MIMO One Hop Networks With No Eve CSIT

Pritam Mukherjee Şennur Ulukuş

University of Maryland, College Park

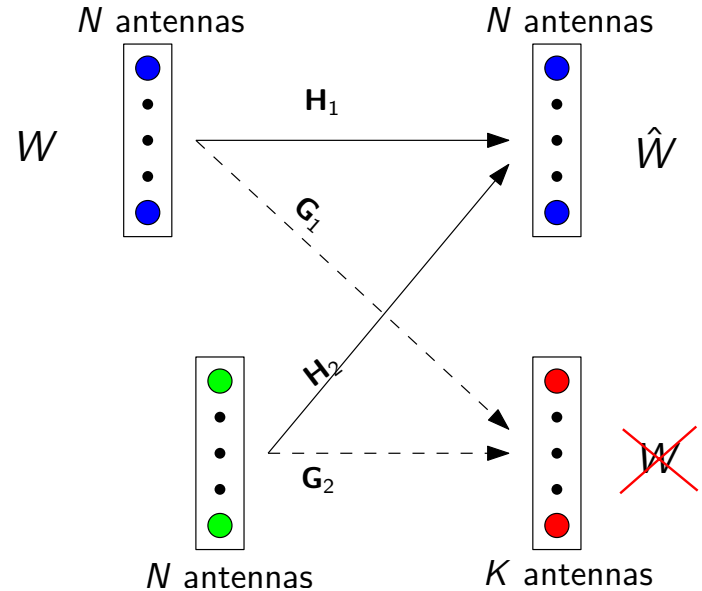
Outline

- Overview of channel models:
  - The MIMO wiretap channel with one helper without Eve CSIT.
  - The MIMO multiple access wiretap channel without Eve CSIT.
- Prior Work:
  - The SISO wiretap channel with helpers.
  - The SISO multiple access wiretap channel.
  - The MIMO wiretap channel with helpers under *full* Eve CSIT.
  - The MIMO multiple access wiretap channel under *full* Eve CSIT.
- Our results.
- Proof sketches.
- Conclusions and future work.

Overview of Channel Models

The MIMO Wiretap channel with a Helper (WTH)

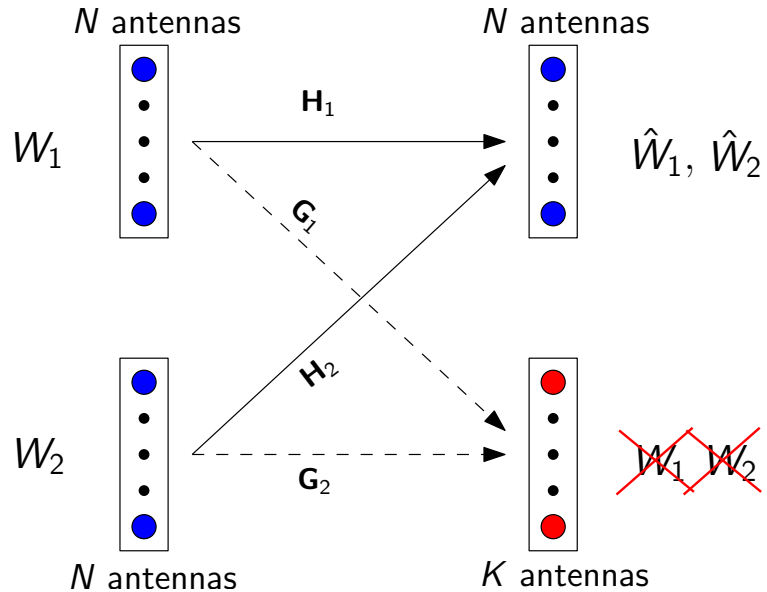
- Consider the two-user MIMO WTH.



- The channel matrices $\mathbf{H}_i$ are *known* at the transmitters.
- The channel matrices $\mathbf{G}_i$ are *unknown* at the transmitters.
- **Question:** What is the optimal secure degrees of freedom (s.d.o.f.)?

The MIMO Multiple Access Wiretap Channel

- Consider the two-user MIMO MAC-WT channel.

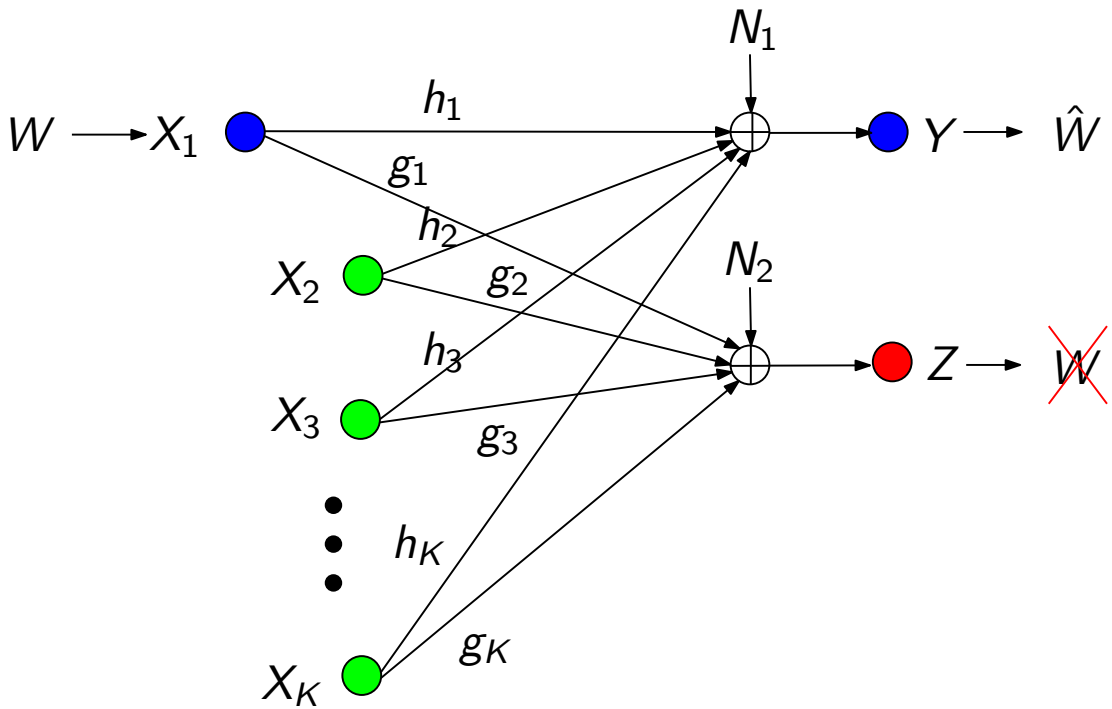


- The channel matrices $\mathbf{H}_i$ are *known* at the transmitters.
- The channel matrices $\mathbf{G}_i$ are *unknown* at the transmitters.
- **Question:** What is the optimal sum s.d.o.f.?

Prior Work

The SISO Wiretap Channel with Helpers

- For the SISO wiretap channels with $K-1$ helpers:

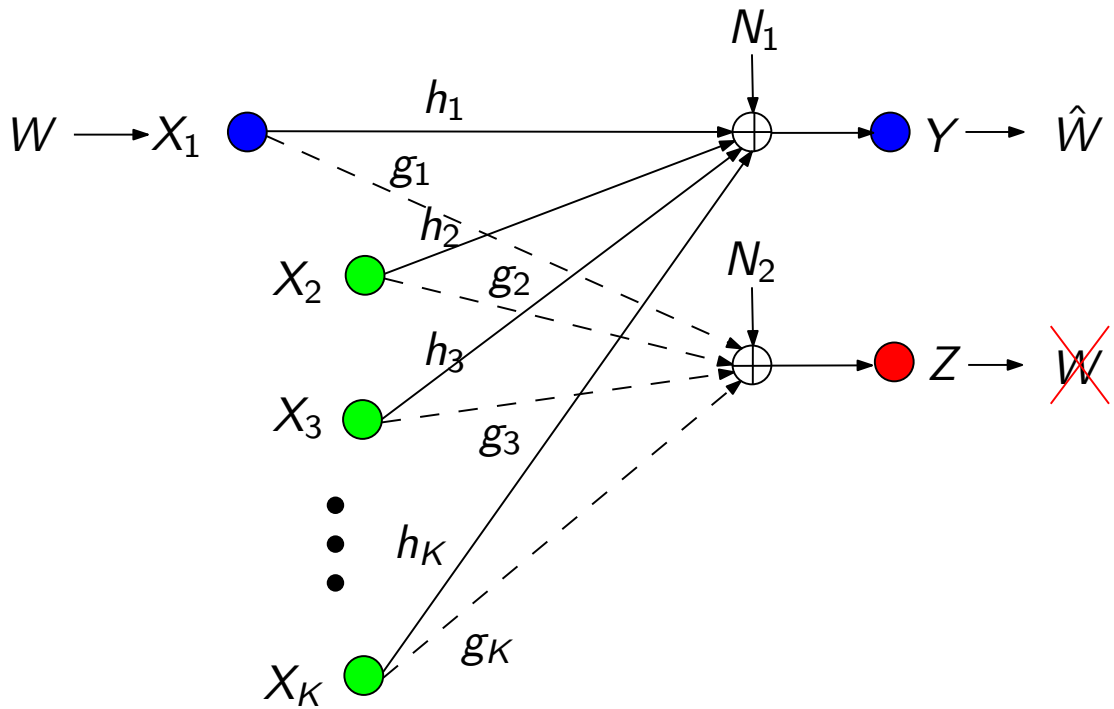


- *With* eavesdropper CSIT[a], optimal s.d.o.f. $= \frac{K-1}{K}$.

[a] Xie, Ulukus (2012)
[b] Xie, Ulukus (2013)

The SISO Wiretap Channel with Helpers

- For the SISO wiretap channels with $K-1$ helpers:

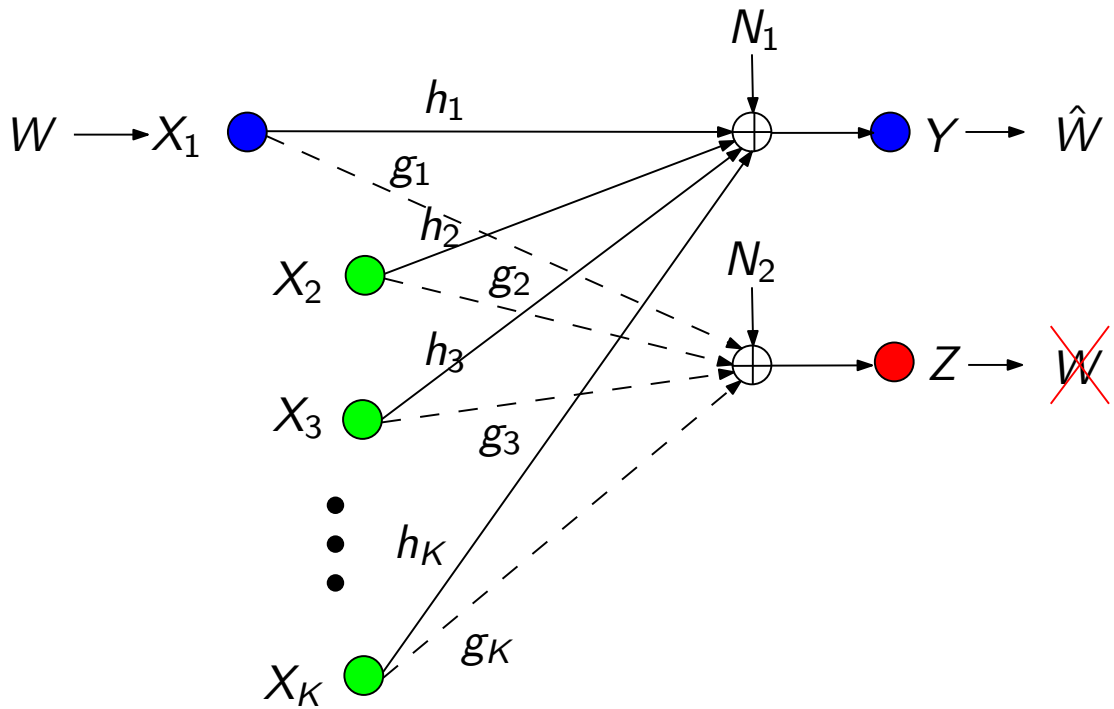


- *With* eavesdropper CSIT[a], optimal s.d.o.f. $= \frac{K-1}{K}$.
- *Without* eavesdropper CSIT[b], optimal s.d.o.f. $= \frac{K-1}{K}$.

[a] Xie, Ulukus (2012)
[b] Xie, Ulukus (2013)

The SISO Wiretap Channel with Helpers

- For the SISO wiretap channels with $K-1$ helpers:

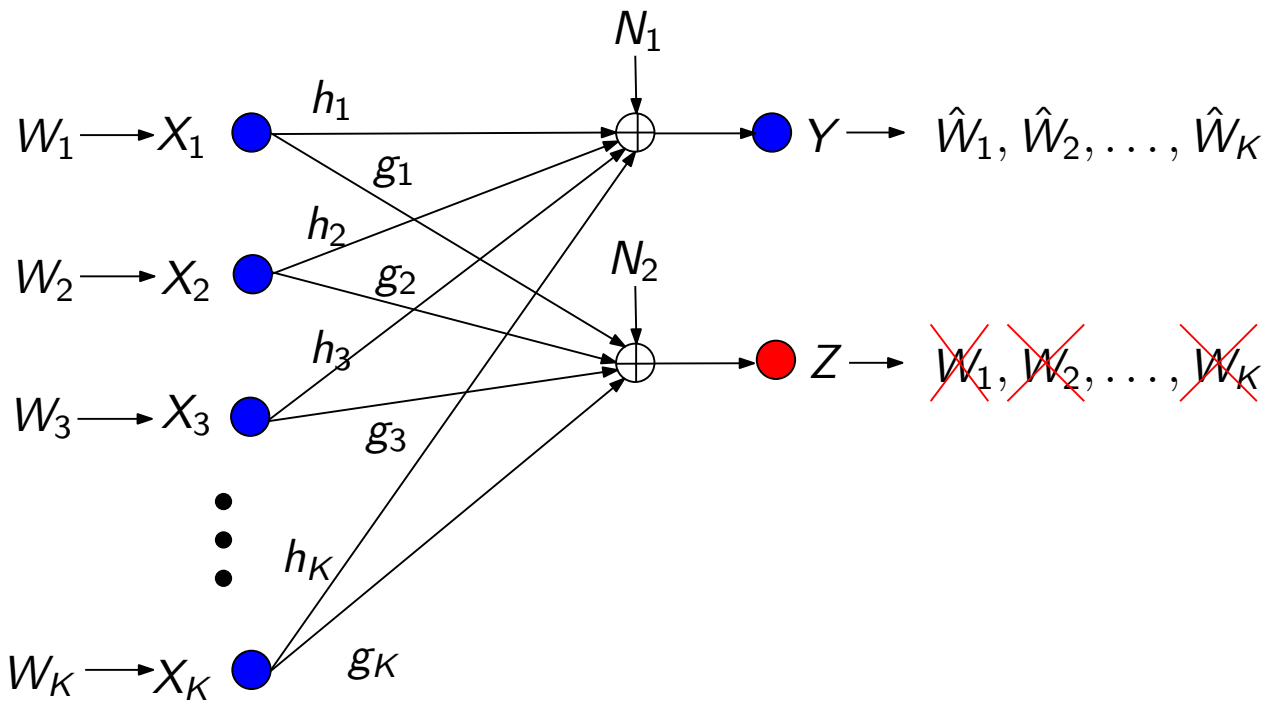


- *With* eavesdropper CSIT[a], optimal s.d.o.f. $= \frac{K-1}{K}$.
- *Without* eavesdropper CSIT[b], optimal s.d.o.f. $= \frac{K-1}{K}$.
- No loss of s.d.o.f. due to lack of eavesdropper CSIT.

[a] Xie, Ulukus (2012)
[b] Xie, Ulukus (2013)

The SISO Multiple Access Wiretap Channel

- For the SISO K-user MAC-WT channel:

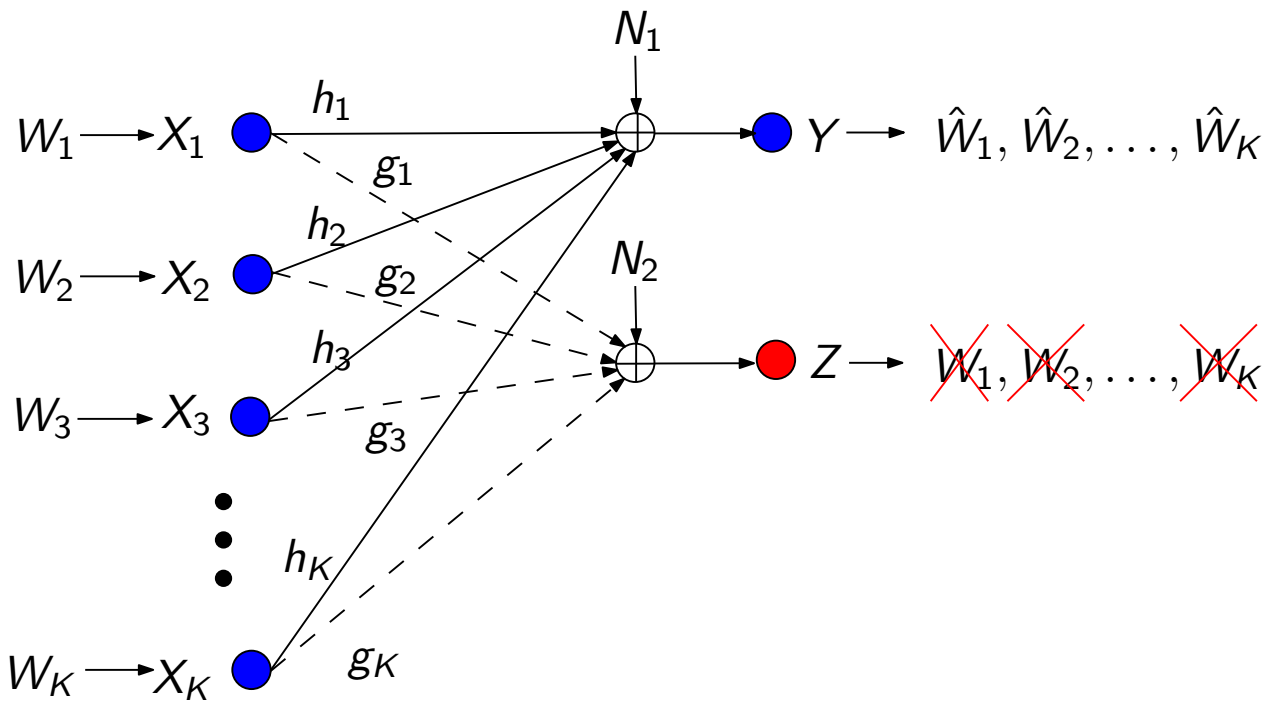


- *With* eavesdropper CSIT[a], optimal sum s.d.o.f. $= \frac{K(K-1)}{K(K-1)+1}$.

[a] Xie, Ulukus (2013)
[b] Mukherjee, Ulukus (2015)

The SISO Multiple Access Wiretap Channel

- For the SISO K-user MAC-WT channel:

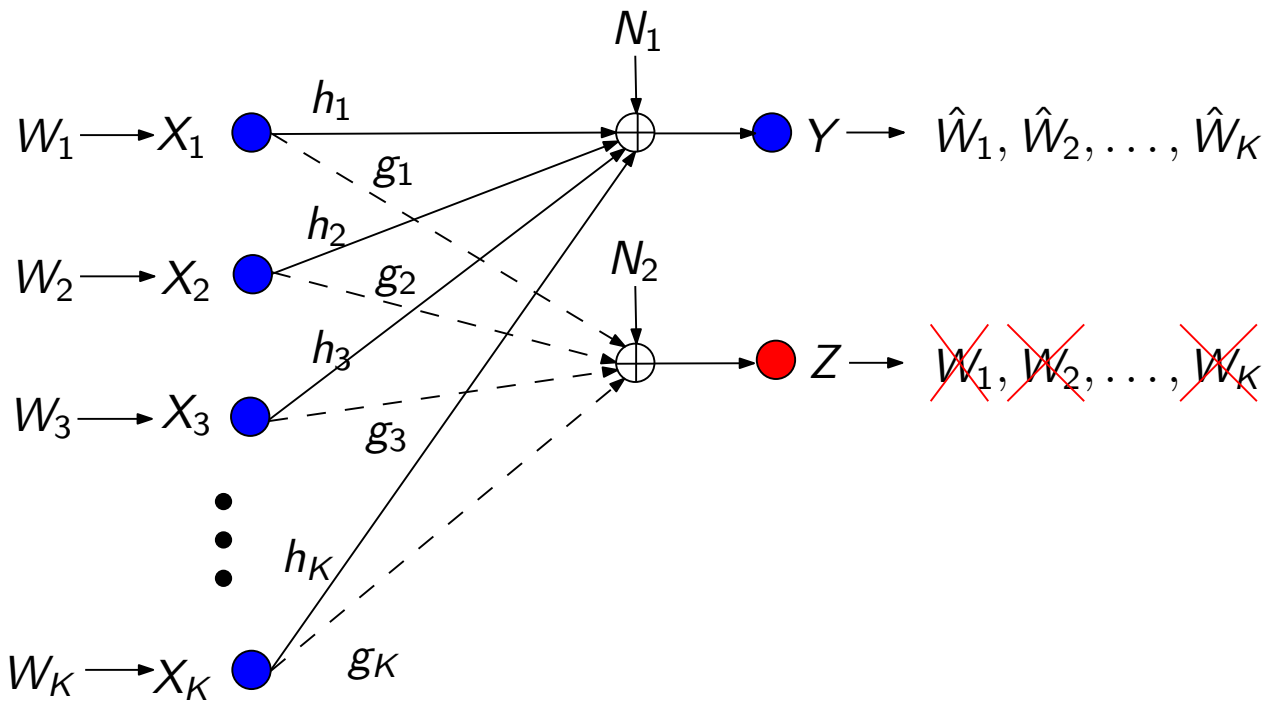


- *With* eavesdropper CSIT[a], optimal sum s.d.o.f. $= \frac{K(K-1)}{K(K-1)+1}$.
- *Without* eavesdropper CSIT[b], optimal sum s.d.o.f. $= \frac{K-1}{K}$.

[a] Xie, Ulukus (2013)
[b] Mukherjee, Ulukus (2015)

The SISO Multiple Access Wiretap Channel

- For the SISO K-user MAC-WT channel:

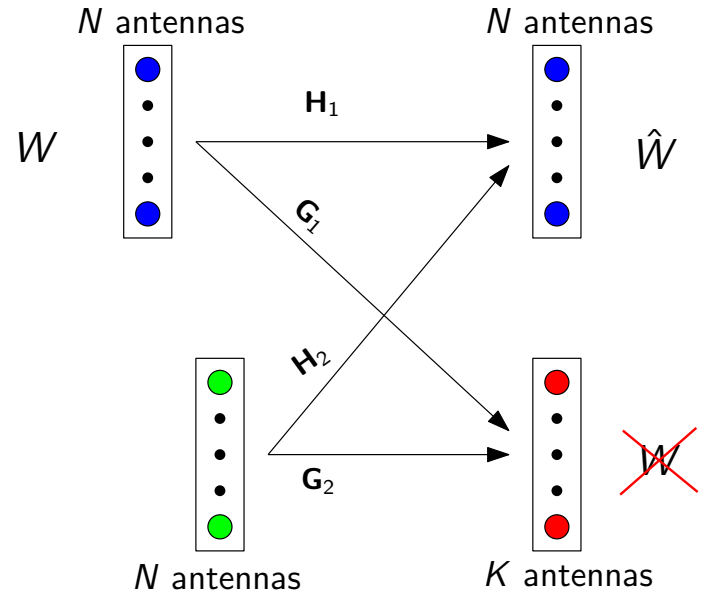


- *With* eavesdropper CSIT[a], optimal sum s.d.o.f. $= \frac{K(K-1)}{K(K-1)+1}$.
- *Without* eavesdropper CSIT[b], optimal sum s.d.o.f. $= \frac{K-1}{K}$.
- Loss of s.d.o.f. due to lack of eavesdropper CSIT.

[a] Xie, Ulukus (2013)
[b] Mukherjee, Ulukus (2015)

The MIMO WTH With Eve CSIT

- Consider the $N \times N \times N \times K$ MIMO WTH:

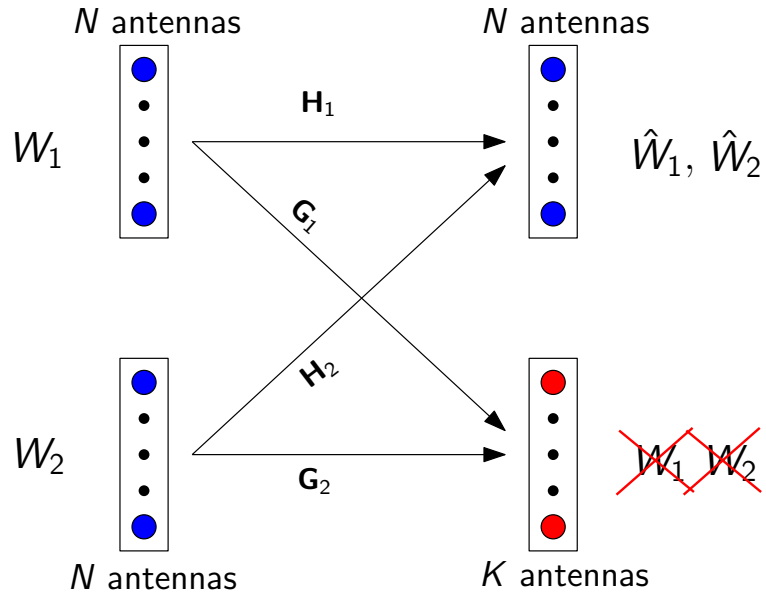


- All channel gains are known perfectly at every terminal.
- The optimal s.d.o.f. is known with Eve CSIT[a].
- **Question:** What is the optimal s.d.o.f. **without** Eve CSIT?

[a] Nafea, Yener (2015)

The MIMO MAC-WT With Eve CSIT

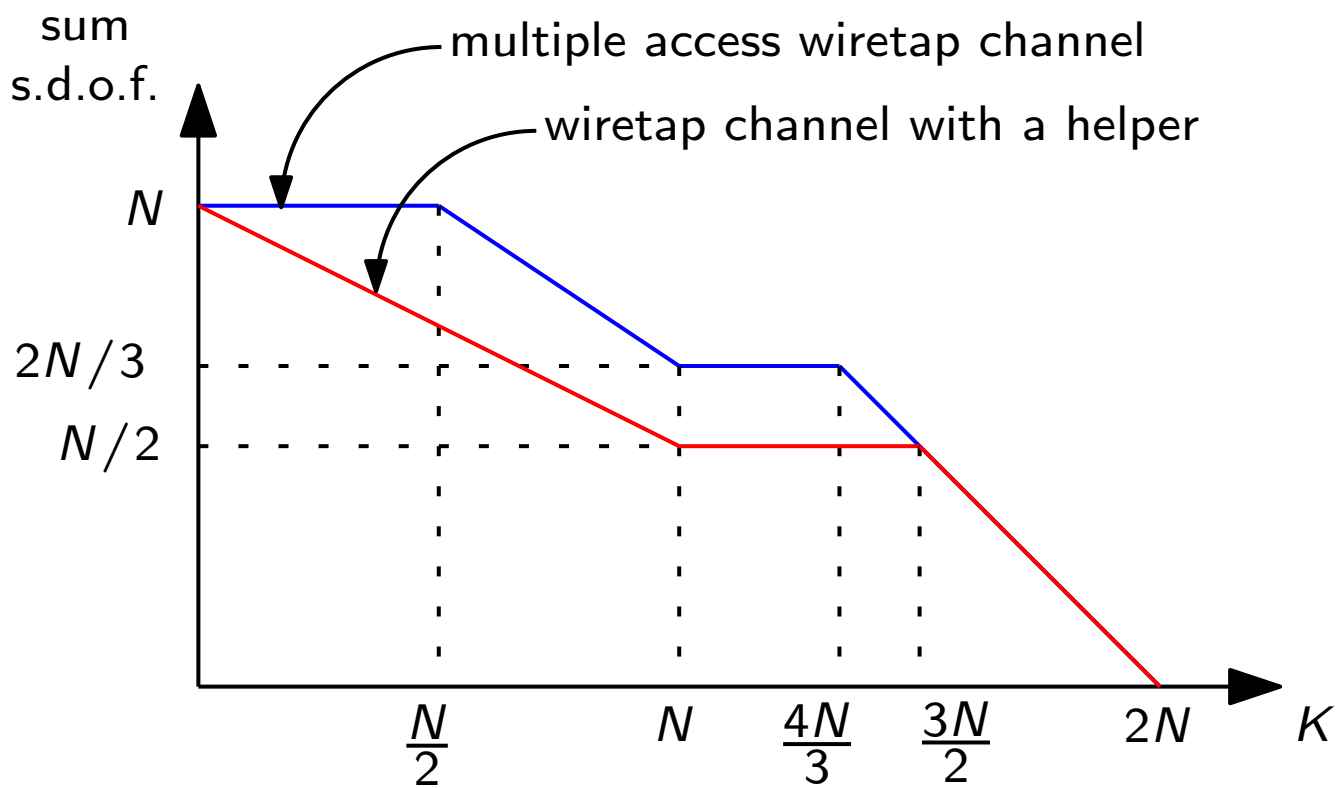
- Consider the two-user $N \times N \times N \times K$ MIMO MAC-WT channel:



- All channel gains are known perfectly at every terminal.
- The optimal s.d.o.f. is known with Eve CSIT[a].
- **Question:** What is the optimal sum s.d.o.f. **without** Eve CSIT?

[a] Mukherjee, Ulukus (2015)

Known Results with Eve CSIT



Our Results

A Linear S.d.o.f. Perspective

- **Linear Encoding Schemes:**
  - Coding blocklength $= n$.
  - $m_i(n)$ information symbols $\mathbf{v}_i \in \mathbb{R}^{m_i(n)}$ from transmitter i.
  - $n_i(n)$ artificial noise symbols, $\mathbf{u}_i \in \mathbb{R}^{n_i(n)}$ from transmitter i.
  - Each symbol $v_i, u_i \sim \mathcal{N}(0, \alpha P)$.
  - At time t, transmitter i sends:

$$\mathbf{X}_i(t) = \mathbf{P}_i(t)\mathbf{v}_i + \mathbf{Q}_i(t)\mathbf{u}_i$$

    where $\mathbf{P}_i(t) \in \mathbb{R}^{N \times m_i(n)}$, $\mathbf{Q}_i(t) \in \mathbb{R}^{N \times n_i(n)}$.
  - α is chosen to satisfy the power constraint.
- Receiver must decode all intended information symbols.
- The information symbols must be buried in artificial noise at Eve.
- Linear s.d.o.f. carried by $\mathbf{v}_i$, denoted by $d_i = \frac{m_i(n)}{n}$.
- Optimal linear s.d.o.f. is the supremum of $d_1 + d_2$ over all **linear encoding schemes**.

Our Results:

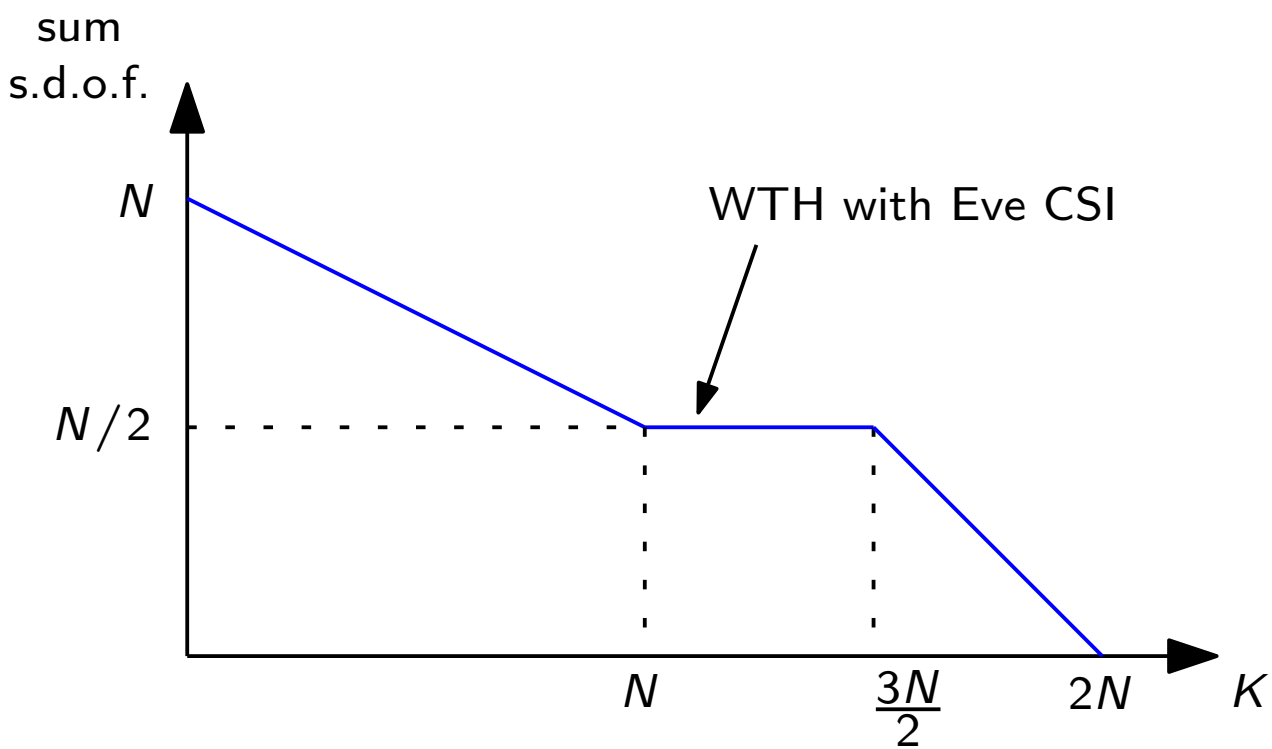
- **Theorem:** For both the $N \times N \times N \times K$ WTH and the MAC-WT channel with no Eve CSIT, the optimal linear sum s.d.o.f. d_s^{lin} is

$$d_s^{lin} = \max\left(\frac{1}{2}(2N-K), 0\right)$$

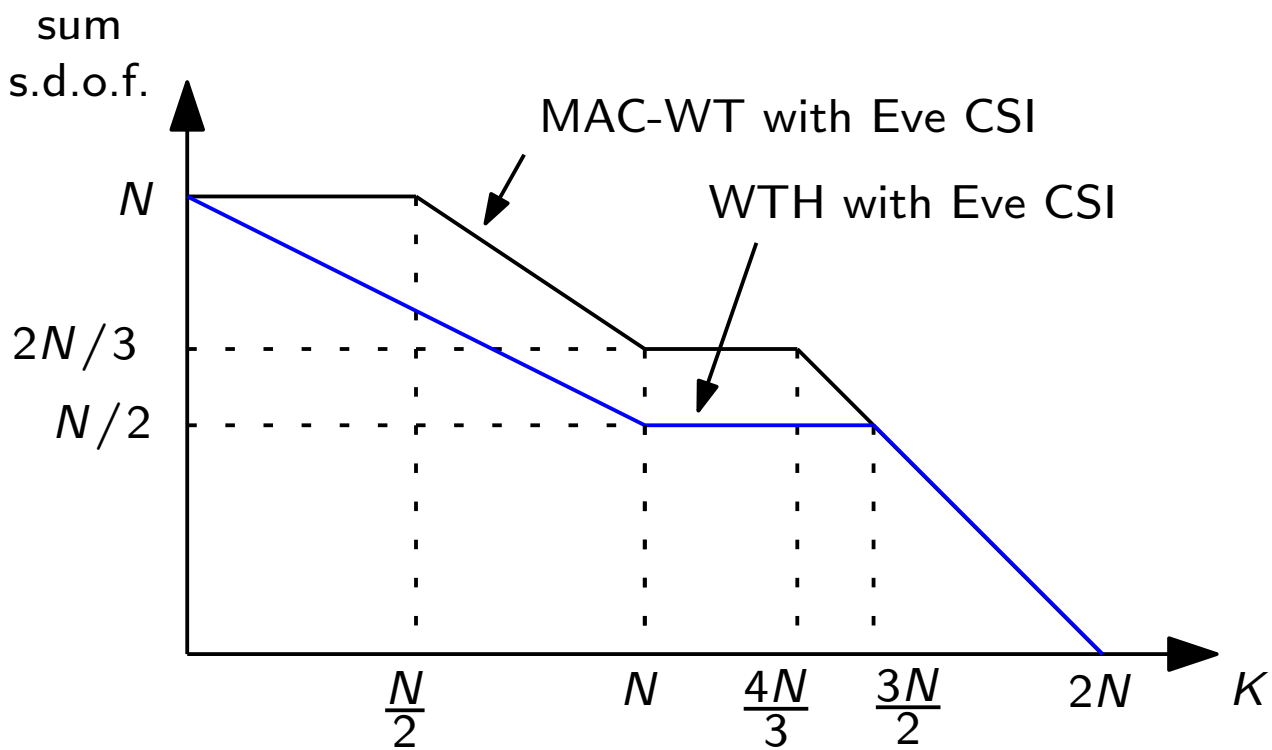
for almost all channel gains. Further, without any linearity constraints, the optimal sum s.d.o.f. d_s is

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

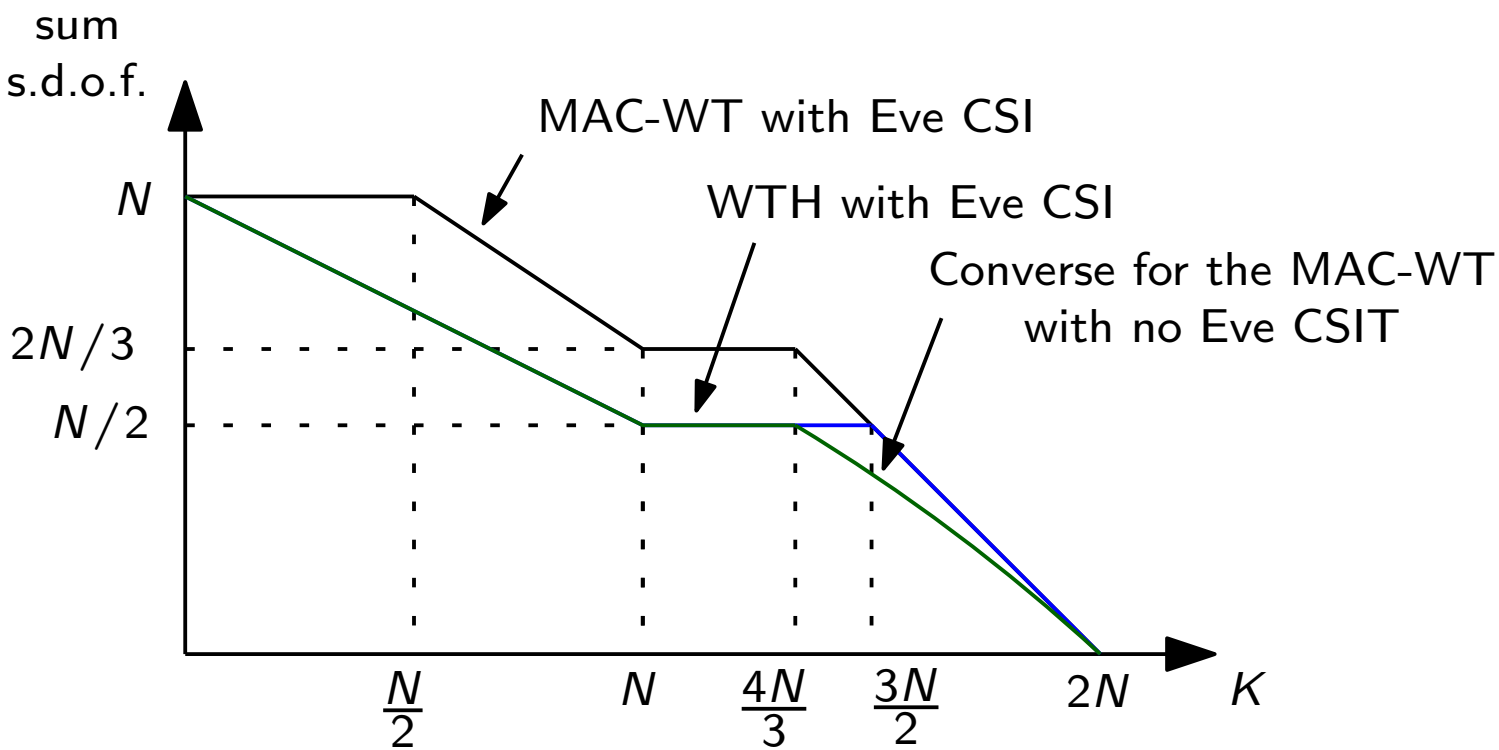
Our Results (Contd.)



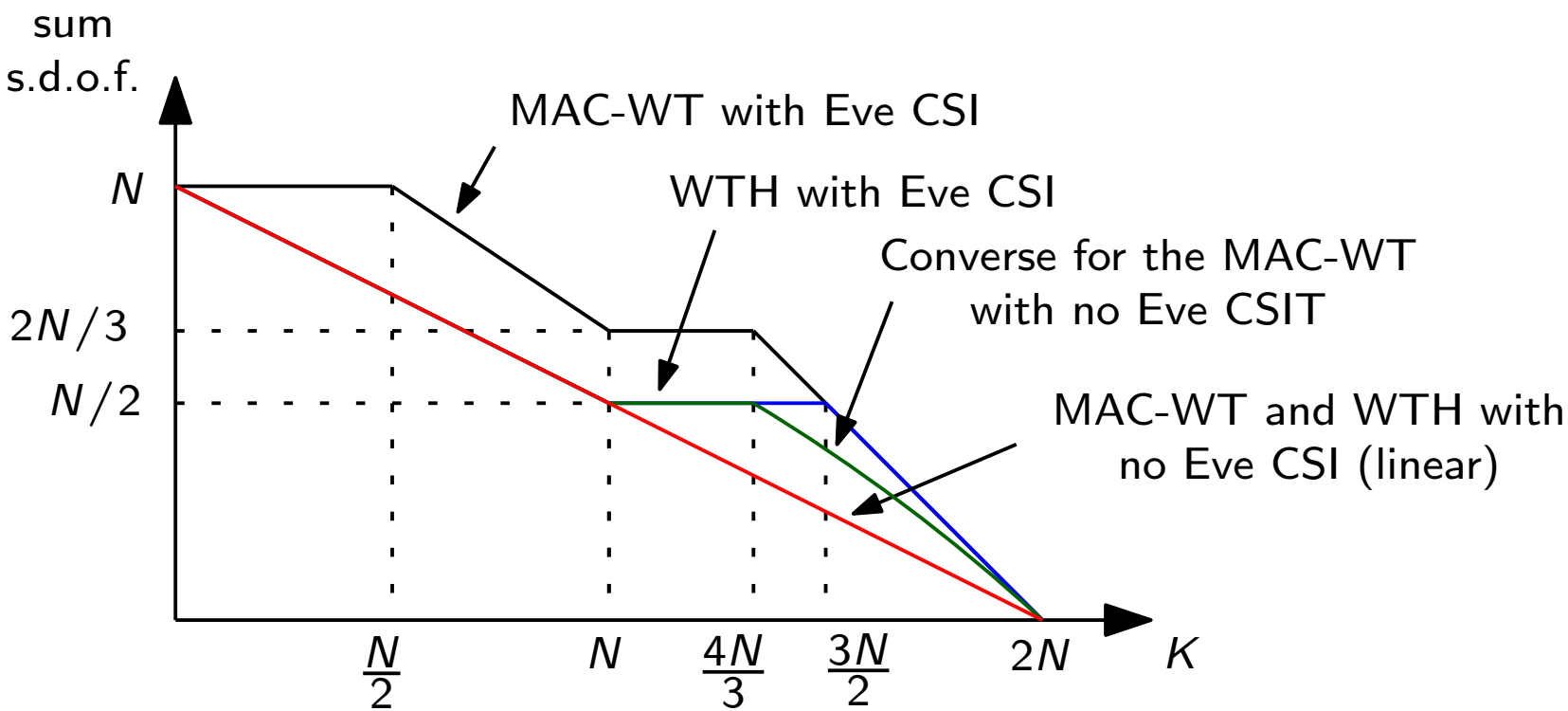
Our Results (Contd.)



Our Results (Contd.)



Our Results (Contd.)



A Few Remarks

- Like the SISO case, there is loss of s.d.o.f. for the MAC-WT channel due to no Eve CSIT for all values of K.
- When $K \leq N$, there is no loss of s.d.o.f. for the WTH due to no Eve CSIT, as in the SISO case.
- Unlike the SISO case, however, there is loss of s.d.o.f. for the WTH due to no Eve CSIT when $K > N$.
- From a linear s.d.o.f. perspective, the MAC-WT channel reduces to a WTH under no Eve CSIT, as in the SISO case.
- Suffices to show a converse for the MAC-WT channel and achievability for the WTH.

Proof Sketches

General Converse for the MAC-WT channel

- **Key Tools:**
  1. Channel symmetry: Since the transmitters have no Eve CSIT, the outputs of Eve's antennas $\mathbf{Z} = \{\mathbf{Z}_1, \ldots, \mathbf{Z}_K\}$ are *entropy symmetric*, i.e., for any subsets A and B of $\{1, \ldots, K\}$, with $|A| = |B| \leq K$,

$$h(\{\mathbf{Z}_i, i \in A\}) = h(\{\mathbf{Z}_i, i \in B\})$$

Lemma[a]**:** For any $M \geq N$, the following holds:

$$\frac{1}{N} h(\mathbf{Z}^N) \geq \frac{1}{M} h(\mathbf{Z}^M)$$

  2. Least alignment lemma[b]: Since no Eve CSIT is available,

$$h(\mathbf{Z}^M) \geq h(\mathbf{Y}^M) + n\, o(\log P) \quad \forall M \leq \min(N, K)$$

[a] Yang et al. (2013)
[b] Davoodi, Jafar (2014)

General Converse: $K \leq N$

- **Step 1:** Use secrecy penalty[a] lemma:

$$n(R_1 + R_2) \leq h(\mathbf{X}_1) + h(\mathbf{X}_2) - h(\mathbf{Z})$$

- **Step 2:** Use role of a helper[a] lemma:

$$\begin{aligned} nR_1 &\leq h(\mathbf{Y}) - h(\mathbf{X}_2) \\ nR_2 &\leq h(\mathbf{Y}) - h(\mathbf{X}_1) \end{aligned}$$

- **Step 3:** Combining the above:

$$2n(R_1 + R_2) \leq 2h(\mathbf{Y}) - h(\mathbf{Z}) \tag{1}$$

[a] Xie, Ulukus (2013)

General Converse: $K \leq N$ (Contd.)

- Consider $N-K$ additional antennas at Eve: $\tilde{\mathbf{Z}} = \left\{\mathbf{Z}, \tilde{\mathbf{Z}}_1, \ldots \tilde{\mathbf{Z}}_{N-K}\right\}$.
- Channel symmetry[a] implies:

$$\frac{1}{K} h(\mathbf{Z}) \geq \frac{1}{N} h(\tilde{\mathbf{Z}})$$

- Least alignment lemma[b] implies:

$$h(\tilde{\mathbf{Z}}) \geq h(\mathbf{Y}) + n\, o(\log P)$$

- **Step 4:** Combining the above:

$$h(\mathbf{Z}) \geq \frac{K}{N} h(\mathbf{Y}) + n\, o(\log P) \tag{2}$$

[a] Yang et al. (2013)
[b] Davoodi, Jafar (2014)

General Converse: $K \leq N$ (Contd.)

- Combining (1) and (2),

$$\begin{aligned} 2n(R_1 + R_2) \leq & 2h(\mathbf{Y}) - h(\mathbf{Z}) \\ \leq & 2h(\mathbf{Y}) - \frac{K}{N} h(\mathbf{Y}) \\ = & \frac{2N - K}{N} h(\mathbf{Y}) \\ \leq & (2N - K) \left(\frac{n}{2} \log P \right) \end{aligned}$$

- Dividing by n and $\log P$, and letting $P \to \infty$

$$d_1 + d_2 \leq \frac{1}{2}(2N - K)$$

General Converse: $K \geq N$

- When $K \geq N$, channel symmetry implies:

$$\begin{aligned} h(\mathbf{Z}) \geq & \frac{K}{2N} h(\mathbf{Z}, \tilde{\mathbf{Z}}_1, \ldots, \tilde{\mathbf{Z}}_{2N-K}) + n\, o(\log P) \\ \geq & \frac{K}{2N} \left(h(\mathbf{X}_1) + h(\mathbf{X}_2) \right) + n\, o(\log P) \end{aligned}$$

- Combining with secrecy penalty and role of a helper lemmas:

$$\begin{aligned} n(R_1 + R_2) \leq & h(\mathbf{X}_1) + h(\mathbf{X}_2) - h(\mathbf{Z}) \\ nR_1 \leq & h(\mathbf{Y}) - h(\mathbf{X}_2) \\ nR_2 \leq & h(\mathbf{Y}) - h(\mathbf{X}_1) \end{aligned}$$

  and using $h(\mathbf{Y}) \leq N \left(\frac{n}{2} \log P \right)$, we have,

$$n(R_1 + R_2) \leq \frac{2N(2N-K)}{(4N-K)} \left(\frac{1}{2} \log P \right) + n\, o(\log P)$$

- Therefore, $d_1 + d_2 \leq \frac{2N(2N-K)}{(4N-K)}$. Also, $d_1 + d_2 \leq \frac{N}{2}$, trivially.

Linear Converse: $0 \leq K \leq 2N$

- The channel input structure is:

$$\mathbf{X}_i = \mathbf{P}_i \mathbf{v}_i + \mathbf{Q}_i \mathbf{u}_i$$

  where $\mathbf{v}_i$ and $\mathbf{u}_i$ denote information and artificial noise symbols. $\mathbf{P}_i$ and $\mathbf{Q}_i$ are channel precoding matrices over n channel uses.

- The channel outputs over n channel uses are

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

- **Correspondence between general and linear quantities**, (normalized by $\frac{1}{2}\log P$):

$$\begin{aligned} h(\mathbf{Y}) &\Leftrightarrow \operatorname{rank}[\mathbf{H}_1\mathbf{P}_1, \mathbf{H}_2\mathbf{P}_2, \mathbf{H}_1\mathbf{Q}_1, \mathbf{H}_2\mathbf{Q}_2] \\ h(\mathbf{Z}) &\Leftrightarrow \operatorname{rank}[\mathbf{G}_1\mathbf{P}_1, \mathbf{G}_2\mathbf{P}_2, \mathbf{G}_1\mathbf{Q}_1, \mathbf{G}_2\mathbf{Q}_2] \\ h(\mathbf{Y}|W_1, W_2) &\Leftrightarrow \operatorname{rank}[\mathbf{H}_1\mathbf{Q}_1, \mathbf{H}_2\mathbf{Q}_2] \\ h(\mathbf{Z}|W_1, W_2) &\Leftrightarrow \operatorname{rank}[\mathbf{G}_1\mathbf{Q}_1, \mathbf{G}_2\mathbf{Q}_2] \end{aligned}$$

Linear Converse: $0 \leq K \leq 2N$ (Contd.)

- **Reliability condition:**

$$\begin{aligned}\text{rank}\left[\mathbf{H}_1\mathbf{P}_1, \mathbf{H}_2\mathbf{P}_2, \mathbf{H}_1\mathbf{Q}_1, \mathbf{H}_2\mathbf{Q}_2\right] =& \text{rank}\left[\mathbf{P}_1\right] + \text{rank}\left[\mathbf{P}_2\right] \\ &+ \text{rank}\left[\mathbf{H}_1\mathbf{Q}_1, \mathbf{H}_2\mathbf{Q}_2\right]\end{aligned}$$

- **Security condition:**

$$\text{rank}\left[\mathbf{G}_1\mathbf{P}_1, \mathbf{G}_2\mathbf{P}_2, \mathbf{G}_1\mathbf{Q}_1, \mathbf{G}_2\mathbf{Q}_2\right] - \text{rank}\left[\mathbf{G}_1\mathbf{Q}_1, \mathbf{G}_2\mathbf{Q}_2\right] \leq o(n)$$

- Intuition: The information symbols must be separable from the artificial noise dimensions at the receiver for reliability, and buried in artificial noise at the eavesdropper for security.

Linear Converse: $0 \leq K \leq 2N$ (Contd.)

- **Key lemma:** Since no alignment is possible at Eve, the artificial noise symbols must occupy the full space at Eve, for security, i.e.,

$$\text{rank}\,[\mathbf{G}_1\mathbf{Q}_1, \mathbf{G}_2\mathbf{Q}_2] = Kn + o(n)$$

- Therefore,

$$\text{rank}\,[\mathbf{G}_1\mathbf{P}_1, \mathbf{G}_2\mathbf{P}_2, \mathbf{G}_1\mathbf{Q}_1, \mathbf{G}_2\mathbf{Q}_2] = Kn + o(n)$$

- Following the converse proof in the general case, we have:

$$2n(R_1 + R_2) \leq 2h(\mathbf{Y}) - h(\mathbf{Z})$$

Linear Converse: $0 \leq K \leq 2N$ (Contd.)

- **Key lemma:** Since no alignment is possible at Eve, the artificial noise symbols must occupy the full space at Eve, for security, i.e.,

$$\text{rank}\,[\mathbf{G}_1\mathbf{Q}_1, \mathbf{G}_2\mathbf{Q}_2] = Kn + o(n)$$

- Therefore,

$$\text{rank}\,[\mathbf{G}_1\mathbf{P}_1, \mathbf{G}_2\mathbf{P}_2, \mathbf{G}_1\mathbf{Q}_1, \mathbf{G}_2\mathbf{Q}_2] = Kn + o(n)$$

- Following the converse proof in the general case, we have:

$$\begin{aligned} 2n(d_1 + d_2) \leq & 2 \times \text{rank}\,[\mathbf{H}_1\mathbf{P}_1, \mathbf{H}_2\mathbf{P}_2, \mathbf{H}_1\mathbf{Q}_1, \mathbf{H}_2\mathbf{Q}_2] \\ & - \text{rank}\,[\mathbf{G}_1\mathbf{P}_1, \mathbf{G}_2\mathbf{P}_2, \mathbf{G}_1\mathbf{Q}_1, \mathbf{G}_2\mathbf{Q}_2] \\ \leq & n(2N - K) + o(n) \end{aligned}$$

- Therefore, $d_1 + d_2 \leq \frac{1}{2}(2N - K)$.

Achievability for the WTH

- Wish to send $(2N - K)$ symbols, $\mathbf{v}$, in 2 time slots.
- Choose $\mathbf{u}_i \sim \mathcal{N}(\mathbf{0}, \alpha P \mathbf{I}_K)$.
- The channel input is (combined over 2 time slots):

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

- Choose $\mathbf{Q}_i = \mathbf{H}_i^{-1} \mathbf{Q}$.
- The channel outputs over n channel uses are

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

- $(\mathbf{u}_1 + \mathbf{u}_2)$ occupies K out of $2N$ dimensions at $\mathbf{Y} \Rightarrow$ Decoding.
- $\mathbf{G}_1 \mathbf{Q}_1 \mathbf{u}_1 + \mathbf{G}_2 \mathbf{Q}_2 \mathbf{u}_2$ occupies $2K$ dimensions at $\mathbf{Z} \Rightarrow$ Security.

Conclusions and Future Work

Conclusions and Future Work

- Determined the optimal s.d.o.f. for the WTH and the MAC-WT channel without Eve CSIT, with linear encoding strategies.
- Showed optimality for **general** strategies when $K \leq N$.
- MAC-WT channel reduces to the WTH without Eve CSIT when $K \leq N$, and for linear encoding strategies when $K > N$.
- There is loss of s.d.o.f. even for the WTH without Eve CSIT.
- **Open problem:** Develop a general matching converse for $K \geq N$.