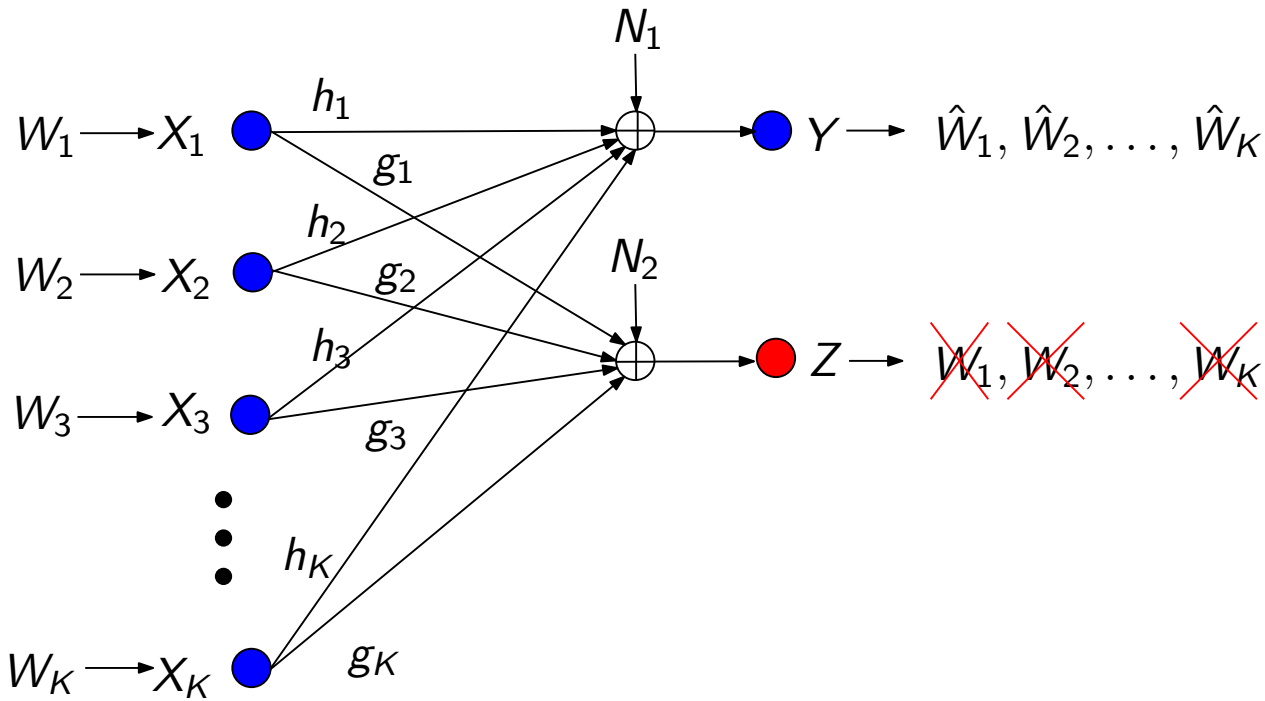
Multiple Access Wiretap Channel with No Eavesdropper CSIT

Pritam Mukherjee Şennur Ulukuş

University of Maryland, College Park

The Mutiple Access Wiretap Channel (MAC-WT)

- Consider the K-user multiple access wiretap channel (MAC-WT)



- **Key factor**: Channel state information at the transmitters (CSIT).
- h_is are known at all the transmitters.
- In practice, g_is are not known at the transmitters.

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,

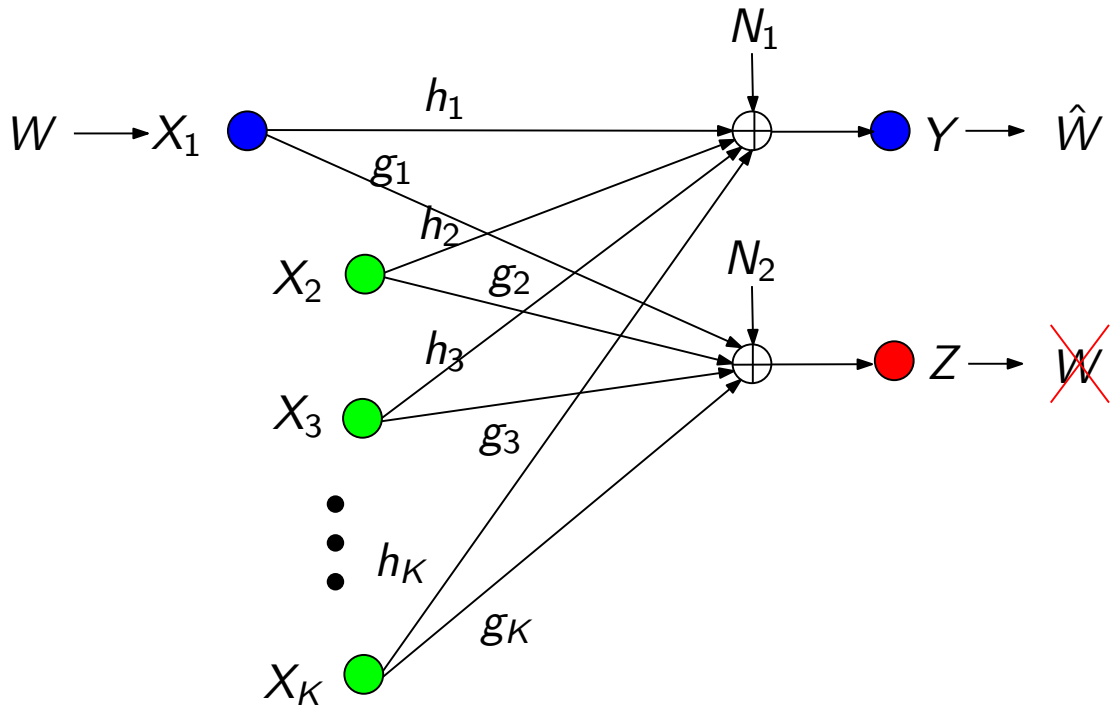
$$\text{d.o.f} = d \quad \Rightarrow \quad C = \frac{d}{2}\log P + o(\log P).$$

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

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

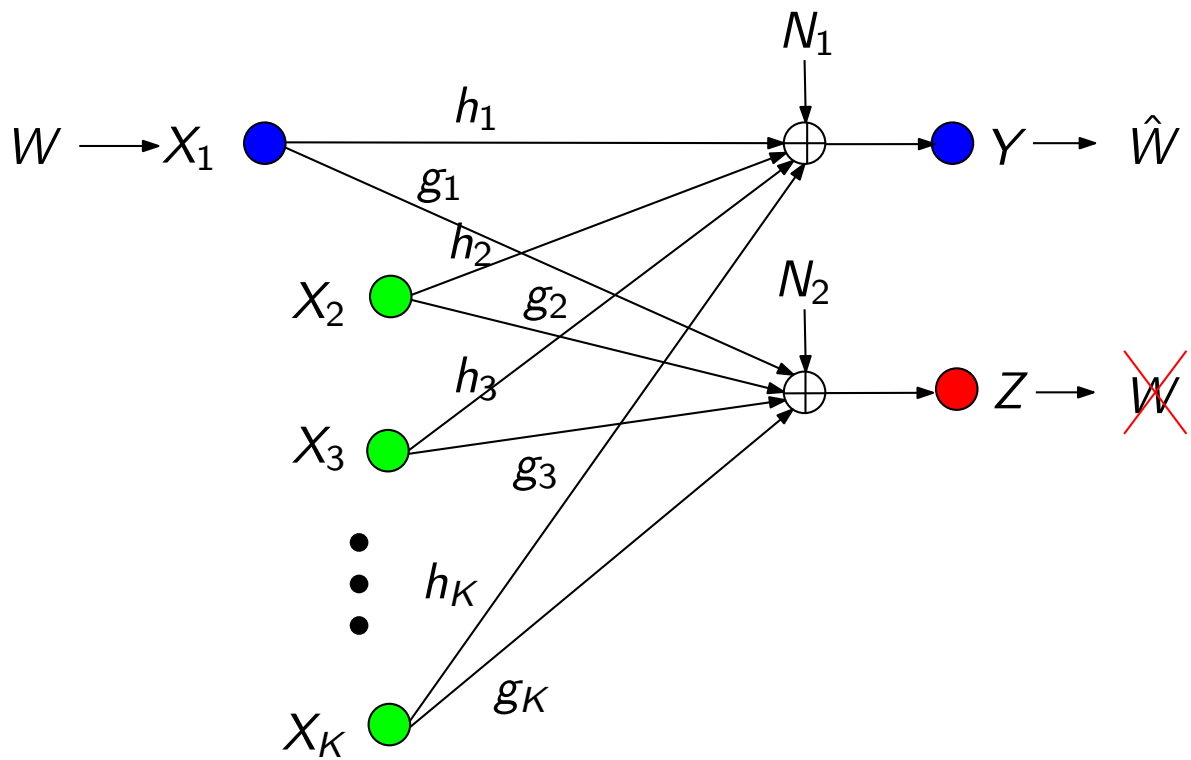
A related model: Wiretap Channel with Helpers (WTH)

- A simpler model: Wiretap channel with $(K-1)$ helpers (WTH).



- Only the first transmitter has a message of its own.
- The other transmitters are *blind* to the first transmitter's message.
- Scheme for WTH + timesharing $\Rightarrow$ Scheme for MAC-WT.

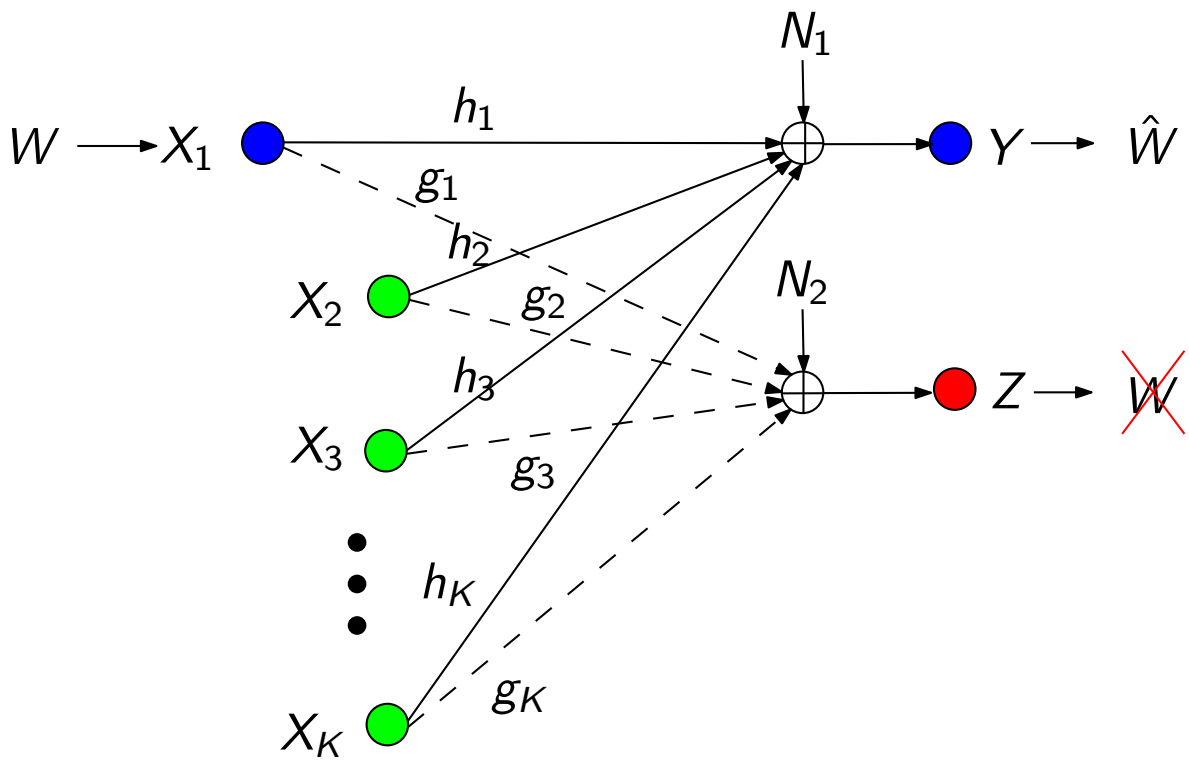
Wiretap Channel with Helpers: Known Results



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

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

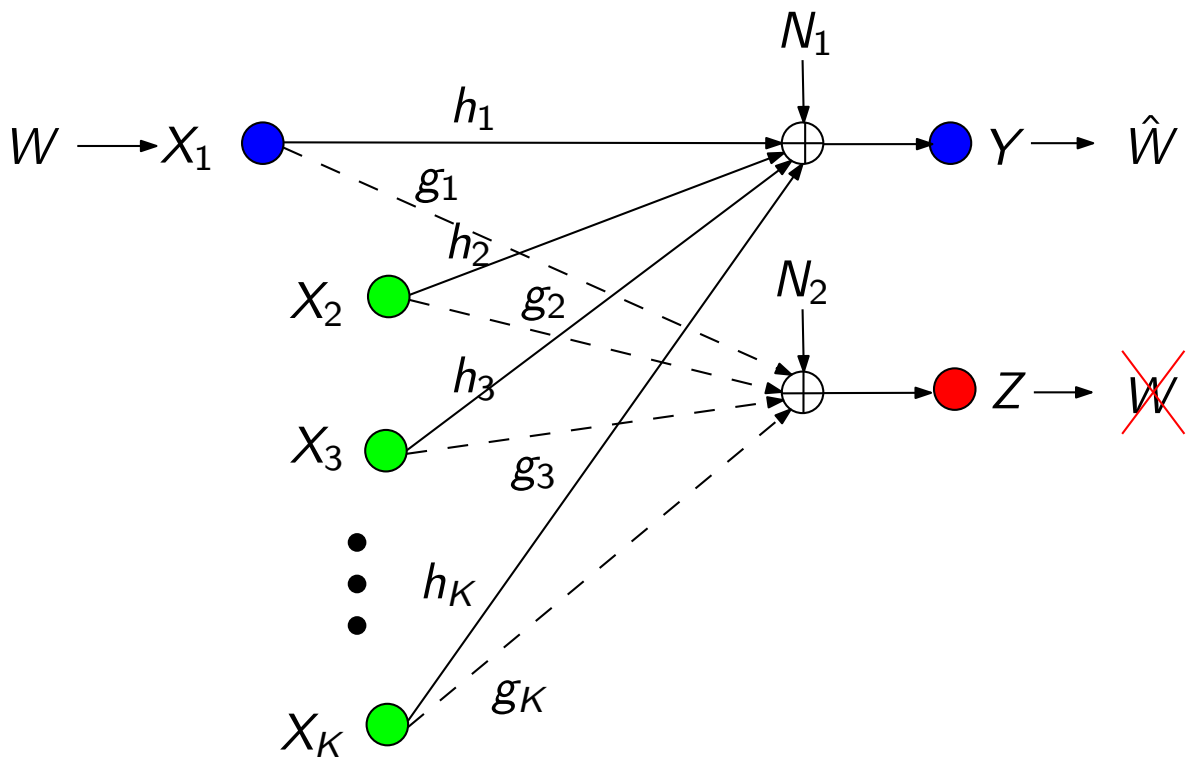
Wiretap Channel with Helpers: Known Results



- *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)

Wiretap Channel with Helpers: Known Results

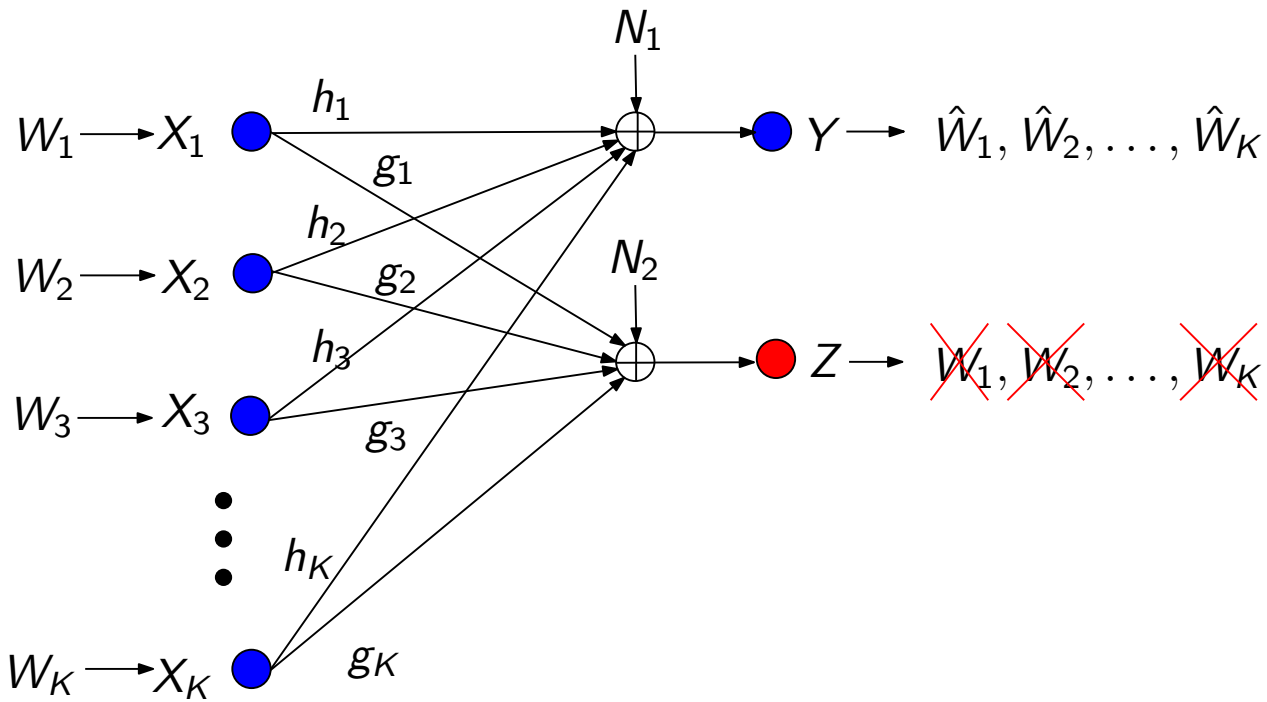


- *With* eavesdropper CSIT[a], optimal s.d.o.f. $= \frac{K-1}{K}$.
- *Without* eavesdropper CSIT[b], optimal s.d.o.f. $= \frac{K-1}{K}$.
- No loss of s.d.o.f. due to lack of eavesdropper CSIT.

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

The MAC-WT with Eavesdropper CSIT

- Assume all the g_is are known at each transmitter.



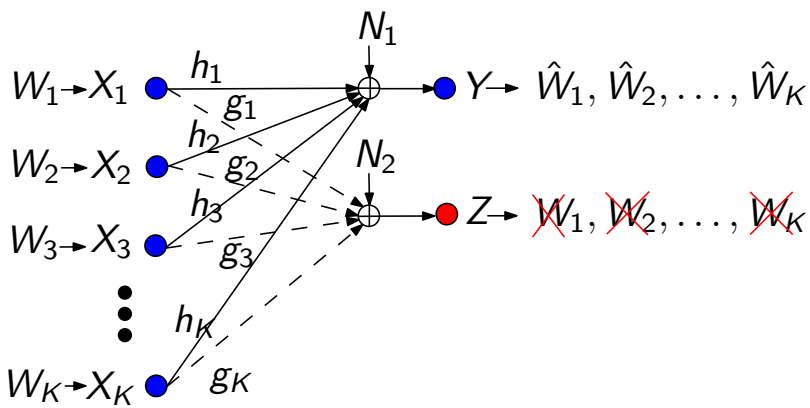
- Optimal sum s.d.o.f.[a] $= \frac{K(K-1)}{K(K-1)+1}$.
- Strictly better than WTH + timesharing, which achieves only $\frac{K-1}{K}$.
- **Question**: What happens when the g_is are unavailable?

[a] Xie, Ulukus (2014)

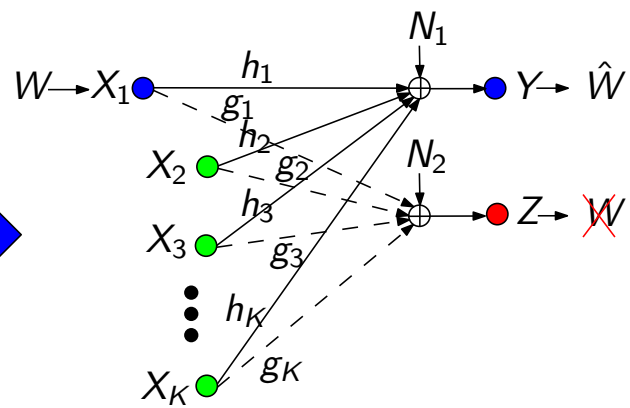
Our Result: MAC-WT with No Eavesdropper CSIT

- With no eavesdropper CSIT, MAC-WT reduces to the WTH.

MAC-WT with no eavesdropper CSIT



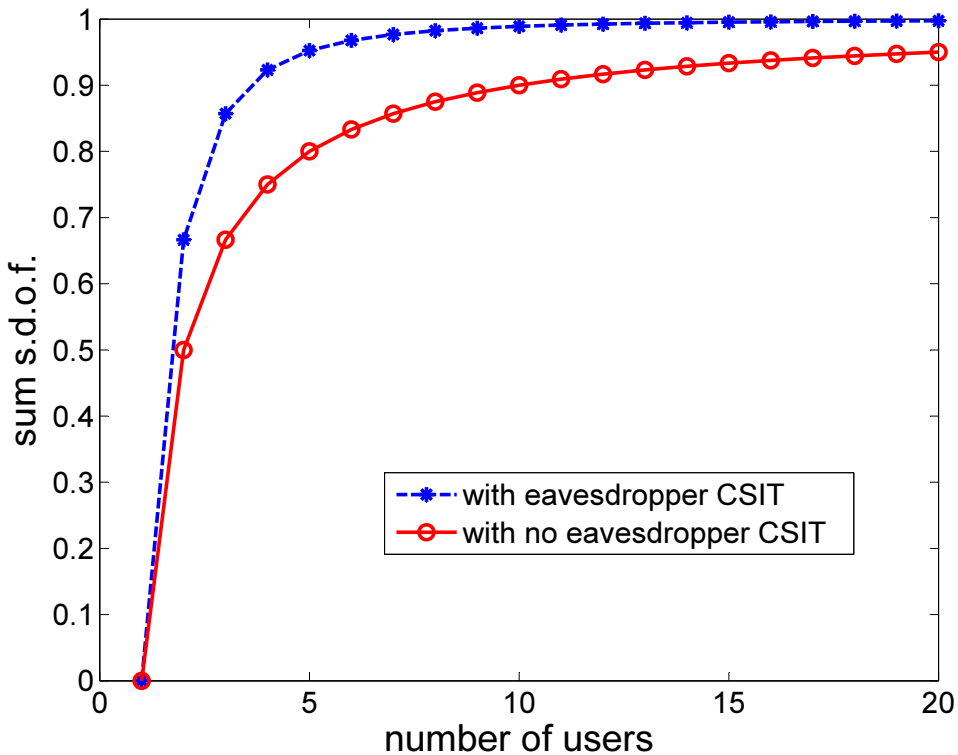
WTH with no eavesdropper CSIT



- Sum s.d.o.f. of MAC-WT with no eavesdropper CSIT $= \frac{K-1}{K}$.
- Scheme for WTH + timesharing $\Rightarrow$ Optimal scheme for MAC-WT.
- S.d.o.f. loss due to lack of eavesdropper CSIT $\left(\frac{K(K-1)}{K(K-1)+1} \Rightarrow \frac{K-1}{K} \right)$.

Our Result: Loss in S.d.o.f.

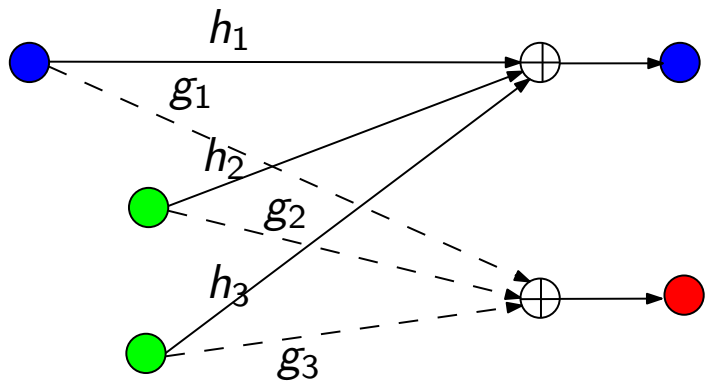
- Optimal sum s.d.o.f., $d_s \to 1$, irrespective of eavesdropper CSIT.



- *With* eavesdropper CSIT, $d_s \to 1$ as $\sim \frac{1}{K^2}$.
- *Without* eavesdropper CSIT, $d_s \to 1$ as $\sim \frac{1}{K}$.

Optimal Transmission Strategy

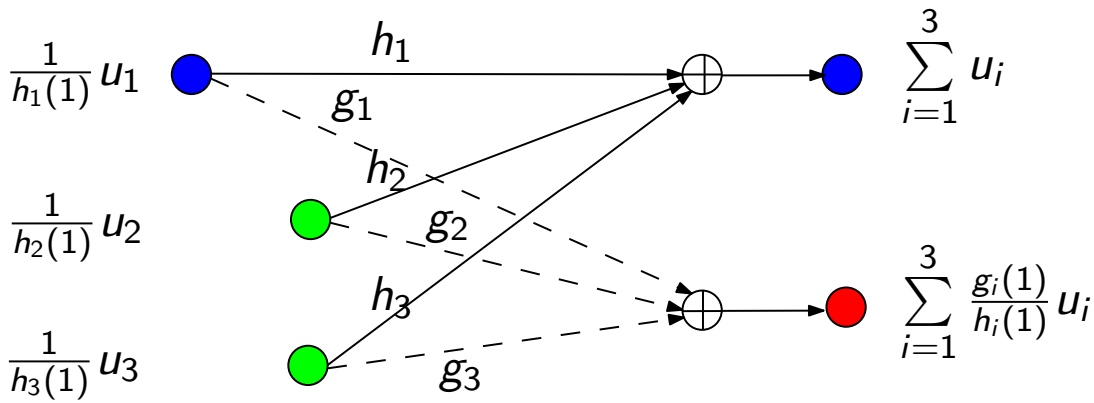
- Treat the MAC-WT as WTH and time-share between transmitters.
- For $K = 3$, send (v_1, v_2) in 3 time slots (optimal sum s.d.o.f. $= \frac{2}{3}$).



Optimal Transmission Strategy

- Treat the MAC-WT as WTH and time-share between transmitters.
- For $K = 3$, send (v_1, v_2) in 3 time slots (optimal sum s.d.o.f. $= \frac{2}{3}$).

$t = 1$

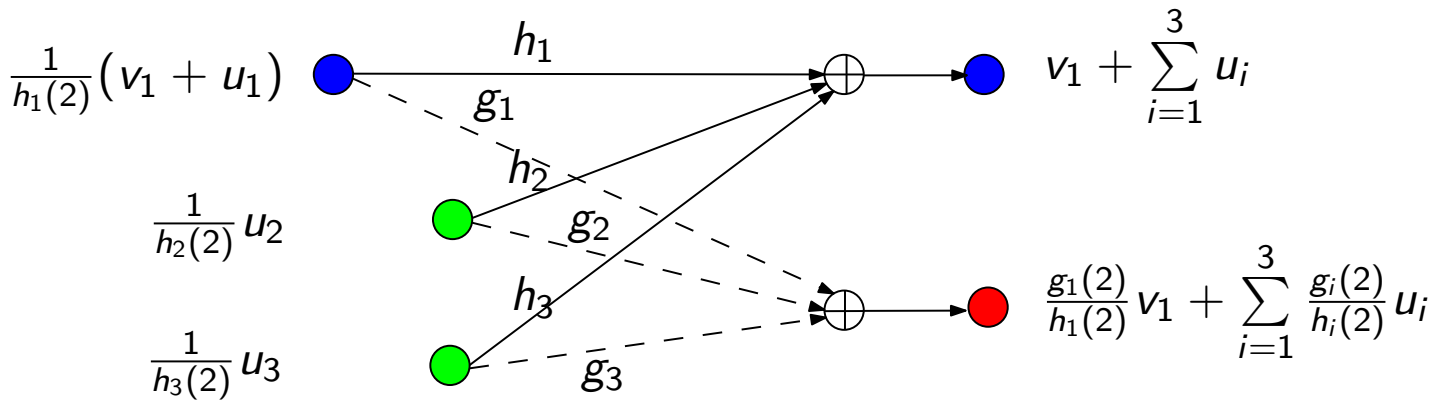


	$t = 1$	$t = 2$	$t = 3$
$Y(t)$	$\sum_{i=1}^{3} u_i$		
$Z(t)$	$\sum_{i=1}^{3} \frac{g_i(1)}{h_i(1)} u_i$		

Optimal Transmission Strategy

- Treat the MAC-WT as WTH and time-share between transmitters.
- For $K = 3$, send (v_1, v_2) in 3 time slots (optimal sum s.d.o.f. $= \frac{2}{3}$).

$t = 2$

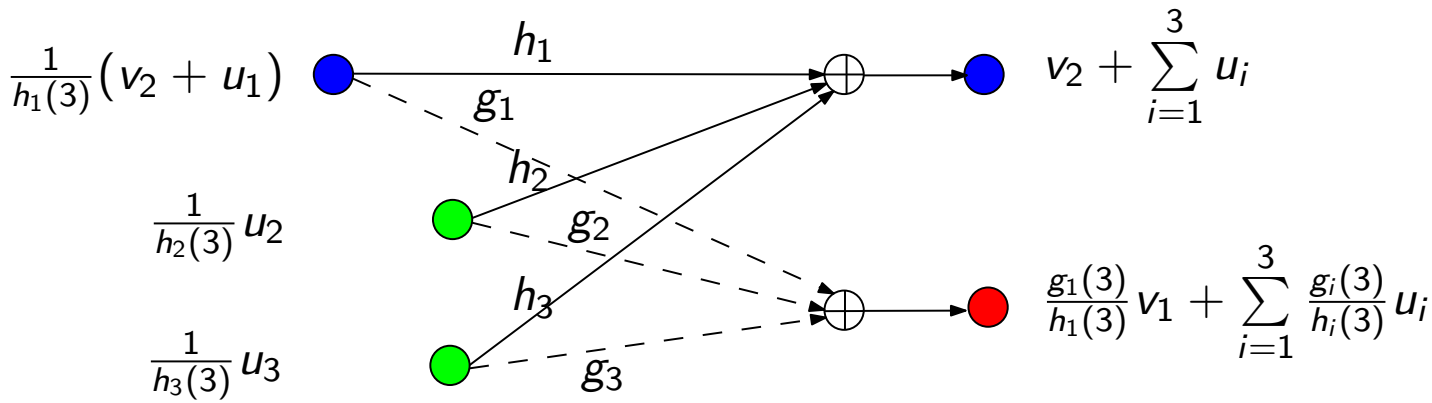


	$t = 1$	$t = 2$	$t = 3$
$Y(t)$	$\sum_{i=1}^{3} u_i$	$v_1 + \sum_{i=1}^{3} u_i$	
$Z(t)$	$\sum_{i=1}^{3} \frac{g_i(1)}{h_i(1)} u_i$	$\frac{g_1(2)}{h_1(2)} v_1 + \sum_{i=1}^{3} \frac{g_i(2)}{h_i(2)} u_i$	

Optimal Transmission Strategy

- Treat the MAC-WT as WTH and time-share between transmitters.
- For $K = 3$, send (v_1, v_2) in 3 time slots (optimal sum s.d.o.f. $= \frac{2}{3}$).

$$t = 3$$

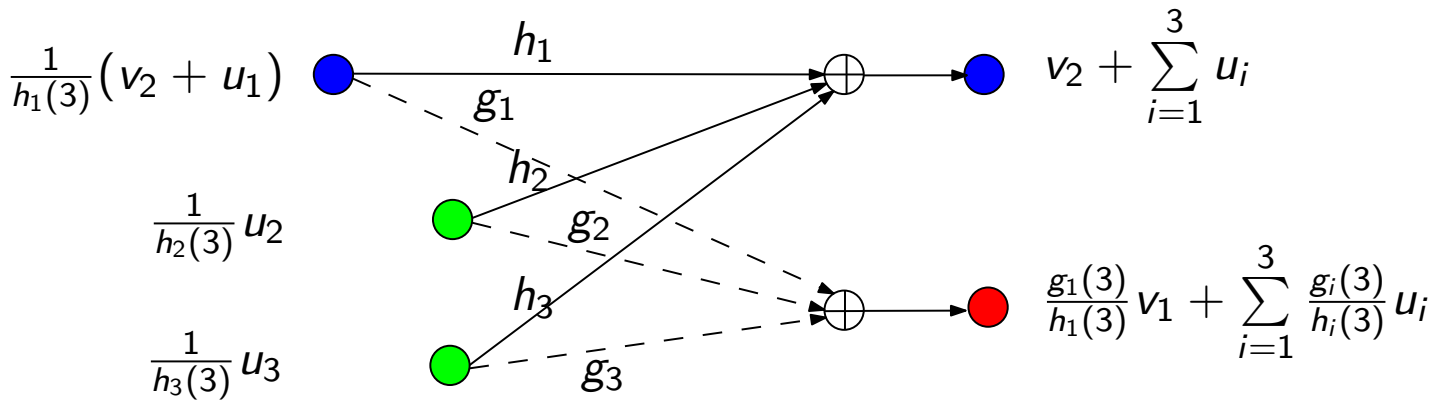


	$t = 1$	$t = 2$	$t = 3$
$Y(t)$	$\sum_{i=1}^{3} u_i$	$v_1 + \sum_{i=1}^{3} u_i$	$v_2 + \sum_{i=1}^{3} u_i$
$Z(t)$	$\sum_{i=1}^{3} \frac{g_i(1)}{h_i(1)} u_i$	$\frac{g_1(2)}{h_1(2)} v_1 + \sum_{i=1}^{3} \frac{g_i(2)}{h_i(2)} u_i$	$\frac{g_1(3)}{h_1(3)} v_1 + \sum_{i=1}^{3} \frac{g_i(3)}{h_i(3)} u_i$

Optimal Transmission Strategy

- Treat the MAC-WT as WTH and time-share between transmitters.
- For $K = 3$, send (v_1, v_2) in 3 time slots (optimal sum s.d.o.f. $= \frac{2}{3}$).

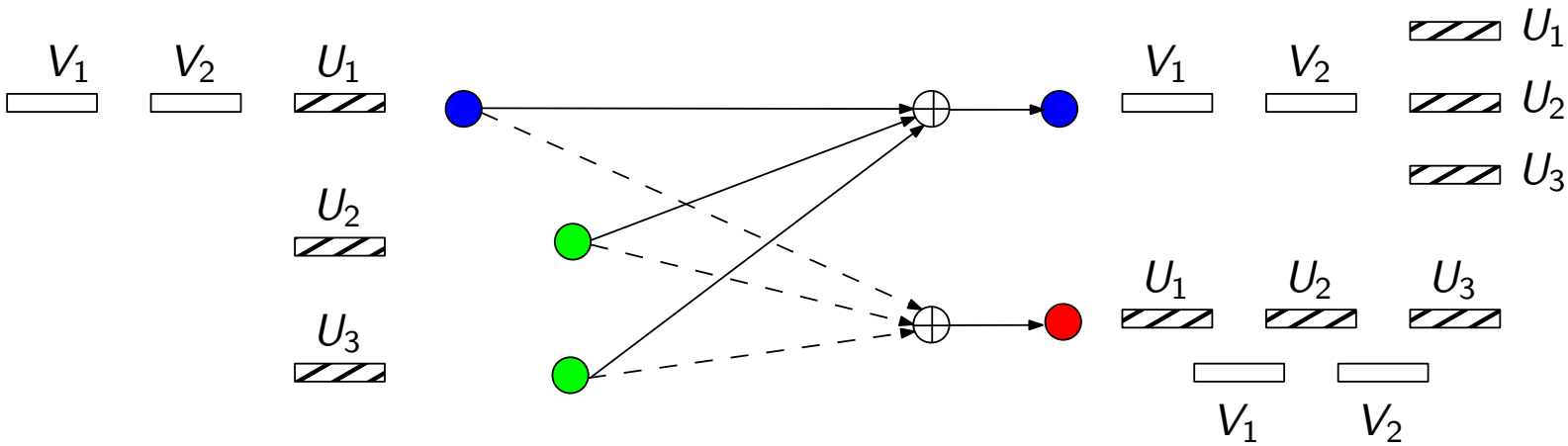
$t = 3$



	$t = 1$	$t = 2$	$t = 3$
$Y(t)$	$\sum_{i=1}^{3} u_i$	$v_1 + \sum_{i=1}^{3} u_i$	$v_2 + \sum_{i=1}^{3} u_i$
$Z(t)$	$\sum_{i=1}^{3} \frac{g_i(1)}{h_i(1)} u_i$	$\frac{g_1(2)}{h_1(2)} v_1 + \sum_{i=1}^{3} \frac{g_i(2)}{h_i(2)} u_i$	$\frac{g_1(3)}{h_1(3)} v_1 + \sum_{i=1}^{3} \frac{g_i(3)}{h_i(3)} u_i$

Main Idea: Signal Alignment

- Signal alignment over 3 time slots.



- At the legitimate receiver:
  - The artificial noise symbols align in a *small* subspace over 3 slots.
  - The desired signals occupy distinct subspaces in the remaining space.
- At the eavesdropper:
  - The artificial noise occupies the *whole* space.
  - The desired signals are buried in the artificial noise.

Converse

- **Step 1**: Consider the linear deterministic MAC-WT channel.

$$Y(t) = \sum_{i=1}^{K} \lfloor h_i(t) X_i(t) \rfloor$$

$$Z(t) = \sum_{i=1}^{K} \lfloor g_i(t) X_i(t) \rfloor$$

with the constraint that

$$X_i \in \left\{0, 1, \ldots, \lfloor \sqrt{P} \rfloor\right\}$$

- Any s.d.o.f. in the Gaussian channel can be achieved on this channel.
- This channel has a **larger** s.d.o.f. region.
- A converse for this channel $\Rightarrow$ A converse for the original channel.
- Consider this channel for the rest of the converse.

Converse (Contd.)

- **Step 2**: Use the secrecy penalty[a] and the role of a helper[a] lemmas.
- Secrecy penalty:

$$n\sum_{i=1}^{K} R_i \leq \sum_{k=1}^{K} H(\mathbf{X}_k) - H(\mathbf{Z}) \tag{1}$$

- Role of a helper:

$$n\sum_{i\neq j} R_i \leq H(\mathbf{Y}) - H(\mathbf{X}_j) \tag{2}$$

- Combine (1) and (2)

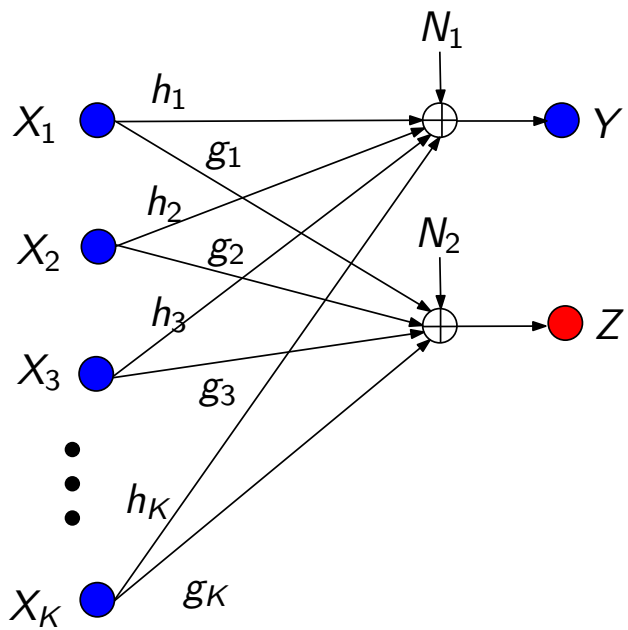
$$\begin{aligned} Kn\sum_{i=1}^{K} R_i \leq & KH(\mathbf{Y}) - H(\mathbf{Z}) \\ = & (K-1)H(\mathbf{Y}) + (H(\mathbf{Y}) - H(\mathbf{Z})) \end{aligned}$$

[a] Xie, Ulukus (2014)

Converse (Contd.)

- **Step 3**: Show that

$$H(\mathbf{Y}) - H(\mathbf{Z}) \leq n\, o(\log P) \tag{3}$$

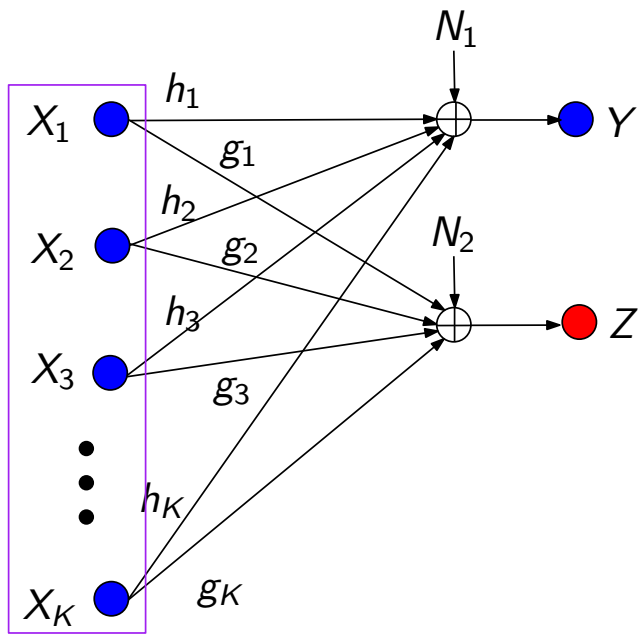


[a] Davoodi, Jafar (2014)

Converse (Contd.)

- **Step 3**: Show that

$$H(\mathbf{Y}) - H(\mathbf{Z}) \leq n\, o(\log P) \tag{3}$$



- **Enhance** to MISO broadcast channel and drop security constraints.
- With no CSIT from user with output $\mathbf{Z}$, (3) holds[a].

[a] Davoodi, Jafar (2014)

Converse (Contd.)

- Thus we have,

$$Kn\sum_{i=1}^{K} R_i = (K-1)H(\mathbf{Y}) + (H(\mathbf{Y}) - H(\mathbf{Z})) \tag{4}$$

$$H(\mathbf{Y}) - H(\mathbf{Z}) \leq no(\log P) \tag{5}$$

- Adding (4) and (5), and using $H(\mathbf{Y}) \leq \frac{n}{2}\log P$,

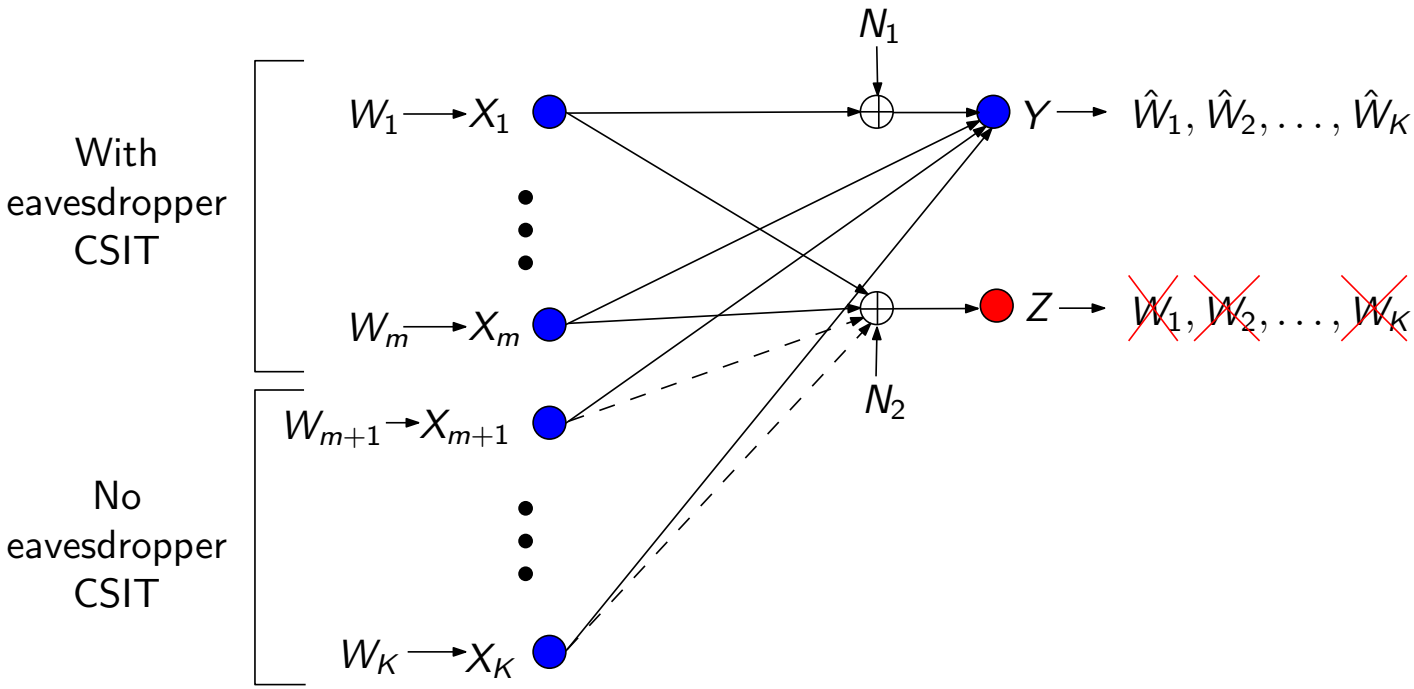
$$Kn\sum_{i=1}^{K} R_i \leq (K-1)\frac{n}{2}\log P + no(\log P)$$

- Taking limits,

$$\sum_{i=1}^{K} d_i \leq \frac{K-1}{K}$$

The MAC-WT with Partial Eavesdropper CSIT

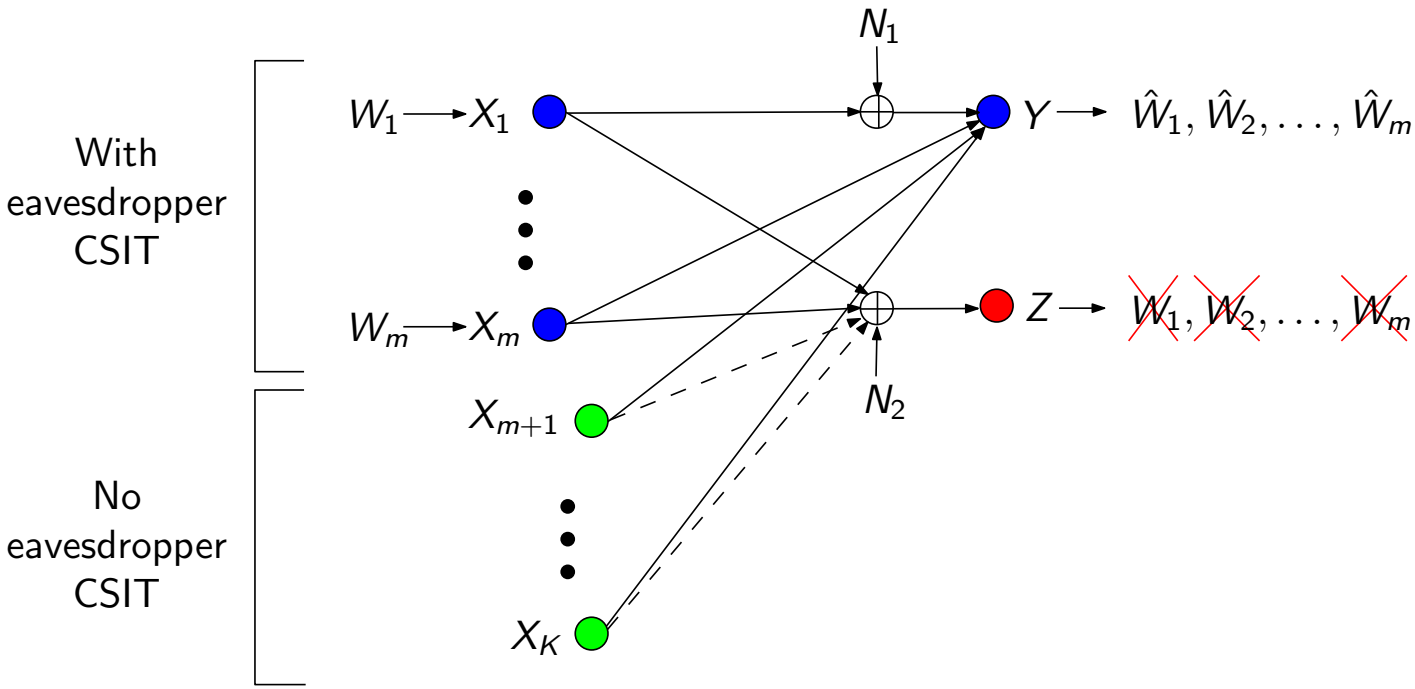
- Suppose $m\,(\geq 1)$ of the K transmitters have eavesdropper CSIT.



- The optimal s.d.o.f. is unknown.

The MAC-WT with Partial Eavesdropper CSIT

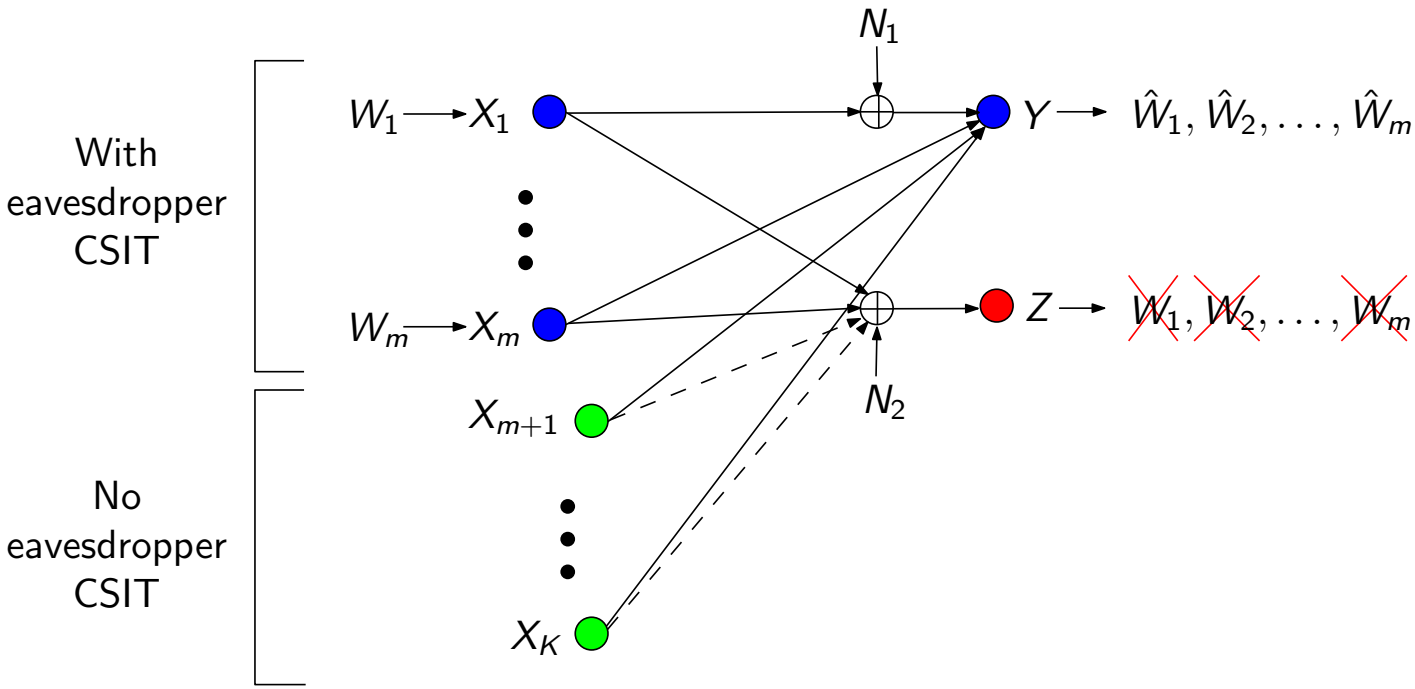
- Suppose $m\,(\geq 1)$ of the K transmitters have eavesdropper CSIT.



- The optimal s.d.o.f. is unknown.
- Can be treated as: m-user MAC-WT with $(K - m)$ helpers.

The MAC-WT with Partial Eavesdropper CSIT

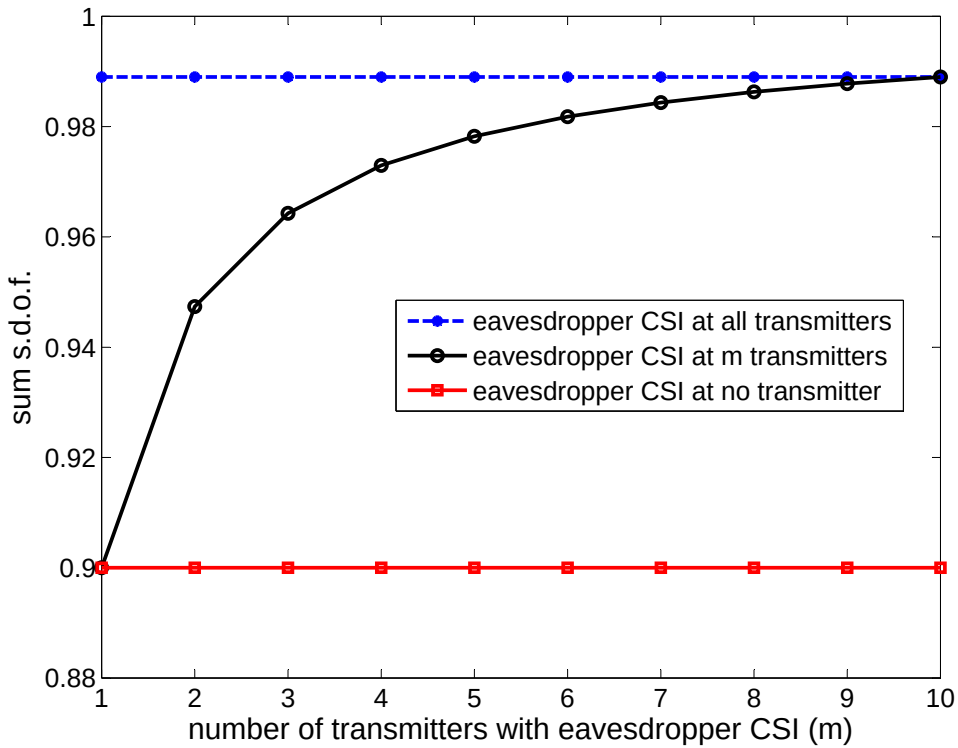
- Suppose $m\,(\geq 1)$ of the K transmitters have eavesdropper CSIT.



- The optimal s.d.o.f. is unknown.
- Can be treated as: m-user MAC-WT with $(K-m)$ helpers.
- An achievable s.d.o.f. $= \frac{m(K-1)}{m(K-1)+1}$.

Benefit of Partial Eavesdropper CSIT

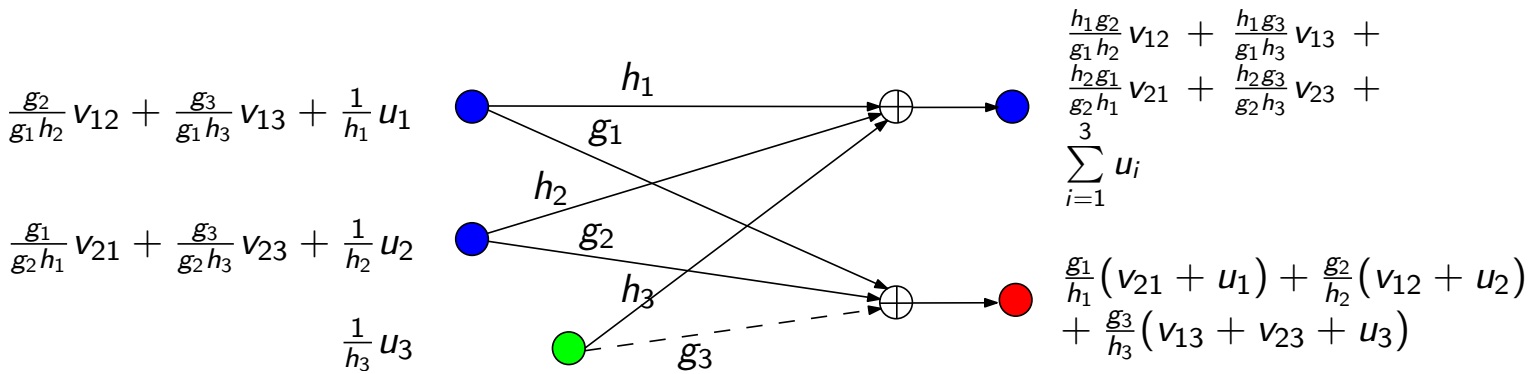
- Consider K=10.



- Our achievable rate is optimal when $m = K$.
- Optimality for intermediate values of m is unknown.

An Achievable Scheme with Partial Eavesdropper CSIT

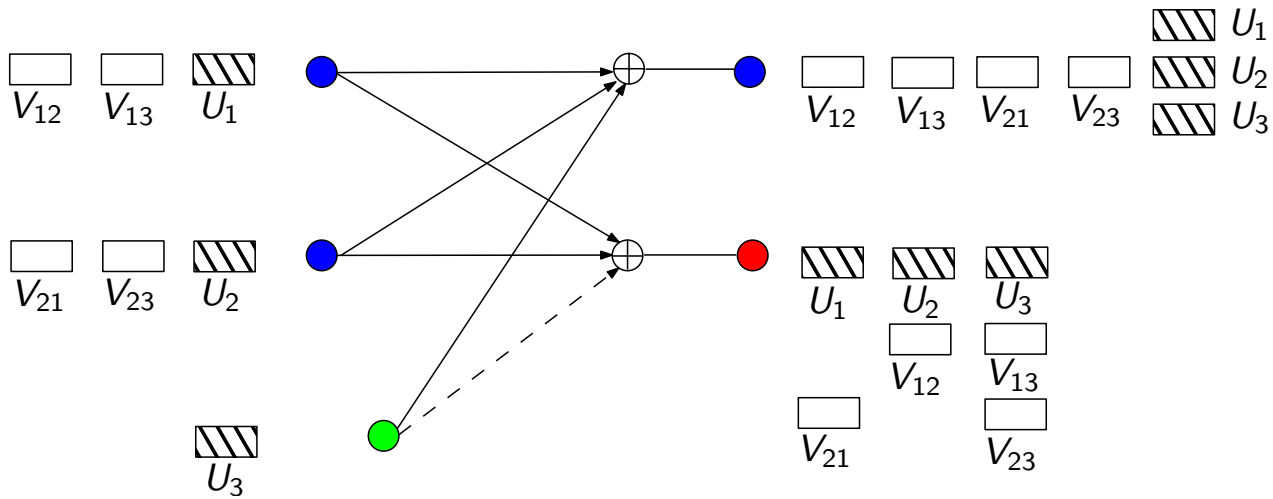
- Consider K=3 and m=2. An achievable sum s.d.o.f. $= \frac{4}{5}$.
- Send 4 symbols (v_{12}, v_{13}) and (v_{21}, v_{23}) in 5 time slots.
- In each time slot, the transmission is as follows:



- Solve for $v_{12}, v_{13}, v_{21}, v_{23}$ and $\sum_{i=1}^{3} u_i$ at legitimate receiver.
- Desired signals are all aligned with artificial noise at eavesdropper.

Signal Alignment Partial Eavesdropper CSIT

- Align signals over 5 time slots.



- At legitimate user:
  - The artificial noise aligns in a *small* subspace over 5 slots.
  - The desired signals occupy distinct subspaces in the remaining space.
- At the eavesdropper:
  - The artificial noise symbols **do not** occupy the *whole* space.
  - The desired signals align with the artificial noise symbols for security.

Conclusions and Future Work

- Determined the optimal sum s.d.o.f. of the MAC-WT without eavesdropper CSIT.
- Showed that without eavesdropper CSIT, the MAC-WT reduces to the WTH.
- Provided an achievable scheme with eavesdropper CSI at some of the transmitters.