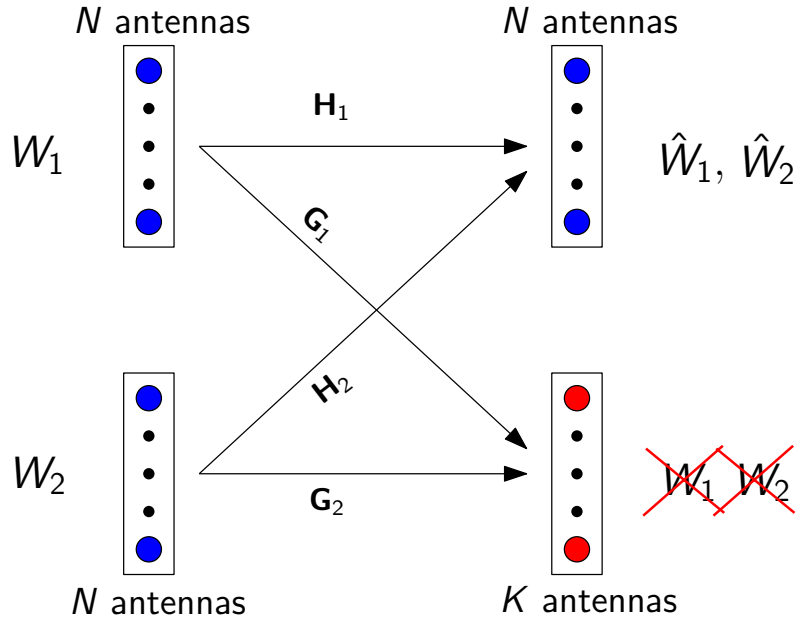
Secure Degrees of Freedom of the MIMO Multiple Access Wiretap Channel

Pritam Mukherjee Şennur Ulukuş

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

A Degrees of Freedom View

- Recall the capacity of a real Gaussian channel

$$Y = X + N$$

  is given by

$$C_G = \frac{1}{2}\log(1+P) \approx \frac{1}{2}\log P \quad \text{at high SNR.}$$

- *Degrees of freedom* (d.o.f.) is defined as

$$d = \lim_{P\to\infty} \frac{C}{C_G} = \lim_{P\to\infty} \frac{C}{\frac{1}{2}\log P}.$$

- Thus,

$$\text{d.o.f} = d \quad \Rightarrow \quad C = \frac{d}{2}\log P + o(\log P).$$

- With security constraints: *secure degrees of freedom* (s.d.o.f.):

$$d_s = \lim_{P\to\infty} \frac{C_s}{\frac{1}{2}\log P}.$$

Our Results

Theorem

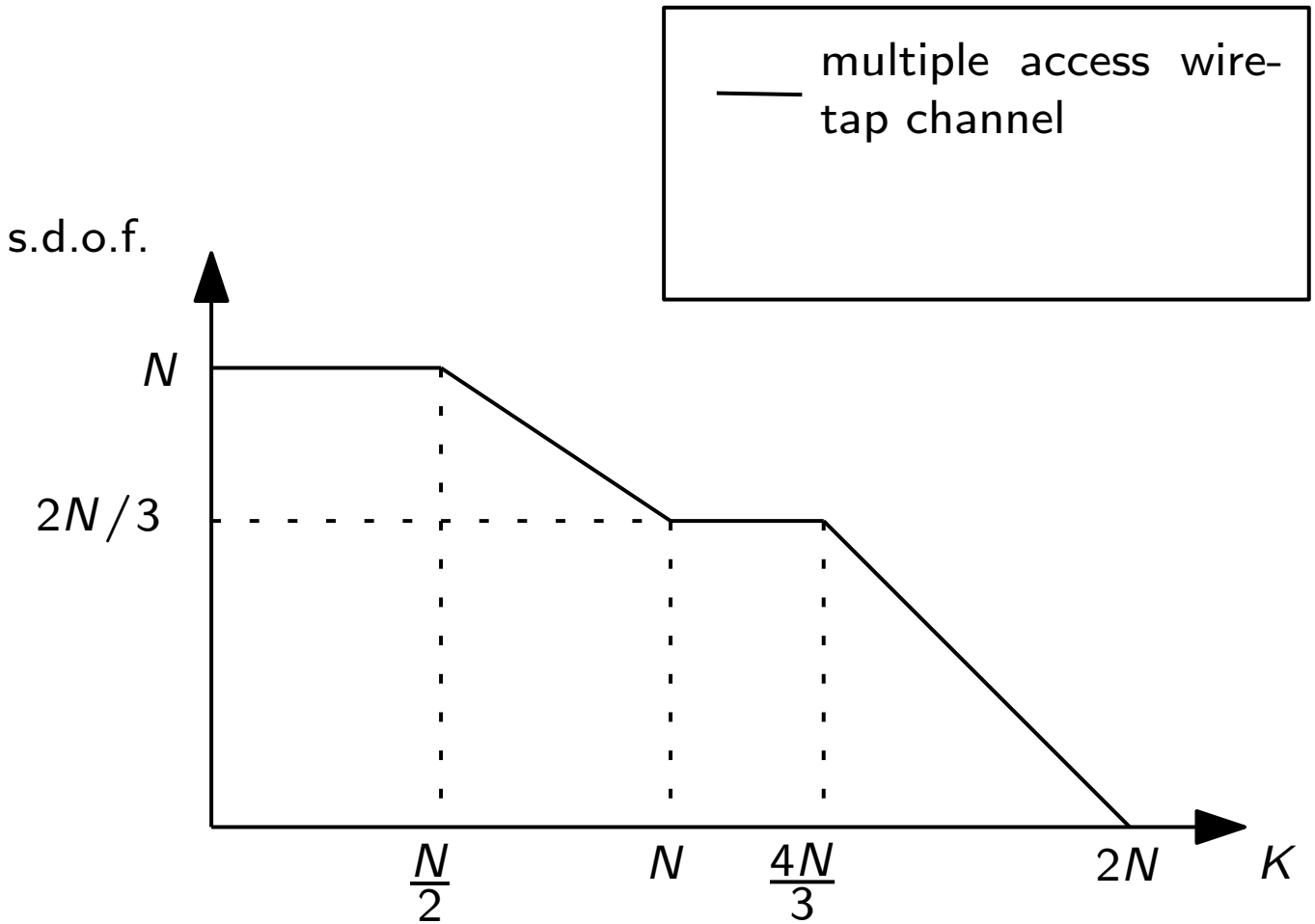
The optimal sum s.d.o.f. of the $N \times N \times N \times K$ MIMO MAC-WT is

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

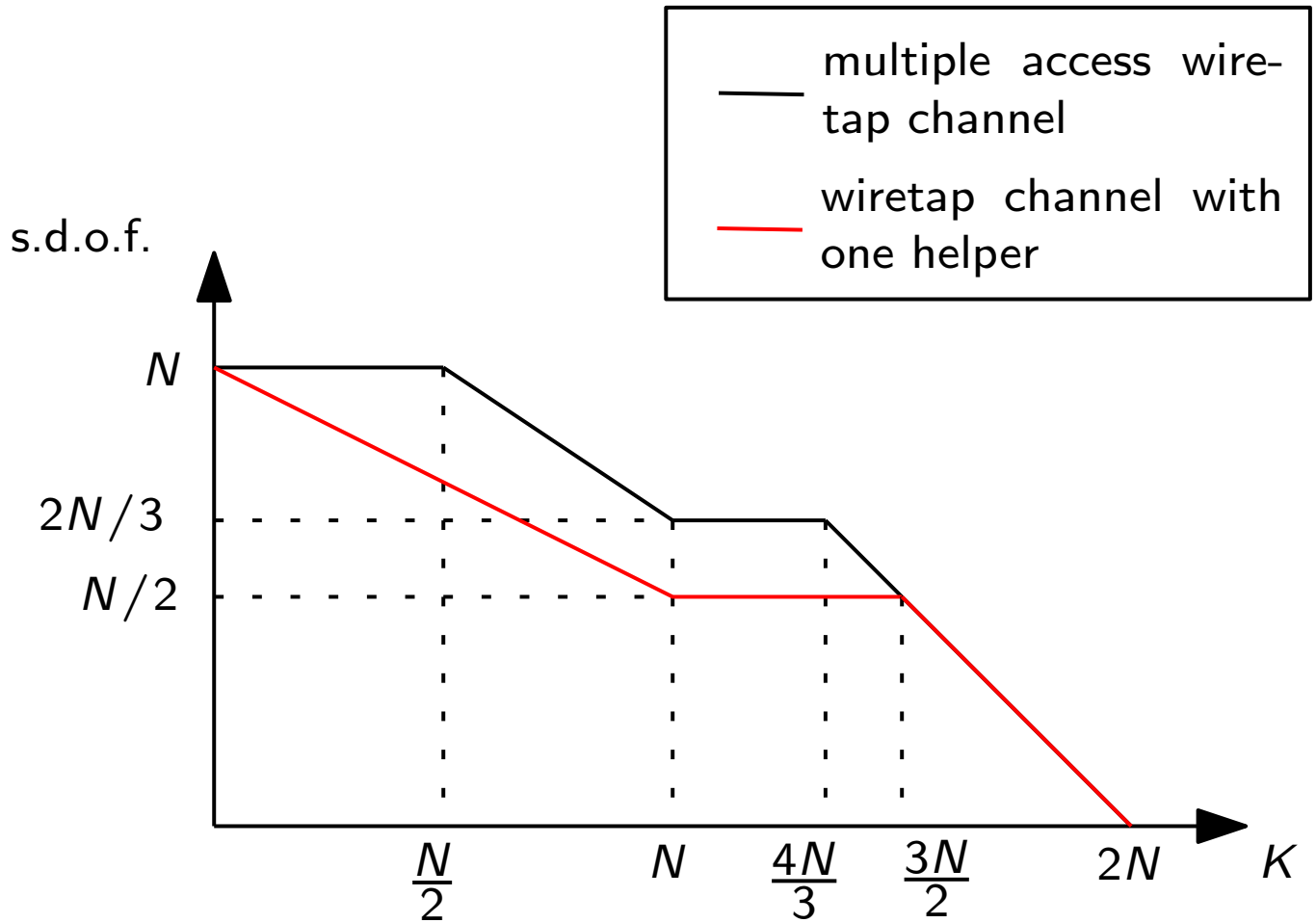
- When $N = K = 1$: s.d.o.f.[a]$= \frac{2}{3}$.

[a] [Xie, Ulukus, 2013]

Our Results (contd.)



Our Results (contd.)

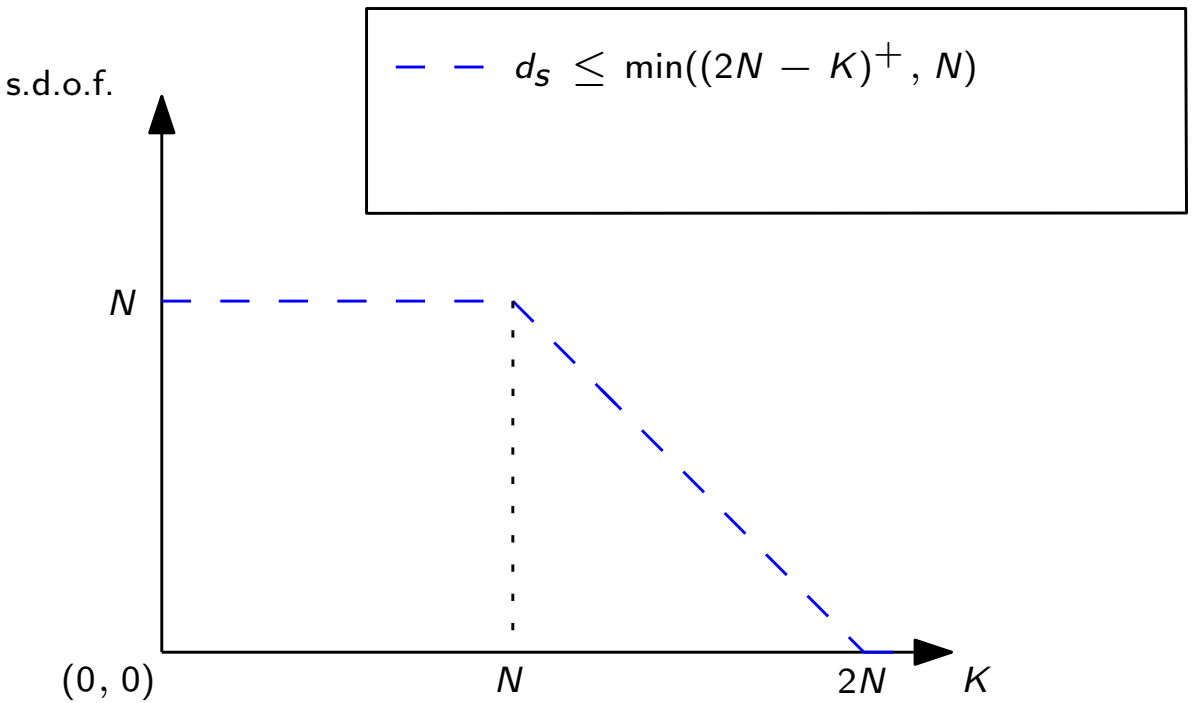


Some Remarks

- $K \leq \frac{N}{2}$: **No** loss due to security constraints!
- $N \leq K \leq \frac{4N}{3}$: **No** loss due to increasing eavesdropper antennas!
- $K \geq \frac{4N}{3}$: **No** loss due to distributed antennas!
- $K \geq \frac{3N}{2}$: The MAC-WT reduces to a wiretap channel with a helper[a].
- $K \geq 2N$: Eavesdropper can *reconstruct* channel inputs; s.d.o.f.$= 0$.

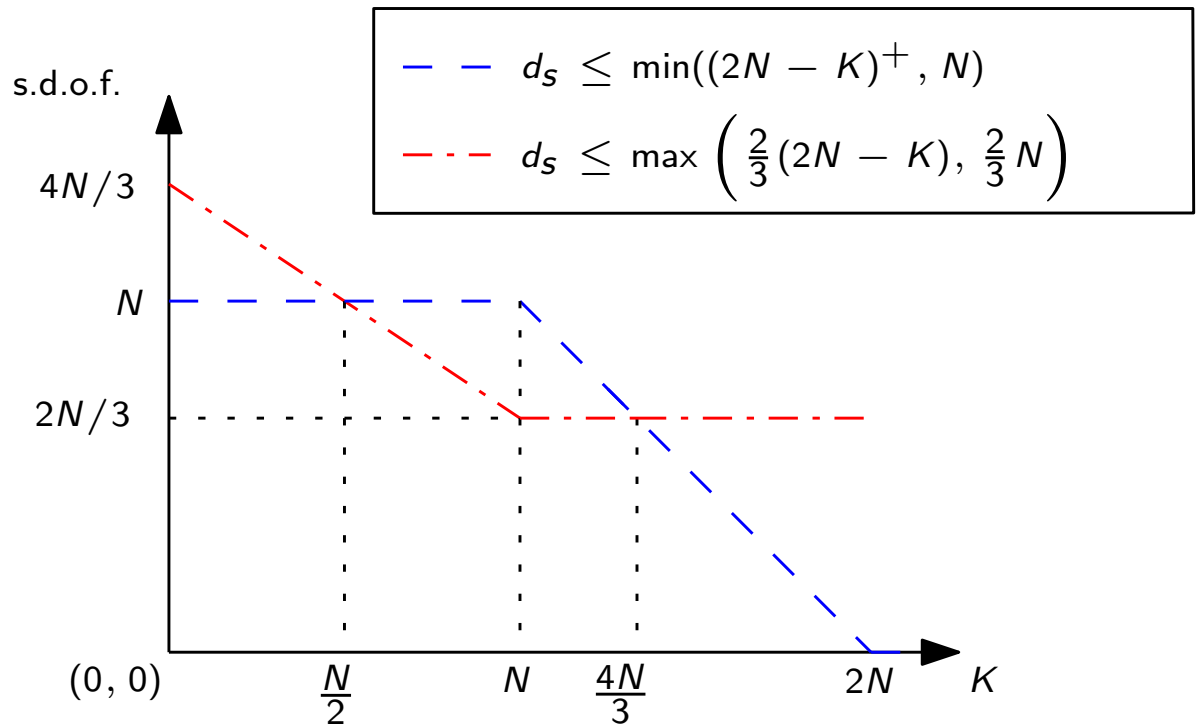
[a] Nafea, Yener, 2015

Converse Outline



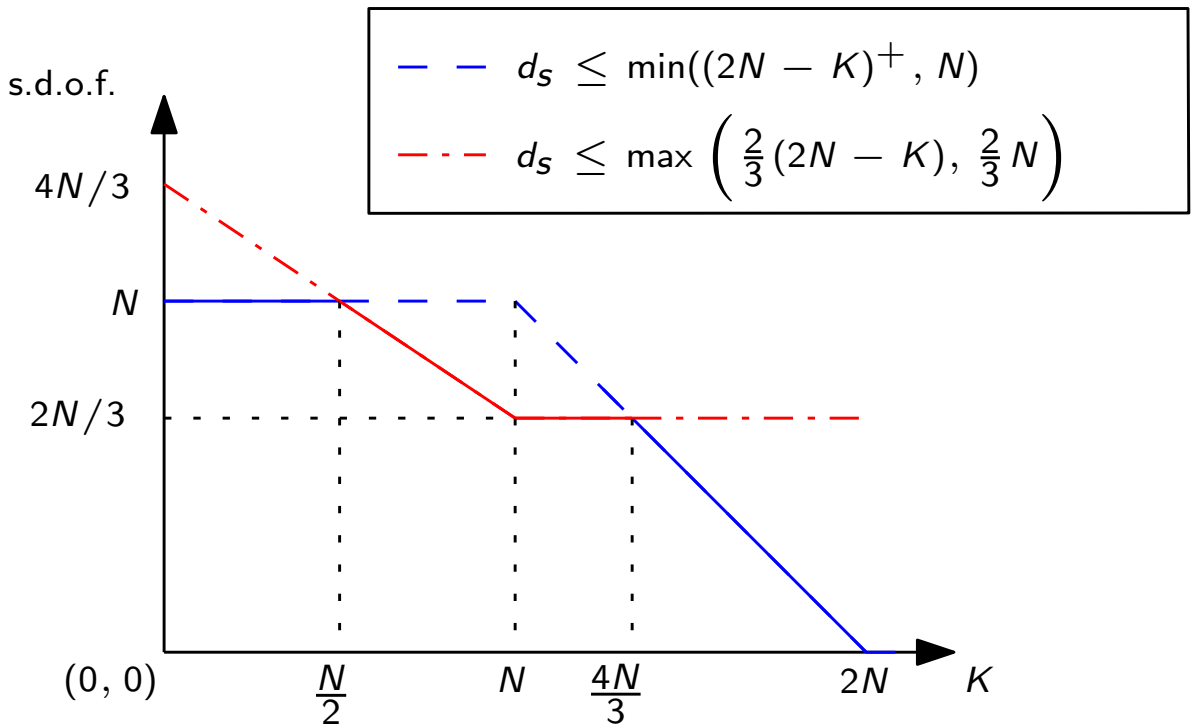
- Cooperation bound: Allow cooperation between transmitters

Converse Outline



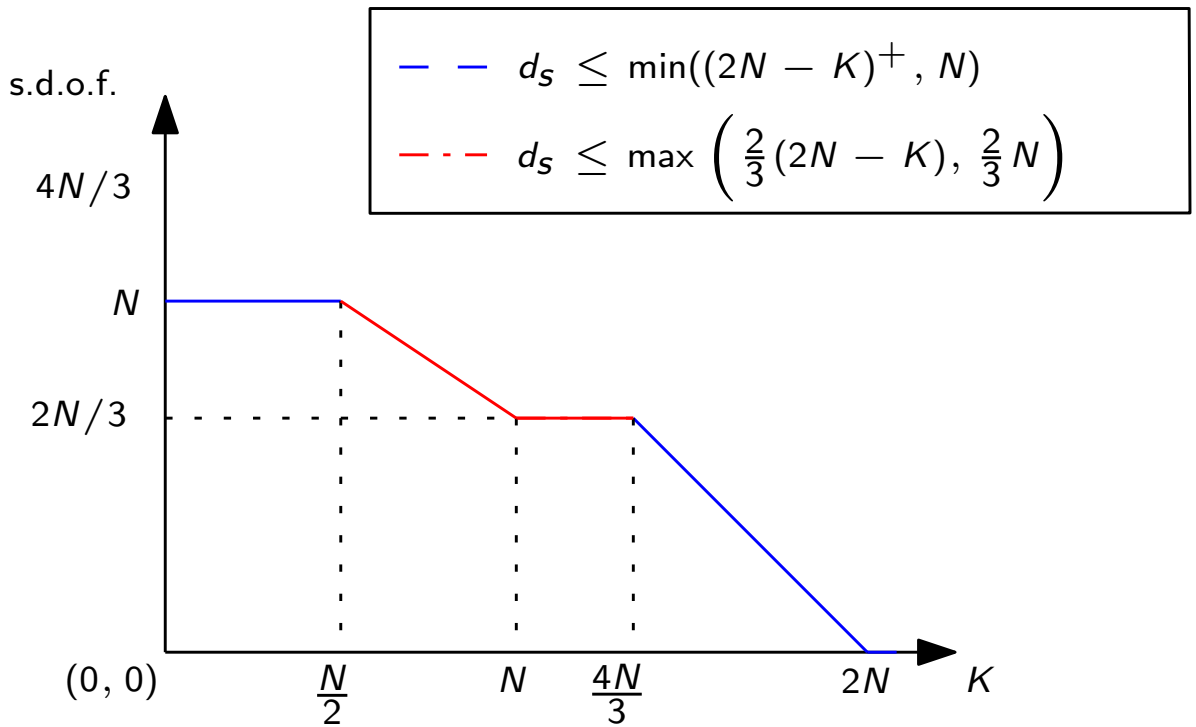
- Cooperation bound: Allow cooperation between transmitters
- MAC-WT bound: Based on
  - MIMO version of secrecy penalty lemma
  - MIMO version of role of a helper lemma

Converse Outline



- Cooperation bound: Allow cooperation between transmitters
- MAC-WT bound: Based on
  - MIMO version of secrecy penalty lemma
  - MIMO version of role of a helper lemma

Converse Outline



- Cooperation bound: Allow cooperation between transmitters
- MAC-WT bound: Based on
  - MIMO version of secrecy penalty lemma
  - MIMO version of role of a helper lemma

MAC-WT Bound

- Consider $K \leq N$.
- MIMO version of secrecy penalty lemma:

$$\begin{aligned} n(R_1 + R_2) \leq & h(\tilde{\mathsf{X}}_1^n) + h(\tilde{\mathsf{X}}_2^n) - h(\mathsf{Z}^n) + nc_1 \\ \leq & h(\tilde{\mathsf{X}}_{1[1:N-K]}^n) + h(\tilde{\mathsf{X}}_2^n) + nc_2 \end{aligned}$$

  where $\tilde{\mathsf{X}}_i = \mathsf{X}_i + \tilde{\mathsf{N}}_i$ where $\tilde{\mathsf{N}}_i \sim \mathcal{N}(0, \rho^2 \mathsf{I}_N)$ with ρ small.
- MIMO version of role of a helper lemma:

$$nR_1 \leq h(\mathsf{Y}^n) - h(\tilde{\mathsf{X}}_2^n) + nc_3$$

- Adding the above equations:

$$\begin{aligned} n(2R_1 + R_2) \leq & h(\mathsf{Y}^n) + h(\tilde{\mathsf{X}}_{1[1:N-K]}^n) + nc_4 \\ \leq & N\left(\frac{n}{2}\log P\right) + (N-K)\left(\frac{n}{2}\log P\right) + nc_4 \end{aligned}$$

MAC-WT Bound (Contd.)

- We have,

$$n(2R_1 + R_2) \leq (2N - K)\left(\frac{n}{2}\log P\right) + nc_4$$

- Dividing by n, and $\frac{1}{2}\log P$ and then letting $P \to \infty$

$$2d_1 + d_2 \leq (2N - K)$$

- By symmetry

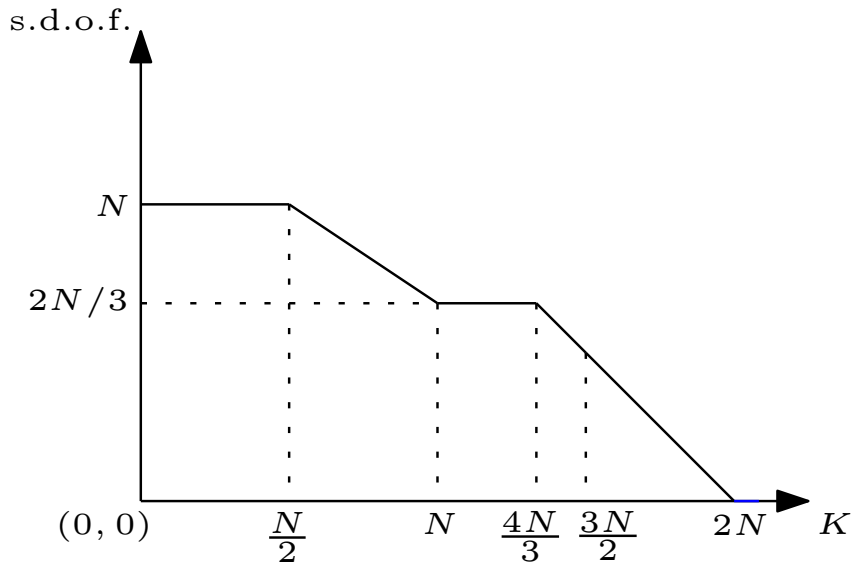
$$d_1 + 2d_2 \leq (2N - K)$$

- Combining the above,

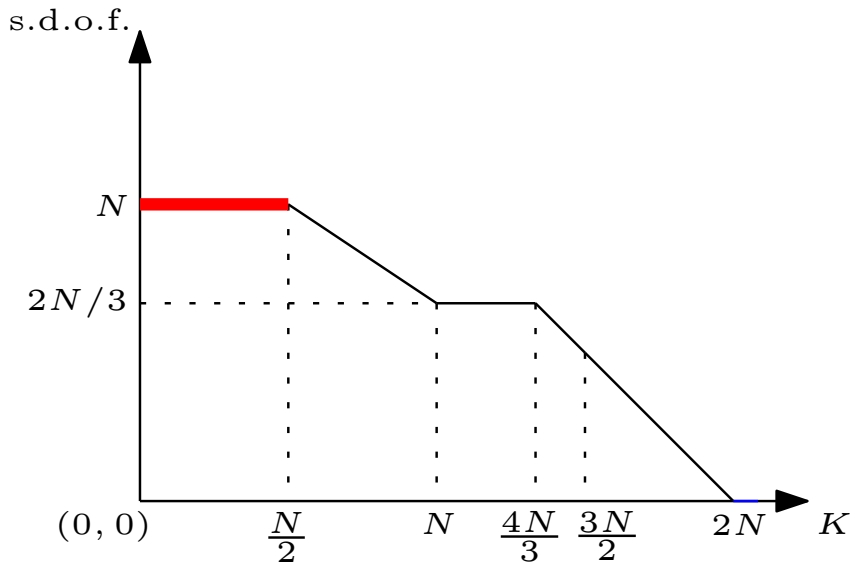
$$d_s \leq \frac{2}{3}(2N - K)$$

- S.d.o.f. is non-increasing with $K \Rightarrow d_s \leq \frac{2}{3}N$, when $K > N$.

Achievable Schemes

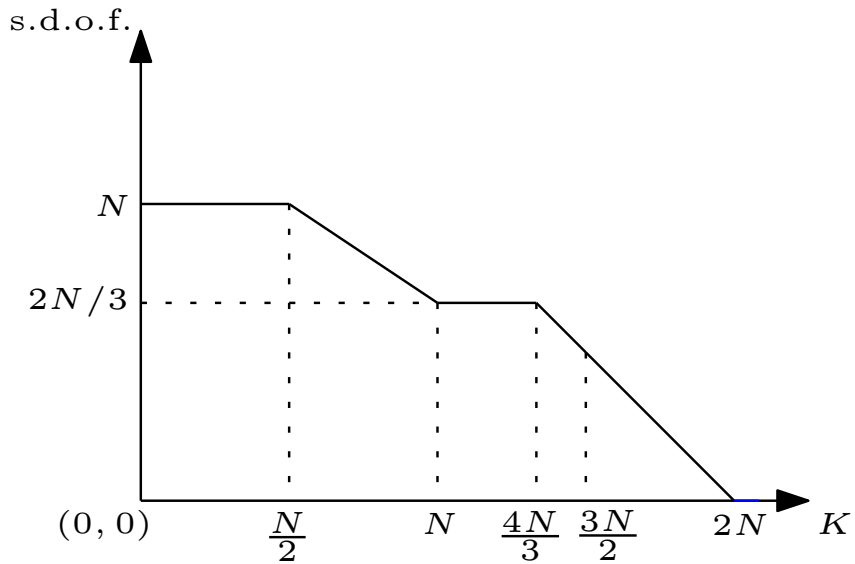


Achievable Schemes

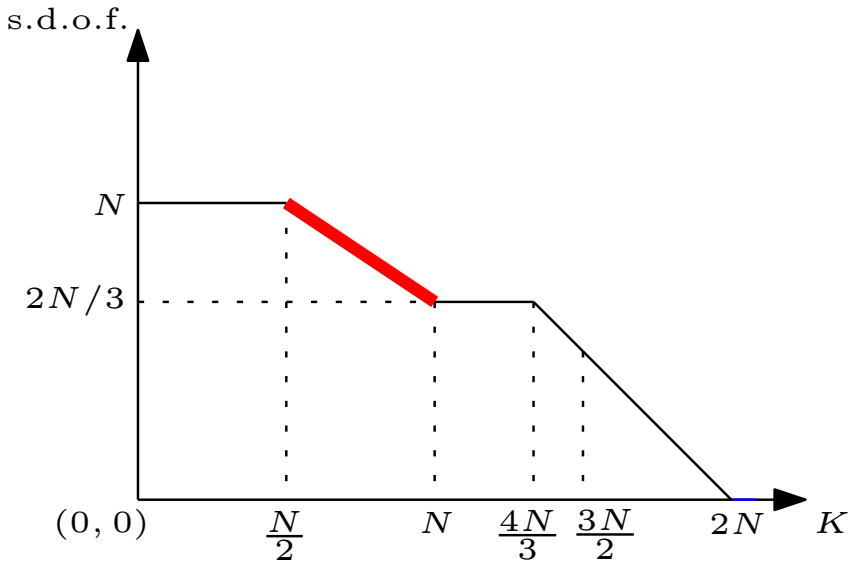


- Optimal sum s.d.o.f.$=N$.
- Beam-forming is optimal when $K \leq \frac{N}{2}$.
- Transmitters 1 and 2 send $N-K$ and K symbols v_1 and v_2, respectively, in the nullspace of the eavesdropper's channels.
- Note that $K \leq N-K$ in this regime.

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



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



- Optimal sum s.d.o.f.$=\frac{2}{3}(2N-K)$.
- Transmitter i sends $(2N-K)$ Gaussian symbols in 3 time slots:

$$\left\{\mathrm{v}_i \in \mathbb{R}^{2K-N}, \tilde{\mathrm{v}}_i(t) \in \mathbb{R}^{N-K}, t = 1, 2, 3\right\}$$

- $\tilde{\mathrm{v}}_i(t)$ is transmitted in the nullspace of eavesdropper in slot t.
- v_i is sent using an alignment scheme.

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

- The channel inputs are:

$$X_i(t) = G_i(t)^{\perp}\tilde{v}_i(t) + P_i(t)v_i + H_i(t)^{-1}Q(t)u_i$$

where u_i are cooperative jamming signals and

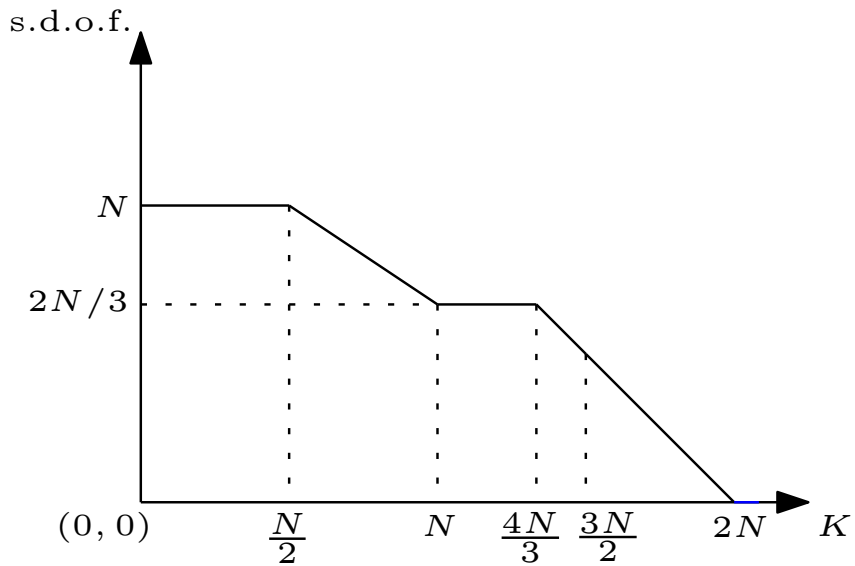
$$P_i(t) = G_i(t)^T(G_i(t)G_i(t)^T)^{-1}(G_j(t)H_j(t)^{-1})Q(t) \quad i \neq j$$

- The channel outputs are:

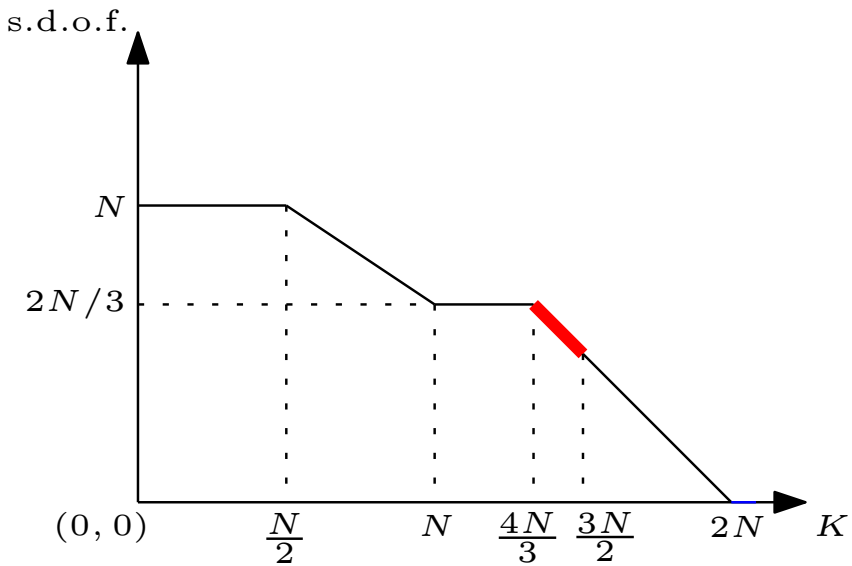
$$\begin{aligned} Y(t) =& H_1(t)G_1(t)^{\perp}\tilde{v}_1(t) + H_1(t)P_1(t)v_1 + H_2(t)P_2(t)v_2 \\ &+ H_2(t)G_2(t)^{\perp}\tilde{v}_2(t) + Q(t)(u_1 + u_2) \\ Z(t) =& (G_2(t)H_2(t)^{-1})Q(t)(u_2 + v_1) + (G_1(t)H_1(t)^{-1})Q(t)(u_1 + v_2) \end{aligned}$$

- **Decodablility:** Number of symbols $= 6(N-K) + 3(2K-N) = 3N$
- **Security:** v_i is buried in the cooperative jamming signal u_j, $j \neq i$.

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



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



- Optimal sum s.d.o.f.$=2N-K$.
- Transmitter 1: $\left\{\mathrm{v}_1 \in \mathbb{R}^{3N-2K}, \tilde{\mathrm{v}} \in \mathbb{R}^{3K-4N}\right\}$, i.e., $K-N$ symbols.
- Transmitter 2: $\left\{\mathrm{v}_2 \in \mathbb{R}^{3N-2K}\right\}$, i.e., $3N-2K$ symbols.
- Total of $2N-K$ symbols in 1 time slot.

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

- The channel inputs are:

$$X_1 = R_1\tilde{v} + P_1 v_1 + H_1^{-1} Q u_1$$
$$X_2 = R_2\tilde{u} + P_2 v_2 + H_2^{-1} Q u_2$$

- The channel outputs are:

$$Y = H_1 R_1 \tilde{v} + H_1 P_1 v_1 + H_2 P_2 v_2 + H_2 R_2 \tilde{u} + Q(u_1 + u_2)$$
$$Z = G_1 R_1 \tilde{v} + G_2 R_2 \tilde{u} + G_1 P_1 v_1 + G_2 H_2^{-1} Q u_2 + G_2 P_2 v_2 + G_1 H_1^{-1} Q u_1$$

- For **security,** enforce:

$$G_1 R_1 = G_2 R_2$$
$$G_1 P_1 = G_2 H_2^{-1} Q$$
$$G_2 P_2 = G_1 H_1^{-1} Q$$

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

- **Feasibility** of $G_1R_1 = G_2R_2$ with $N \times (3K - 4N)$ matrix R_i:

$$[G_1 \quad -G_2] \begin{bmatrix} R_1 \\ R_2 \end{bmatrix} = 0$$

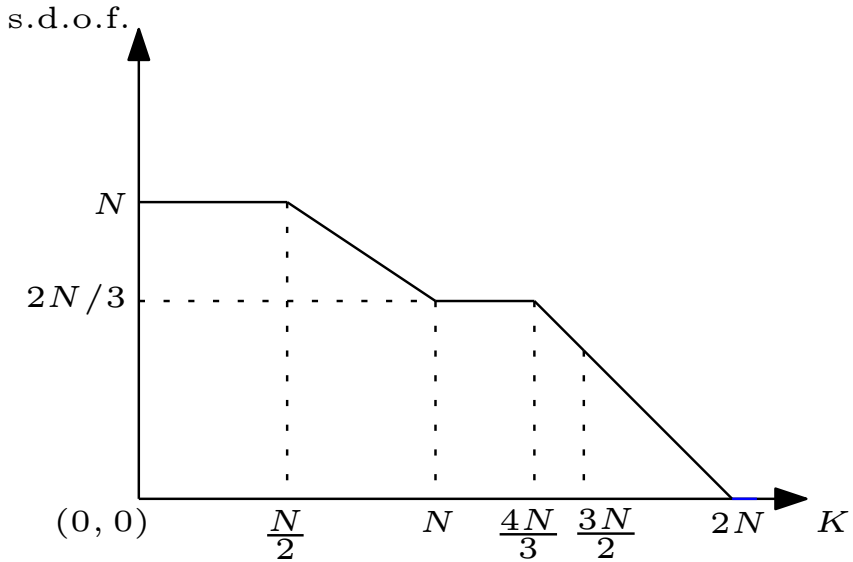
- This is feasible since $3K - 4N \leq 2N - K$ in this regime.
- Choose P_i and Q as solutions of:

$$\begin{bmatrix} G_1 & 0_{K\times N} & -G_2H_2^{-1} \\ 0_{K\times N} & G_2 & -G_1H_1^{-1} \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ Q \end{bmatrix} = 0$$

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

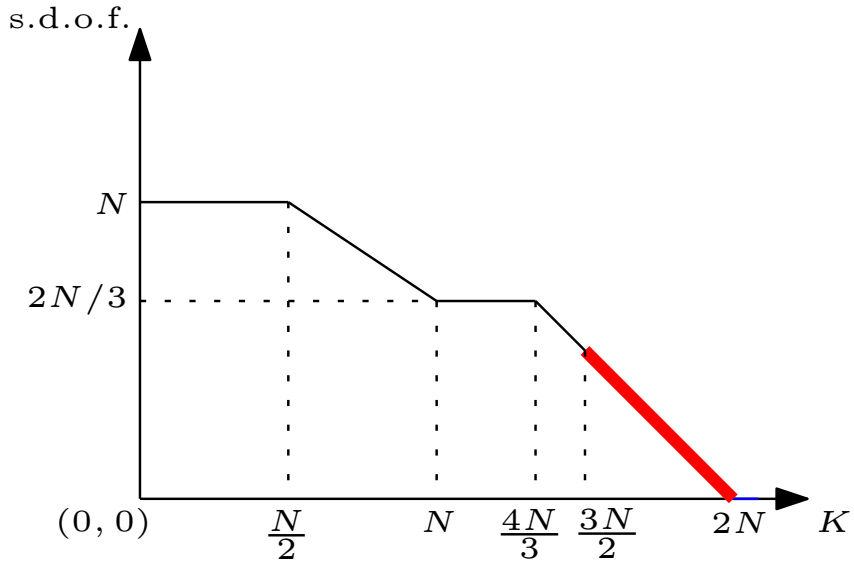
$$\underbrace{(2N-K)}_{\text{desired symbols}} + \underbrace{(3K-4N)}_{\tilde{u}} + \underbrace{(3N-2K)}_{u_1+u_2} = N$$

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



[a] [Nafea, Yener, 2015]

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



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

[a] [Nafea, Yener, 2015]

Achievable Scheme for $K \geq \frac{3N}{2}$ (Contd.)

- The channel inputs are:

$$\begin{aligned} X_1 &= Pv \\ X_2 &= Qu \end{aligned}$$

- The received signals are

$$\begin{aligned} Y &= H_1 Pv + H_2 Qu \\ Z &= G_1 Pv + G_2 Qu \end{aligned}$$

- For **security**, choose P and Q as the solutions to

$$[G_1 \quad -G_2] \begin{bmatrix} P \\ Q \end{bmatrix} = 0$$

- **Decodability:** Receiver can decode both v and u, since

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

Conclusions and Future Work

- Determined the optimal sum s.d.o.f. of the $N \times N \times N \times K$ MIMO MAC-WT with fading channel gains.
- Achievable schemes based on beam-forming, vector space alignment.
- **Question:** What happens when the channel gains are fixed?
  - Converse still holds.
  - Achievable Schemes for the regime $\frac{N}{2} \leq K \leq \frac{4N}{3}$ do not extend.
  - Will be investigated in future work.