennas. The performance of PAS converges to that of AS, and the convergence ϕ value decreases with increasing the number of antennas as the increased diversity allows easier matching. The performance of conventional transmission converges to that of proposed schemes as $\phi \rightarrow 1$, and the proposed schemes have significant advantage otherwise. The performance at Eve waterfalls with ϕ, confirming that ϕ is the dominating factor in noisy reception as the high diversity greatly improves SNR.

Figs. 4, and 5 show the BER as a function of SNR for $\phi = 30\%$ and $\phi = 70\%$, respectively. The theoretical limits derived in [11] for the optimally precoded and combined

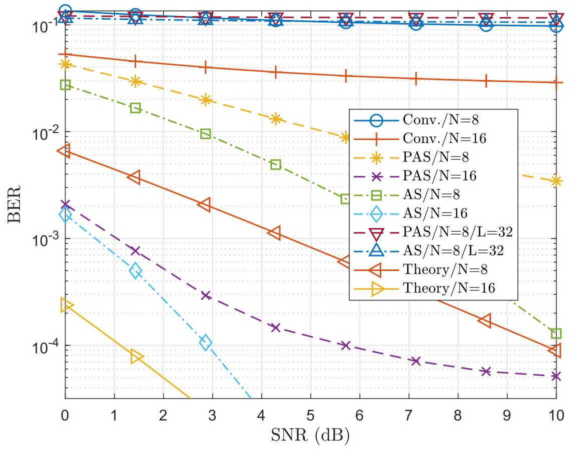

Fig. 4. BER at various receivers for $\phi = 30\%$.

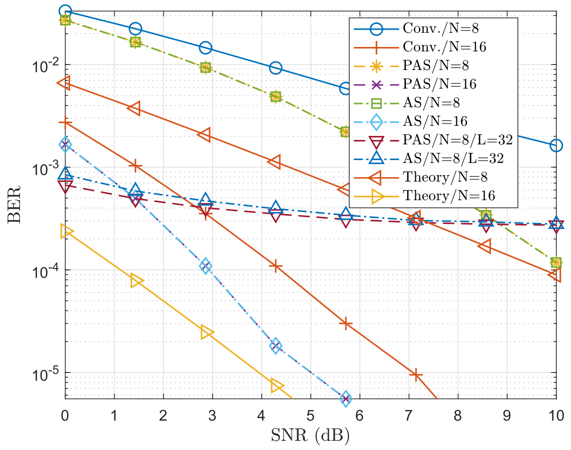

Fig. 5. BER at various receivers for $\phi = 70\%$.

transmission described by (2) are also presented for comparison. The performance of the conventional scheme is bottlenecked by ϕ independent of SNR for low ϕ, whereas the performance of PAS increases before being bottlenecked by ϕ for low ϕ values. On the other hand, the performance of AS converges to the theoretical limit with increasing SNR regardless of ϕ, a phenomenon commonly observed in fading channels with suboptimum equalization, of which optimization falls beyond the scope of this letter. The gap between theoretical limit and AS performance is independent of ϕ for $\phi > 30\%$ in accord with Fig. 3. Furthermore, the gap between PAS and AS closes as ϕ increases in accord with Fig. 3. The BER at Eve, which has 8 times the diversity of Bob, remains bottlenecked by ϕ and does not depend much on SNR for both proposed schemes at both ϕ values, showing that the security gap between the two proposed signal designs is insignificant in practical SNRs.

V. Concluding Remarks

We proposed two different approaches to construct an artificial signal, which can mitigate the mismatch between the channel and the codebook-based precoders. The constructed signal is able to reduce the BER experienced by legitimate user, while keeping eavesdropper's BER at a high level. The secrecy performance of PAS and AS are theoretically different at infinite SNR, but for practical SNR values the approaches are indifferent. If the hardware allows full digital beamforming this increases the capacity at the intended receiver, whereas the eavesdropper will keep believing a precoder is used, creating additional confusion. The performance of precoded method converges to that of nonprecoded beyond a certain correlation, of which value decreases as diversity rank increases. Even though the proposed algorithms still enhances the performance in case of low or no correlation, we suggest that it would be more beneficial to keep the operating point around 0.6 to 0.9. At that operating range, both the performance of legitimate user and the secrecy gap experience a satisfying enhancement.

References

[1] A. Goldsmith, S. A. Jafar, N. Jindal, and S. Vishwanath, "Capacity limits of MIMO channels," *IEEE J. Sel. Areas Commun.*, vol. 21, no. 5, pp. 684–702, Jun. 2003.

[2] R. W. Heath, Jr., N. Gonzalez-Prelcic, S. Rangan, W. Roh, and A. M. Sayeed, "An overview of signal processing techniques for millimeter wave MIMO systems," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 3, pp. 436–453, Apr. 2016.

[3] E. Dahlman, S. Parkvall, and J. Skold, "Multi-antenna transmission," in *5G NR: The Next Generation Wireless Access Technology*, E. Dahlman, S. Parkvall, and J. Skold, Eds. New York, NY, USA: Academic, 2018, ch. 11, pp. 225–240. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780128143230000119

[4] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. Boca Raton, FL, USA: CRC Press, 2013.

[5] F. Dong, W. Wang, and Z. Wei, "Low-complexity hybrid precoding for multi-user MmWave systems with low-resolution phase shifters," *IEEE Trans. Veh. Technol.*, vol. 68, no. 10, pp. 9774–9784, Oct. 2019.

[6] S. S. Thoota, P. Babu, and C. R. Murthy, "Codebook-based precoding and power allocation for MU-MIMO systems for sum rate maximization," *IEEE Trans. Commun.*, vol. 67, no. 12, pp. 8290–8302, Dec. 2019.

[7] X. Wang, Y. Wang, W. Ni, R. Sun, and S. Meng, "Sum rate analysis and power allocation for massive MIMO systems with mismatch channel," *IEEE Access*, vol. 6, pp. 16997–17009, 2018.

[8] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[9] S.-H. Tsai and H. V. Poor, "Power allocation for artificial-noise secure MIMO precoding systems," *IEEE Trans. Signal Process.*, vol. 62, no. 13, pp. 3479–3493, Jul. 2014.

[10] R. G. Gallager, "Waveform channels," in *Information Theory and Reliable Communication*. New York, NY, USA: Wiley, 1968, pp. 355–441. [Online]. Available: http://catalog.hathitrust.org/api/volumes/oclc/253841.html

[11] E. Telatar, "Capacity of multi-antenna Gaussian channels," *Eur. Trans. Telecommun.*, vol. 10, no. 6, pp. 585–595, Sep. 2008. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4460100604

[12] M. Grant and S. Boyd, "Graph implementations for nonsmooth convex programs," in *Recent Advances in Learning and Control* (Lecture Notes in Control and Information Sciences), V. Blondel, S. Boyd, and H. Kimura, Eds. New York, NY, USA: Springer-Verlag, 2008, pp. 95–110.

[13] X. Huang, Y. Jay Guo, and J. D. Bunton, "A hybrid adaptive antenna array," *IEEE Trans. Wireless Commun.*, vol. 9, no. 5, pp. 1770–1779, May 2010.

[14] A. A. Gheethan, M. C. Jo, R. Guldiken, and G. Mumcu, "Microfluidic based ka-band beam-scanning focal plane array," *IEEE Antennas Wireless Propag. Lett.*, vol. 12, pp. 1638–1641, 2013.

[15] G. Mumcu, M. Kacar, and J. Mendoza, "Mm-wave beam steering antenna with reduced hardware complexity using lens antenna subarrays," *IEEE Antennas Wireless Propag. Lett.*, vol. 17, no. 9, pp. 1603–1607, Sep. 2018.

[16] R. Mendez-Rial, C. Rusu, N. Gonzalez-Prelcic, and R. W. Heath, Jr., "Dictionary-free hybrid precoders and combiners for mmWave MIMO systems," in *Proc. IEEE 16th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Stockholm, Sweden, Jun. 2015, pp. 151–155.

[17] M. Grant and S. Boyd. *CVX: MATLAB Software for Disciplined Convex Programming, Version 2.1*. Accessed: Mar. 2014. [Online]. Available: http://cvxr.com/cvx