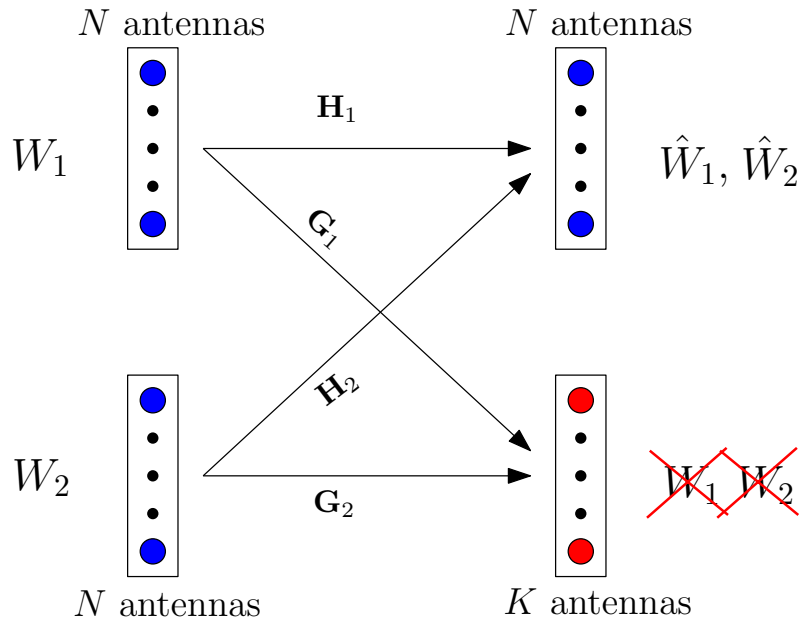
Real Interference Alignment for the MIMO Multiple Access Wiretap Channel

Pritam Mukherjee Ṣennur Ulukuṣ

University of Maryland, College Park

The MIMO Multiple Access Wiretap Channel (MAC-WT)

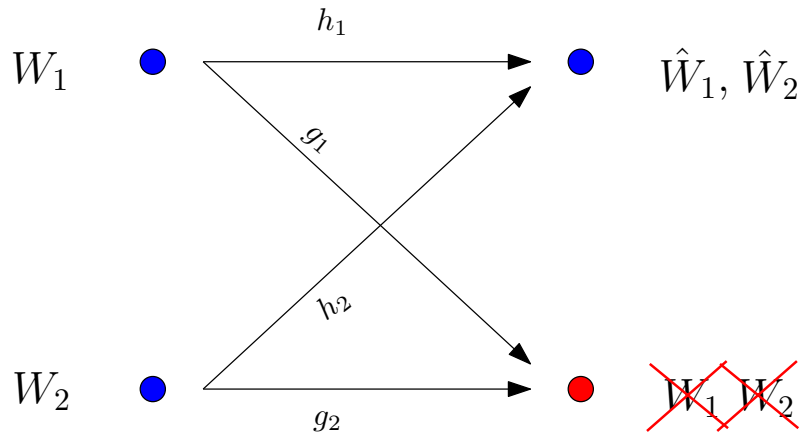
- Consider the two-user $N \times N \times N \times K$ MIMO MAC-WT:



- The channel gains are fixed across time-slots.
- All channel gains are known perfectly at every terminal.
- **Question:** What is the optimal sum secure degrees of freedom?

Prior Work: The SISO MAC-WT Channel

- For the case $N = K = 1$, i.e., the SISO MAC-WT channel:

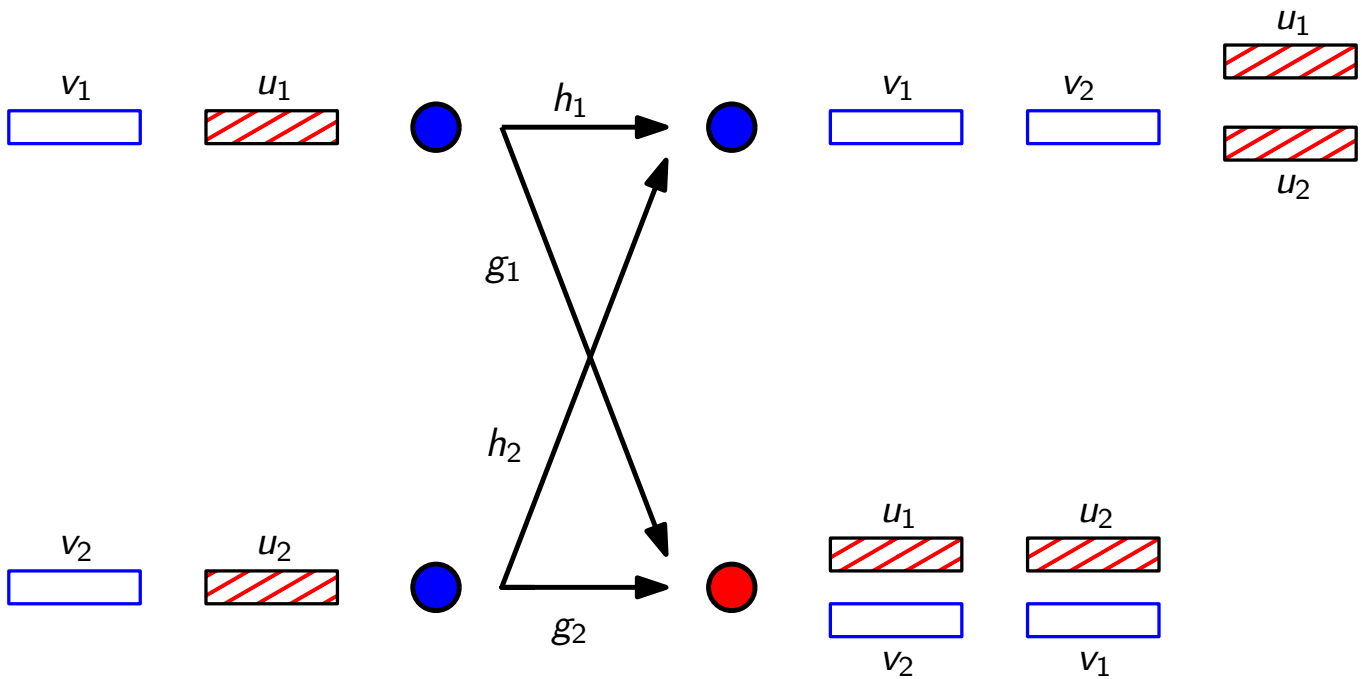


- Optimal sum s.d.o.f.[a]$= \frac{2}{3}$.
- Achievable scheme based on real interference alignment.

[a] [Xie, Ulukus, 2013]

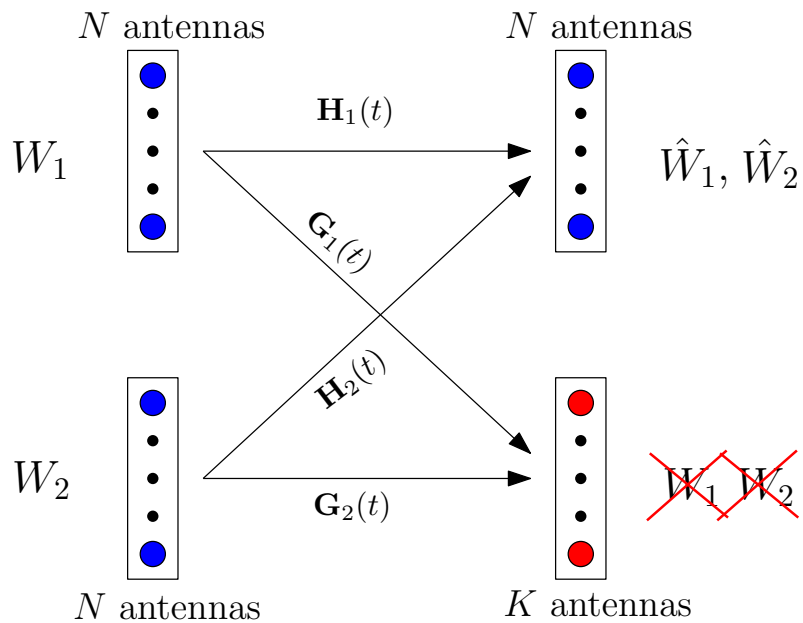
Prior Work: The SISO MAC-WT Channel (contd.)

- The alignment of signals in this case is as follows:



Prior Work: The *Fading* MIMO MAC-WT Channel

- The fading two-user $N \times N \times N \times K$ MIMO MAC-WT:



- The channel gains are i.i.d. across time slots.
- **Question:** What is the optimal sum secure degrees of freedom?

The *Fading* MIMO MAC-WT Channel (contd.)

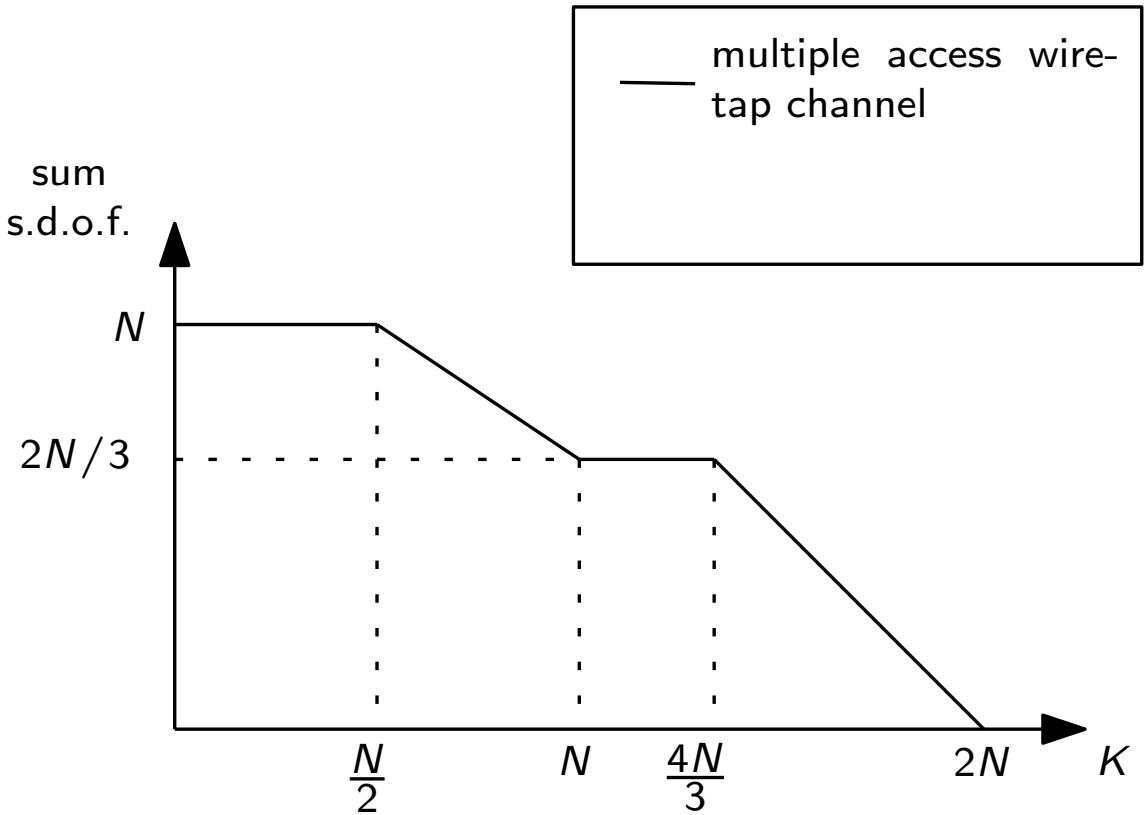
- **Theorem:** [Mukherjee, Ulukus, Asilomar 2015]: The optimal sum s.d.o.f. of the $N \times N \times N \times K$ *fading* MIMO MAC-WT is

$$d_s = \begin{cases} N, & \text{if } K \leq \frac{1}{2}N \\ \frac{2}{3}(2N-K), & \text{if } \frac{1}{2}N \leq K \leq N \\ \frac{2}{3}N, & \text{if } N \leq K \leq \frac{4}{3}N \\ 2N-K, & \text{if } \frac{4}{3}N \leq K \leq 2N \\ 0, & \text{if } K \geq 2N. \end{cases}$$

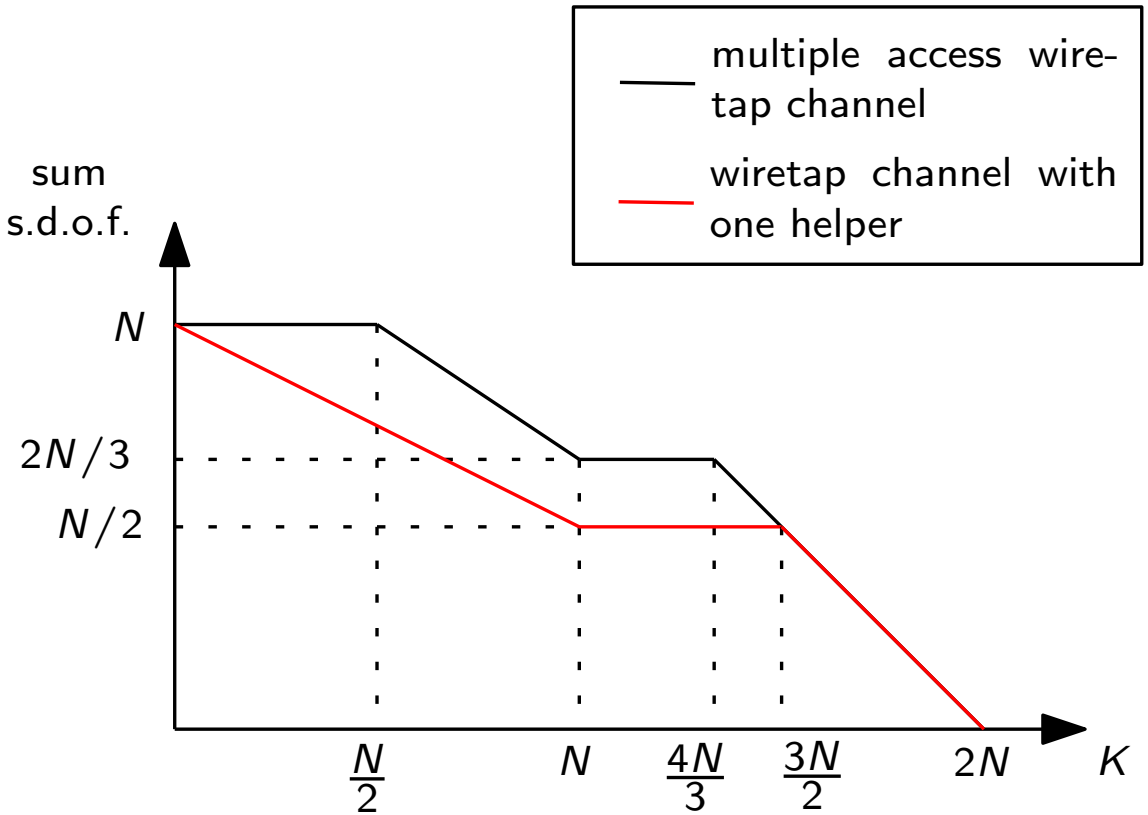
- Note that when $N = K = 1$, the optimal sum s.d.o.f.[a] $= \frac{2}{3}$.

[a] [Xie, Ulukus, 2013]

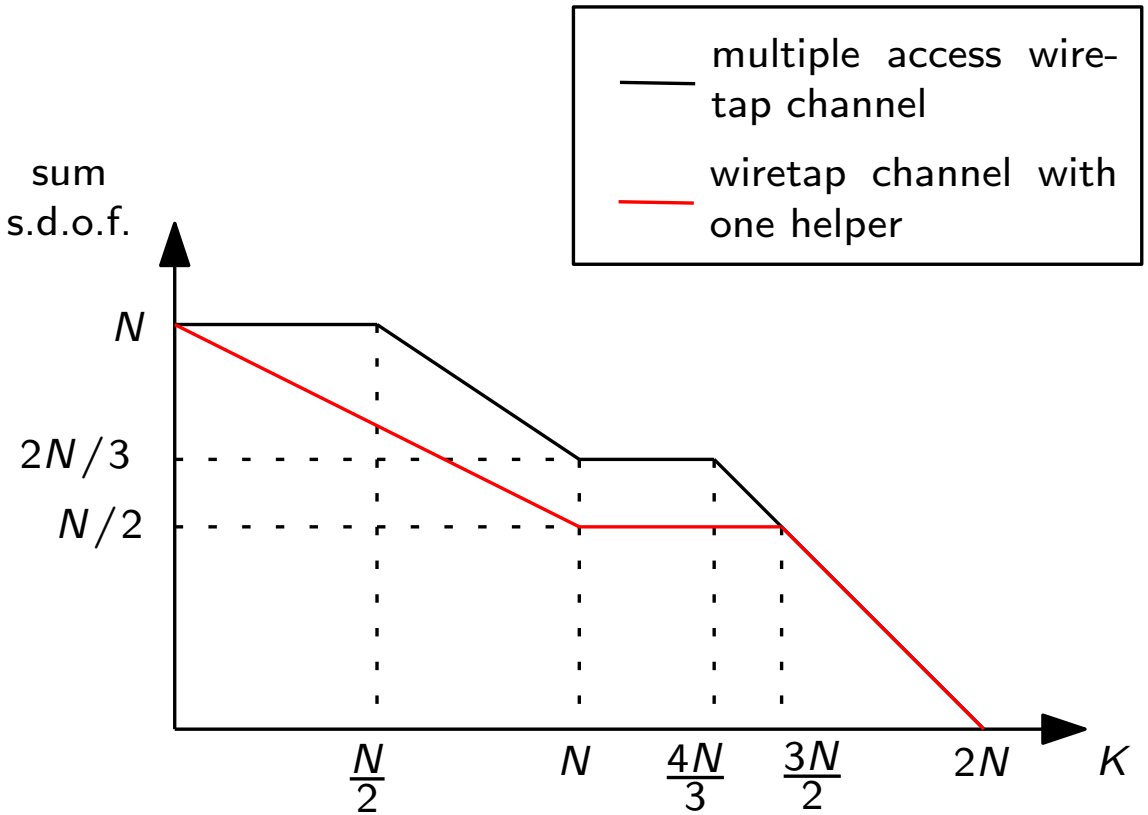
The *Fading* MIMO MAC-WT Channel (contd.)



The *Fading* MIMO MAC-WT Channel (contd.)

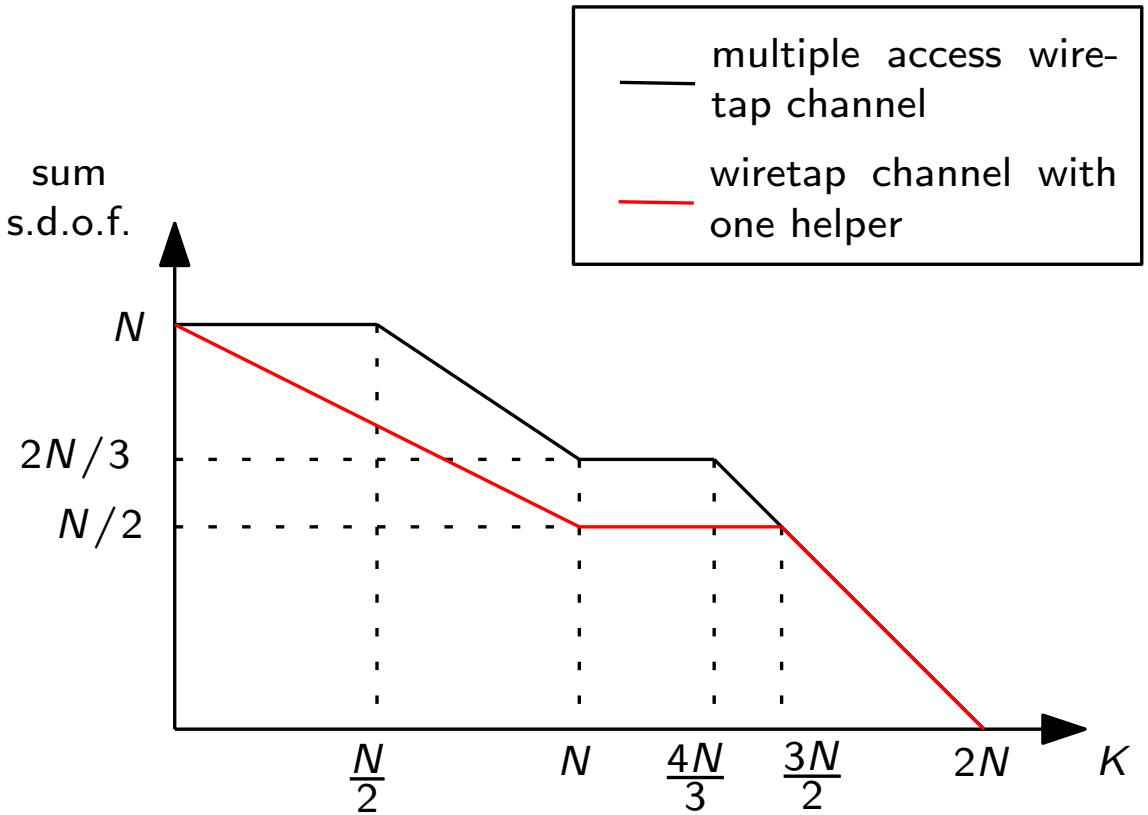


The *Fading* MIMO MAC-WT Channel (contd.)



- Converse proof holds for fixed channel gains as well.
- **Question:** Is the same s.d.o.f. achievable with fixed channel gains?

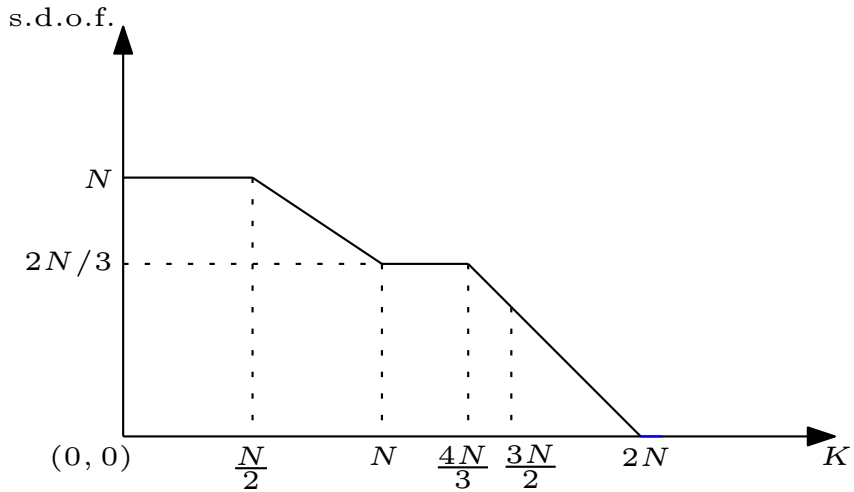
The *Fading* MIMO MAC-WT Channel (contd.)



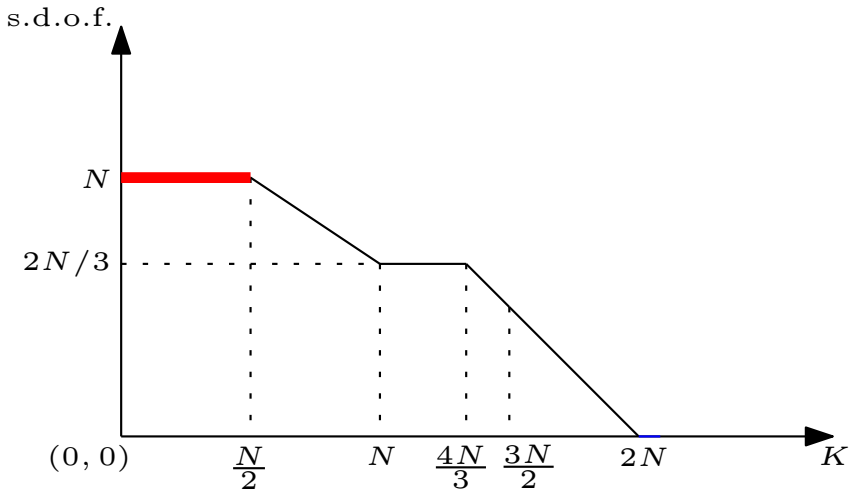
- Converse proof holds for fixed channel gains as well.
- **Question:** Is the same s.d.o.f. achievable with fixed channel gains?

Yes!

Achievable Scheme for $K \leq \frac{N}{2}$

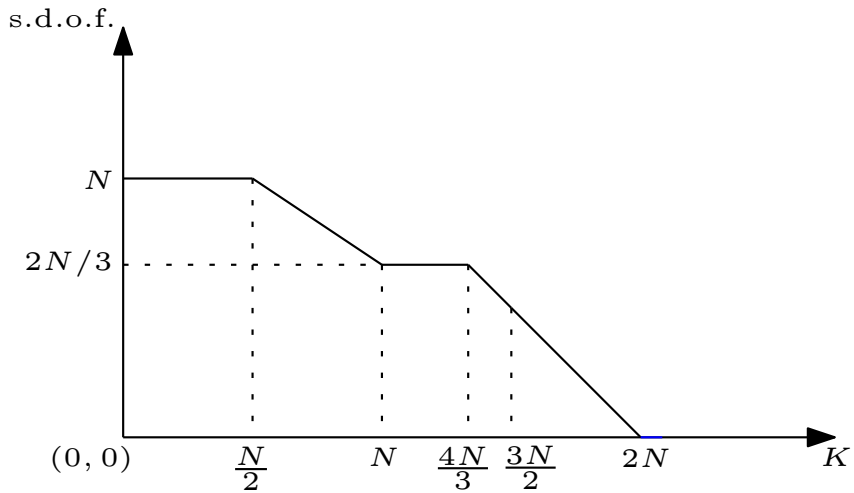


Achievable Scheme for $K \leq \frac{N}{2}$

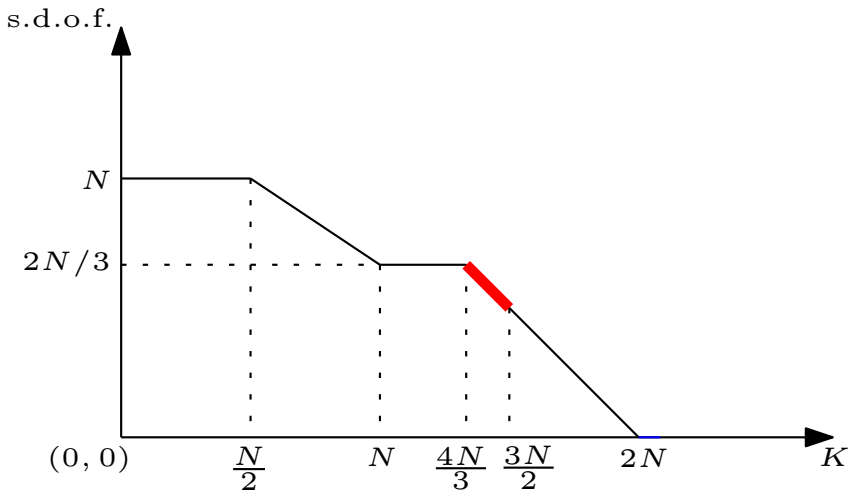


- Running example: $N = 6$. This case: $K \leq 3$.
- Optimal sum s.d.o.f.$=N$.
- Beam-forming is optimal when $K \leq \frac{N}{2}$.
- Transmitters 1 and 2 send $N - K$ and K symbols $\mathbf{v}_1$ and $\mathbf{v}_2$, respectively, in the nullspace of the eavesdropper's channels.
- Note that $K \leq N - K$ in this regime.

Achievable Scheme for $\frac{4N}{3} \leq K \leq \frac{3N}{2}$



Achievable Scheme for $\frac{4N}{3} \leq K \leq \frac{3N}{2}$



- Running example: $N = 6$. This case: $8 \leq K \leq 9$.
- Optimal sum s.d.o.f.$= 2N - K$.
- Transmitter 1: $\left\{\mathbf{v}_1 \in \mathbb{R}^{3N-2K}, \tilde{\mathbf{v}} \in \mathbb{R}^{3K-4N}\right\}$, i.e., $K - N$ symbols.
- Transmitter 2: $\left\{\mathbf{v}_2 \in \mathbb{R}^{3N-2K}\right\}$, i.e., $3N - 2K$ symbols.
- Total of $2N - K$ symbols in each time slot.

Achievable Scheme for $\frac{4N}{3} \leq K \leq \frac{3N}{2}$ (contd.)

- The channel inputs are:

$$\mathbf{X}_1 = \mathbf{R}_1\tilde{\mathbf{v}} + \mathbf{P}_1\mathbf{v}_1 + \mathbf{H}_1^{-1}\mathbf{Q}\mathbf{u}_1$$
$$\mathbf{X}_2 = \mathbf{R}_2\tilde{\mathbf{u}} + \mathbf{P}_2\mathbf{v}_2 + \mathbf{H}_2^{-1}\mathbf{Q}\mathbf{u}_2$$

- The channel outputs are:

$$\mathbf{Y} = \mathbf{H}_1\mathbf{R}_1\tilde{\mathbf{v}} + \mathbf{H}_1\mathbf{P}_1\mathbf{v}_1 + \mathbf{H}_2\mathbf{P}_2\mathbf{v}_2 + \mathbf{H}_2\mathbf{R}_2\tilde{\mathbf{u}} + \mathbf{Q}(\mathbf{u}_1 + \mathbf{u}_2)$$
$$\mathbf{Z} = \mathbf{G}_1\mathbf{R}_1\tilde{\mathbf{v}} + \mathbf{G}_2\mathbf{R}_2\tilde{\mathbf{u}} + \mathbf{G}_1\mathbf{P}_1\mathbf{v}_1 + \mathbf{G}_2\mathbf{H}_2^{-1}\mathbf{Q}\mathbf{u}_2 + \mathbf{G}_2\mathbf{P}_2\mathbf{v}_2 + \mathbf{G}_1\mathbf{H}_1^{-1}\mathbf{Q}\mathbf{u}_1$$

- For **security,** enforce:

$$\mathbf{G}_1\mathbf{R}_1 = \mathbf{G}_2\mathbf{R}_2$$
$$\mathbf{G}_1\mathbf{P}_1 = \mathbf{G}_2\mathbf{H}_2^{-1}\mathbf{Q}$$
$$\mathbf{G}_2\mathbf{P}_2 = \mathbf{G}_1\mathbf{H}_1^{-1}\mathbf{Q}$$

Achievable Scheme for $\frac{4N}{3} \leq K \leq \frac{3N}{2}$ (contd.)

- **Feasibility** of $\mathbf{G}_1\mathbf{R}_1 = \mathbf{G}_2\mathbf{R}_2$ with $N \times (3K - 4N)$ matrix $\mathbf{R}_i$:

$$[\mathbf{G}_1 \quad -\mathbf{G}_2] \begin{bmatrix} \mathbf{R}_1 \\ \mathbf{R}_2 \end{bmatrix} = \mathbf{0}$$

- This is feasible since $3K - 4N \leq 2N - K$ in this regime.
- Choose $\mathbf{P}_i$ and $\mathbf{Q}$ as solutions of:

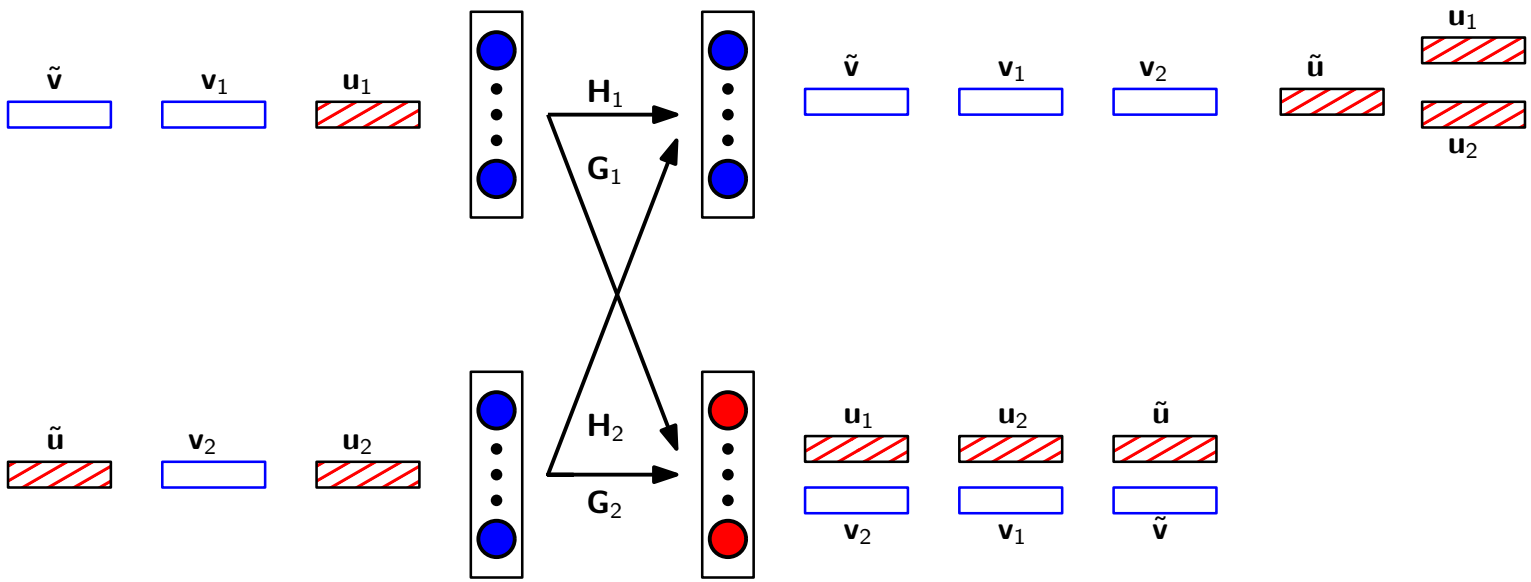
$$\begin{bmatrix} \mathbf{G}_1 & \mathbf{0}_{K\times N} & -\mathbf{G}_2\mathbf{H}_2^{-1} \\ \mathbf{0}_{K\times N} & \mathbf{G}_2 & -\mathbf{G}_1\mathbf{H}_1^{-1} \end{bmatrix} \begin{bmatrix} \mathbf{P}_1 \\ \mathbf{P}_2 \\ \mathbf{Q} \end{bmatrix} = \mathbf{0}$$

- **Security:** Guaranteed by design.
- **Decodability:** Number of symbols to decode:

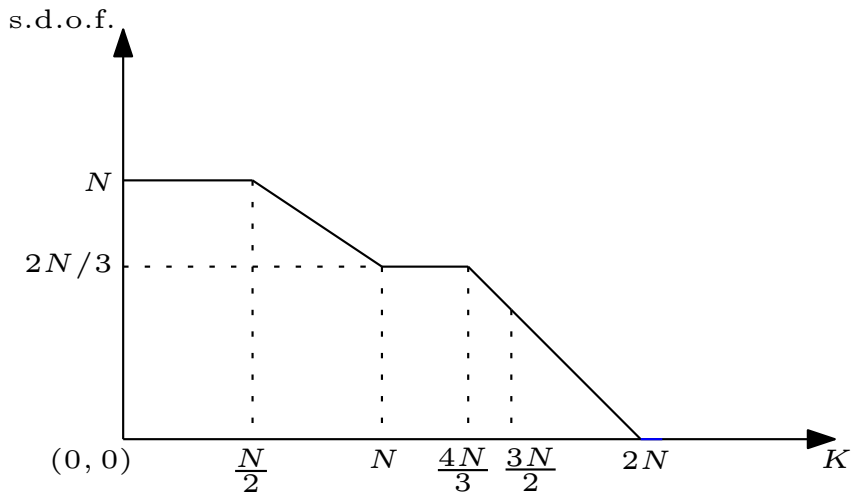
$$\underbrace{(2N - K)}_{\text{desired symbols}} + \underbrace{(3K - 4N)}_{\tilde{\mathbf{u}}} + \underbrace{(3N - 2K)}_{\mathbf{u}_1+\mathbf{u}_2} = N$$

Achievable Scheme for $\frac{4N}{3} \leq K \leq \frac{3N}{2}$ (contd.)

- The alignment structure in this case has the following form:

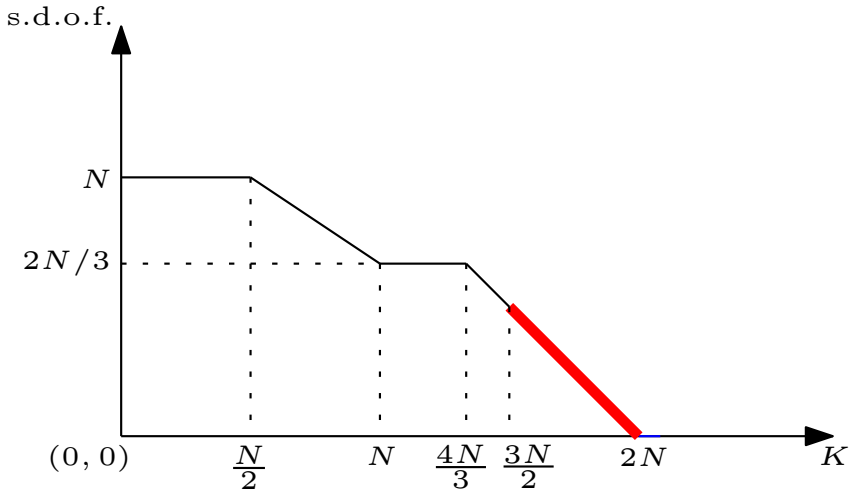


Achievable Scheme for $\frac{3N}{2} \leq K \leq 2N$



[a] [Nafea, Yener, 2015]

Achievable Scheme for $\frac{3N}{2} \leq K \leq 2N$



- Running example: $N = 6$. This case: $9 \leq K \leq 12$.
- Optimal sum s.d.o.f.$= 2N - K$.
- The MAC-WT *reduces* to the wiretap channel with one helper[a].
- Transmitter 1: $\mathbf{v} \in \mathbb{R}^{2N-K}$, i.e., $(2N - K)$ information symbols.
- Transmitter 2 sends *only* cooperative jamming signals.

[a] [Nafea, Yener, 2015]

Achievable Scheme for $\frac{3N}{2} \leq K \leq 2N$ (contd.)

- The channel inputs are:

$$\mathbf{X}_1 = \mathbf{P}\mathbf{v}$$
$$\mathbf{X}_2 = \mathbf{Q}\mathbf{u}$$

- The received signals are

$$\mathbf{Y} = \mathbf{H}_1\mathbf{P}\mathbf{v} + \mathbf{H}_2\mathbf{Q}\mathbf{u}$$
$$\mathbf{Z} = \mathbf{G}_1\mathbf{P}\mathbf{v} + \mathbf{G}_2\mathbf{Q}\mathbf{u}$$

- For **security**, choose $\mathbf{P}$ and $\mathbf{Q}$ as the solutions to

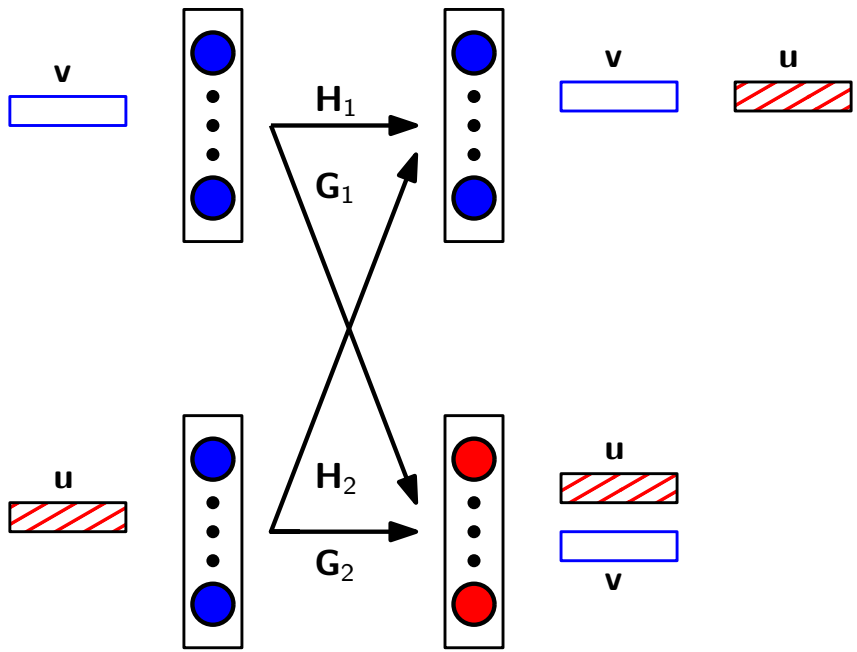
$$[\mathbf{G}_1 \quad -\mathbf{G}_2] \begin{bmatrix} \mathbf{P} \\ \mathbf{Q} \end{bmatrix} = \mathbf{0}$$

- **Decodability:** Receiver can decode both $\mathbf{v}$ and $\mathbf{u}$, since

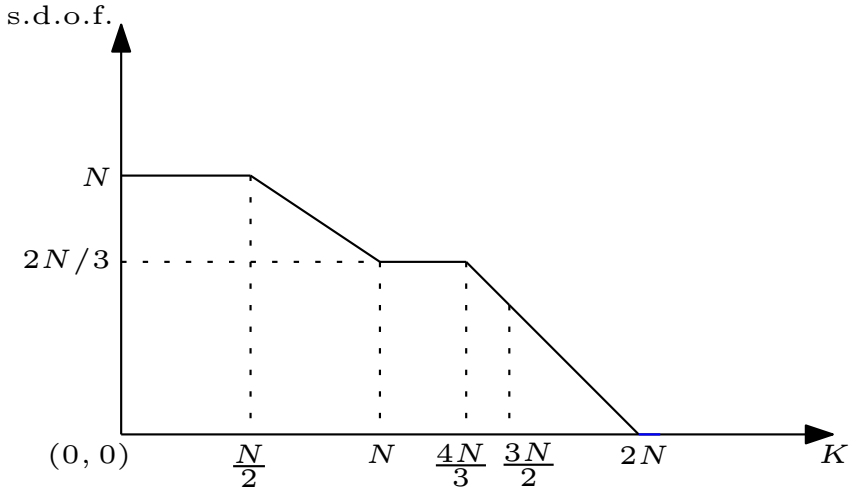
$$2(2N - K) \leq N$$

Achievable Scheme for $\frac{3N}{2} \leq K \leq 2N$ (contd.)

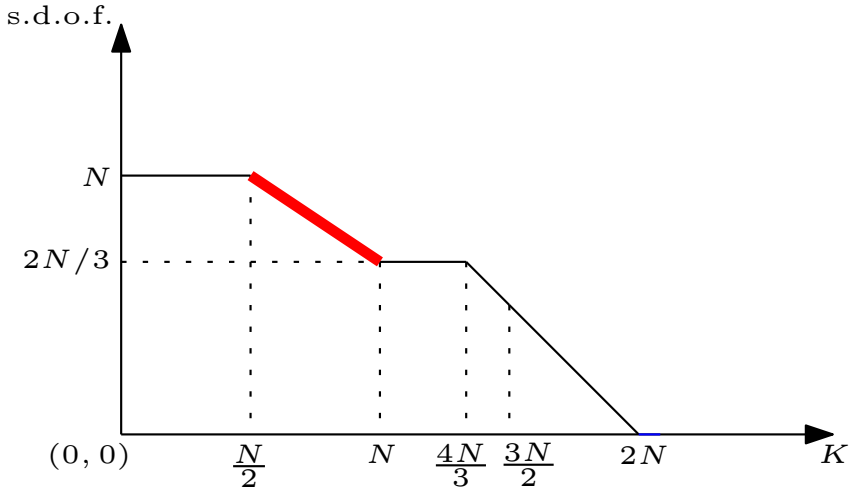
- The alignment structure in this case has the following form:



Achievable Scheme for $\frac{N}{2} \leq K \leq N$



Achievable Scheme for $\frac{N}{2} \leq K \leq N$



- Running example: $N = 6$. This case: $3 \leq K \leq 6$.
- Optimal sum s.d.o.f.$=\frac{2}{3}(2N - K) = 2\left(N - K + d + \frac{l}{3}\right)$, where

$$d = \left\lfloor \frac{2K - N}{3} \right\rfloor, \quad l = (2N - K) \bmod 3$$

- **Examples:**
  1. When $K = 4$, sum s.d.o.f.$=\frac{16}{3}$, $d = 0$, $l = 2$.
  2. When $K = 5$, sum s.d.o.f.$=\frac{14}{3}$, $d = 1$, $l = 1$.

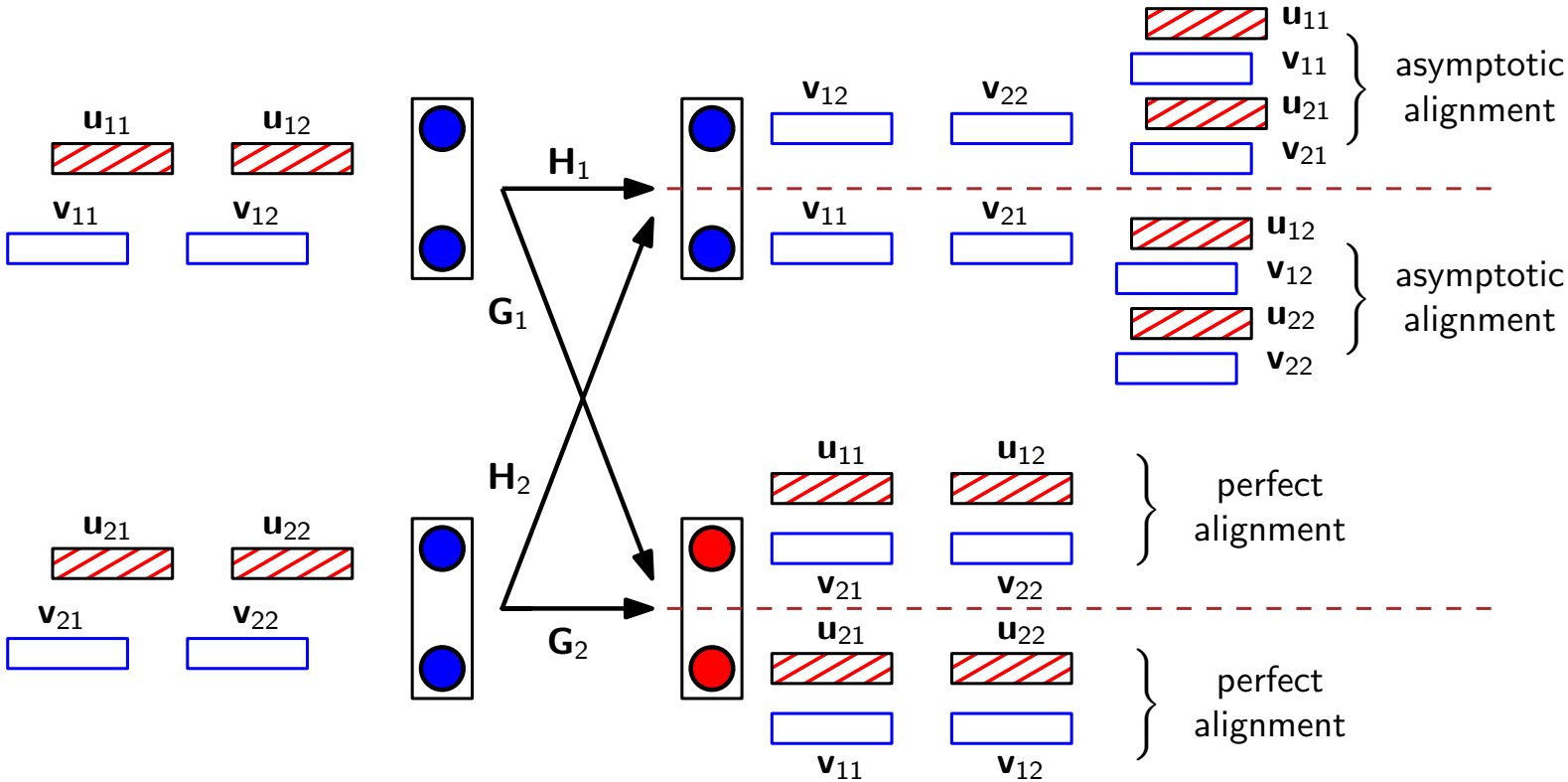
Achievable Scheme for $\frac{N}{2} \leq K \leq N$ (contd.)

- **Main idea:** Decompose the channel input at *each* transmitter into:
  1. $N - K$ Gaussian symbols sent in the nullspace of Eve.
  2. Gaussian symbols carrying d s.d.o.f.
  3. structured PAM symbols carrying $\frac{l}{3}$ s.d.o.f.
- Use channel precoding for the Gaussian symbols.
- Use real alignment schemes for the $l \times l \times l \times l$ MAC-WT achieving $\frac{2l}{3}$ sum s.d.o.f. for $l = 1, 2$.
- For $l = 1$: Real alignment scheme for the SISO MAC-WT is known[a].
- **Needed:** Real alignment scheme for the $2 \times 2 \times 2 \times 2$ MAC-WT.

[a] [Xie, Ulukus, 2013]

Achievable Scheme for the $2 \times 2 \times 2 \times 2$ MAC-WT channel

- Optimal sum 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. $=\frac{4}{3}$.

The General Scheme for $\frac{N}{2} \leq K \leq N$

- Each transmitter wants to send $\left(N - K + d + \frac{I}{3}\right)$ s.d.o.f.
- At transmitter i, information bearing symbols: $(\tilde{\mathbf{v}}_i, \mathbf{v}_i^{(1)}, \mathbf{v}_i^{(2)})$
  - $\tilde{\mathbf{v}}_i$: $N - K$ Gaussian symbols that can be sent using Eve's nullspace
  - $\mathbf{v}_i^{(1)}$: d Gaussian symbols each carrying 1 d.o.f.
  - $\mathbf{v}_i^{(2)}$: I structured symbols each carrying $\frac{1}{3}$ d.o.f.
- Cooperative jamming signals: $\mathbf{u}_i = (\mathbf{u}_i^{(1)}, \mathbf{u}_i^{(2)})$.
- Let $\mathbf{v}_i = (\mathbf{v}_i^{(1)}, \mathbf{v}_i^{(2)})$. Transmitter i sends:

$$\mathbf{X}_i = \mathbf{G}_i^{\perp} \tilde{\mathbf{v}}_i + \mathbf{P}_i \mathbf{v}_i + \mathbf{H}_i^{-1} \mathbf{Q} \mathbf{u}_i$$

- The received signals are:

$$\mathbf{Y} = \mathbf{H}_1 \mathbf{G}_1^{\perp} \tilde{\mathbf{v}}_1 + \mathbf{H}_1 \mathbf{P}_1 \mathbf{v}_1 + \mathbf{H}_2 \mathbf{P}_2 \mathbf{v}_2 + \mathbf{H}_2 \mathbf{G}_2^{\perp} \tilde{\mathbf{v}}_2 + \mathbf{Q}(\mathbf{u}_1 + \mathbf{u}_2) + \mathbf{N}_1$$

$$\mathbf{Z} = \mathbf{G}_1 \mathbf{P}_1 \mathbf{v}_1 + \mathbf{G}_2 \mathbf{H}_2^{-1} \mathbf{Q} \mathbf{u}_2 + \mathbf{G}_2 \mathbf{P}_2 \mathbf{v}_2 + \mathbf{G}_1 \mathbf{H}_1^{-1} \mathbf{Q} \mathbf{u}_1 + \mathbf{N}_2$$

The General Scheme for $\frac{N}{2} \leq K \leq N$ (contd.)

- Let $\mathbf{Q}$ to be any $N \times (d + l)$ matrix with full column rank.
- Set $\mathbf{P}_i = \mathbf{G}_i^T(\mathbf{G}_i\mathbf{G}_i^T)^{-1}(\mathbf{G}_j\mathbf{H}_j^{-1})\mathbf{Q}$.
- Eve's observation is:

$$\mathbf{Z} = \mathbf{G}_2\mathbf{H}_2^{-1}\mathbf{Q}(\mathbf{v}_1 + \mathbf{u}_2) + \mathbf{G}_1\mathbf{H}_1^{-1}\mathbf{Q}(\mathbf{v}_2 + \mathbf{u}_1) + \mathbf{N}_2$$

- Perfect alignment ensures security.
- **Decoding:** Consider $\mathbf{B}_{N\times l}$ such that

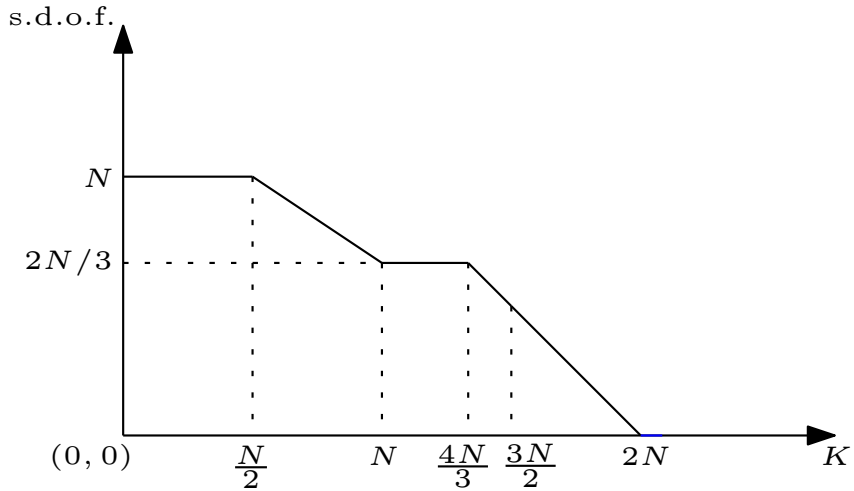
$$\mathbf{B}^T[\mathbf{H}_1\mathbf{G}_1^{\perp} \quad \mathbf{H}_2\mathbf{G}_2^{\perp} \quad \mathbf{H}_1\mathbf{P}_1^{(1)} \quad \mathbf{H}_1\mathbf{P}_1^{(1)} \quad \mathbf{Q}^{(1)}]_{N\times(N-l)} = \mathbf{0}$$

- Consider $\tilde{\mathbf{Y}} = (\mathbf{B}^T\mathbf{Q}^{(2)})^{-1}\mathbf{B}^T\mathbf{Y}$

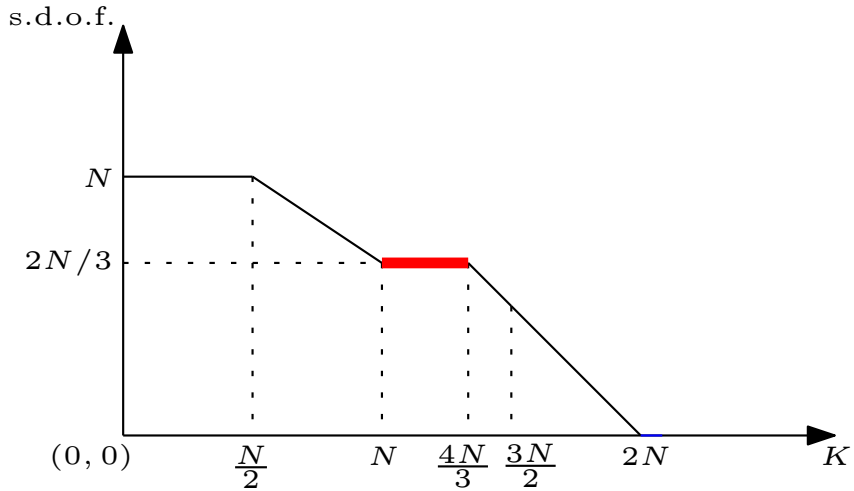
$$\tilde{\mathbf{Y}} = \mathbf{D}\mathbf{H}_1\mathbf{P}_1^{(2)}\mathbf{v}_1^{(2)} + \mathbf{D}\mathbf{H}_2\mathbf{P}_2^{(2)}\mathbf{v}_2^{(2)} + (\mathbf{u}_1^{(2)} + \mathbf{u}_2^{(2)}) + \mathbf{D}\mathbf{N}_1$$

- Decode $(\mathbf{v}_1^{(2)}, \mathbf{v}_2^{(2)})$ using the $l \times l \times l \times l$ MAC-WT scheme.
- Eliminate $(\mathbf{v}_1^{(2)}, \mathbf{v}_2^{(2)}, \mathbf{u}_1^{(2)} + \mathbf{u}_2^{(2)})$ from $\mathbf{Y}$ and decode $(\mathbf{v}_1^{(1)}, \mathbf{v}_2^{(1)})$.

Achievable Scheme for $N \leq K \leq \frac{4N}{3}$

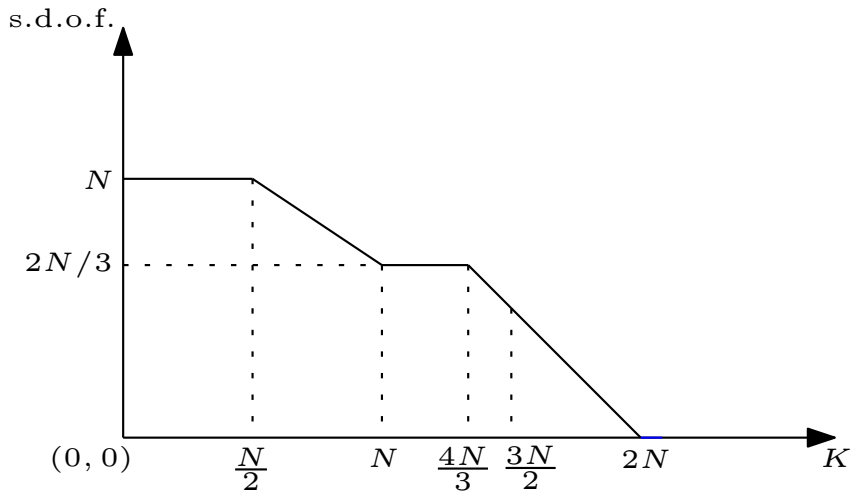


Achievable Scheme for $N \leq K \leq \frac{4N}{3}$

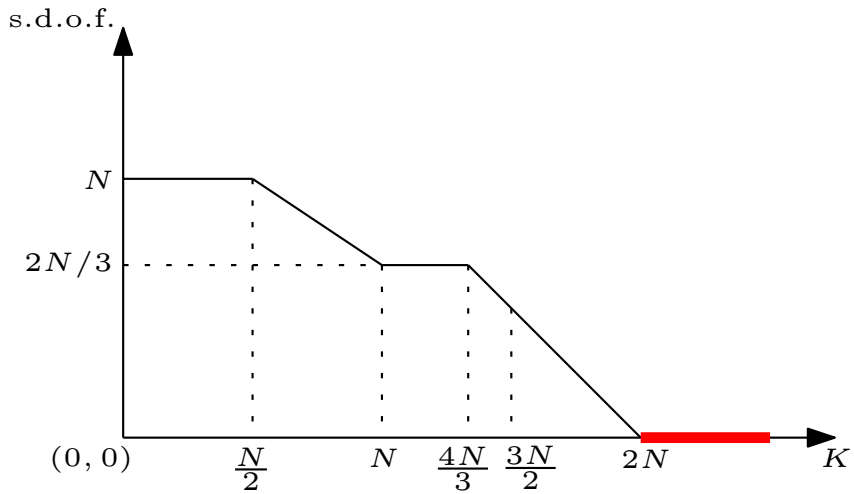


- Running example: $N = 6$. This case: $6 \leq K \leq 8$.
- Optimal sum s.d.o.f.$=\frac{2N}{3}$.
- The point $K = N$ is achievable using the scheme for $\frac{N}{2} \leq K \leq N$.
- The point $K = \frac{4N}{3}$ is achievable using the scheme for $\frac{4N}{3} \leq K \leq \frac{3N}{2}$.
- The intermediate points $N \leq K \leq \frac{4N}{3}$ are achievable since increasing Eve's antennas does not increase the sum s.d.o.f.

Achievable Scheme for $K \geq 2N$



Achievable Scheme for $K \geq 2N$



- Running example: $N = 6$. This case: $K \geq 12$.
- Optimal sum s.d.o.f.=0.
- Since Eve has more than $2N$ antennas, the input of both transmitters can be decoded to within noise variance.

Conclusions and Future Work

- Provided achievable schemes for the MIMO MAC-WT with fixed channel gains.
- The achievable scheme for the regime $\frac{N}{2} < K < N$:
  - Is based on asymptotic real interference alignment
  - Uses a combination of Gaussian and structured PAM symbols.
  - Combines channel precoding with real interference alignment
- **Open question:** What happens if Eve's CSIT is not available?