Distributed Beamforming in Adversarial Environments

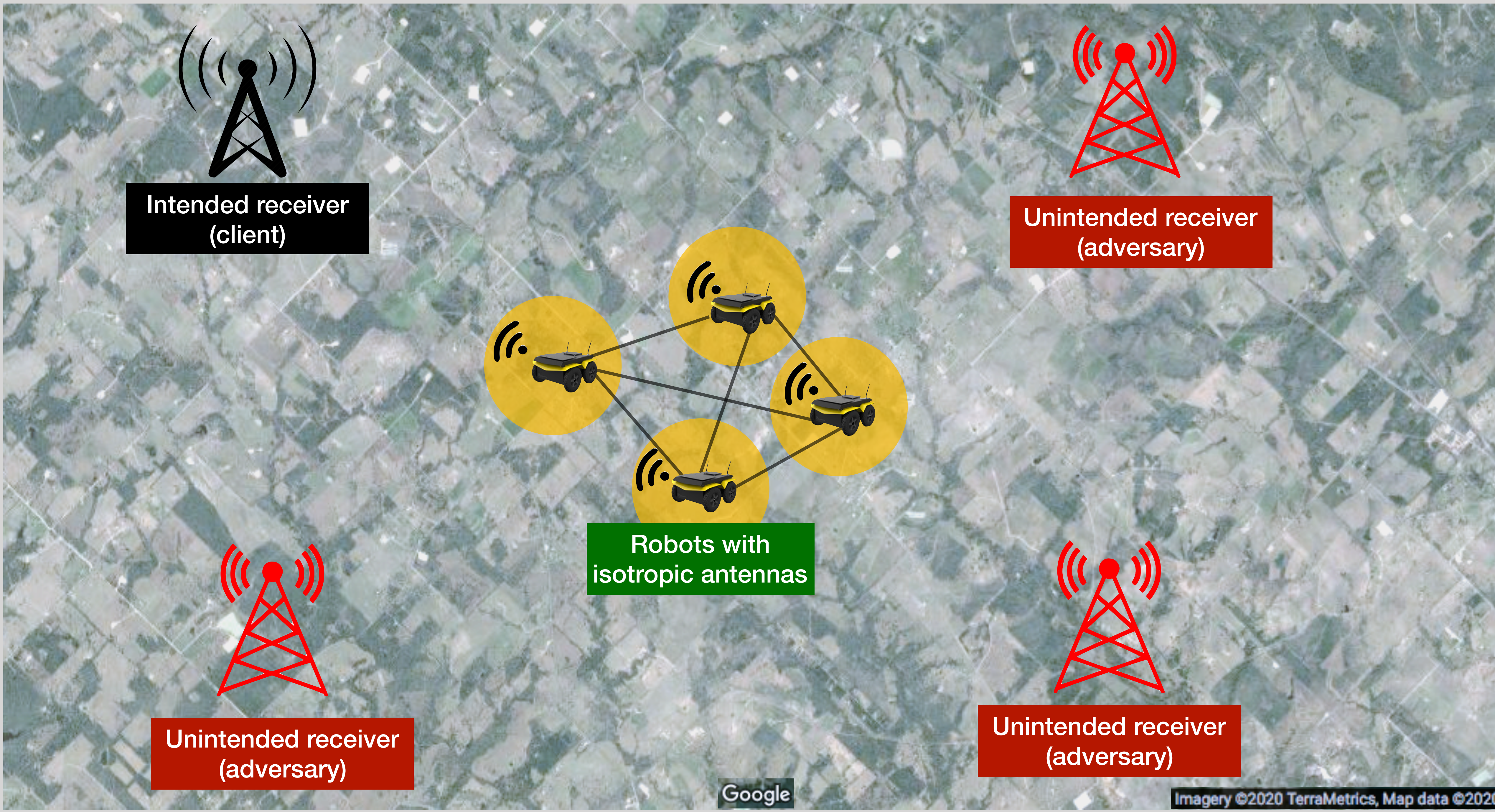
Yagiz Savas and Ufuk Topcu

in collaboration with Abolfazl Hashemi, Abraham P. Vinod, Brian M. Sadler

autonomous SYSTEMS GROUP

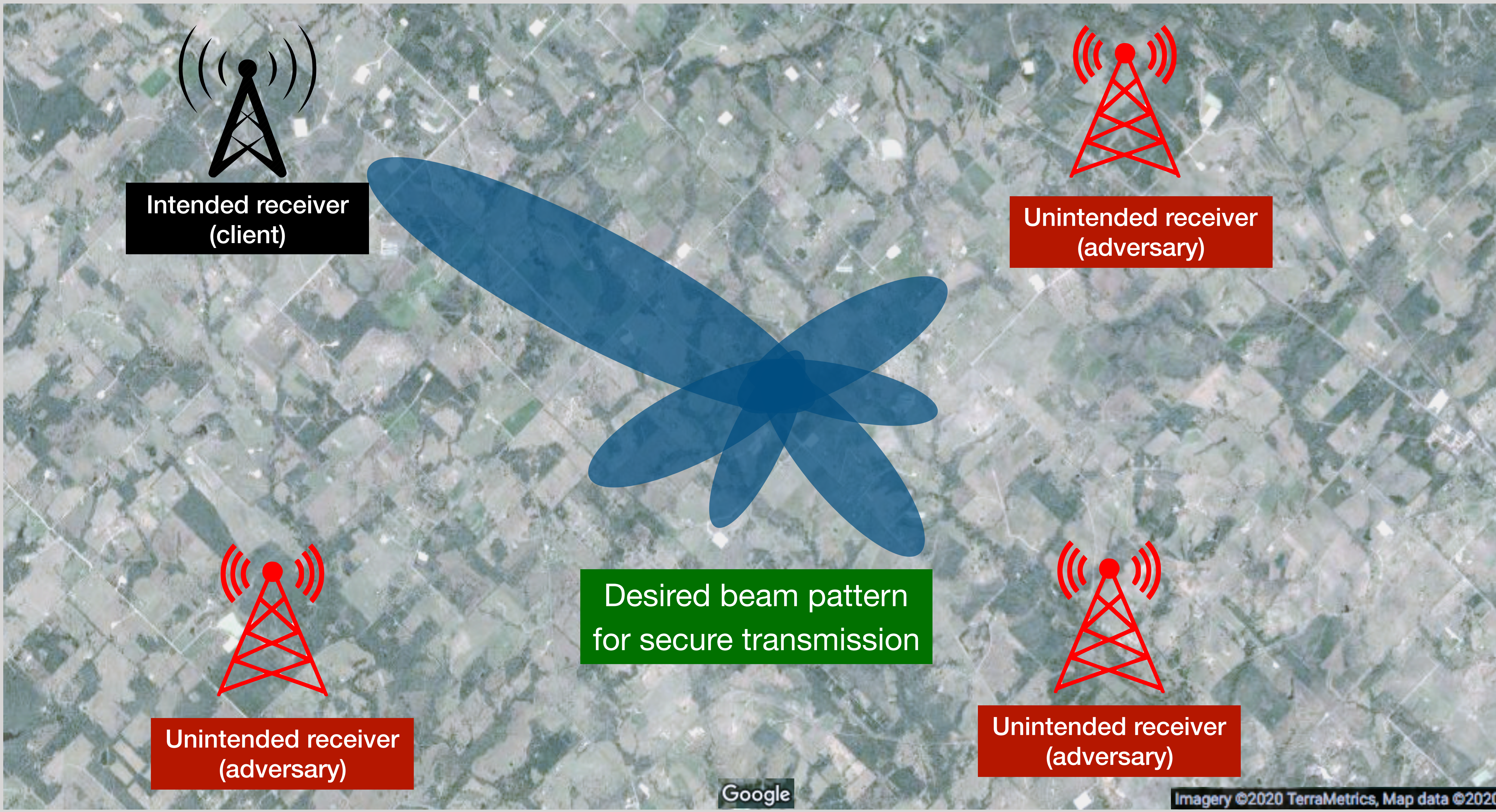
TEXAS The University of Texas at Austin

Wireless Communications in the Presence of Adversaries



- Robot image credit: https://clearpathrobotics.com/

Wireless Communications in the Presence of Adversaries



- Robot image credit: https://clearpathrobotics.com/

Objective and Structure

Develop a time-varying transmission strategy
that enables secure communication

Distributed beamforming

Physical-layer security

Semi-definite programming

Beamforming as a Wireless Communication Technique: Main Idea

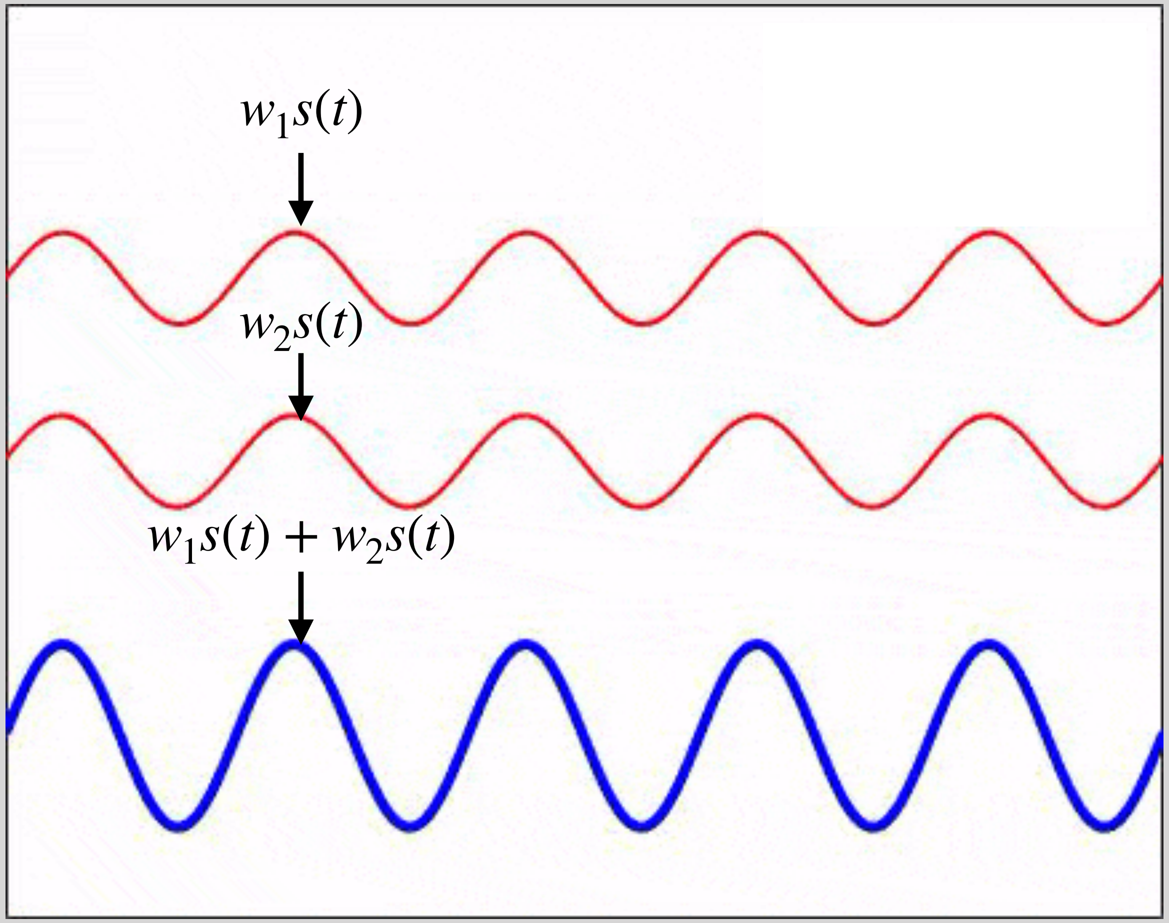
amplitude

phase

Message signal: $s(t) = ae^{j\phi}$

Adjust phase and amplitude: $w_i s(t) = \bar{a}e^{j\bar{\phi}}$

Transmit collectively: $y(t) = \sum_i w_i s(t)$



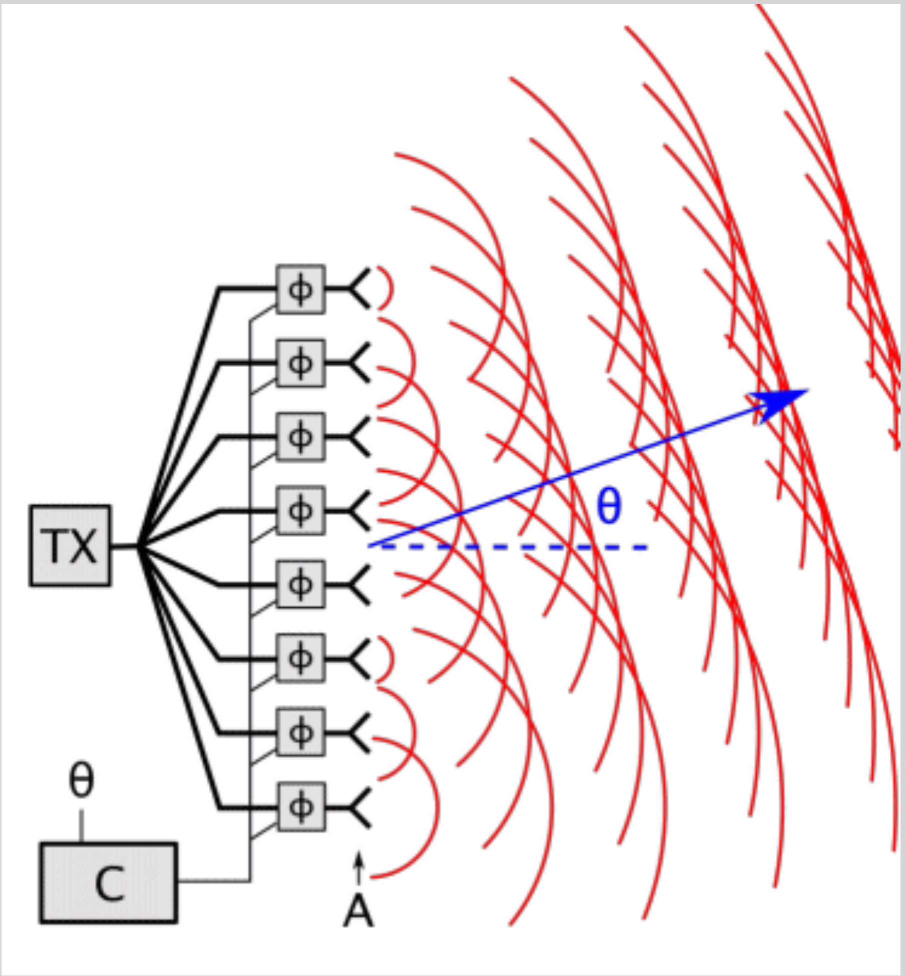
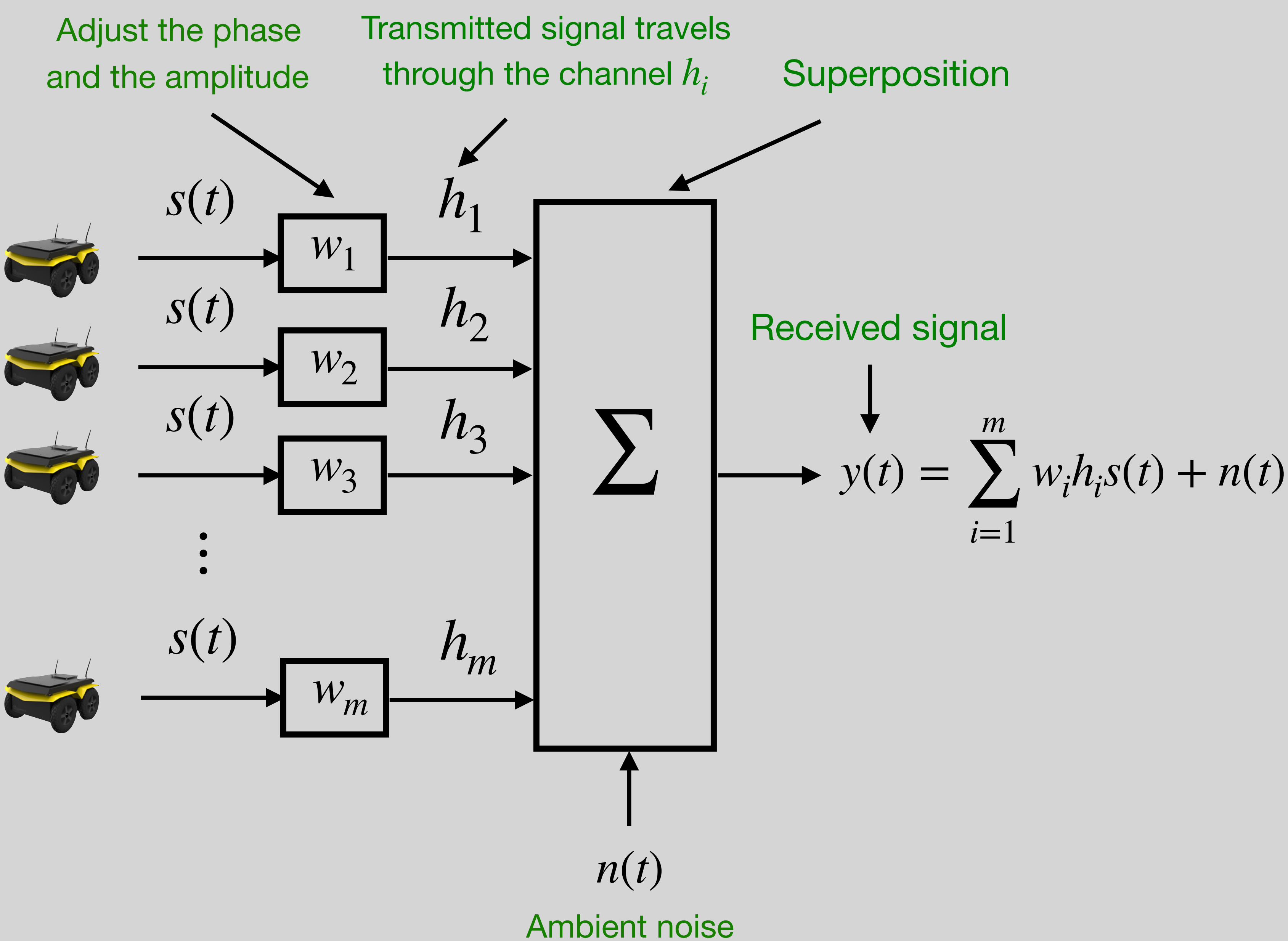


Illustration: https://en.wikipedia.org/wiki/Phased_array

Beamforming as a Wireless Communication Technique: Main Idea



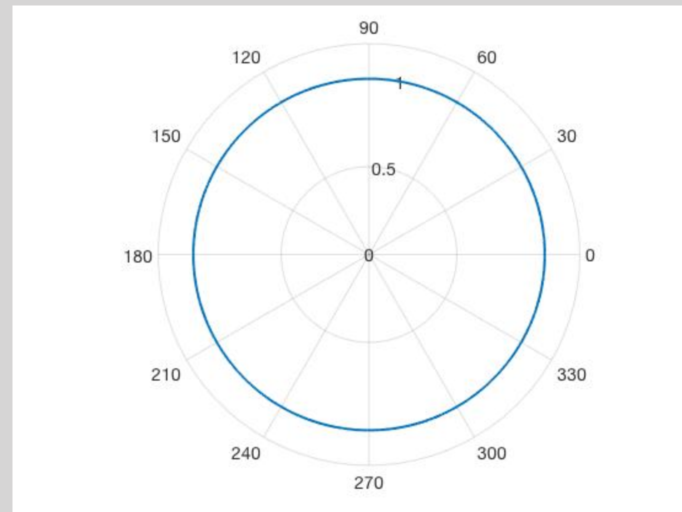
Received signal-to-interference -plus-noise ratio (SINR)

$$SINR = \frac{|\sum w_i h_i|^2}{\mathrm{Var}(n(t))}$$

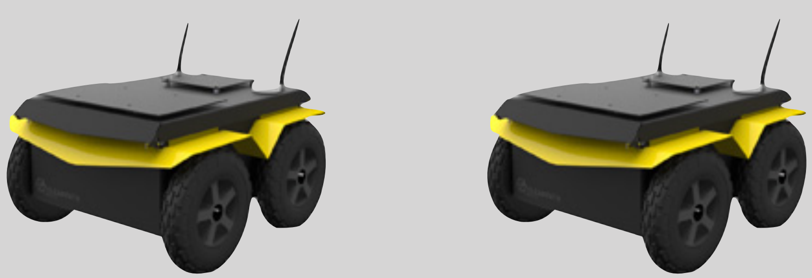
High SINR implies reliable communication

Beamforming as a Wireless Communication Technique: Benefits

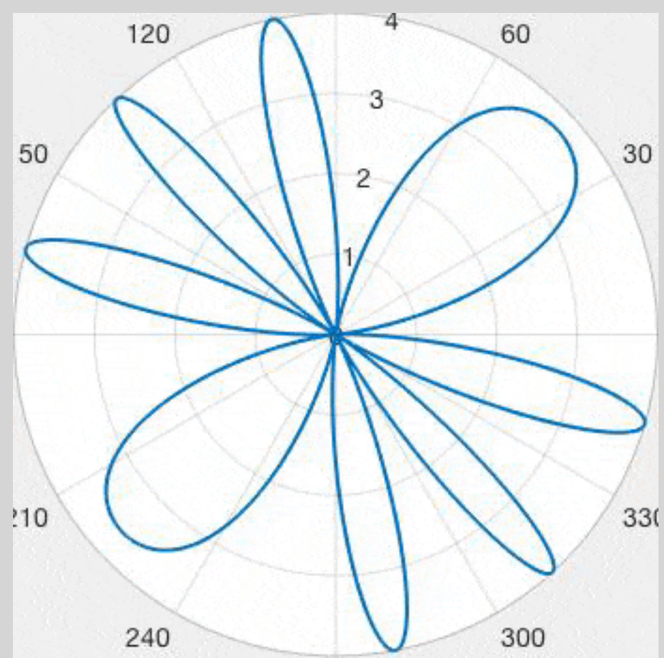
Single robot equipped
with an isotropic antenna



- **No directionality**
- **Low SINR**

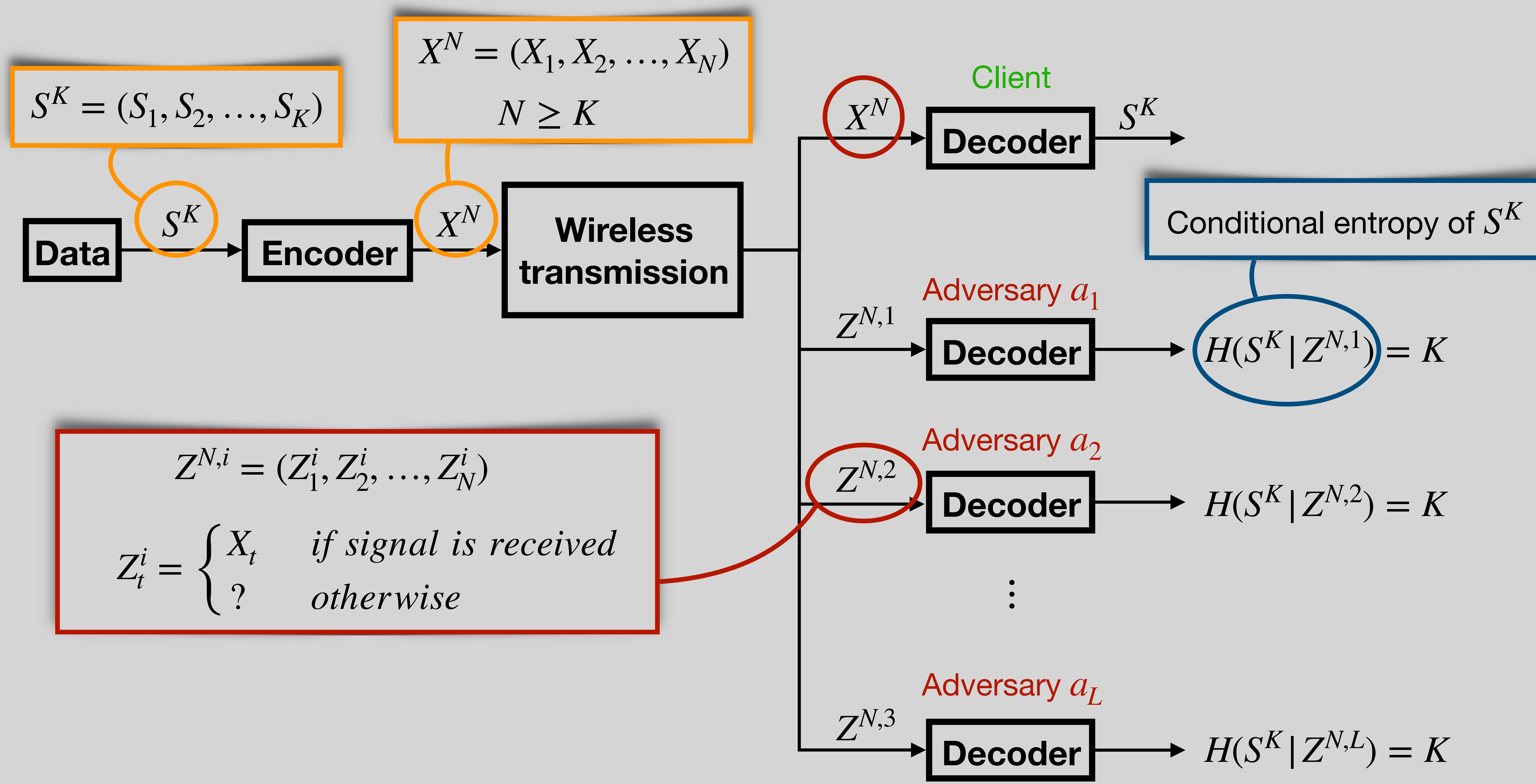


Two robots each equipped
with an isotropic antenna



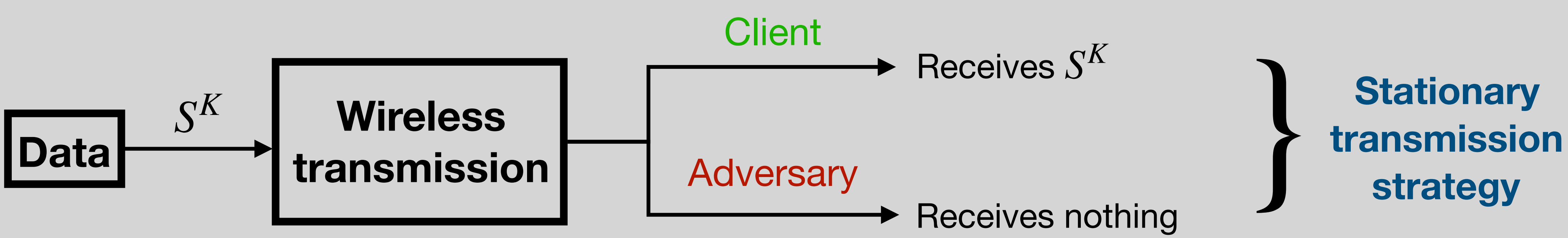
- **Improved directionality**
- **Improved SINR**

Secure Communication Problem: An Informal Problem Statement



Related Work

- No adversaries: optimal beamformer can be found analytically [1]
- Adversaries with known locations: convex optimization-based beamformers [2]
- Adversaries with unknown locations: minimize SINR in all directions by broadcasting artificial noise [3]



- Ozarow and Wyner[4] showed in 1984 that if S^K is encoded into X^N, then

μ_i : number of symbols received by adversary a_i

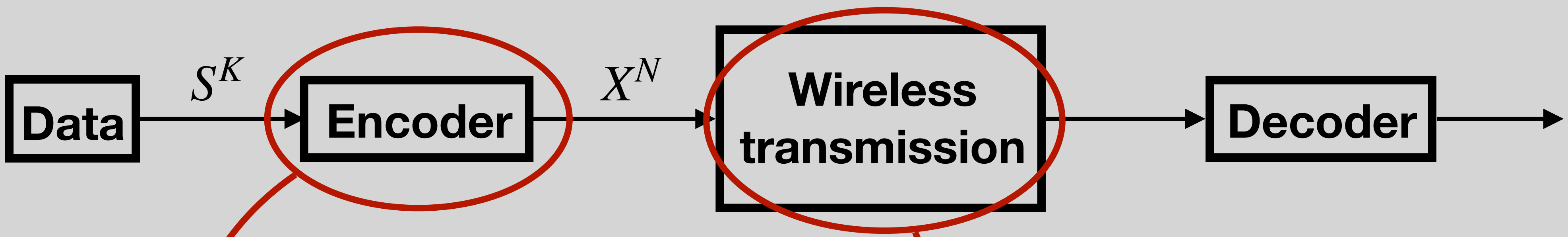
$$\mu_i \leq N - K \implies H(S^K | Z^{N,i}) = K$$

Implication: We can let each adversary receive $N - K$ symbols and still establish a secure communication

[1] Lorenz, R. G. and Boyd, S. P., ``Robust minimum variance beamforming”, IEEE Transactions on Signal Processing, 2005
[2] Liao et al, ``QoS-Based Transmit Beamforming in the Presence of Eavesdroppers”, IEEE Transactions on Signal Processing, 2010
[3] Goel, S. And Negi, R., ``Guaranteeing Secrecy Using Artificial Noise”, IEEE Transactions on Wireless Communications, 2008
[4] Ozarow, L. H. and Wyner, A. D., ``Wire-Tap Channel II'', AT&T Bell Laboratories technical journal, 1984

Contributions

We approach the problem from a sequential decision-making perspective

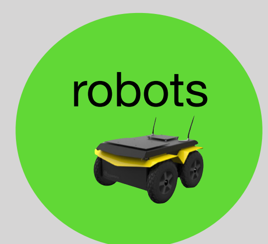


Maps K bits into $N = KL$ symbols where $L \in \mathbb{N}$ is the number of adversaries

Periodic transmission strategy ensures that each adversary receives at most $K(L-1)$ symbols

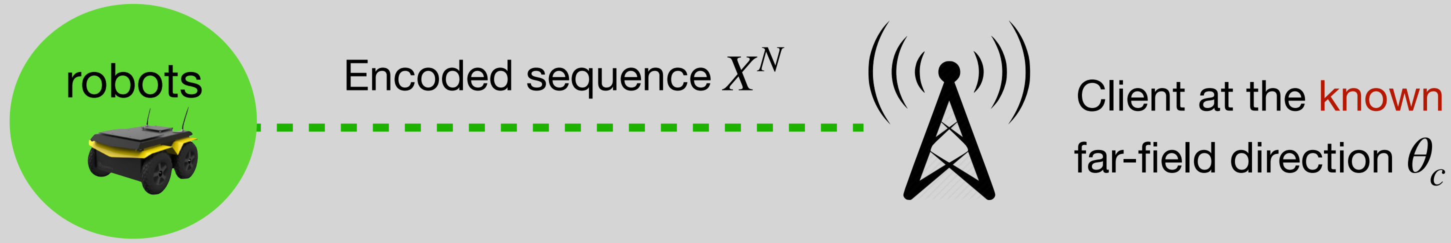
The proposed periodic strategy enables the agents to securely communicate with the client in scenarios in which all stationary strategies fail to ensure security

Environment Model

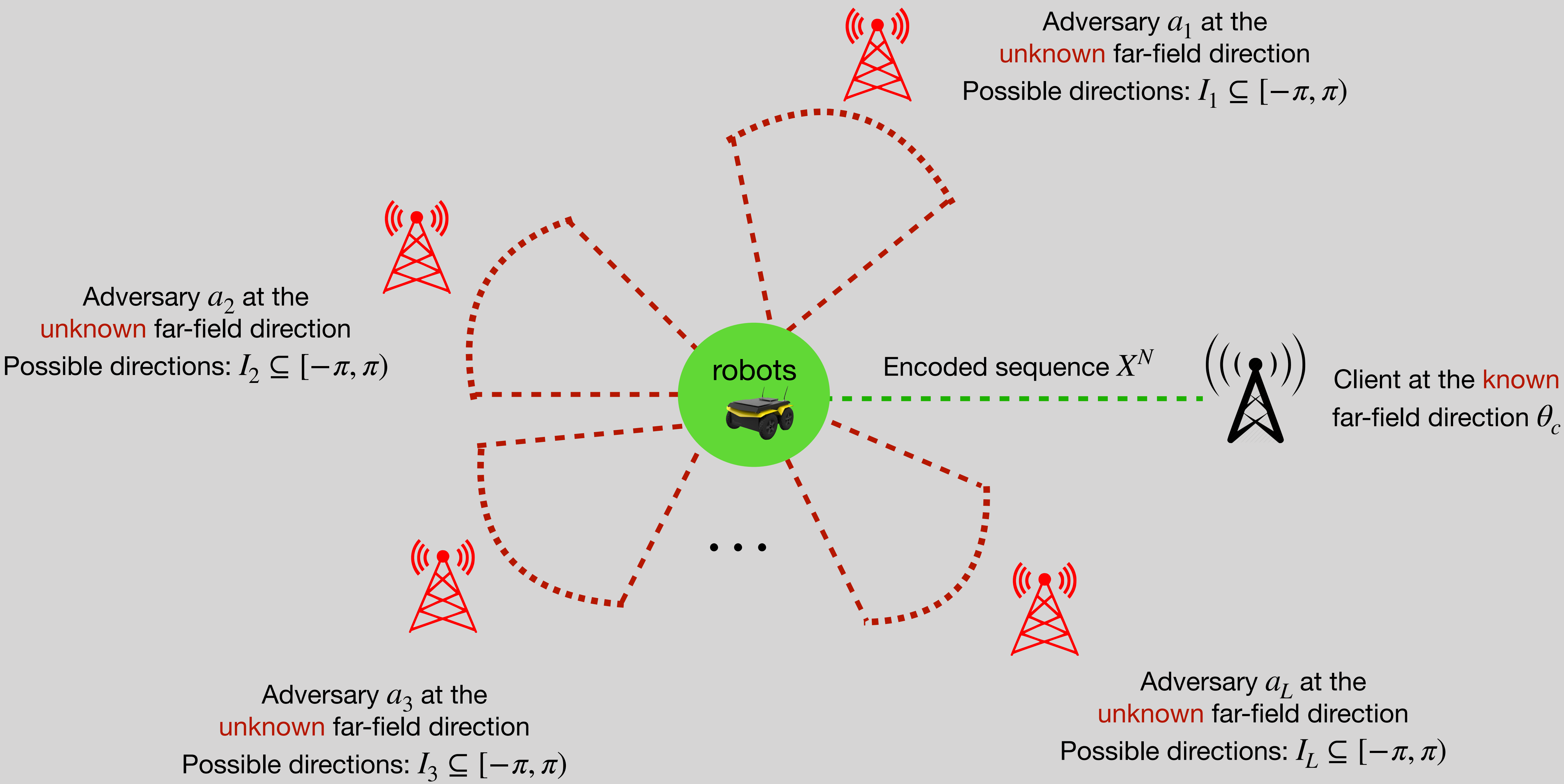


Isotropic antenna with
max transmit power $P > 0$

Environment Model



Environment Model



Transmission model

At time $t \in [N]$, the agents transmit the encoded symbol X_t as a continuous signal s_t.

The vector of signals transmitted by the agents is

$$y_{transmit}[t] = \mathbf{w}_t s_t + \mathbf{v}_t$$

Beamforming vector $\mathbf{w}_t = [w_1, w_2, \ldots, w_m]'$

Artificial noise $\mathbf{v}_t \sim \mathscr{C}\mathscr{N}(0, \Sigma_t)$

Transmission model

At time $t \in [N]$, the agents transmit the encoded symbol X_t as a continuous signal s_t.

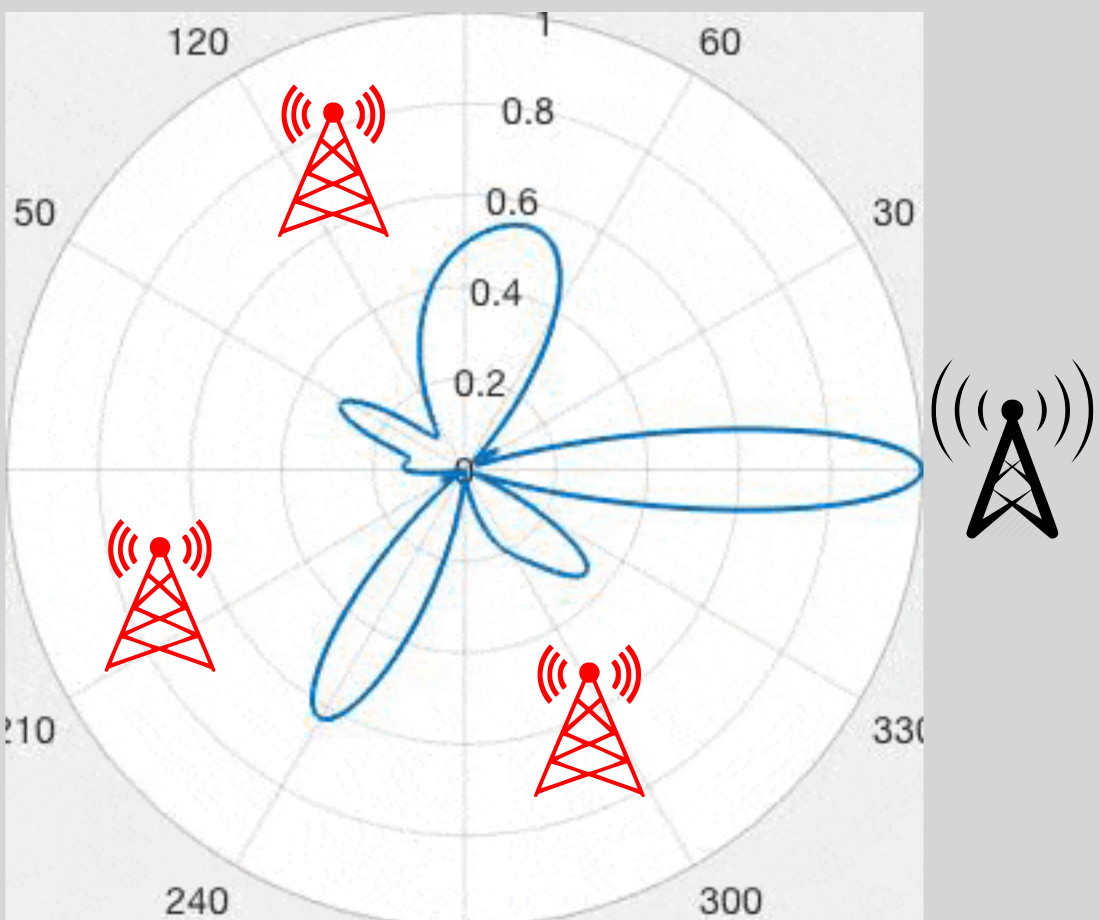
The vector of signals transmitted by the agents is

$$y_{transmit}[t] = \mathbf{w}_t s_t + \mathbf{v}_t$$

Beamforming vector $\mathbf{w}_t = [w_1, w_2, \dots, w_m]'$

Artificial noise $\mathbf{v}_t \sim \mathscr{C}\mathscr{N}(0,\Sigma_t)$

What is the effect of artificial noise? [1]



If the agents had infinite transmit power, they would minimize the SINR in all adversary directions simultaneously

[1] Goel, S. And Negi, R., ``Guaranteeing Secrecy Using Artificial Noise”, IEEE Transactions on Wireless Communications,2008

Transmission model

At time $t \in [N]$, the agents transmit the encoded symbol X_t as a continuous signal s_t.

The vector of signals transmitted by the agents is

$$y_{transmit}[t] = \mathbf{w}_t s_t + \mathbf{v}_t$$

Beamforming vector $\mathbf{w}_t = [w_1, w_2, \ldots, w_m]'$

Artificial noise $\mathbf{v}_t \sim \mathscr{CN}(0, \Sigma_t)$

Since the maximum transmit power is P, we have $w_t(i) + \Sigma_t(i,i) \leq P$.

The known narrowband channel between the agent $i \in [m]$ and a receiver in the direction $\theta \in [-\pi, \pi)$ is denoted by $h_i(\theta) \in \mathbb{C}$.

- Finally, the SINR received from the direction θ is

Channel matrix $\mathbf{H}(\theta) = \mathbf{h}(\theta)\mathbf{h}(\theta)^H$

$$SINR_t(\theta) = \frac{\mathbf{w}_t^H \mathbf{H}(\theta) \mathbf{w_t}}{Tr(\mathbf{H}(\theta)\Sigma_t) + \sigma_t^2}$$

$Tr(M)$ denotes the trace of the matrix M

Variance of the ambient noise

Ensuring Security with a Periodic Transmission Strategy

The objective is to find a sequence $((\mathbf{w}_1, \Sigma_1), (\mathbf{w}_2, \Sigma_2), \ldots, (\mathbf{w}_N, \Sigma_N))$ of pairs $(\mathbf{w}_t, \Sigma_t)$ such that

(I) The client receives all transmitted symbols X_t

(II) Each adversary receives at most $N - K$ symbols

STEP 1: Encoding by $[N, N-K]$ linear maximum-distance-separable codes.

STEP 2: Transmission by the periodic strategy

$$((\mathbf{w}_1, \Sigma_1), \underbrace{(\mathbf{w}_2, \Sigma_2), \ldots,}_{\text{First cycle}} (\mathbf{w}_L, \Sigma_L), (\mathbf{w}_1, \Sigma_1), \underbrace{(\mathbf{w}_2, \Sigma_2), \ldots,}_{\text{Second cycle}} (\mathbf{w}_L, \Sigma_L), \ldots, (\mathbf{w}_1, \Sigma_1), \underbrace{(\mathbf{w}_2, \Sigma_2), \ldots,}_{K\text{-th cycle}} (\mathbf{w}_L, \Sigma_L))$$

$$\min_{\mathbf{w}_k \in \mathbb{C}^m, \Sigma_k \succcurlyeq 0} \quad Tr(\Sigma_k) + \|\mathbf{w}_k\|_2^2 \qquad \text{Minimize total transmit power}$$

$$\text{subject to:} \quad SINR_k(\theta_c) \geq \gamma_c \qquad \text{Client's SINR constraint}$$

$$\forall \theta \in I_k, \quad SINR_k(\theta) \leq \gamma_a \qquad \text{Adversary } a_k\text{'s SINR constraint}$$

$$\forall i \in [m], \quad \mathbf{w}_k(i) + \Sigma_k(i,i) \leq P \qquad \text{Agents' power constraints}$$

Semi-Definite Program Relaxation and Probabilistic Approximation

Semi-infinite nonconvex optimization problem

$$
\begin{aligned}
\min_{\mathbf{W}_k \succcurlyeq 0, \Sigma_k \succcurlyeq 0} \quad & Tr(\Sigma_k) + Tr(\mathbf{W}_k) \\
s.t. \quad & Tr(\mathbf{H}(\theta_c)\mathbf{W}_k) \geq \gamma_c \left(Tr(\mathbf{H}(\theta_c)\Sigma_k) + \sigma_k^2 \right) \\
\forall \theta \in I_k, \quad & Tr(\mathbf{H}(\theta)\mathbf{W}_k) \leq \gamma_a \left(Tr(\mathbf{H}(\theta)\Sigma_k) + \sigma_k^2 \right) \\
\forall i \in [m], \quad & \mathbf{W}_k(i,i) + \Sigma_k(i,i) \leq P \\
& rank(\mathbf{W_k}) = 1
\end{aligned}
$$

Source of infiniteness

Source of nonconvexity

Semi-Definite Program Relaxation and Probabilistic Approximation

Semi-infinite **convex** optimization problem

$$\begin{aligned}
\min_{\mathbf{W}_k \succcurlyeq 0, \Sigma_k \succcurlyeq 0} \quad & Tr(\Sigma_k) + Tr(\mathbf{W}_k) \\
s.t. \quad & Tr(\mathbf{H}(\theta_c)\mathbf{W}_k) \geq \gamma_c \Big(Tr(\mathbf{H}(\theta_c)\Sigma_k) + \sigma_k^2 \Big) \\
\forall \theta \in I_k, \quad & Tr(\mathbf{H}(\theta)\mathbf{W}_k) \leq \gamma_a \Big(Tr(\mathbf{H}(\theta)\Sigma_k) + \sigma_k^2 \Big) \\
\forall i \in [m], \quad & \mathbf{W}_k(i,i) + \Sigma_k(i,i) \leq P \\
& \cancel{rank(\mathbf{W}_k) = 1}
\end{aligned}$$

Result: The convex relaxation is exact

Semi-Definite Program Relaxation and Probabilistic Approximation

Semi-infinite convex optimization problem

$$
\begin{aligned}
\min_{\mathbf{W}_k \succcurlyeq 0, \Sigma_k \succcurlyeq 0} \quad & Tr(\Sigma_k) + Tr(\mathbf{W}_k) \\
s.t. \quad & Tr(\mathbf{H}(\theta_c)\mathbf{W}_k) \geq \gamma_c \Big(Tr(\mathbf{H}(\theta_c)\Sigma_k) + \sigma_k^2 \Big) \\
\forall \theta \in I_k, \quad & Tr(\mathbf{H}(\theta)\mathbf{W}_k) \leq \gamma_a \Big(Tr(\mathbf{H}(\theta)\Sigma_k) + \sigma_k^2 \Big) \\
\forall i \in [m], \quad & \mathbf{W}_k(i,i) + \Sigma_k(i,i) \leq P
\end{aligned}
$$

Source of infiniteness

Semi-Definite Program Relaxation and Probabilistic Approximation

Finite convex optimization problem

Randomly sample $B \in \mathbb{N}$ points from the set I_k

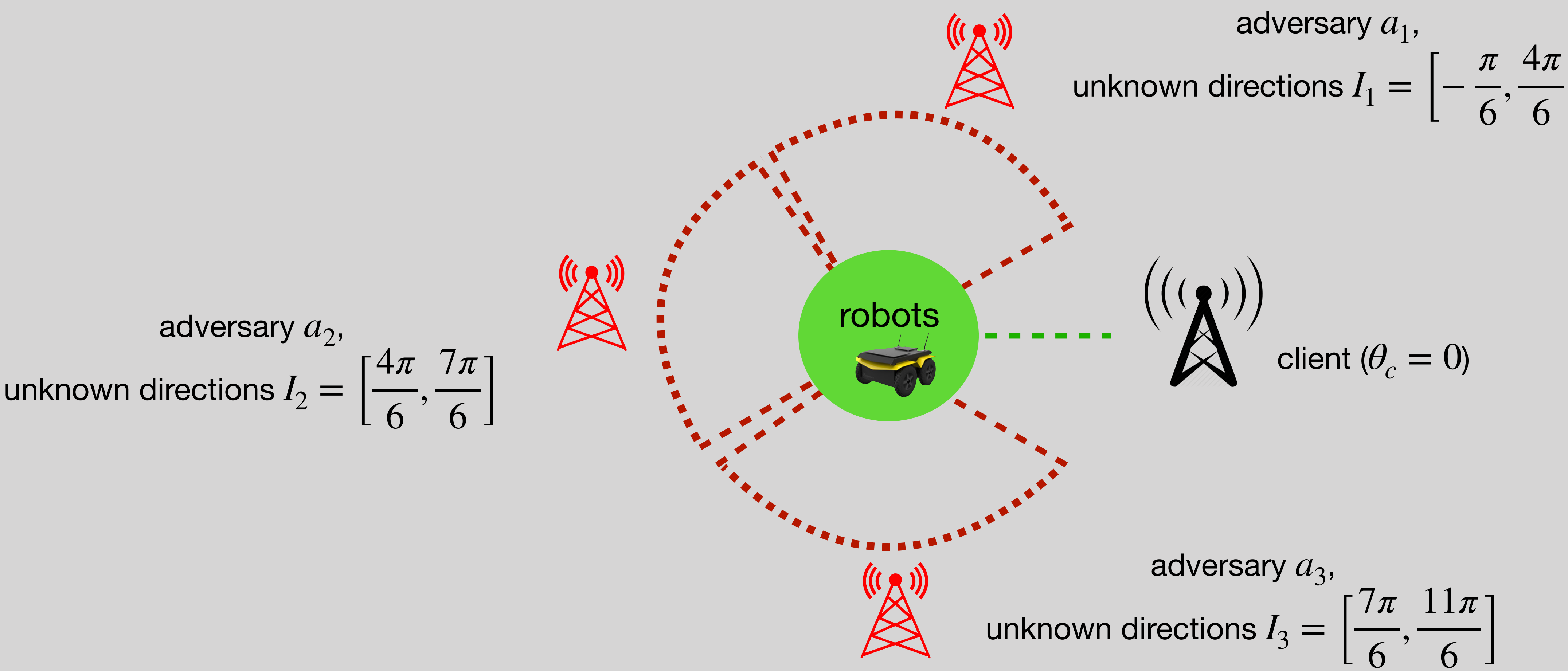
$$
\begin{aligned}
\min_{\mathbf{W}_k \succcurlyeq 0, \Sigma_k \succcurlyeq 0} \quad & Tr(\Sigma_k) + Tr(\mathbf{W}_k) \\
s.t. \quad & Tr(\mathbf{H}(\theta_c)\mathbf{W}_k) \geq \gamma_c \left(Tr(\mathbf{H}(\theta_c)\Sigma_k) + \sigma_k^2 \right) \\
\forall \theta \in \Theta_B, \quad & Tr(\mathbf{H}(\theta)\mathbf{W}_k) \leq \gamma_a \left(Tr(\mathbf{H}(\theta)\Sigma_k) + \sigma_k^2 \right) \\
\forall i \in [m], \quad & \mathbf{W}_k(i,i) + \Sigma_k(i,i) \leq P
\end{aligned}
$$

Result [1]: The following statement is true with probability $1 - \beta_2$:

If $B \geq (2\log_e(\beta_2^{-1}) + 16m^2)/\beta_1$, the problems are equivalent with probability $1 - \beta_1$.

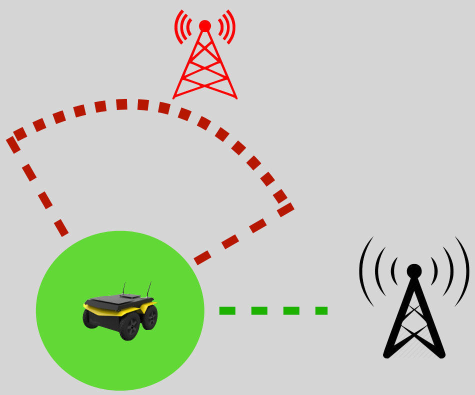
[1] Campi, M.C., Garatti, S., and Prandini, M., `` The scenario approach for systems and control design", Annual Reviews in Control, 2009

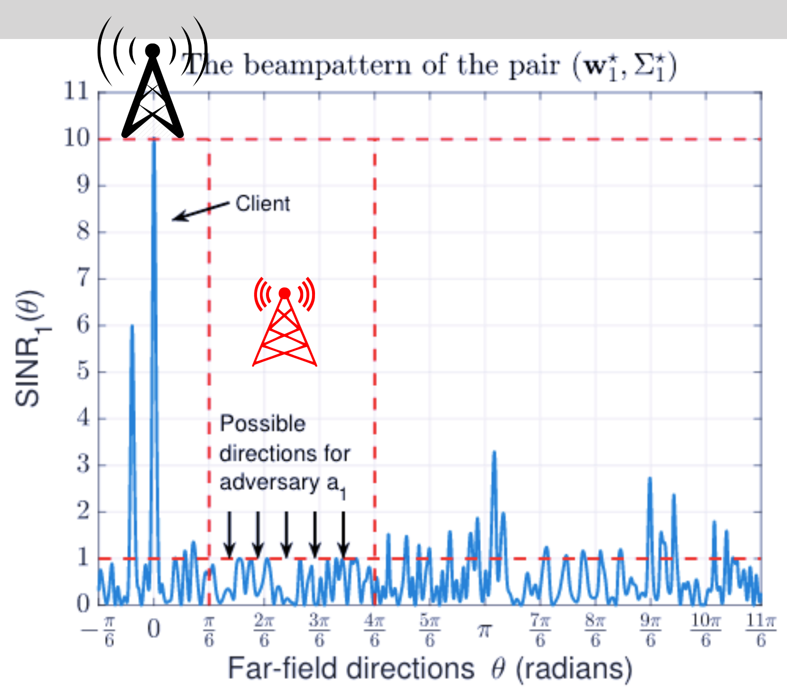
A Numerical Example



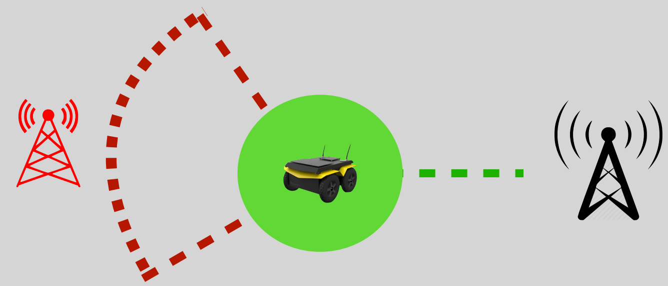
A Numerical Example

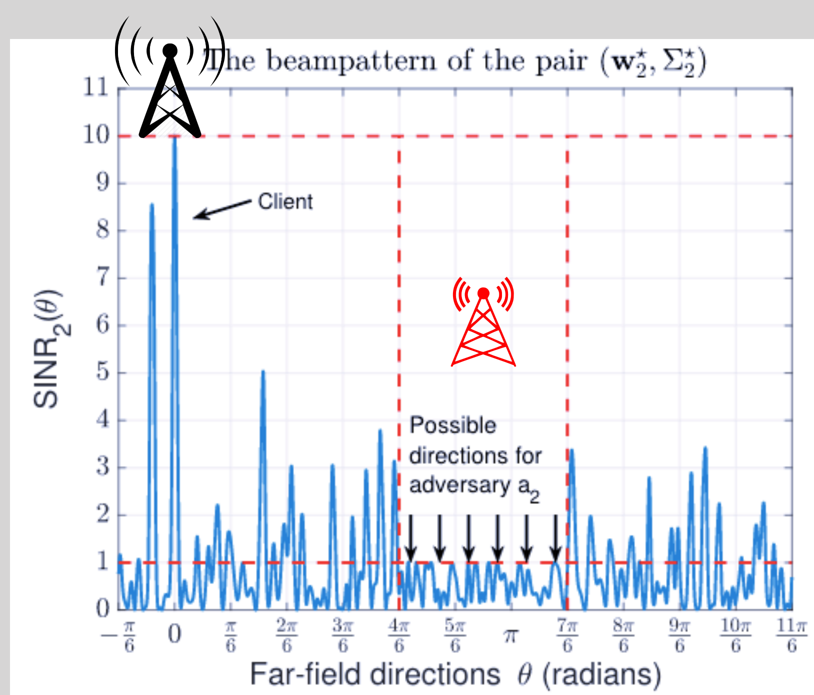
First time step:



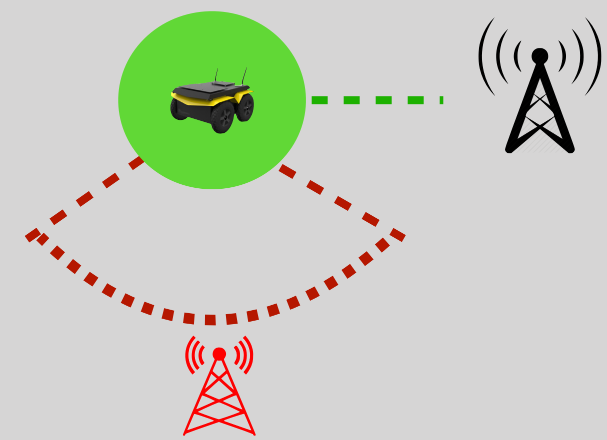


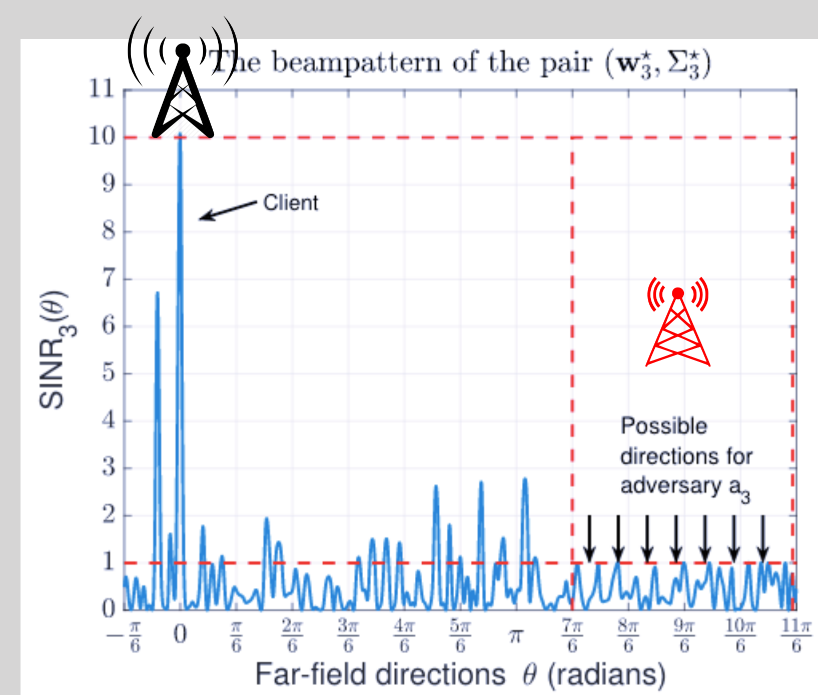
Second time step:





Third time step:



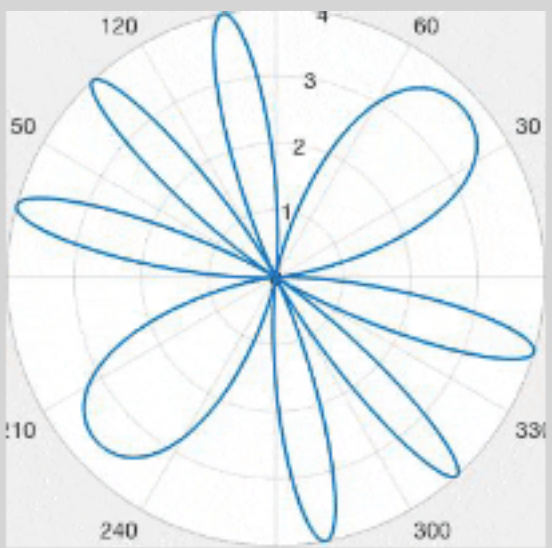


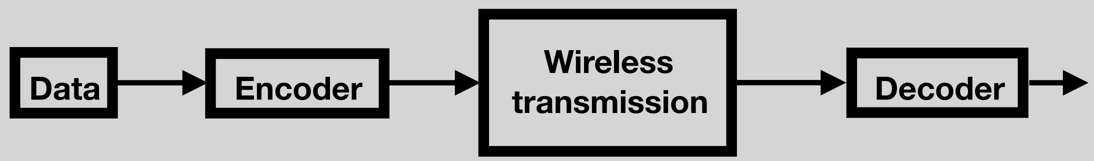
Conclusions

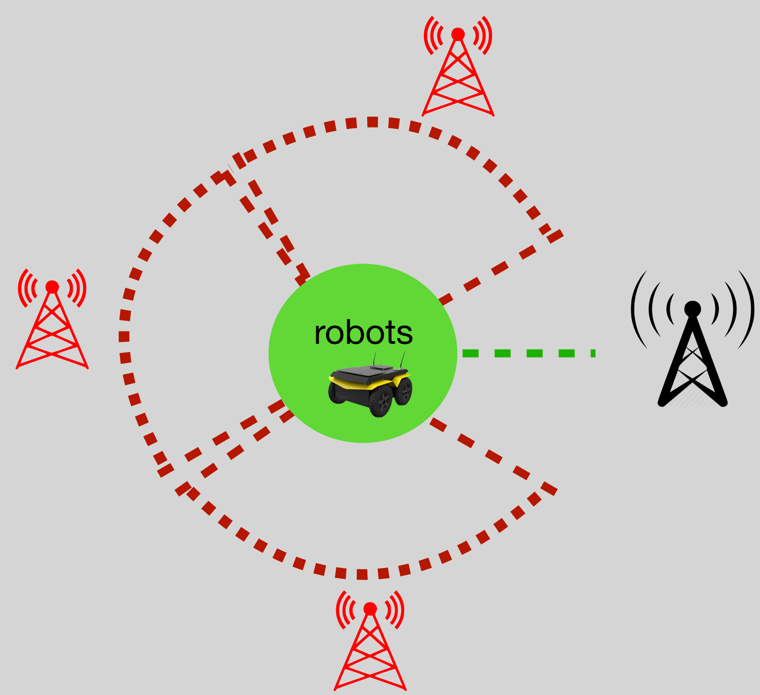
Distributed beamforming

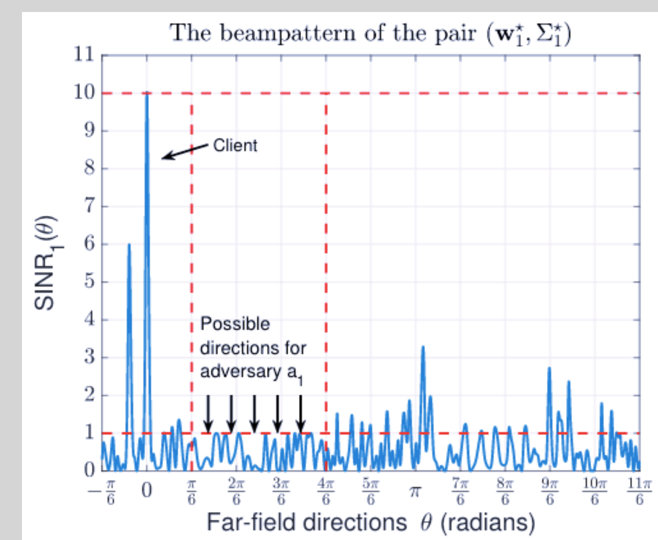
Physical-layer security

Semi-definite programming









Thank you for listening

E-mail: yagiz.savas@utexas.edu