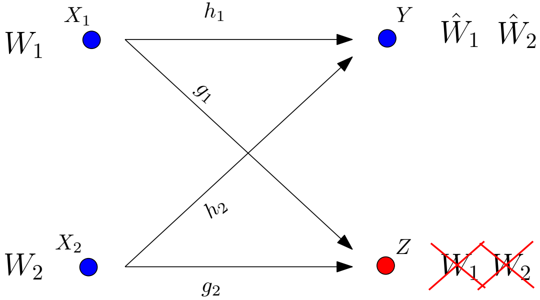
# Real Interference Alignment for Vector Channels

Pritam Mukherjee   Şennur Ulukuş

University of Maryland, College Park

# Real Interference Alignment

- Introduced by [Motahari et al., 2009].
- Effective for providing achievable schemes with fixed channel gains.
- Consider the single antenna multiple access wiretap channel:




- Optimal sum secure degrees of freedom (s.d.o.f.) $= \frac{2}{3}$.

# Real Interference Alignment: Main Ideas

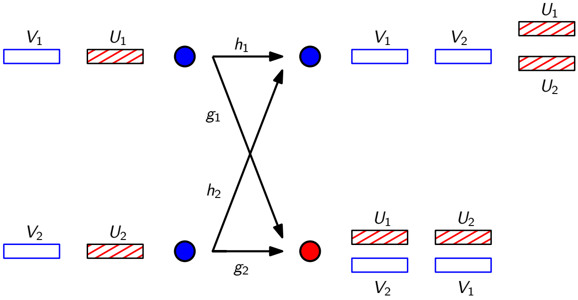
- **Encoding:** Transmitter $i$:
  - Encodes $W_i$ as *symbol stream* $V_i$.
  - $V_1$ and $V_2$ are drawn from the same PAM constellation

    $$C(a, Q) = a\{-Q, -Q+1, \ldots, 0, \ldots, Q-1, Q\}$$

    where $Q$ is a positive integer.
  - Generates *artificial noise stream* $U_i$, drawn uniformly from $C(a, Q)$.
  - Transmits:

    $$X_i = \frac{g_j}{g_i h_j} V_i + \frac{1}{h_i} U_i, \quad i \neq j$$

# Real Interference Alignment: Main Ideas (contd.)




- The channel outputs are:

$$Y = \frac{h_1 g_2}{g_1 h_2} V_1 + \frac{h_2 g_1}{g_2 h_1} V_2 + (U_1 + U_2) + N_1$$
$$Z = \frac{g_1}{h_1}(V_2 + U_1) + \frac{g_2}{h_2}(V_1 + U_2) + N_2$$

# Real Interference Alignment: Main Ideas (contd.)

- **Security:** Note that $(V_i + U_j)$ lies in $C(a, 2Q)$. Therefore,

$$
\begin{aligned}
I(W_1, W_2; Z) \leq & I(V_1, V_2; (V_2 + U_1), (V_1 + U_2)) \\
= & I(V_1; V_1 + U_2) + I(V_2; V_2 + U_1) \\
= & H(V_1 + U_2) - H(U_2) + H(V_2 + U_1) - H(U_1) \\
\leq & 2 \log \frac{4Q + 1}{2Q + 1} \\
\leq & 2 \log 2
\end{aligned}
$$

- **Decoding:** First, consider there is no noise.
  - Note that $\frac{h_1 g_2}{g_1 h_2}$, $\frac{h_2 g_1}{g_2 h_1}$ and 1 are rationally independent almost surely.
  - Therefore, $V_1$, $V_2$ and $(U_1 + U_2)$ can be decoded *without* any error.

# Real Interference Alignment: Decoding with Noise

- The received constellation is a subset of

$$\frac{h_1 g_2}{g_1 h_2} C(a, 2Q) + \frac{h_2 g_1}{g_2 h_1} C(a, 2Q) + C(a, 2Q)$$

- To bound the minimum distance, use Khintchine-Groshev theorem:
- **Theorem [Khintchine-Groshev]:** For any $\epsilon > 0$, and any integers $p_1, \ldots, p_m, q$, with $|q| \le Q$ there exists a constant $\kappa > 0$, such that

$$\left| \sum_{i=1}^{m} \alpha_i p_i + q \right| > \frac{\kappa}{Q^{m-\epsilon}}$$

for Lebesgue almost all $(\alpha_1, \ldots, \alpha_l) \in \mathbb{R}^m$.

- Therefore, the minimum distance of the constellation is:

$$d_{\min} > \frac{a\kappa}{(2Q)^{2-\epsilon}}$$

# Real Interference Alignment: Decoding (contd.)

- To facilitate decoding, we let $d_{\min}$ increase with power by setting:

$$\frac{a\kappa}{(2Q)^{2-\epsilon}} = P^{\delta}$$

  for some $\delta > 0$. Then probability of error $P_e \approx e^{-\tau d_{\min}^2} \to 0$.

- Also to satisfy the power constraint, we must have

$$aQ = \gamma P^{\frac{1}{2}}$$

- We choose

$$a \approx P^{\frac{1}{3}}, \quad Q \approx P^{\frac{1}{6}}$$

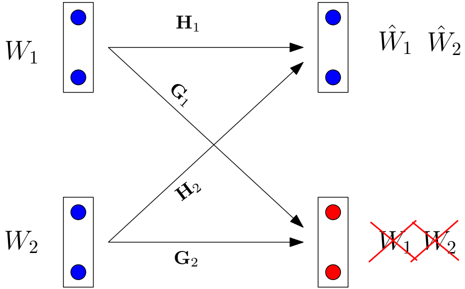
- The rate of information carried by data stream $V_i$ is

$$R_1 \approx H(V_i) = \log(2Q+1) \approx \frac{1}{3}\left(\frac{1}{2}\log P\right)$$

- S.d.o.f. of each stream $= \frac{1}{3}$; sum s.d.o.f. $= \frac{2}{3}$.

# Real Interference Alignment with Multiple Antennas

- Consider the two-antenna multiple access wiretap channel:



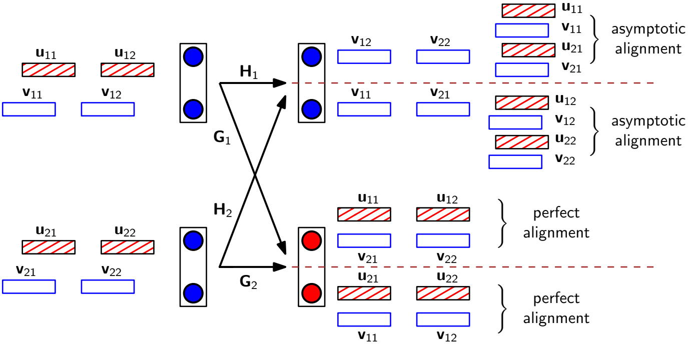

- **Question:** How to use real interference alignment here?

# Asymptotic Real Interference Alignment Approach

- Consider decoding on each antenna separately.
- Requires using asymptotic real interference alignment.
- Each data stream is broken up into **many** smaller substreams.
- Each substream is sent along a different rational dimension.
- These rational dimensions are *designed* to achieve **approximate** alignment as desired at each antenna.
- Perfect alignment as the number of substreams goes to infinity.

# Asymptotic Real Interference Alignment Scheme

- Optimal s.d.o.f. $= \frac{4}{3}$.




- Perfect alignment at the eavesdropper ensures security.
- At receiver, d.o.f. at each antenna $= \frac{2}{3}$; total s.d.o.f.$=\frac{4}{3}$.

# A Few Remarks

- The alignment structure bears little resemblance to the single antenna case.
- The design of the alignment structure is more intricate.
- In practice, asymptotic alignment requires very high SNR to be be feasible.

# Our Results: An Alternative Approach

- **Main Idea:** Use all available antennas simultaneously for decoding.
- Each data stream in the single antenna case is divided into two substreams, one for each antenna.
- Use the alignment structure of the single antenna case.
- Employ a vector generalization of the Khintchine-Groshev theorem for bounding the decoding error.

# Encoding Procedure

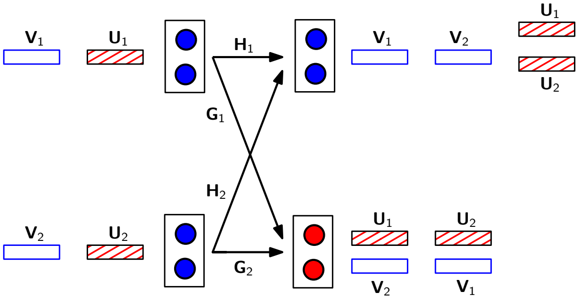
- Encode $W_i$ as a **vector** symbol stream $\mathbf{V}_i$
- $\mathbf{V}_i$ is drawn from the constellation

$$C(a, Q) \times C(a, Q)$$

- Generate **vector** artificial noise stream $\mathbf{U}_i$.
- $\mathbf{U}_i$ is drawn uniformly from $C(a, Q) \times C(a, Q)$.
- The channel input of transmitter $i$ is:

$$\mathbf{X}_i = \mathbf{G}_i^{-1}\mathbf{G}_j\mathbf{H}_j^{-1}\mathbf{V}_i + \mathbf{H}_i^{-1}\mathbf{U}_i, \quad i \neq j$$

# Alignment Structure




- The channel outputs are:

$$\mathbf{Y} = \mathbf{A}_1\mathbf{V}_1 + \mathbf{A}_2\mathbf{V}_2 + (\mathbf{U}_1 + \mathbf{U}_2)$$
$$\mathbf{Z} = \mathbf{G}_1\mathbf{H}_1^{-1}(\mathbf{V}_2 + \mathbf{U}_1) + \mathbf{G}_2\mathbf{H}_2^{-1}(\mathbf{V}_1 + \mathbf{U}_2)$$

where $\mathbf{A}_i = \mathbf{H}_i\mathbf{G}_i^{-1}\mathbf{G}_j\mathbf{H}_j^{-1}, i \neq j$

# Security and Decoding

- At the eavesdropper, the symbol stream aligns with the noise stream.

$$\begin{aligned} I(\mathbf{V}_1, \mathbf{V}_2; \mathbf{Z}) &\leq I(\mathbf{V}_1, \mathbf{V}_2; (\mathbf{V}_2 + \mathbf{U}_1), (\mathbf{V}_1 + \mathbf{U}_2)) \\ &= I(\mathbf{V}_1; \mathbf{V}_1 + \mathbf{U}_2) + I(\mathbf{V}_2; \mathbf{V}_2 + \mathbf{U}_1) \\ &\leq 4 \log 2 \end{aligned}$$

- **Decoding:** First, consider there is no noise.
- Assume $(\hat{\mathbf{V}}_1, \hat{\mathbf{V}}_2, \hat{\mathbf{U}}_1 + \hat{\mathbf{U}}_2)$ is an alternate **integer** solution. Then,

$$\mathbf{A}_1(\mathbf{V}_1 - \hat{\mathbf{V}}_1) + \mathbf{A}_2(\mathbf{V}_2 - \hat{\mathbf{V}}_2) + (\mathbf{U}_1 - \hat{\mathbf{U}}_1) + (\mathbf{U}_2 - \hat{\mathbf{U}}_2) = \mathbf{0}$$

- The elements of $\mathbf{A_i}$ are drawn from a continuous distribution.
- The rows of $\mathbf{A_i}$ are rationally independent almost surely.
- Therefore, we must have:

$$\mathbf{V}_1 = \hat{\mathbf{V}}_1, \quad \mathbf{V}_2 = \hat{\mathbf{V}}_2, \quad \mathbf{U}_1 + \mathbf{U}_2 = \hat{\mathbf{U}}_1 + \hat{\mathbf{U}}_2$$

- Unique decoding with no error is possible, if there is no noise.

# Decoding with Noise

- Wish to bound the minimum distance of the received constellation.
- Use generalized Khintchine-Groshev theorem:
- **Theorem [Generalized KG]:** Let $\omega(\boldsymbol{A})$, the Diophantine exponent for the $m \times n$ matrix $\boldsymbol{A}$, be the supremum of $\nu > 0$ for which there exists infinitely many $\boldsymbol{q} \in \mathbb{Z}^n$ such that

$$\|\boldsymbol{Aq} + \boldsymbol{p}\|_\infty < \|\boldsymbol{q}\|_\infty^{-\nu}$$

for some $\boldsymbol{p} \in \mathbb{Z}^m$. Then,

$$\omega(\boldsymbol{A}) = \frac{n}{m}$$

for Lebesgue almost every $\boldsymbol{A}$.

# Decoding with Noise (contd.)

- **Generalized KG** implies that there exists $\kappa(\epsilon) > 0$ such that

$$\|\boldsymbol{A}\boldsymbol{q} + \boldsymbol{p}\|_\infty > \kappa(\epsilon) \|\boldsymbol{q}\|_\infty^{-\frac{n}{m}-\epsilon}$$

holds for all $\boldsymbol{p} \in \mathbb{Z}^m$, $\boldsymbol{q} \in \mathbb{Z}^n$.

- The minimum distance of the received constellation is:

$$\begin{aligned} d_{\min} &= \min \left\| [\mathbf{A}_1, \mathbf{A}_2] \begin{bmatrix} \mathbf{V}_1 - \hat{\mathbf{V}}_1 \\ \mathbf{V}_2 - \hat{\mathbf{V}}_2 \end{bmatrix} + \mathbf{U}_1 + \mathbf{U}_2 - \hat{\mathbf{U}}_1 - \hat{\mathbf{U}}_2 \right\|_2 \\ &\geq \min \left\| [\mathbf{A}_1, \mathbf{A}_2] \begin{bmatrix} \mathbf{V}_1 - \hat{\mathbf{V}}_1 \\ \mathbf{V}_2 - \hat{\mathbf{V}}_2 \end{bmatrix} + \mathbf{U}_1 + \mathbf{U}_2 - \hat{\mathbf{U}}_1 - \hat{\mathbf{U}}_2 \right\|_\infty \\ &\geq \frac{a\tau}{Q^{2+\epsilon}} \end{aligned}$$

# Decoding with Noise (contd.)

- To ensure vanishing probability of error, set

$$\frac{a}{Q^2} \approx P^{\delta}$$

- To satisfy the power constraint, set

$$aQ \approx \gamma P^{\frac{1}{2}}$$

- Together, we have

$$a \approx P^{\frac{1}{3}}, \quad Q \approx P^{\frac{1}{6}}$$

- The rate of information carried in vector datastream $\mathbf{V}_i$ is

$$R \approx H(\mathbf{V}_i) = \log(2Q+1)^2 \approx \frac{2}{3}\left(\frac{1}{2}\log P\right)$$

- S.d.o.f. of each $\mathbf{V}_i = \frac{2}{3}$; sum s.d.o.f. $= \frac{4}{3}$.

# Some Remarks and Conclusions

- We introduced a new real interference alignment technique for vector channels.
- The main idea is to use **all** antenna outputs **together** for decoding, rather than separately
- We proposed an alignment scheme that is
  1. much simpler than the asymptotic alignment based scheme
  2. strongly resembles the single antenna scheme.
- We employed a vector generalization of the Khintchine-Groshev theorem for bounding decoding error.
- Similar techniques is useful for other channel models such as MIMO wiretap channels with helpers and MIMO interference channels.