# Secrecy for MISO Broadcast Channels via Alternating CSIT

Pritam Mukherjee[1] Ravi Tandon[2] Şennur Ulukuş[1]

[1]University of Maryland, College Park

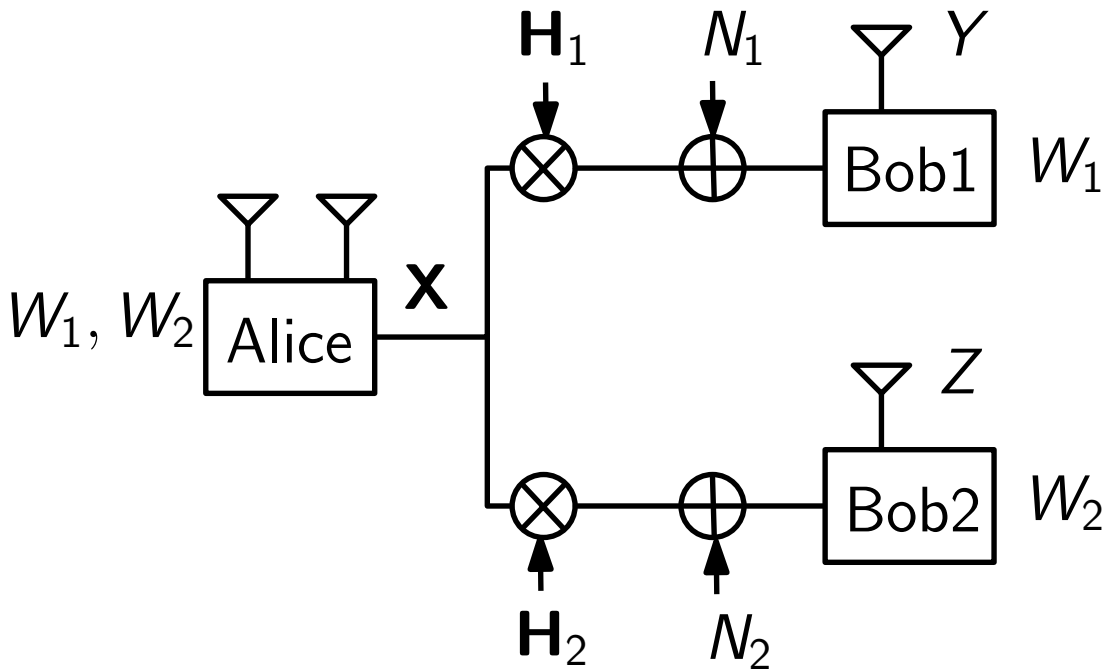
[2]Virginia Tech, Blacksburg

# Outline

- Multi-antenna broadcast channels with delayed CSIT
- Alternating CSIT: exploiting channel knowledge variations
- Secrecy for broadcast channels with delayed CSIT
- This talk: Secrecy for broadcast channels with alternating CSIT

# The MISO Broadcast Channel

- Consider the following fading MISO broadcast channel:

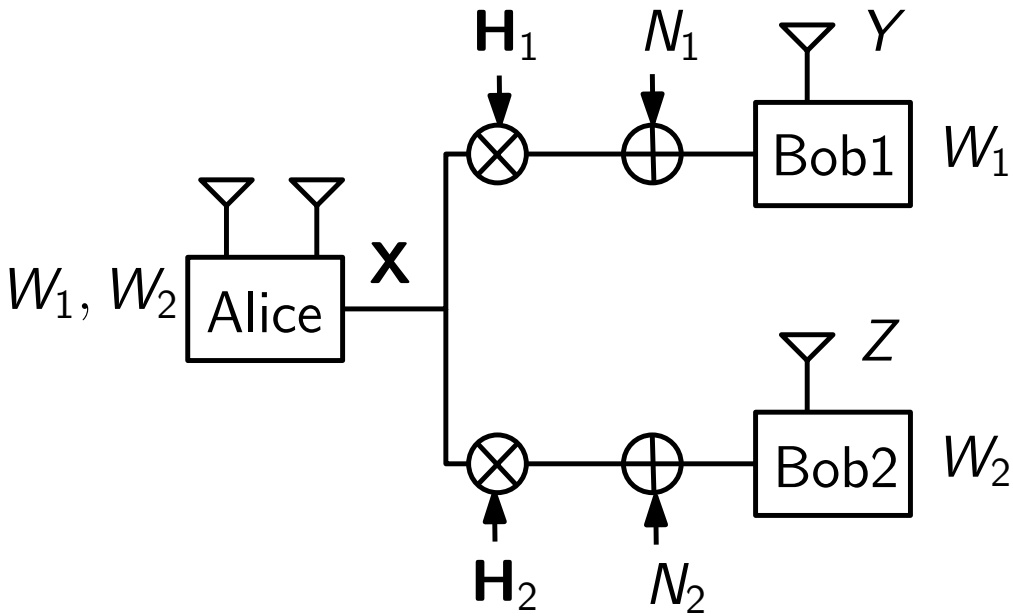



- **Key enabler**: Channel state information at the transmitter (CSIT).
- Assume that the receivers have full channel knowledge.

# Modeling of CSIT

- Two aspects of CSIT - precision and delay.
- In practice, it is usually imprecise and delayed.
- Consider **full precision** and focus on the aspect of delay.
- A simple model of the delay:
  1. perfect (P): The CSIT is available at the start of communication.
  2. delayed (D) : The CSIT is available after a delay of coherence time.
  3. none (N): The CSIT of the user is not available.
- With **two** users, define *state* by $I_1 I_2$, where $I_1, I_2 \in \{\text{P, D, N}\}$.
- There can be 9 states: PP, DD, NN, PD, DP, PN, NP, DN, ND.
- *Homogeneous* CSIT states: PP, DD, NN.
- *Heterogeneous* CSIT states: PD, DP, PN, NP, DN, ND.

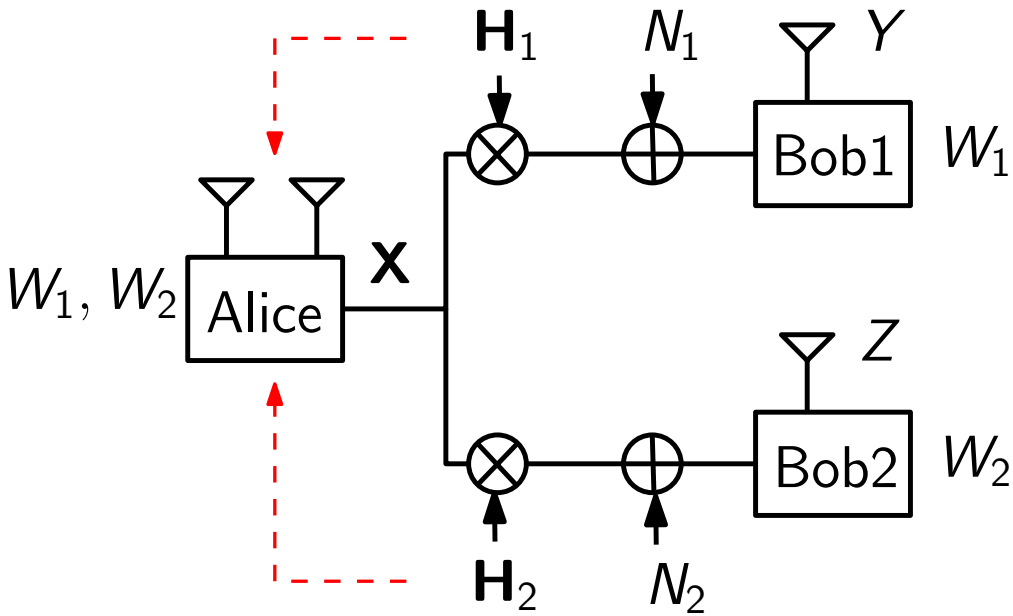
# MISO BC with Homogeneous CSIT




- No CSIT (N) from any user, sum degrees of freedom (d.o.f.) $= 1$.

*Maddah-Ali, Tse (2010)

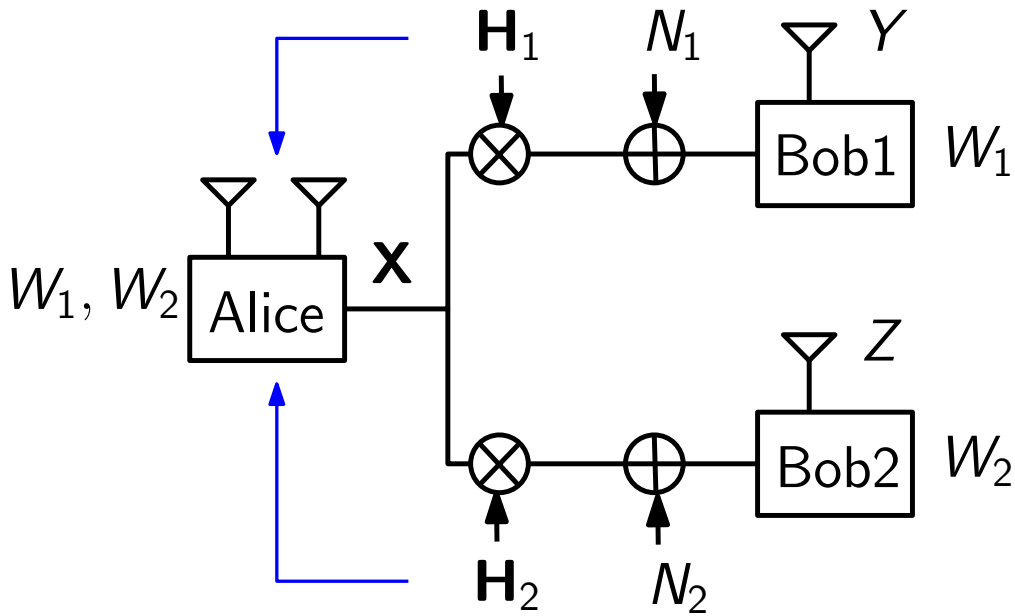
# MISO BC with Homogeneous CSIT




- No CSIT (N) from any user, sum degrees of freedom (d.o.f.) $= 1$.
- Delayed CSIT (D) from both users*, sum d.o.f $= \frac{4}{3}$.

*Maddah-Ali, Tse (2010)

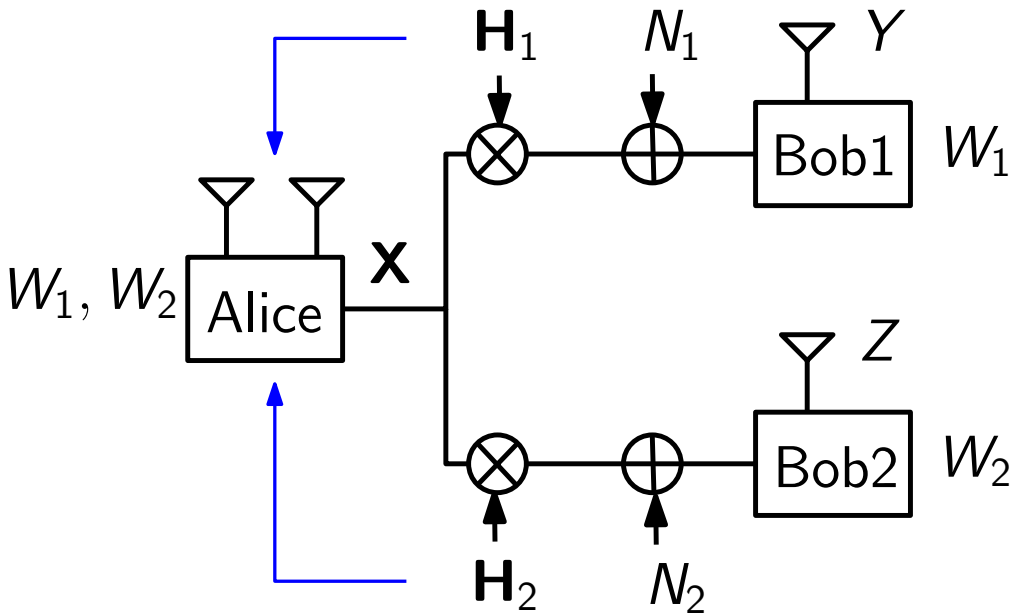
# MISO BC with Homogeneous CSIT




- No CSIT (N) from any user, sum degrees of freedom (d.o.f.) $= 1$.
- Delayed CSIT (D) from both users*, sum d.o.f $= \frac{4}{3}$.
- Perfect CSIT (P) from both users, sum d.o.f $=2$.

*Maddah-Ali, Tse (2010)

# MISO BC with Homogeneous CSIT



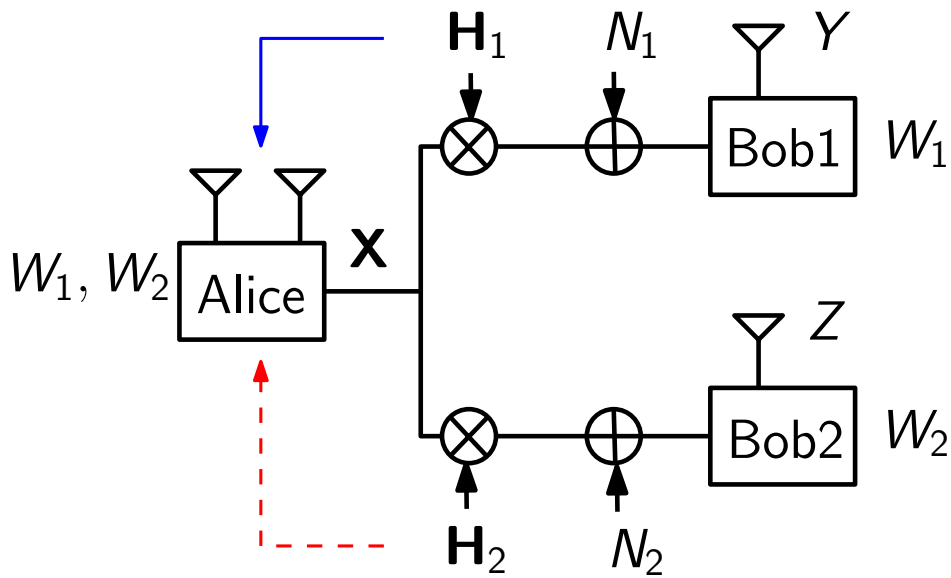

- No CSIT (N) from any user, sum degrees of freedom (d.o.f.) $= 1$.
- Delayed CSIT (D) from both users*, sum d.o.f $= \frac{4}{3}$.
- Perfect CSIT (P) from both users, sum d.o.f $=2$.

Even completely outdated CSIT is useful!

*Maddah-Ali, Tse (2010)

# MISO BC with *Heterogeneous* CSIT

- CSIT can vary from user to user

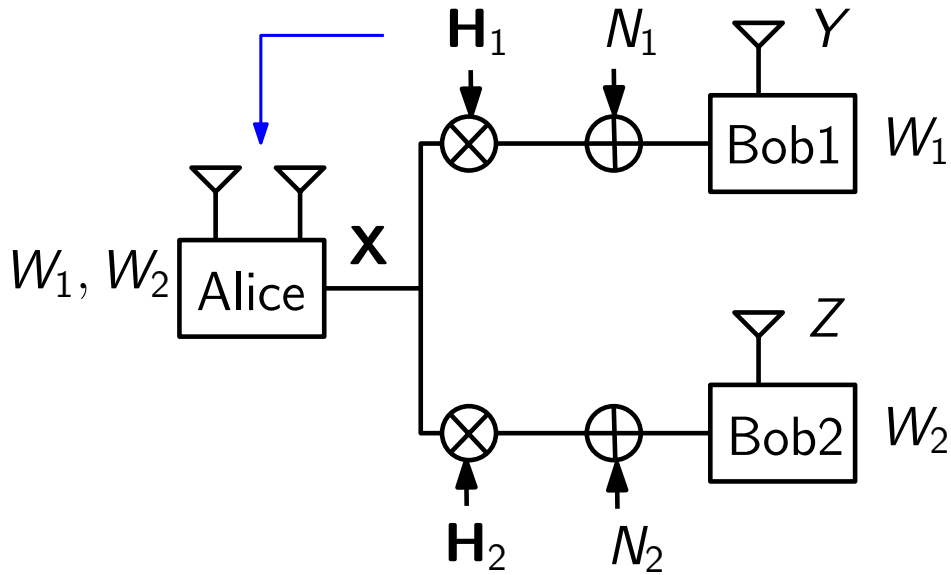



- With perfect and delayed CSIT from the users*: Sum d.o.f $= \frac{3}{2}$.

*Maleki et al. (2012)
**Davoodi, Jafar (2014)

# MISO BC with *Heterogeneous* CSIT

- CSIT can vary from user to user

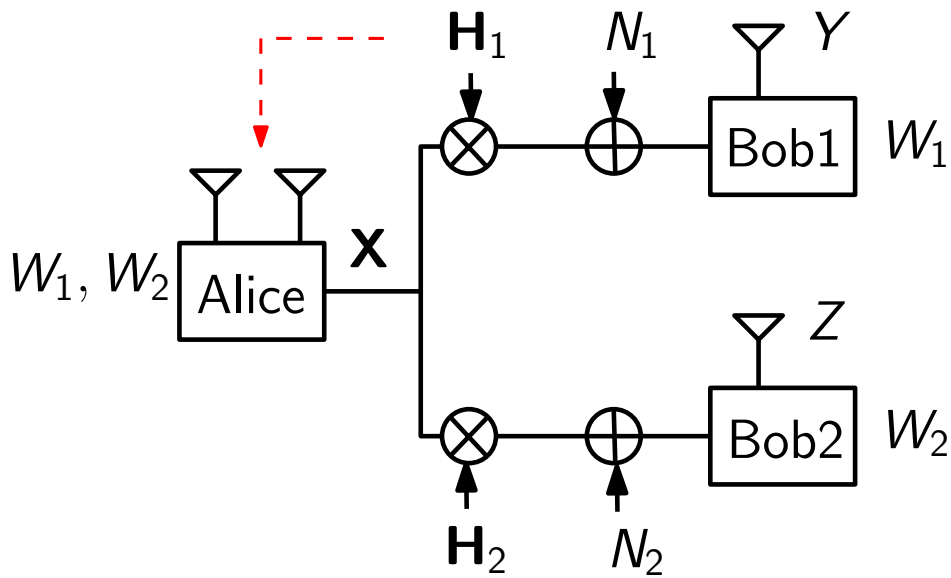



- With perfect and delayed CSIT from the users*: Sum d.o.f $= \frac{3}{2}$.
- With perfect and no CSIT from the users** (PN): Sum d.o.f $= 1$.

*Maleki et al. (2012)
**Davoodi, Jafar (2014)

# MISO BC with *Heterogeneous* CSIT

- CSIT can vary from user to user




- With perfect and delayed CSIT from the users*: Sum d.o.f $= \frac{3}{2}$.
- With perfect and no CSIT from the users** (PN): Sum d.o.f $= 1$.
- With delayed and no CSIT from the users (DN): Sum d.o.f $= 1$.

*Maleki et al. (2012)
**Davoodi, Jafar (2014)

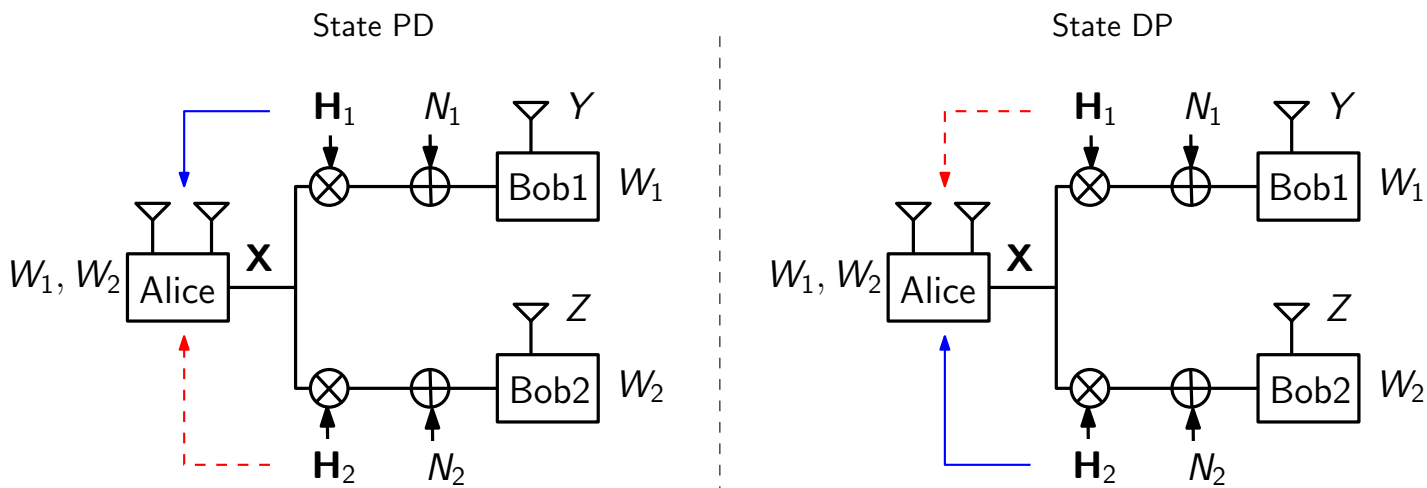
# Alternating CSIT

- The availability of CSIT usually varies with time.
- The variation can be due to changing network conditions, mobility of users or even by design.
- **Question**: Can this variation be exploited?

Tandon et al. (2013)

# Alternating CSIT

- The availability of CSIT usually varies with time.
- The variation can be due to changing network conditions, mobility of users or even by design.
- **Question**: Can this variation be exploited? YES!

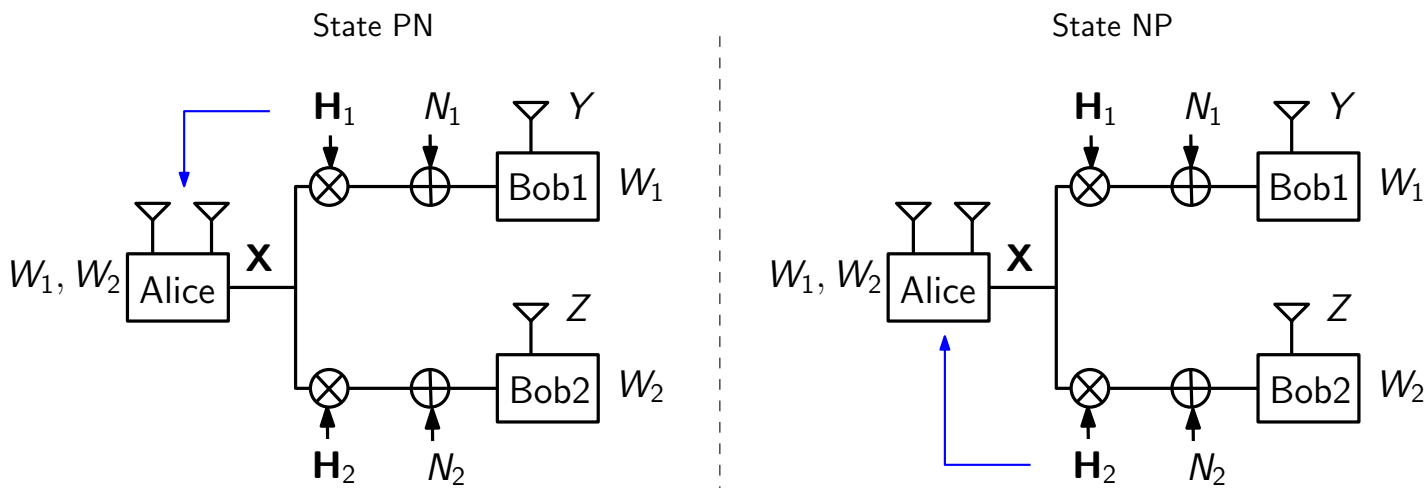



- With states PD and DP together, the sum d.o.f. increases to $\frac{5}{3}$.

Tandon et al. (2013)

# Alternating CSIT

- The availability of CSIT usually varies with time.
- The variation can be due to changing network conditions, mobility of users or even by design.
- **Question**: Can this variation be exploited? YES!

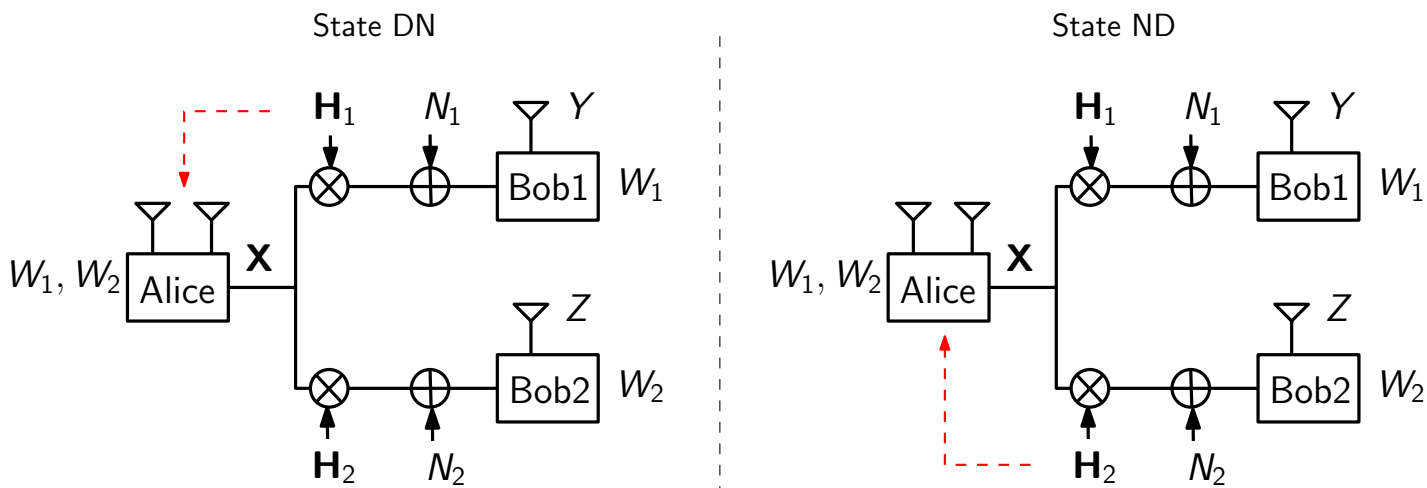



- With states PD and DP together, the sum d.o.f. increases to $\frac{5}{3}$.
- With states PN and NP together, the sum d.o.f. increases to $\frac{3}{2}$.

Tandon et al. (2013)

# Alternating CSIT

- The availability of CSIT usually varies with time.
- The variation can be due to changing network conditions, mobility of users or even by design.
- **Question**: Can this variation be exploited? YES!

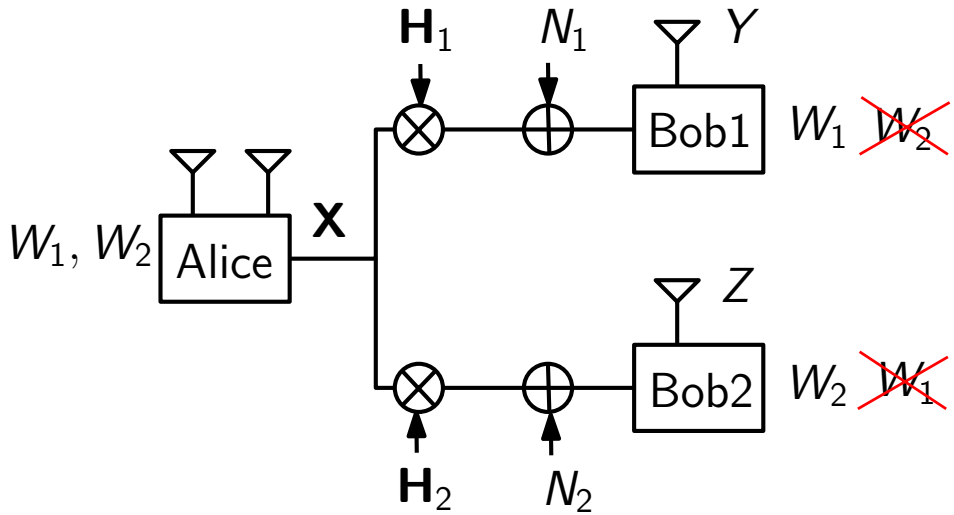



- With states PD and DP together, the sum d.o.f. increases to $\frac{5}{3}$.
- With states PN and NP together, the sum d.o.f. increases to $\frac{3}{2}$.
- With states DN and ND together, the sum d.o.f. increases to $\frac{4}{3}$.

Tandon et al. (2013)

# Security aspects

- We focus on the security aspect of the problem.
- MISO Broadcast channel with confidential messages (BCCM).

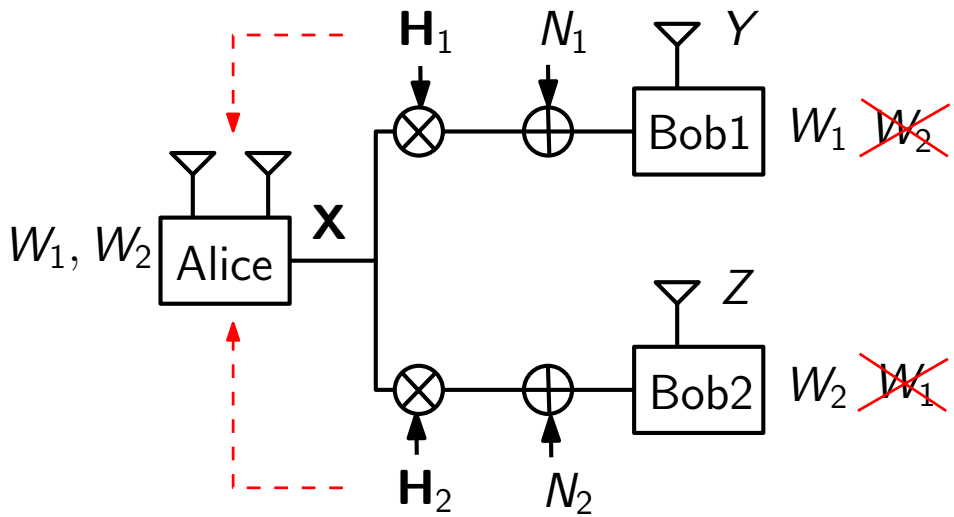



- No CSIT (N): statistically equivalent users; sum s.d.o.f.= 0.

S. Yang et al. (2013)

# Security aspects

- We focus on the security aspect of the problem.
- MISO Broadcast channel with confidential messages (BCCM).

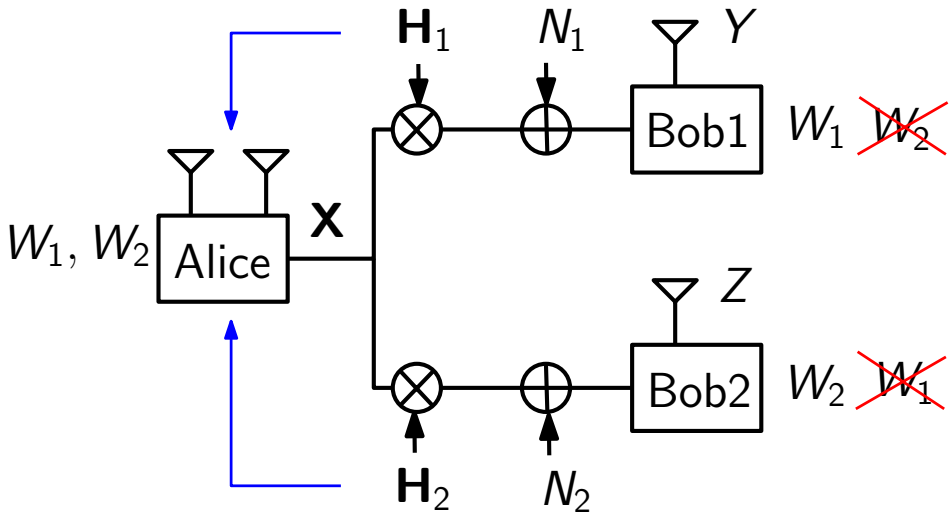



- No CSIT (N): statistically equivalent users; sum s.d.o.f.= 0.
- Delayed CSIT (D) from both users*: sum s.d.o.f. = 1.

S. Yang et al. (2013)

# Security aspects

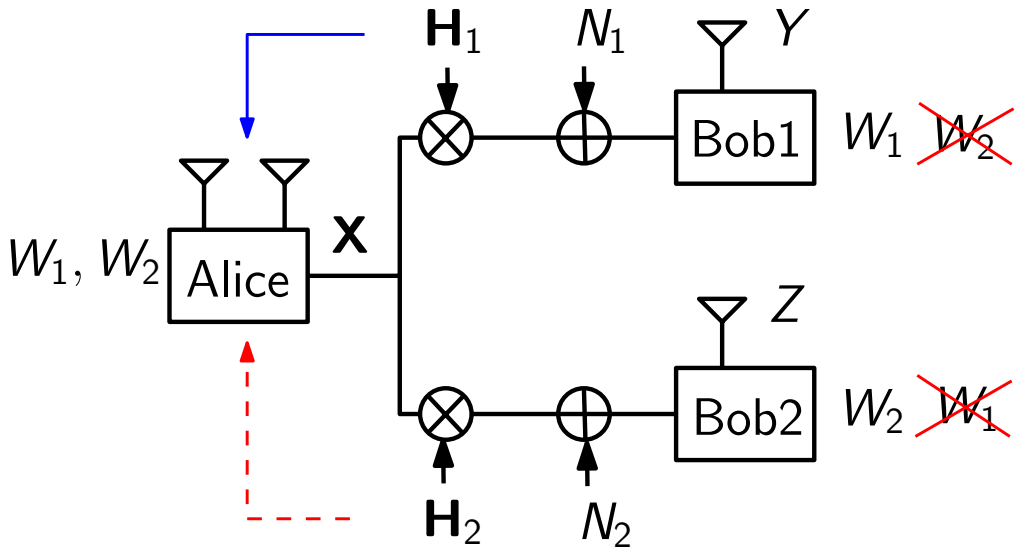
- We focus on the security aspect of the problem.
- MISO Broadcast channel with confidential messages (BCCM).




- No CSIT (N): statistically equivalent users; sum s.d.o.f.= 0.
- Delayed CSIT (D) from both users*: sum s.d.o.f. = 1.
- Instantaneous CSIT (P) from both users: sum s.d.o.f. = 2.

S. Yang et al. (2013)

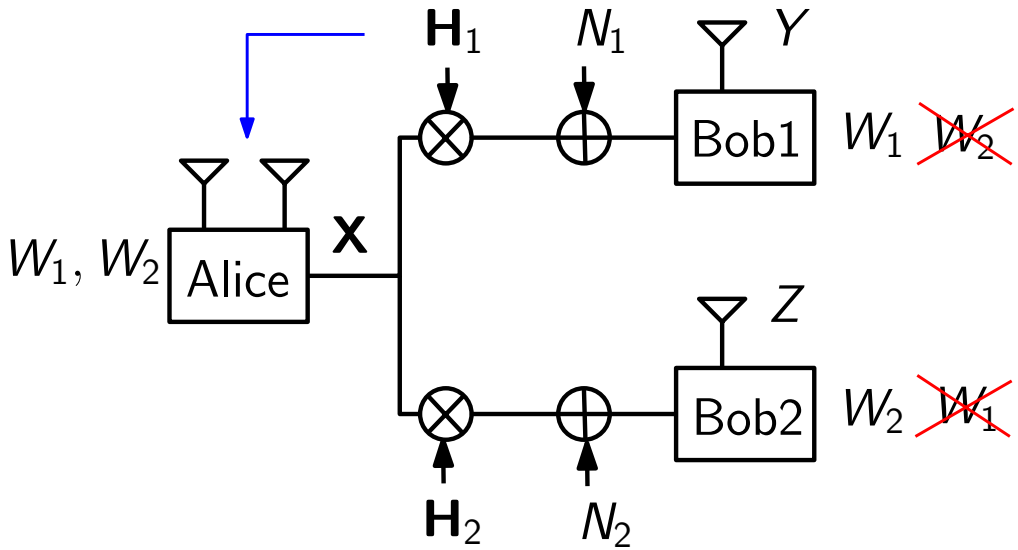
# MISO BCCM with *Heterogeneous* CSIT




- With perfect and delayed CSIT from users (PD)*: Sum s.d.o.f = 1.

*Mukherjee, R. Tandon and S. Ulukus (submitted 2015)
**Davoodi, Jafar (2014)

# MISO BCCM with *Heterogeneous* CSIT

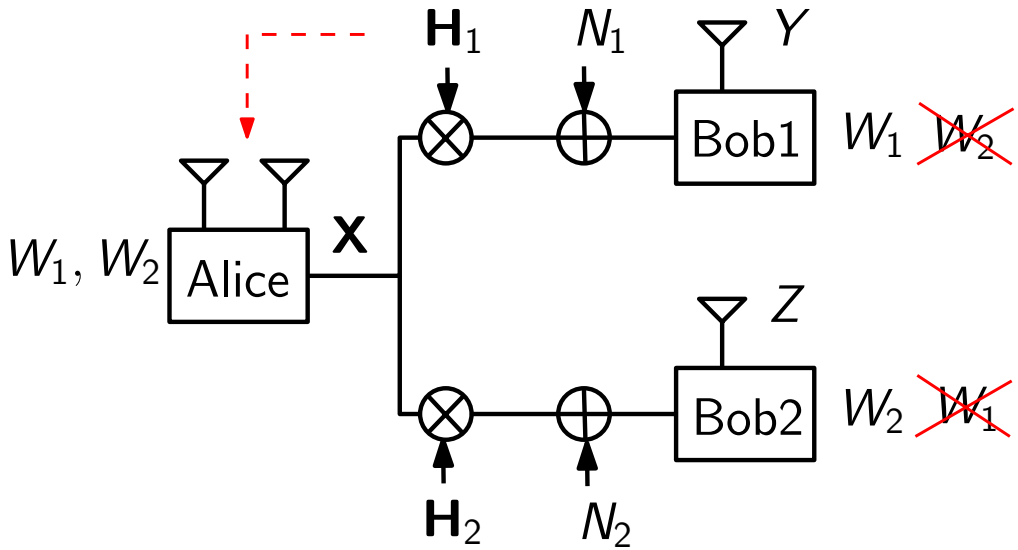



- With perfect and delayed CSIT from users (PD)*: Sum s.d.o.f = 1.
- With perfect and no CSIT from the users (PN)**: Sum d.o.f = 1.

*Mukherjee, R. Tandon and S. Ulukus (submitted 2015)

**Davoodi, Jafar (2014)

# MISO BCCM with *Heterogeneous* CSIT

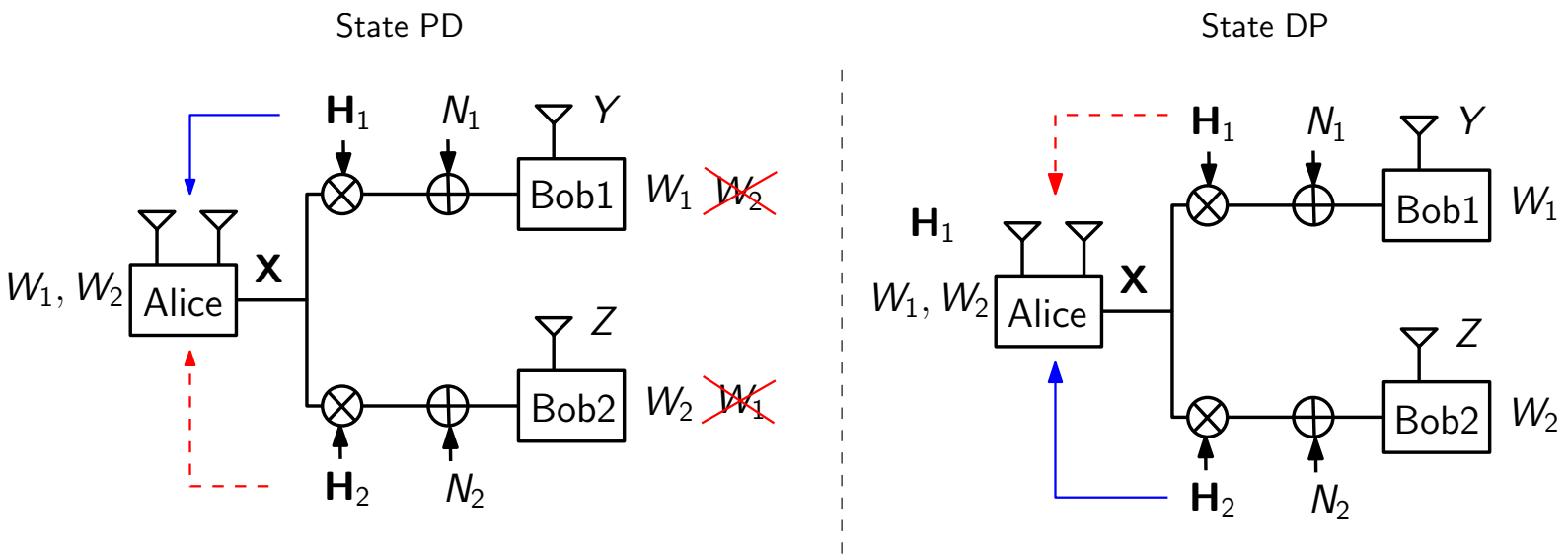



- With perfect and delayed CSIT from users (PD)*: Sum s.d.o.f = 1.
- With perfect and no CSIT from the users (PN)**: Sum d.o.f = 1.
- With delayed and no CSIT from the users (DN)*: Sum d.o.f = $\frac{1}{2}$

*Mukherjee, R. Tandon and S. Ulukus (submitted 2015)
**Davoodi, Jafar (2014)

# This Talk: Security with Alternating CSIT

- Can *alternation* of CSIT states be exploited for security? YES!
- Consider the alternating scenario with only PD and DP states.




- With states PD and DP occurring separately, optimal s.d.o.f. $= 1$.
- With states PD and DP occurring together*, optimal s.d.o.f. $= \frac{3}{2}$.
- What happens in the general case with all 9 states?

*P.Mukherjee, R. Tandon and S. Ulukus (2014)

# Main Result

- Suppose state $I_1 I_2$ occurs for $\lambda_{I_1 I_2}$ fraction of the time.
- Assume **symmetry**: $\lambda_{I_1 I_2} = \lambda_{I_2 I_1}$ for $I_1 \neq I_2$.
- Define:

$$\lambda_P \triangleq \lambda_{PP} + \lambda_{PD} + \lambda_{PN}$$
$$\lambda_D \triangleq \lambda_{PD} + \lambda_{DD} + \lambda_{DN}$$
$$\lambda_N \triangleq \lambda_{PN} + \lambda_{DN} + \lambda_{NN}.$$

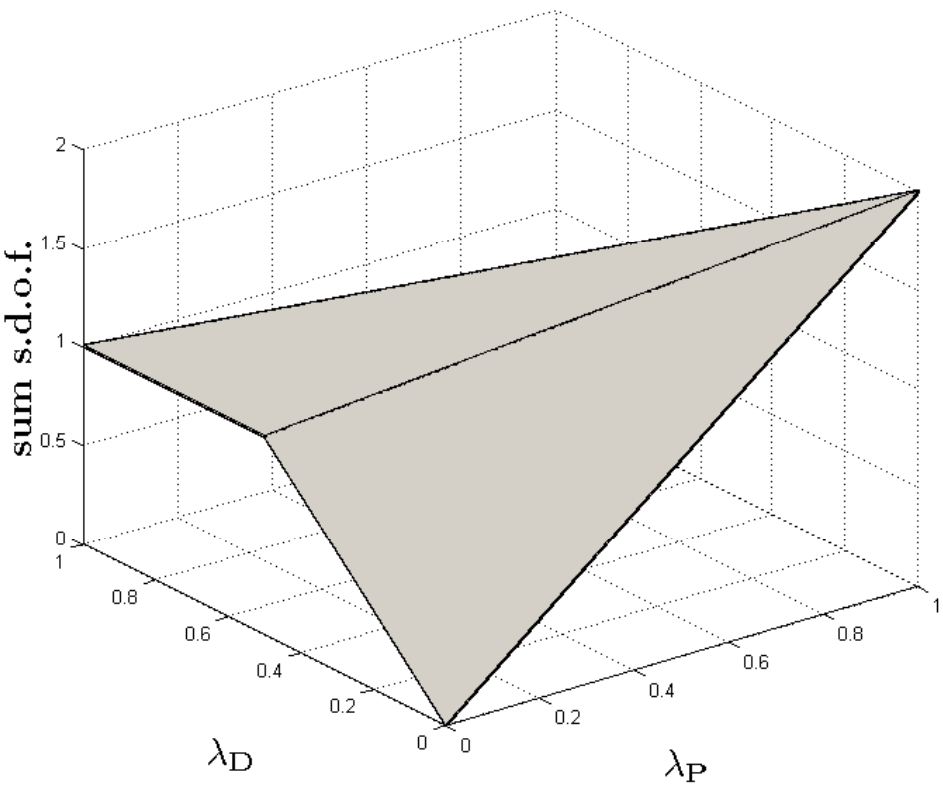
- The s.d.o.f. region is given by:

$$d_1 \leq \min\left(\frac{2 + 2\lambda_P - \lambda_{PP}}{3}, 1 - \lambda_{NN}\right)$$
$$d_2 \leq \min\left(\frac{2 + 2\lambda_P - \lambda_{PP}}{3}, 1 - \lambda_{NN}\right)$$
$$3d_1 + d_2 \leq 2 + 2\lambda_P$$
$$d_1 + 3d_2 \leq 2 + 2\lambda_P$$
$$d_1 + d_2 \leq 2(\lambda_P + \lambda_D).$$

# Sum S.d.o.f.

- The sum s.d.o.f. is given by

$$\text{sum s.d.o.f.} = 2\lambda_P + \lambda_D + \min(\lambda_D, \lambda_N)$$



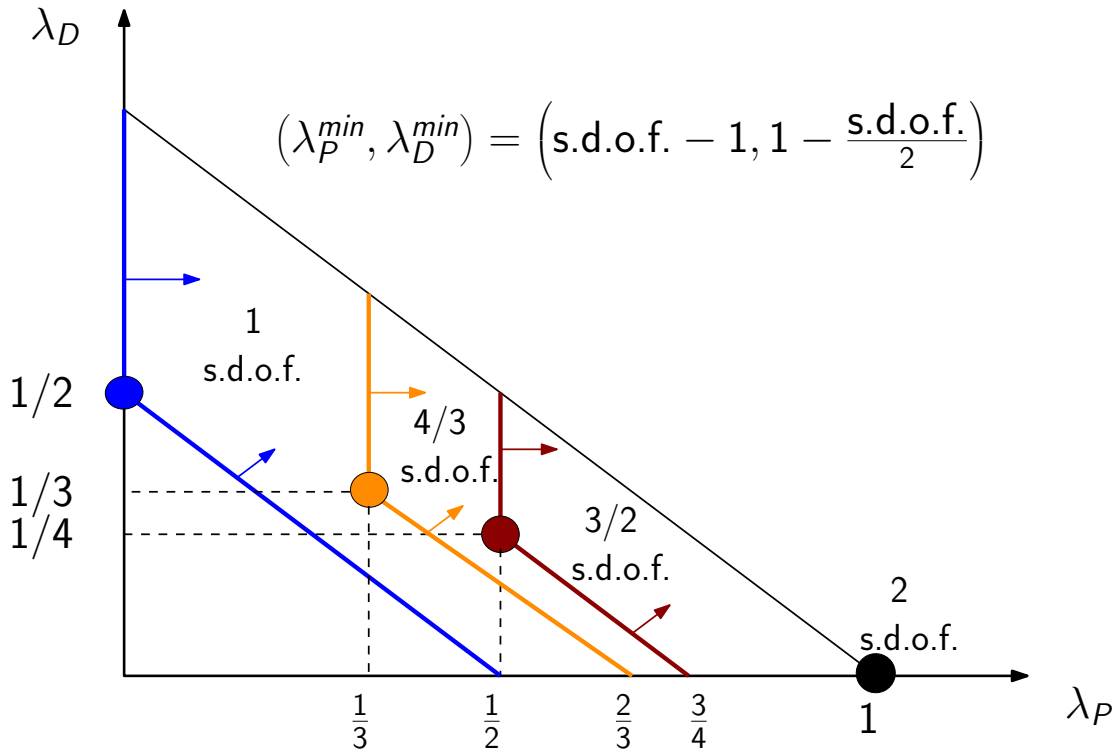
# Benefits of Alternating CSIT

- **Example 1**: States PD and DP, each occurring for half of the time.
  - Optimal s.d.o.f. for each state alone $= 1$.
  - Optimal s.d.o.f. with alternation $= \frac{3}{2}$. (Benefit!)
- **Example 2**: States PD, DP and NN, each occurring for a third of the time.
  - S.d.o.f. with optimal encoding for each state separately $= \frac{2}{3}$.
  - Optimal s.d.o.f. with alternation $= \frac{4}{3}$. (Benefit!)
- **Example 3**: States PN, NP and DD, each occurring for a third of the time.
  - S.d.o.f. with optimal encoding for each state separately $= 1$.
  - Optimal s.d.o.f. with alternation $= \frac{4}{3}$. (Benefit!)
- **Example 4**: States PN and NP, each occurring for half of the time.
  - Optimal s.d.o.f. for each state alone $= 1$.
  - Optimal s.d.o.f. with alternation $= 1$. (NO BENEFIT!)

# Minimum CSIT Requirements

- For sum s.d.o.f. $= s$, the minimum CSIT requirements are given by:

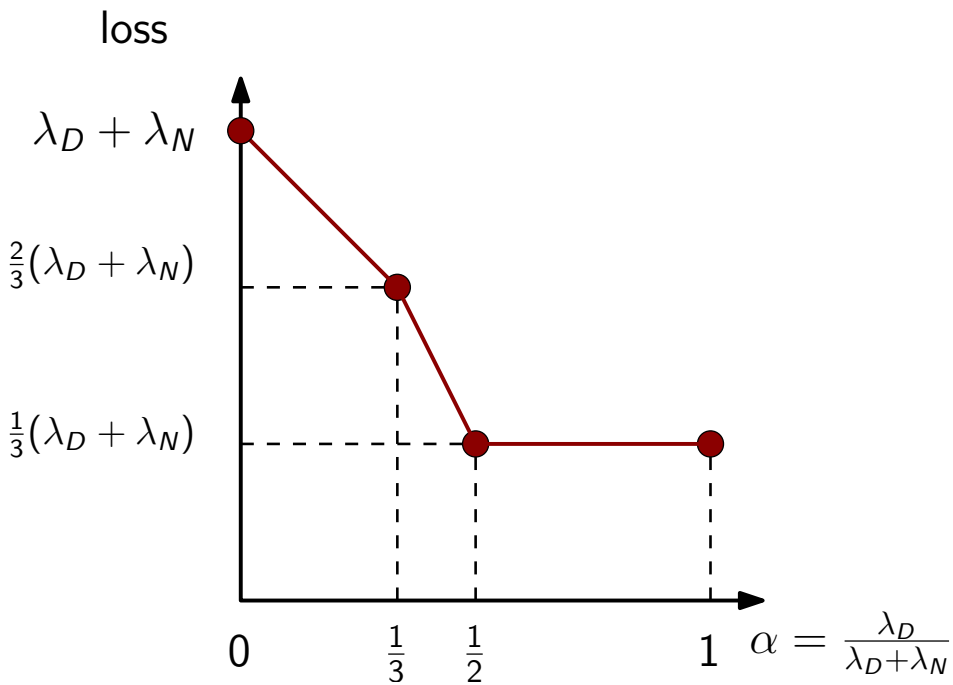
$$(\lambda_P, \lambda_D)_{\min} = \begin{cases} \left(s-1, 1-\frac{s}{2}\right), & \text{if } 1 \le s \le 2 \\ \left(0, \frac{s}{2}\right), & \text{if } 0 \le s \le 1. \end{cases}$$



# Cost of Security

- Let $\alpha = \lambda_D/(\lambda_D + \lambda_N)$. The s.d.o.f. loss due to security constraints:

$$\text{loss} = (\lambda_D + \lambda_N) \times \begin{cases} (1-\alpha), & \text{if } \alpha \leq \frac{1}{3} \\ \left(\frac{4}{3} - 2\alpha\right), & \text{if } \frac{1}{2} \geq \alpha \geq \frac{1}{3} \\ \frac{1}{3}, & \text{if } \alpha \geq \frac{1}{2}. \end{cases}$$



# Sketch of the Achievability

- **Step 1**: Identify key subproblems, each with a subset of states.
- **Step 2**: Find optimal achievable schemes for the subproblems.
- **Step 3**: Combine the optimal sub-schemes judiciously.

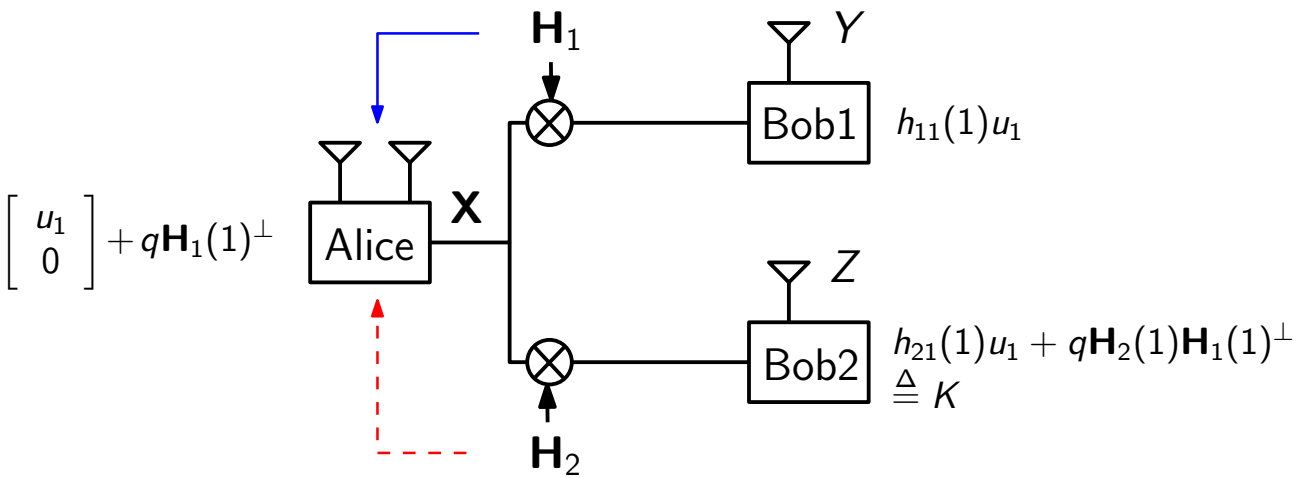
| Summary of Constituent Schemes (CS) | | | |
|---|---|---|---|
| Sum s.d.o.f. | CS Notation | CSIT States | Fractions of States |
| 2 | $S^2$ | PP | 1 |
| 3/2 | $S_1^{3/2}$ | PD, DP | $\left(\frac{1}{2}, \frac{1}{2}\right)$ |
| | $S_2^{3/2}$ | PD, DP, PN, NP | $\left(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}\right)$ |
| 4/3 | $S_1^{4/3}$ | PD, DP, NN | $\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right)$ |
| | $S_2^{4/3}$ | PN, NP, DD | $\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right)$ |
| 1 | $S_1^1$ | DD | 1 |
| | $S_2^1$ | DD, NN | $\left(\frac{1}{2}, \frac{1}{2}\right)$ |
| | $S_3^1$ | DN, ND | $\left(\frac{1}{2}, \frac{1}{2}\right)$ |
| 2/3 | $S_1^{2/3}$ | DD | 1 |
| | $S_2^{2/3}$ | DD, NN | $\left(\frac{2}{3}, \frac{1}{3}\right)$ |
| | $S_3^{2/3}$ | DN, ND, NN | $\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right)$ |

# Sketch of the Achievability (Contd.)

## Example: Scheme with PD/DP/NN states that achieves sum s.d.o.f. of $\frac{4}{3}$

- With states PD, DP and NN occurring equally, optimal s.d.o.f. $= \frac{4}{3}$.
- Send $(u_1, u_2)$ and $(v_1, v_2)$ to the first and second users in 3 slots.

State PD

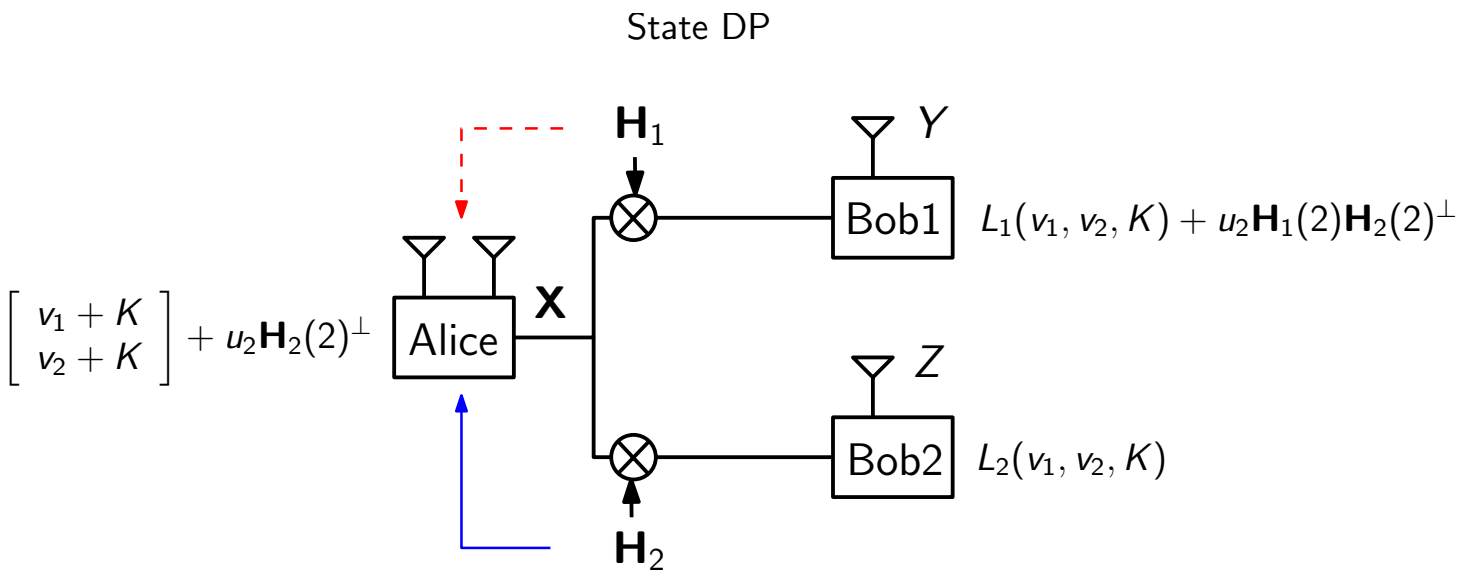



| | State PD | |
|---|---|---|
| $Y$ | $h_{11}(1)u_1$ | |
| $Z$ | $h_{21}(1)u_1 + q\mathbf{H}_2(1)\mathbf{H}_1(1)^{\perp} \triangleq K$ | |

# Sketch of the Achievability (Contd.)

## Example: Scheme with PD/DP/NN states that achieves sum s.d.o.f. of $\frac{4}{3}$

- With states PD, DP and NN occurring equally, optimal s.d.o.f. $= \frac{4}{3}$.
- Send $(u_1, u_2)$ and $(v_1, v_2)$ to the first and second users in 3 slots.



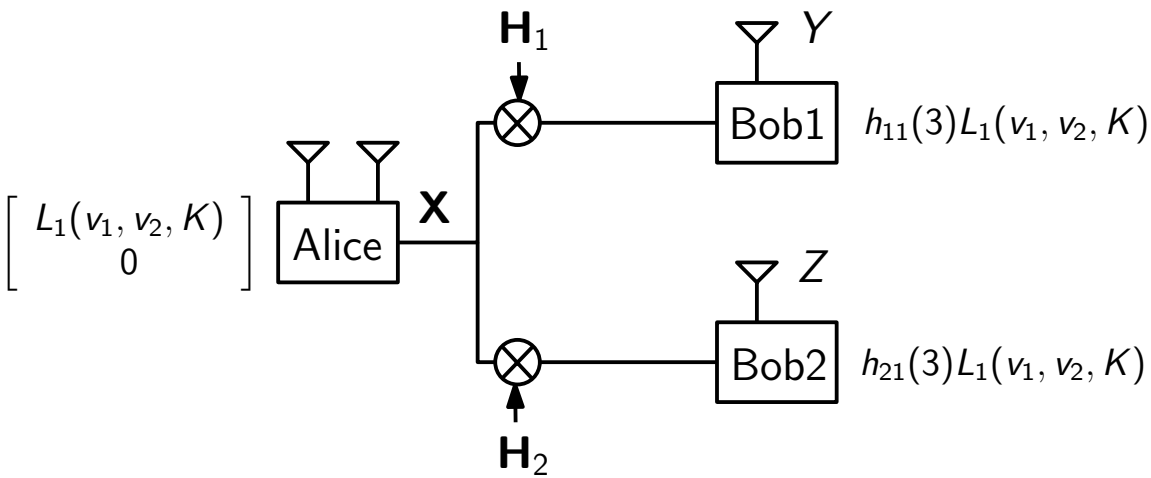

| | State PD | State DP | |
|---|---|---|---|
| $Y$ | $h_{11}(1)u_1$ | $L_1(v_1, v_2, K) + u_2\mathbf{H}_1(2)\mathbf{H}_2(2)^\perp$ | |
| $Z$ | $h_{21}(1)u_1 + q\mathbf{H}_2(1)\mathbf{H}_1(1)^\perp \triangleq K$ | $L_2(v_1, v_2, K)$ | |

# Sketch of the Achievability (Contd.)

## Example: Scheme with PD/DP/NN states that achieves sum s.d.o.f. of $\frac{4}{3}$

- With states PD, DP and NN occurring equally, optimal s.d.o.f. $= \frac{4}{3}$.
- Send $(u_1, u_2)$ and $(v_1, v_2)$ to the first and second users in 3 slots.

State NN



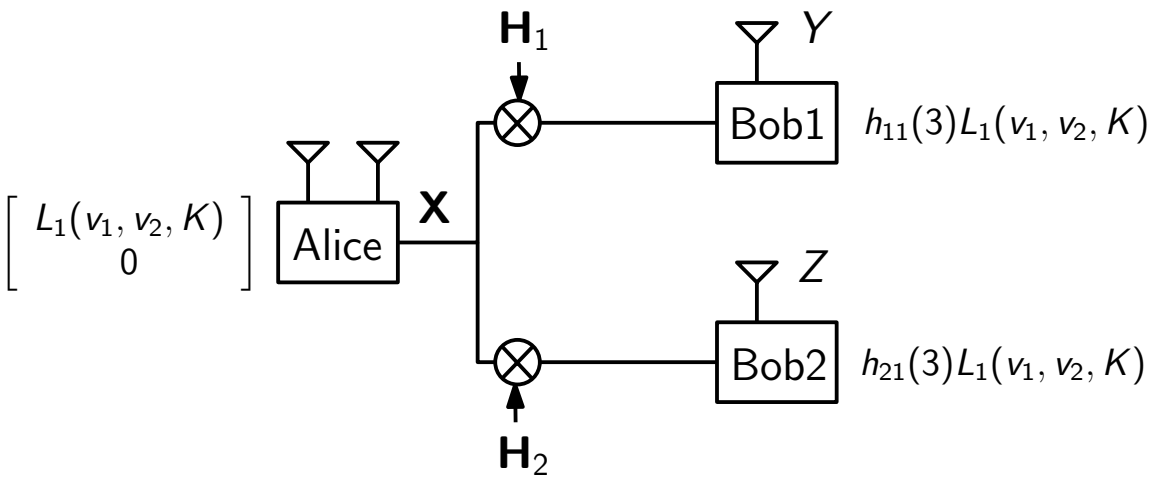

| | State PD | State DP | State NN |
|---|---|---|---|
| $Y$ | $h_{11}(1)u_1$ | $L_1(v_1, v_2, K) + u_2\mathbf{H}_1(2)\mathbf{H}_2(2)^{\perp}$ | $h_{11}(3)L_1(v_1, v_2, K)$ |
| $Z$ | $h_{21}(1)u_1 + q\mathbf{H}_2(1)\mathbf{H}_1(1)^{\perp}$ $\triangleq K$ | $L_2(v_1, v_2, K)$ | $h_{21}(3)L_1(v_1, v_2, K)$ |

# Sketch of the Achievability (Contd.)

## Example: Scheme with PD/DP/NN states that achieves sum s.d.o.f. of $\frac{4}{3}$

- With states PD, DP and NN occurring equally, optimal s.d.o.f. $= \frac{4}{3}$.
- Send $(u_1, u_2)$ and $(v_1, v_2)$ to the first and second users in 3 slots.

State NN




| | State PD | State DP | State NN |
|---|---|---|---|
| $Y$ | $h_{11}(1)u_1$ | $L_1(v_1, v_2, K) + u_2\mathbf{H}_1(2)\mathbf{H}_2(2)^{\perp}$ | $h_{11}(3)L_1(v_1, v_2, K)$ |
| $Z$ | $h_{21}(1)u_1 + q\mathbf{H}_2(1)\mathbf{H}_1(1)^{\perp} \triangleq K$ | $L_2(v_1, v_2, K)$ | $h_{21}(3)L_1(v_1, v_2, K)$ |

# Conclusions

- Introduced and studied the MISO BCCM with alternating CSIT.
- Characterized the **full s.d.o.f region** with all nine states.
- Determined the **minimum** CSIT requirements for a given s.d.o.f.
- **Synergistic gains** of alternating CSIT to yield higher s.d.o.f.
- Full details available at arXiv:

  http://arxiv.org/abs/1502.02647