# Privacy-Aware Design of Cell-Free MIMO ISAC Systems

Henrik Åkesson

Communication Systems, ISY, Linköpings universitet

# Outline and basic idea

- Motivation
- System Model
- Attack Model
- Proposed Mitigation Method
- Results

# Why should we consider Integrated Sensing and Communication (ISAC)?

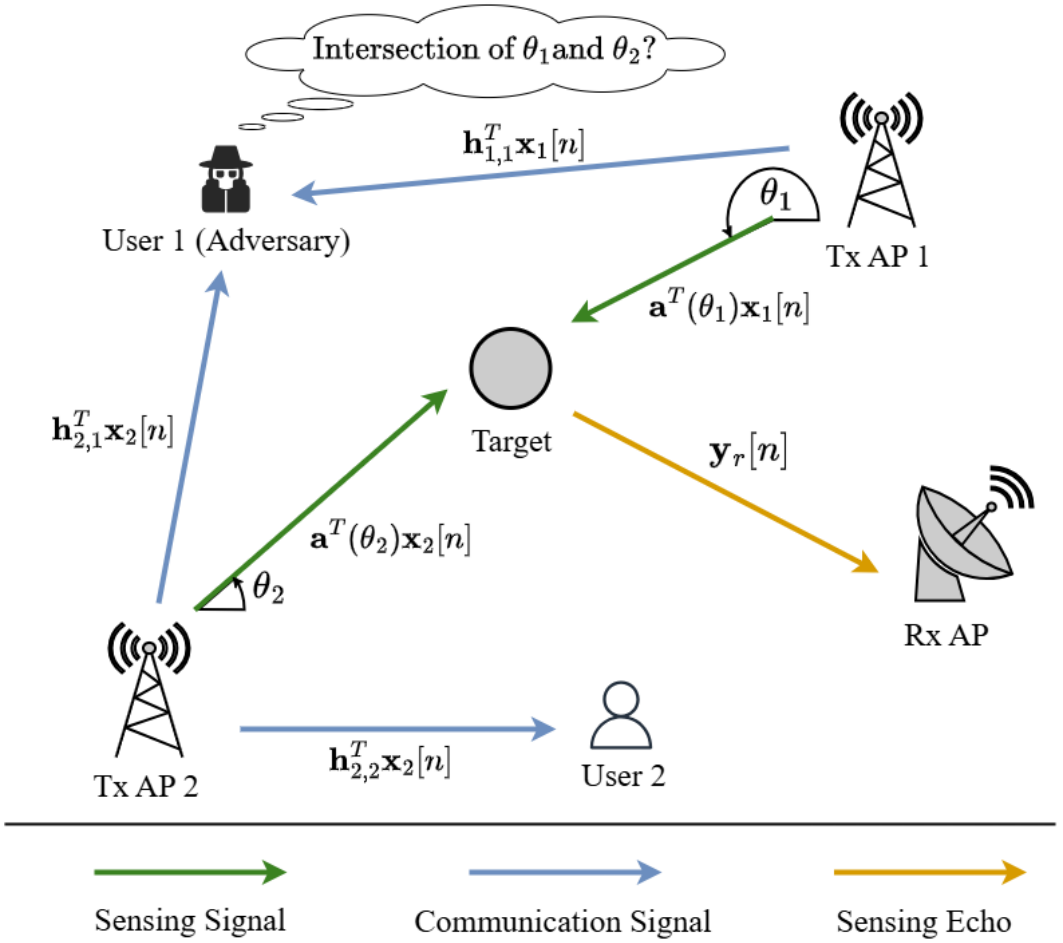
- New use cases
- Spectrum reuse
- Hardware reuse

# Motivation of paper

- ISAC enables sensitive data acquisition and must be secure(er)
- Cannot only ensure privacy and security in higher layers
- Aim is to show that relatively simple methods can have large impact

# System Model

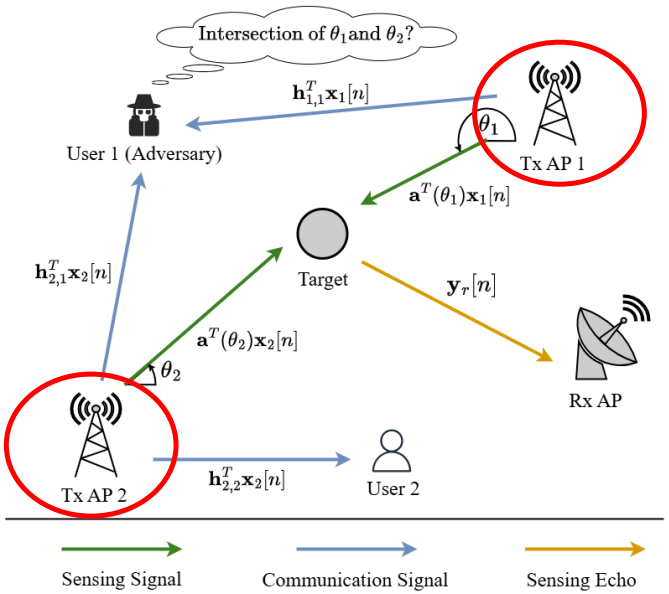
- Cell-Free MIMO ISAC System
- Multiple users and APs (with different functionalities)
- APs are detecting/scanning a position
- One malicious user



# Delimitations/Assumptions

- Adversary cannot utilize radar echoes
- Vast system knowledge
- Adversary has knowledge of system layout
- No parameter estimation or detection algorithms, only illumination

# Signal Models – Transmitted signal from the transmitting APs




For transmitting AP j: $\mathbf{x}_j[n] = \sum_{i=1}^{N_{\mathrm{UE}}} \mathbf{w}_{j,i} s_i[n] + \mathbf{w}_{j,t} s_s[n].$

Communication precoder and symbols

Sensing precoder and symbols

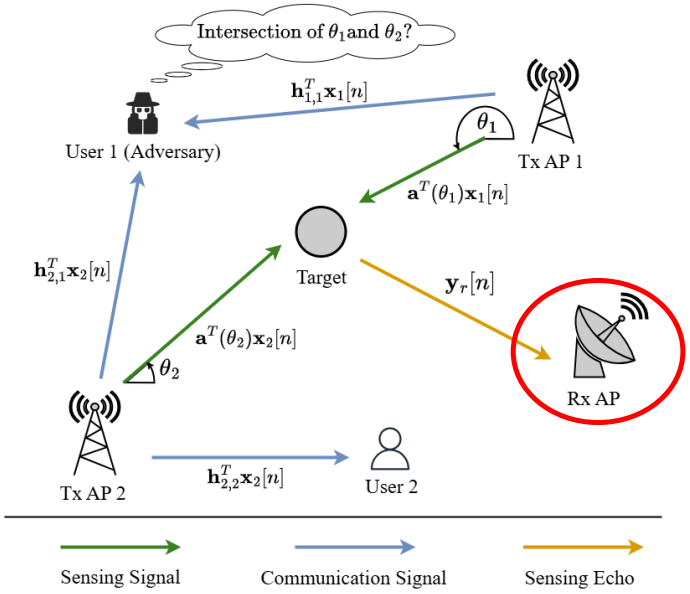
# Signal Models – Received signal at the receiver APs

For receiving AP r: $$\mathbf{y}_r[n] = \sum_{j=1}^{N_{\text{Tx}}} \alpha_{j,r} \sqrt{\beta_{j,r}} \mathbf{a}(\theta_r)\mathbf{a}(\theta_j)^T \mathbf{x}_j[n] + \mathbf{n}[n],$$

Large scale fading coefficient

RCS and phase shift of path

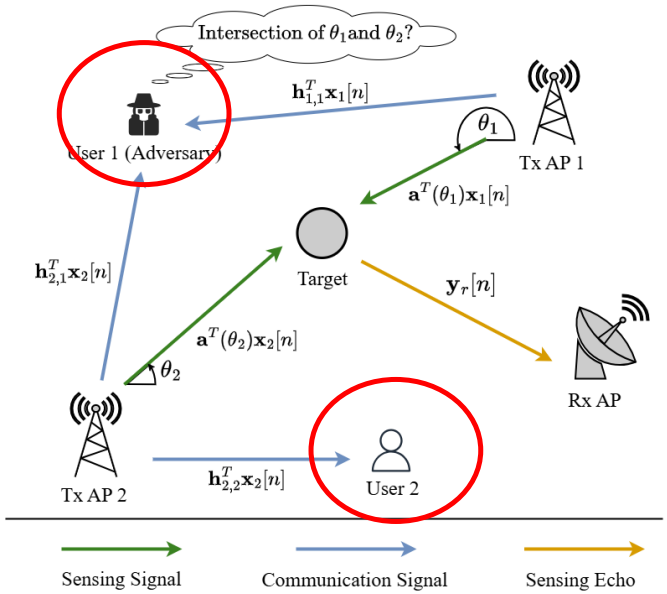
Antenna array steering vectors for angle from target to receiver, and transmitter to target, respectively



# Signal Models – Received signal at the users

For user $i$:

$$y_i[n] = \underbrace{\sum_{j=1}^{N_{\text{Tx}}} \mathbf{h}_{j,i}^H \mathbf{w}_{j,i} s_i[n]}_{\text{Desired Signal}} + \underbrace{\sum_{j=1}^{N_{\text{Tx}}} \sum_{\substack{k=1 \\ k \neq i}}^{N_{\text{UE}}} \mathbf{h}_{j,i}^H \mathbf{w}_{j,k} s_k[n]}_{\text{Communication Interference}} + \underbrace{\sum_{j=1}^{N_{\text{Tx}}} \mathbf{h}_{j,i}^H \mathbf{w}_{j,t} s_s[n]}_{\text{Sensing Interference}} + \underbrace{n_i[n]}_{\text{Noise}},$$



# Sensing-Centric Naive Precoder Design

- Optimize sensing receiver SINR w.r.t. joint precoder matrix
- Communication SINR per user constraint
- Power consumption per antenna element constraint

$$\begin{aligned} \max_{\mathbf{W}} \quad & \gamma_s(\mathbf{W}) \\ \text{s.t.} \quad & \gamma_{\text{UE}_i} \geq \gamma, \forall i \\ & P_{j,a} \leq P_{max}, \forall j, \forall a, \end{aligned}$$

# Attack Model

- Adversarial user of the system
- Unknown to the network
- Goal of the adversary is to identify the currently illuminated location

# Attack Model

- Sensing precoder present in received signal
- Expectation Maximization for $\boldsymbol{x}$
- Sample covariance gives the sensing precoders
- Intersecting angles

Signal received by user:

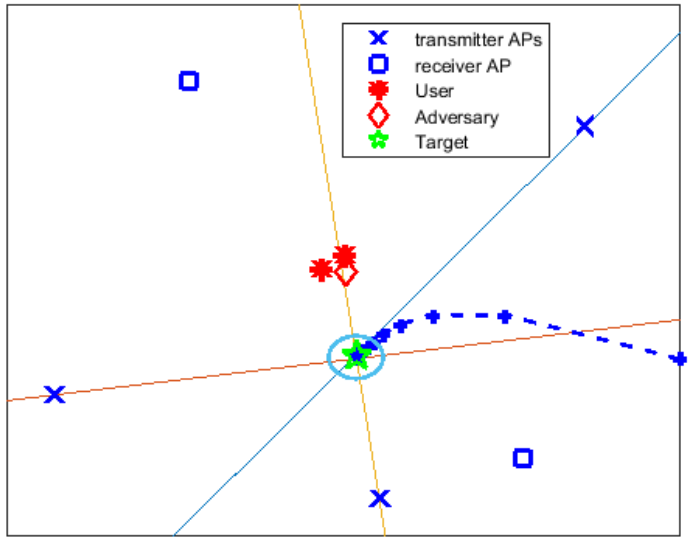
$$y_i[n] = \underbrace{\sum_{j=1}^{N_{\text{Tx}}} \mathbf{h}_{j,i}^H \mathbf{w}_{j,i} s_i[n]}_{\text{Desired Signal}} + \underbrace{\sum_{j=1}^{N_{\text{Tx}}} \sum_{\substack{k=1 \\ k \neq i}}^{N_{\text{UE}}} \mathbf{h}_{j,i}^H \mathbf{w}_{j,k} s_k[n]}_{\text{Communication Interference}}$$

$$+ \underbrace{\sum_{j=1}^{N_{\text{Tx}}} \mathbf{h}_{j,i}^H \mathbf{w}_{j,t} s_s[n]}_{\text{Sensing Interference}} + \underbrace{n_i[n]}_{\text{Noise}},$$

Sensing Precoder

# Attack Model

- Gradient descent approach
- Correct detection by the adversary if real target is within a certain radius of its estimated guess



# Mitigation Method

- System design

- Mutual Information (MI) reduction by:
  1. Precoders
  2. AP Selection

$$I(y_i; \mathbf{x}_j^s) \leq \log_2 \left(1 + \left|\mathbf{h}_{j,i}^H \mathbf{x}_j^s\right|^2\right)$$

# Mitigation Method – Precoder

- Minimize the sum MI for each user w.r.t. joint precoder matrix
- Communication and sensing SINR per user constraint
- Power constraint per AP

$$\min_{\mathbf{W}} \quad \sum_{i=1}^{N_{\mathrm{UE}}} \sum_{j=1}^{N_{\mathrm{Tx}}} \sum_{n=1}^{N} \left| \mathbf{h}_{j,i}^{H} \mathbf{x}_{j}^{s} \right|^{2}$$

$$\text{s.t.} \quad \gamma_s \geq \gamma_1$$

$$\gamma_{\mathrm{UE}_i} \geq \gamma_2, \forall i$$

$$P_j \leq P_{max}, \forall j,$$

# Mitigation Method – Precoder: Definitions

$$\mathbf{h}_i = \left[\mathbf{h}_{1,i}^T, \mathbf{h}_{2,i}^T, ..., \mathbf{h}_{N_{\text{Tx}},i}^T\right]^T$$
$$\mathbf{w}_i = \left[\mathbf{w}_{1,i}^T, \mathbf{w}_{2,i}^T, ..., \mathbf{w}_{N_{\text{Tx}},i}^T\right]^T.$$

: Effective channel and precoder for user $i$

---

$$\mathbf{A}_{j,m} = \sqrt{\beta_{j,r}\beta_{m,r}}\mathbf{a}(\theta_j)^*\mathbf{a}(\theta_r)^H\alpha_{j,r}^*\alpha_{m,r}\mathbf{a}(\theta_r)\mathbf{a}(\theta_m)^T. \qquad \mathbf{A}_r = \begin{bmatrix} \mathbf{A}_{1,1} & \cdots & \mathbf{A}_{1,N_{\text{Tx}}} \\ \vdots & \ddots & \vdots \\ \mathbf{A}_{N_{\text{Tx}},1} & \cdots & \mathbf{A}_{N_{\text{Tx}},N_{\text{Tx}}} \end{bmatrix},$$

: Concatenated pairwise “spatial cross-correlation”

---

$$\mathbf{W} = [\mathbf{w}_1, \mathbf{w}_2, \ldots \mathbf{w}_{N_{\text{Tx}}}, \mathbf{w}_s]$$

: Precoder matrix. Each column is the total precoder to a user from all APs. Each row is the precoder for one antenna element to all users + sensing target

# Mitigation Method – Precoder: Final Expressions

Sensing SINR:

$$\gamma_s(\mathbf{W}) = \frac{\sum_{r=1}^{N_{\text{Rx}}} \sum_{n=1}^{N} \mathbf{s}[n]^H \mathbf{W}^H \mathbf{A}_r \mathbf{W} \mathbf{s}[n]}{N_{\text{Rx}} N M \sigma_n^2}.$$

$$\Rightarrow$$

$$\gamma_s(\mathbf{W}) = \frac{\sum_{r=1}^{N_{\text{Rx}}} \sum_{n=1}^{N} \mathbf{s}[n]^H P_1^r(\mathbf{W}) \mathbf{s}[n]}{N_{\text{Rx}} N M \sigma_n^2}.$$

User SINR:

$$\gamma_{\text{UE}_i} = \frac{\left|\mathbf{h}_i^H \mathbf{w}_i\right|^2}{\left|\sum_{\substack{k=1 \\ k \neq i}}^{N_{\text{UE}}} \mathbf{h}_i^H \mathbf{w}_k\right|^2 + \left|\mathbf{h}_i^H \mathbf{w}_t\right|^2 + \sigma_n^2},$$

$$\Rightarrow$$

$$(\mathbf{w}_i^H)_{(p-1)} \mathbf{h}_i \mathbf{h}_i^H (\mathbf{w}_i)_{(p-1)} + 2(\mathbf{w}_i^H)_{(p-1)} \mathbf{h}_i \mathbf{h}_i^H ((\mathbf{w}_i)_p - (\mathbf{w}_i)_{(p-1)}) \geq \tau_n$$

$$\left|\sum_{\substack{k=1 \\ k \neq i}}^{N_{\text{UE}}} \mathbf{h}_i^H \mathbf{w}_k\right|^2 + \left|\mathbf{h}_i^H \mathbf{w}_t\right|^2 + \sigma_n^2 \leq \tau_d$$

$$\tau_n \geq \tau_d \gamma.$$

# Mitigation Method – Selection

- “Given the number of receivers, which ones out of all APs should be the receivers to minimize the MI sum?”
- Formulate this mathematically:

$$\min_{\mathcal{R}\subset\mathcal{A}} \quad \sum_{i=1}^{N_{\mathrm{UE}}} \sum_{l=1}^{N_{\mathrm{AP}}} \sum_{n=1}^{N} \left| \mathbf{h}_{l,i}^{H} \mathbf{x}_{l}^{s} \right|^{2},$$

- Largest MI contributors become receivers

# Mitigation Method – Selection

- MI-Matrix

$$\mathbf{M} = \sum_{n=1}^{N} \begin{bmatrix} \left|\mathbf{h}_{1,1}^{H}\mathbf{x}_{1}^{s}\right|^{2} & \cdots & \left|\mathbf{h}_{N_{\mathrm{AP}},1}^{H}\mathbf{x}_{N_{\mathrm{AP}}}^{s}\right|^{2} \\ \vdots & \ddots & \vdots \\ \left|\mathbf{h}_{1,N_{\mathrm{UE}}}^{H}\mathbf{x}_{1}^{s}\right|^{2} & \cdots & \left|\mathbf{h}_{N_{\mathrm{AP}},N_{\mathrm{UE}}}^{H}\mathbf{x}_{N_{\mathrm{AP}}}^{s}\right|^{2} \end{bmatrix},$$

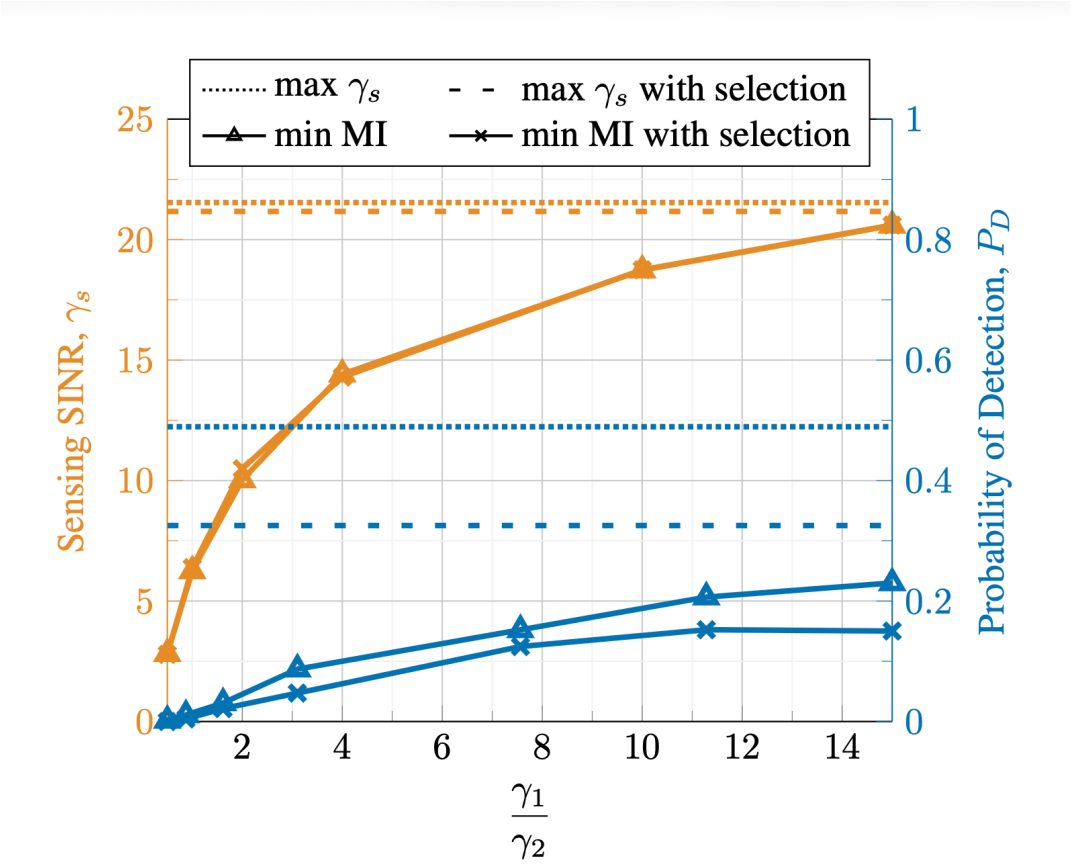
- Alternate with precoder computations until same APs have been selected twice in a row

- Pick the column indexes of the largest column norms as the receivers

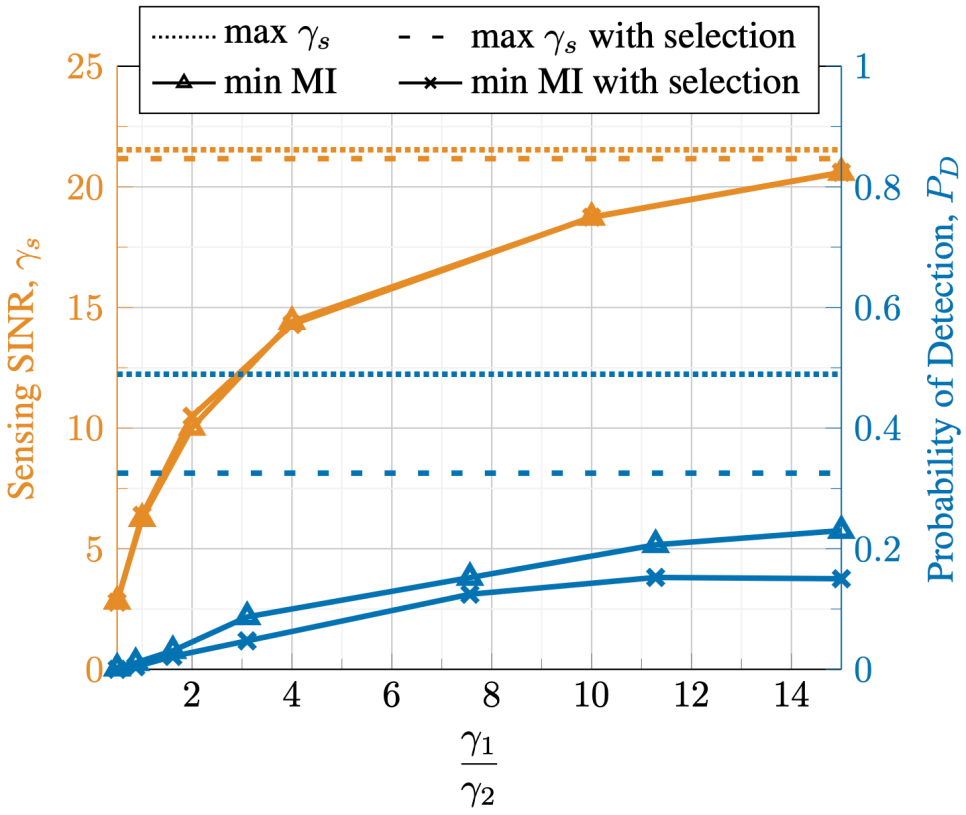
$$\mathcal{R} = \left\{ a_l \in \mathcal{A}\ \forall l \in \mathbf{l}_{\mathrm{Rx}} : \underset{\mathbf{l}_{\mathrm{Rx}}}{\operatorname{argmax}} \sum_{l \in \mathbf{l}_{\mathrm{Rx}}} ||\mathbf{m}_l|| \right\},$$

# Results

- Fraction of sensing and communication constraint
- Fixed communication constraint
- Similar sensing performance eventually



# Results




- Percentage of trials where the adversary correctly guessed the location within a radius
- Both countermeasures are beneficial
- Higher fraction → no precoder convergence

# Summary

- Our goal is to implement privacy-aware mechanisms in the design of ISAC systems
- Attack based on sensing precoders being present in received communication signal
- Primitive method proposed showed reduction in the probability of detection from this type of attack is possible

Thank you for listening!