Distributed Beamforming in Adversarial Environments

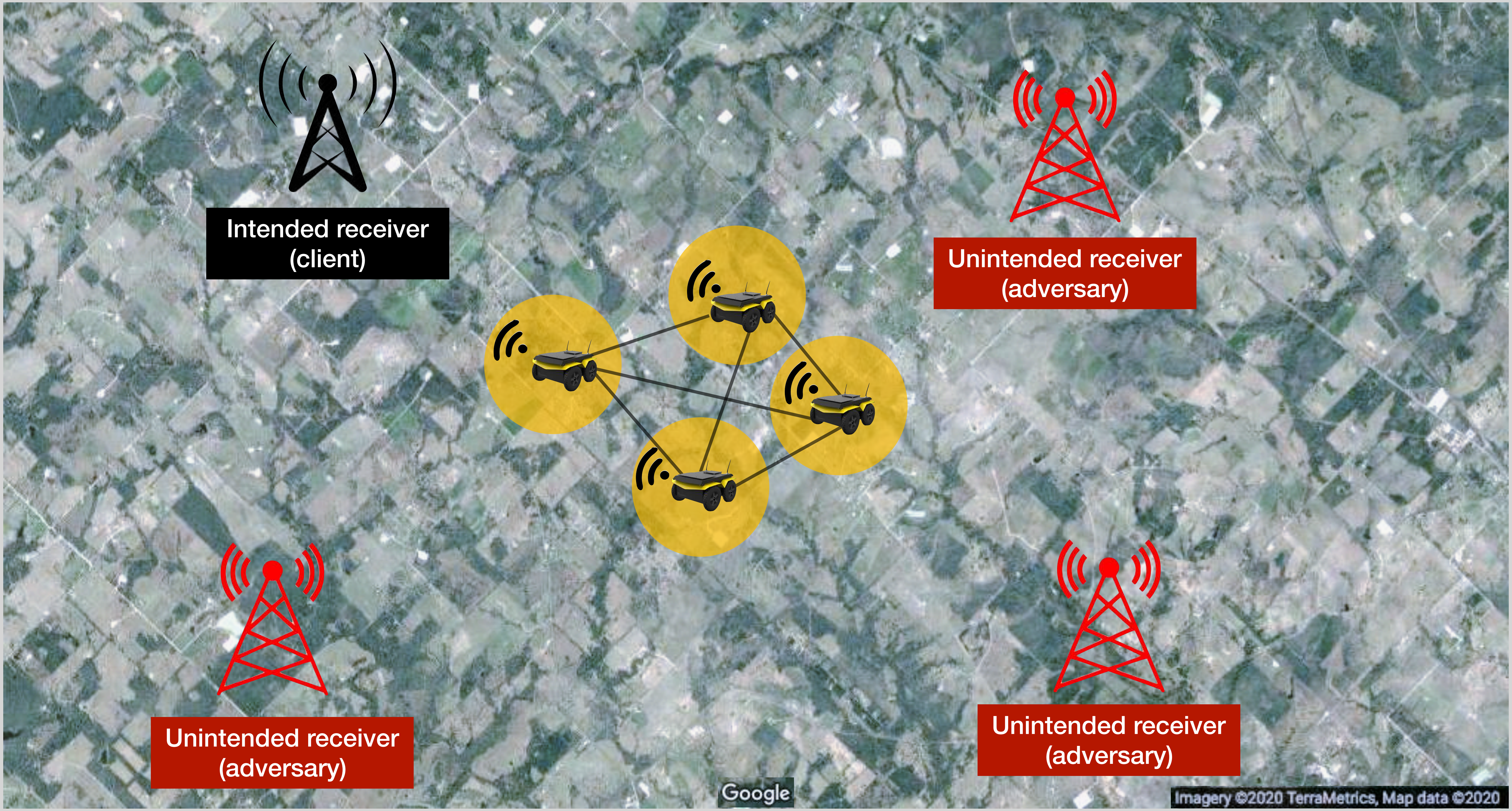
Yagiz Savas and Ufuk Topcu

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

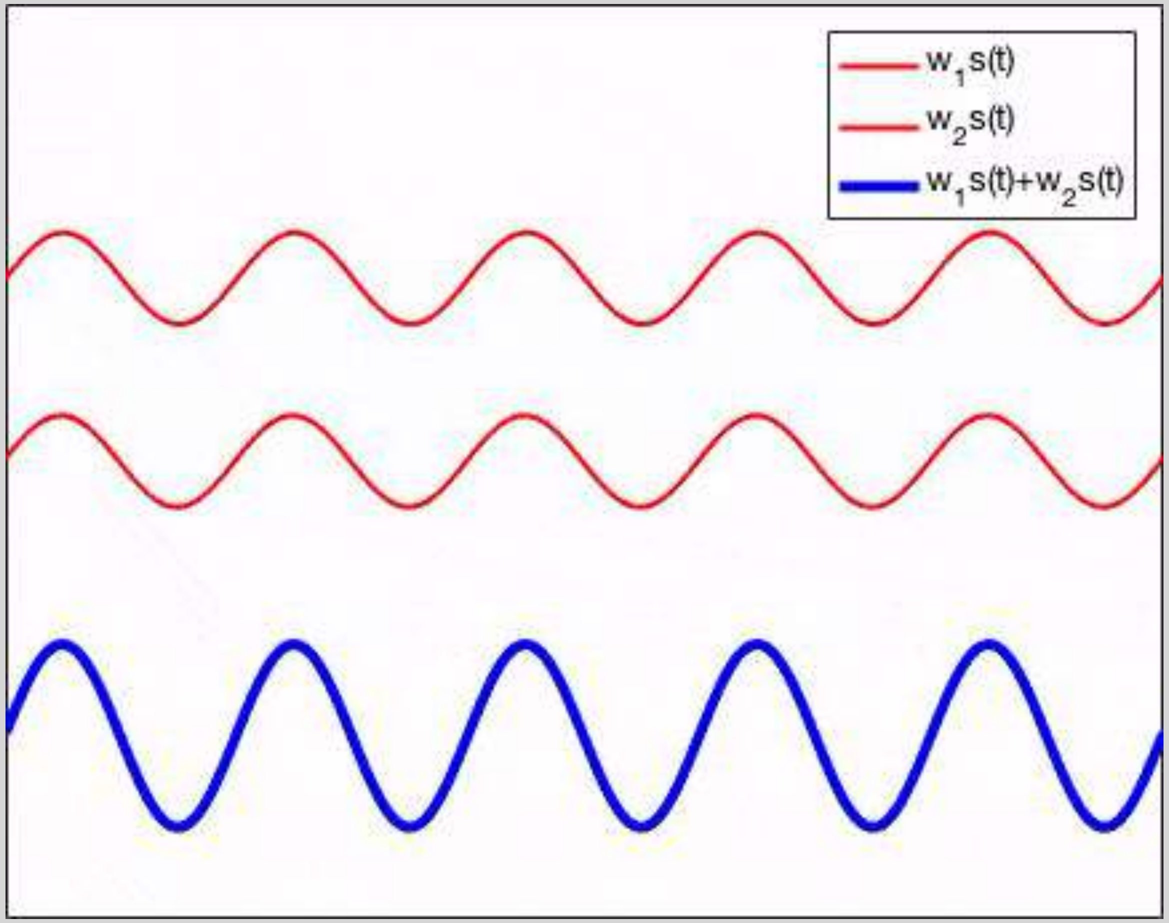


A group of robots are deployed in an environment from which they collect confidential data. Each robot carries a single antenna. The robots aim to securely communicate the data with the client in the presence of adversaries whose locations are unknown to the robots.

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

Beamforming as a Wireless Communication Technique: Main Idea

- A message signal $s(t)$ has a phase and an amplitude.
- Each robot multiplies the signal $s(t)$ with a complex number $w_i \in \mathbb{C}$ and adjusts the phase and the amplitude of the transmitted signal.
- Superposition of the transmitted signals result in a constructive (or destructive) interference.



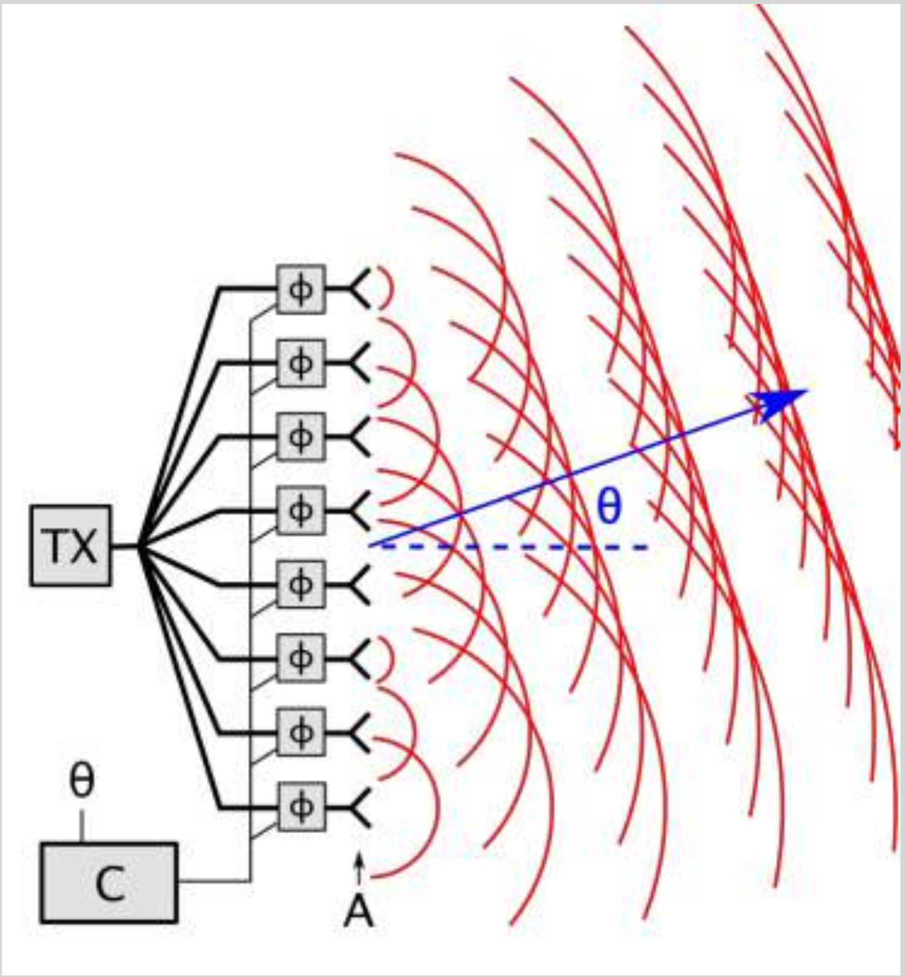
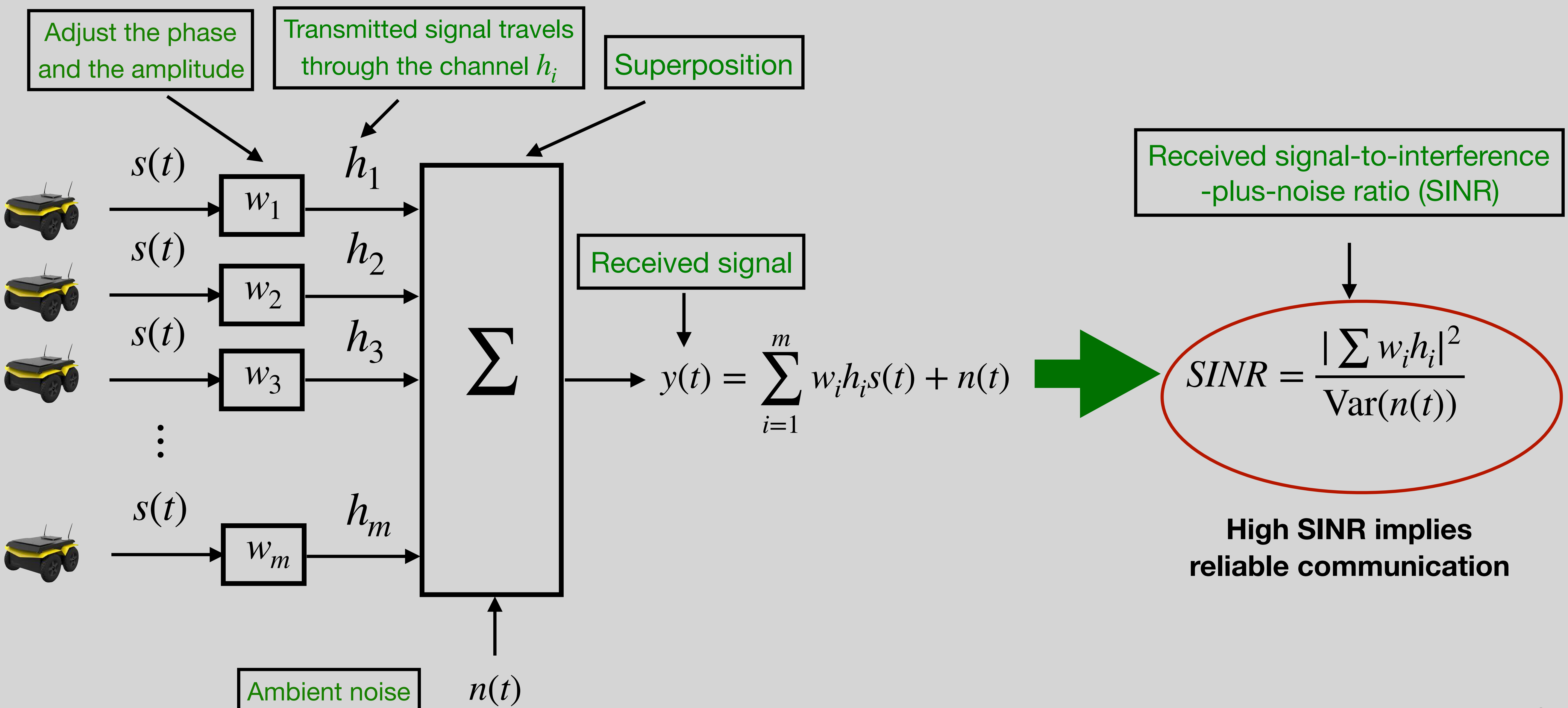


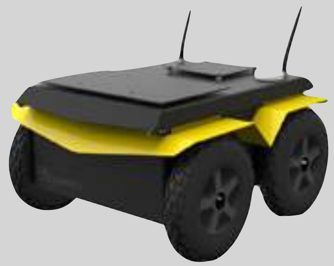
Illustration: https://en.wikipedia.org/wiki/Phased_array

Beamforming as a Wireless Communication Technique: Main Idea

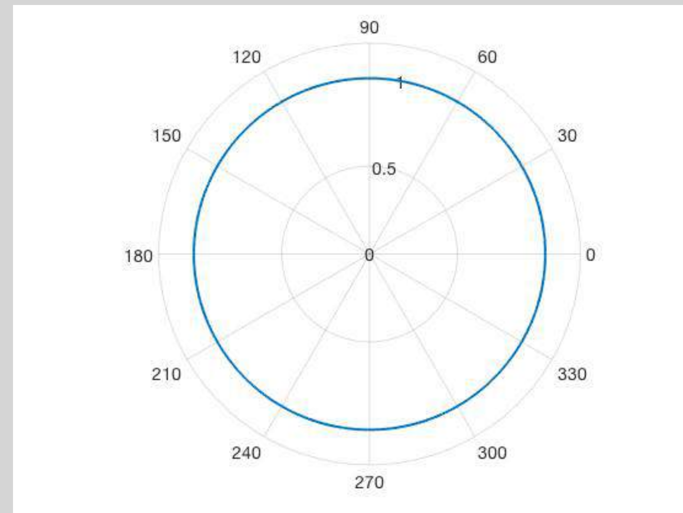
- A message signal $s(t)$ has a phase and an amplitude.
- Each robot multiplies the signal $s(t)$ with a complex number $w_i \in \mathbb{C}$ and adjusts the phase and the amplitude of the transmitted signal.
- Superposition of the transmitted signals result in a constructive (or destructive) interference.



Beamforming as a Wireless Communication Technique: Benefits

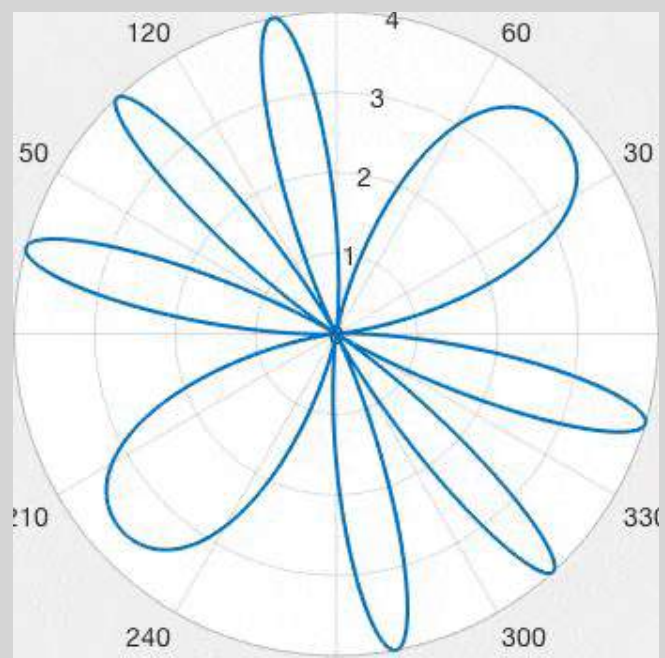


Single robot equipped with an isotropic antenna



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

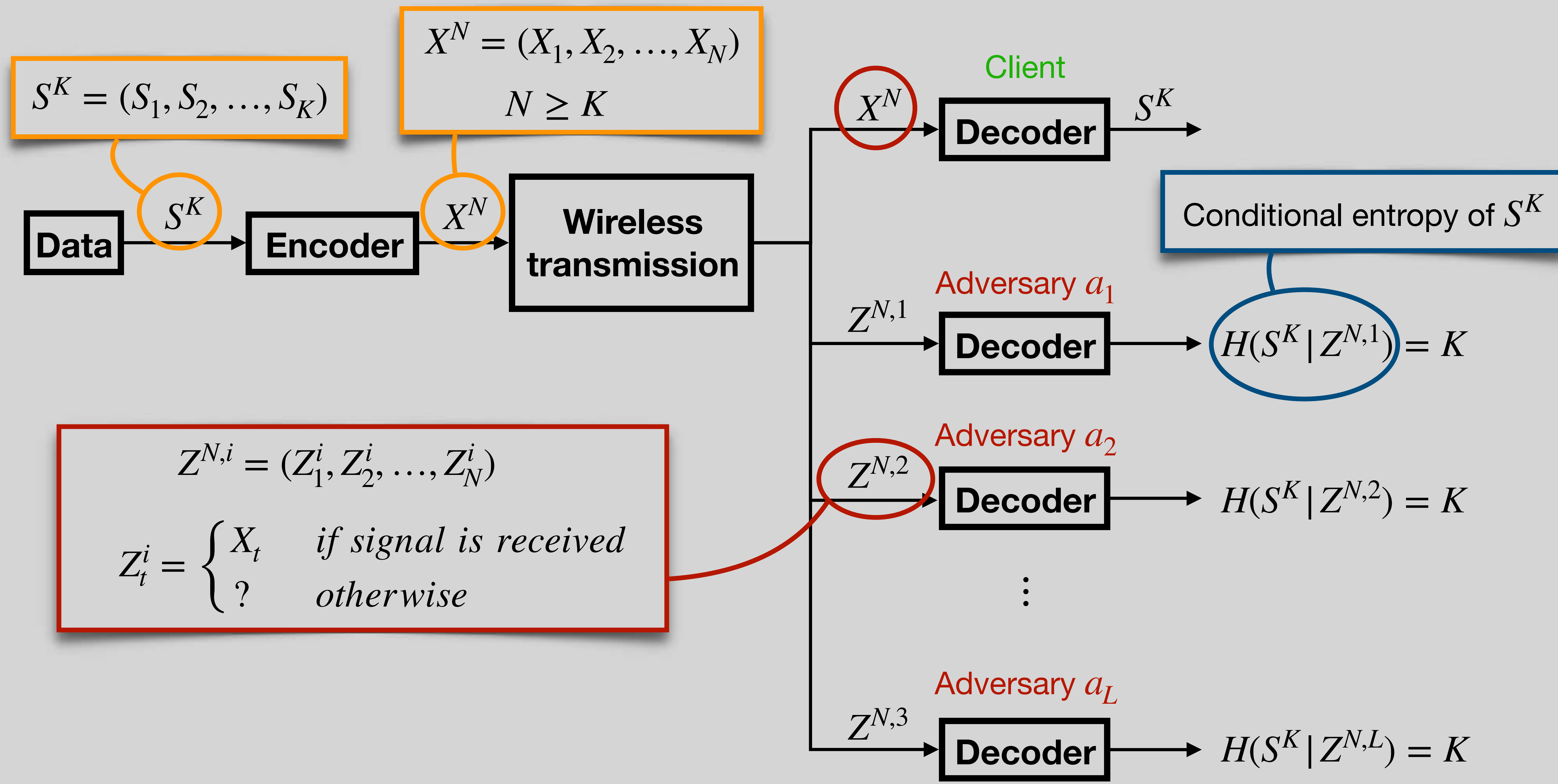
Two robots each equipped with an isotropic antenna



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

Distributed beamforming enables a group of robots to control the directionality of the transmission and to enhance the reliability of the communication link.

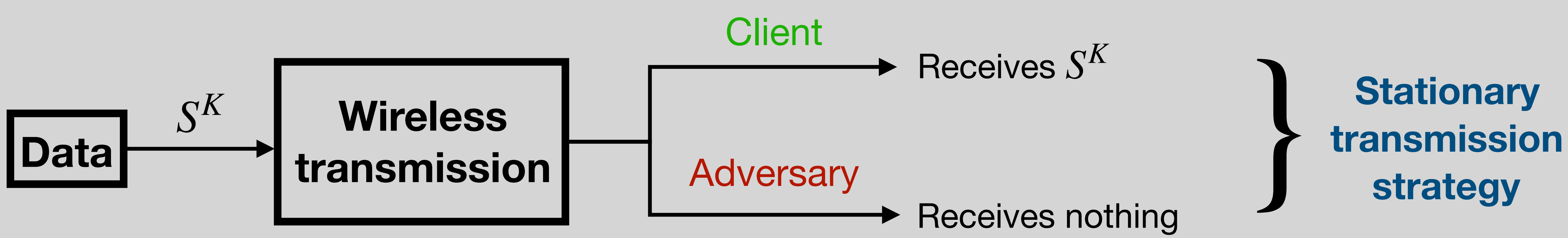
Secure Communication Problem: An Informal Problem Statement



Design a transmission strategy and an encoder-decoder pair such that the client recovers the data S^K and no adversary can decrease its uncertainty on S^K by eavesdropping on the transmission.

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

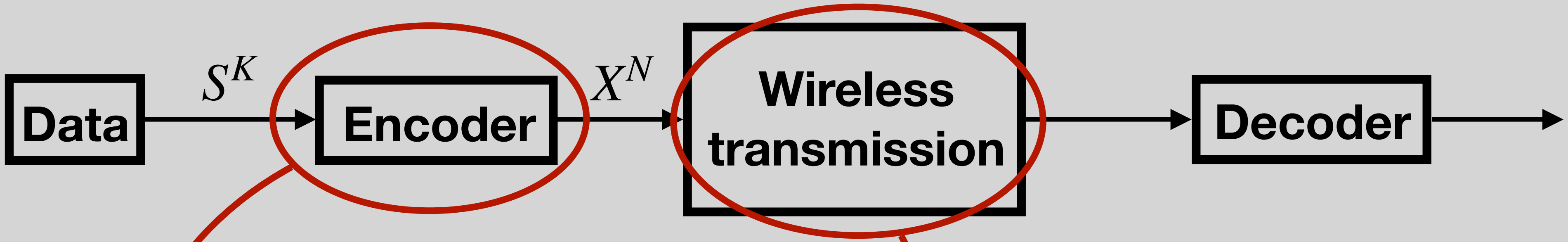
$$\mu_i \leq N - K \implies H(S^K | Z^{N,i}) = K$$

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



If there are $L \in \mathbb{N}$ adversaries in the environment, we choose $N = LK$.

Security requirement:

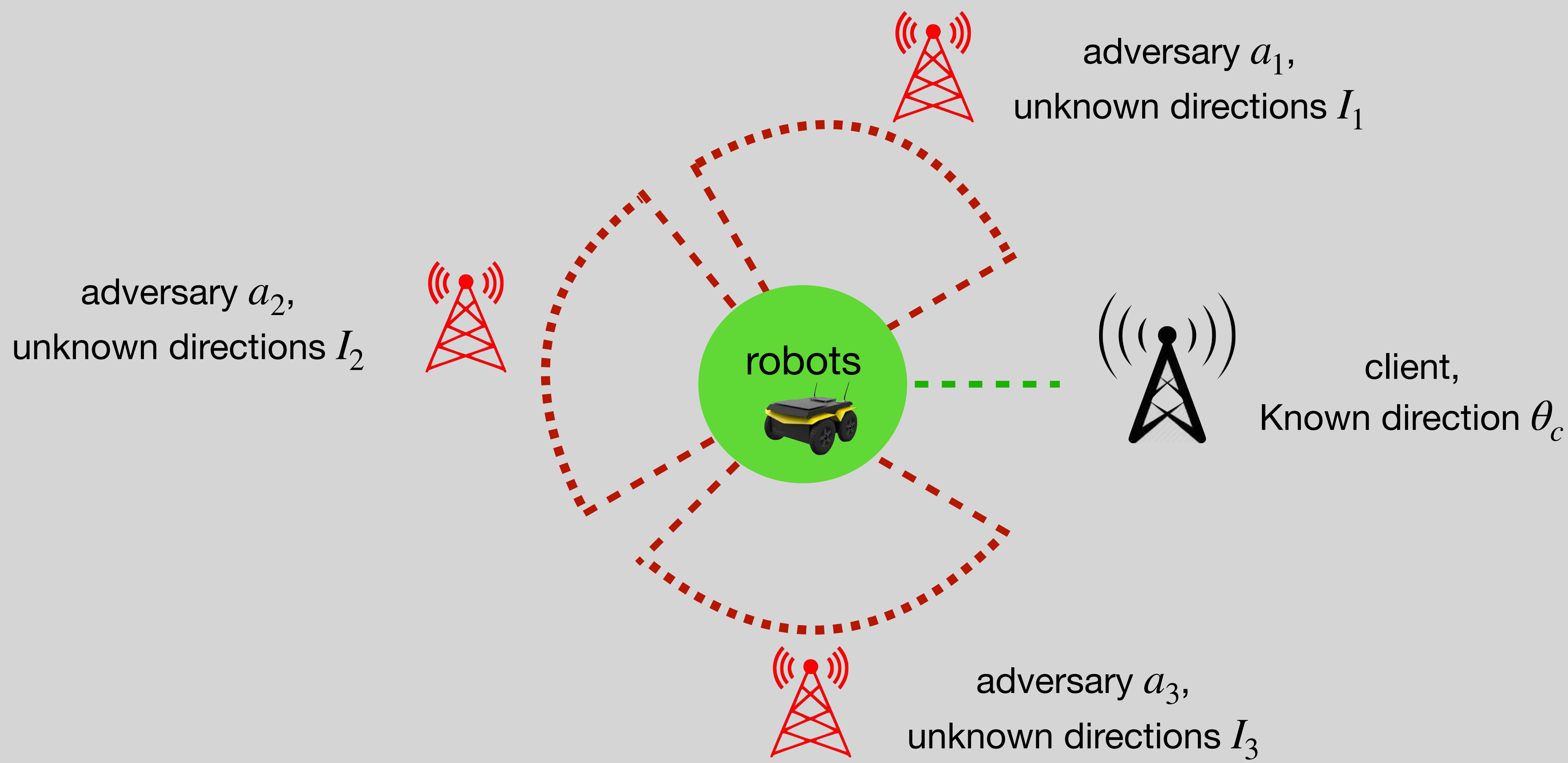
$\mu_i \leq N - K = K(L-1)$

We design a periodic transmission strategy which ensures that each adversary a_i receives at most $K(L-1)$ symbols although the exact locations of the adversaries are unknown to the agents

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

- A group of $m \in \mathbb{N}$ agents aim to communicate an information sequence $S^K = (S_1, S_2, \ldots, S_K)$ with a client located in the far-field direction $\theta_c \in [-\pi, \pi)$.
- Each agent carries an ideal isotropic antenna with maximum transmit power $P > 0$.
- The agents map S^K into an encoded sequence $X^N = (X_1, X_2, \ldots, X_N)$, where $N \geq K$, and transmit X^N.
- There are $L \in \mathbb{N}$ adversaries $\{a_i : i \in [L]\}$, located also in the far-field region, that eavesdrop on the transmission.
- Exact directions of the adversaries are unknown to the agents; however, for each $i \in [L]$, there exists a continuous direction interval $I_i \subseteq [-\pi, \pi)$ that represents all possible directions for a_i.



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

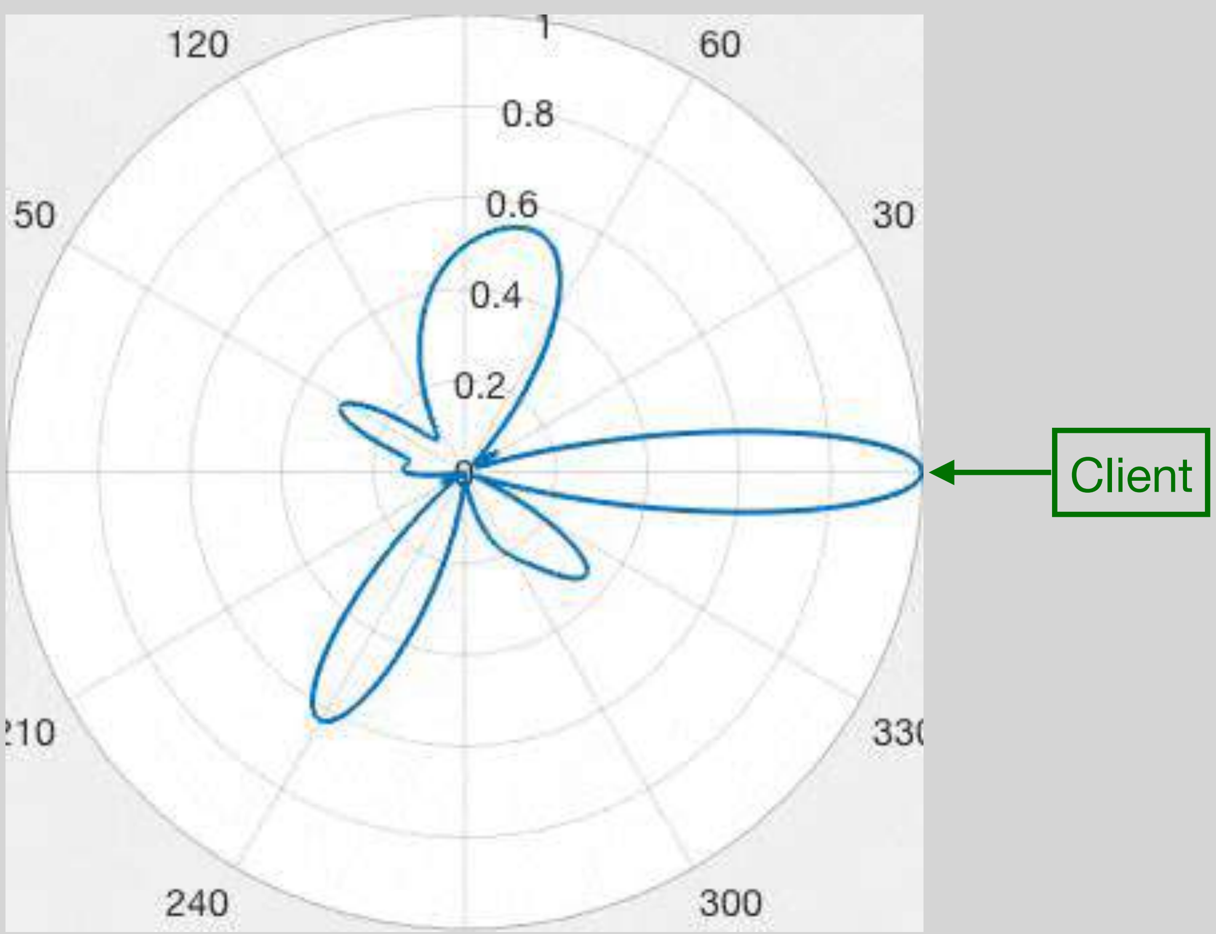
- At time $t \in [N]$, the agents transmit the encoded symbol X_t as a continuous signal s_t.
- The vector of signals transmitted by the agents is

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

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

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

What is the effect of artificial noise? [1]



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

[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 $\mathbf{v}_t \sim \mathcal{CN}(0, \Sigma_t)$

- Since the maximum transit 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

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

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

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

σ_t^2 is the 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: Let $N = LK$, i.e., information rate is $R = 1/L$. Such an encoding can be achieved by using $[N, N-K]$ linear maximum-distance-separable codes.

STEP 2: Synthesize a periodic transmission strategy

$$((\mathbf{w}_1, \Sigma_1), (\mathbf{w}_2, \Sigma_2), \ldots, (\mathbf{w}_L, \Sigma_L), (\mathbf{w}_1, \Sigma_1), (\mathbf{w}_2, \Sigma_2), \ldots, (\mathbf{w}_L, \Sigma_L), \ldots, (\mathbf{w}_1, \Sigma_1), (\mathbf{w}_2, \Sigma_2), \ldots, (\mathbf{w}_L, \Sigma_L))$$

First cycle — Second cycle — K-th cycle

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

$$s.t. \quad SINR_k(\theta_c) \geq \gamma_c$$ ← Client receives the transmitted symbol

$$\forall \theta \in I_k, \quad SINR_k(\theta) \leq \gamma_a$$ ← Adversary a_k cannot receive the transmitted symbol

$$\forall i \in [m], \quad \mathbf{w}_k(i) + \Sigma_k(i,i) \leq P$$ ← Power constraints are satisfied

Semi-Definite Program Relaxation and Probabilistic Approximation

$$\begin{aligned} \min_{\mathbf{w}_k \in \mathbb{C}^m, \Sigma_k \succcurlyeq 0} \quad & Tr(\Sigma_k) + \|\mathbf{w}_k\|_2^2 \\ s.t. \quad & SINR_k(\theta_c) \geq \gamma_c \\ \forall \theta \in I_k, \quad & SINR_k(\theta) \leq \gamma_a \\ \forall i \in [m], \quad & \mathbf{w}_k(i) + \Sigma_k(i,i) \leq P \end{aligned}$$

writing explicitly $\Longleftrightarrow$

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

$\Updownarrow$ We show that SDP relaxation is exact!

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

with probability $1 - \beta_1$ $\Longleftrightarrow$

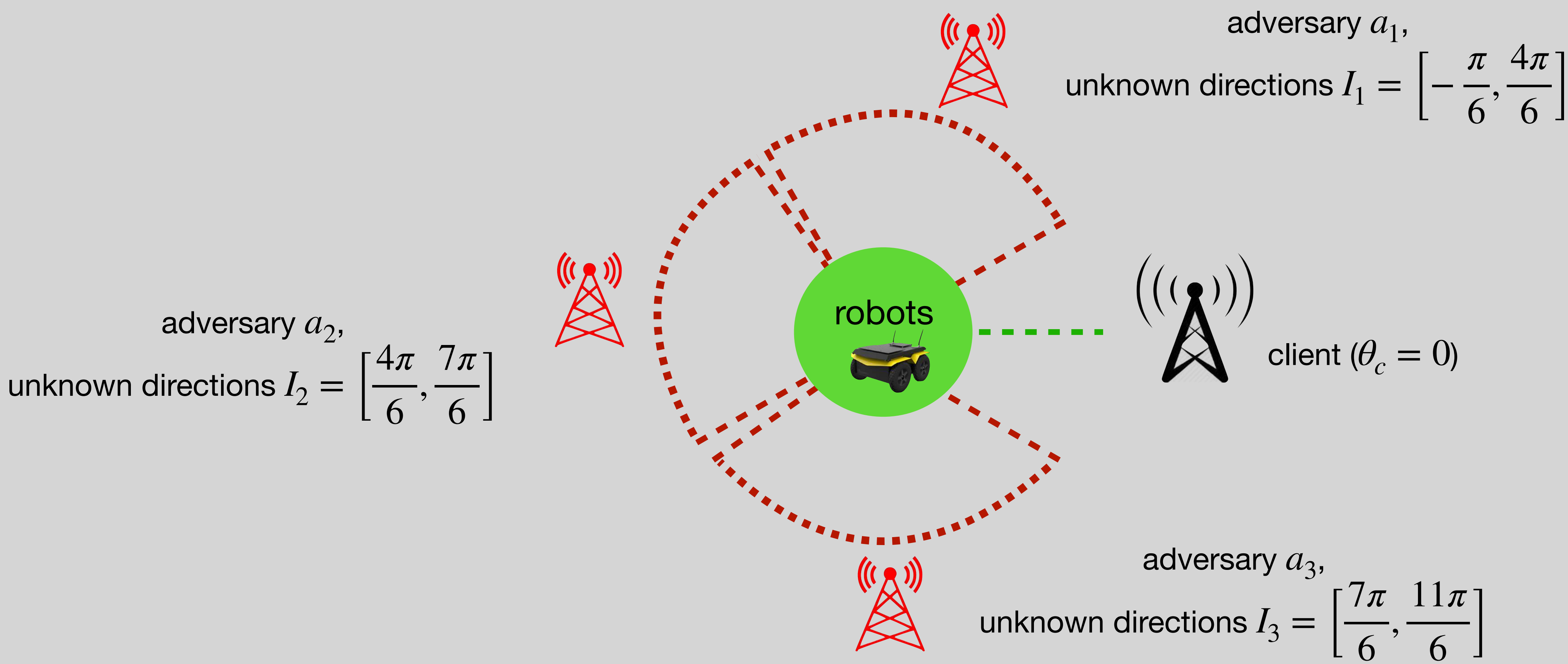
$$\begin{aligned} \min_{\mathbf{W}_k \succcurlyeq 0, \Sigma_k \succcurlyeq 0} \quad & Tr(\Sigma_k) + Tr(\mathbf{W}_k) \\ s.t. \quad & Tr(\mathbf{H}(\theta_c)\mathbf{W}_k) \geq \gamma_c \Big(Tr(\mathbf{H}(\theta_c)\Sigma_k) + \sigma_k^2 \Big) \\ \forall \theta \in \Theta_B, \quad & Tr(\mathbf{H}(\theta)\mathbf{W}_k)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

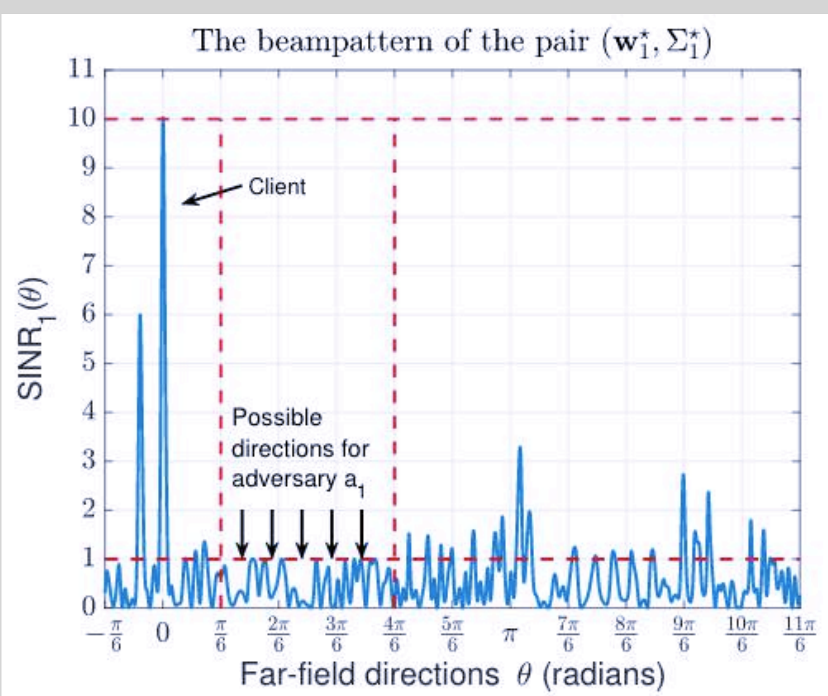
randomly sample $B \in \mathbb{N}$ points from the infinite set I_k

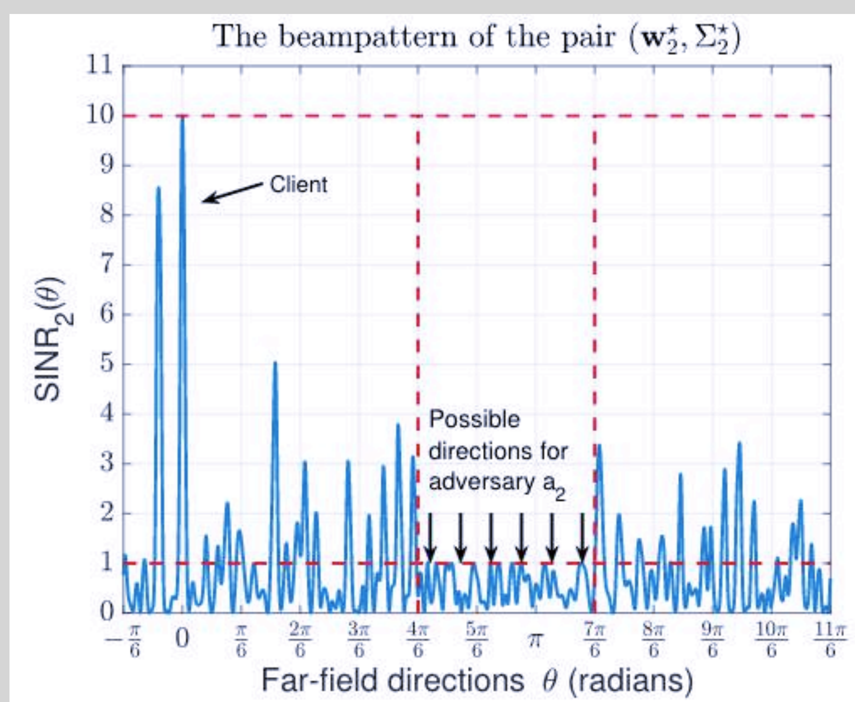
The following statement is true with probability $1 - \beta_2$:
If $B \geq (2 \log_e(\beta_2^{-1}) + 16m^2)/\beta_1$, the problems are equivalent with probability $1 - \beta_1$.[1]

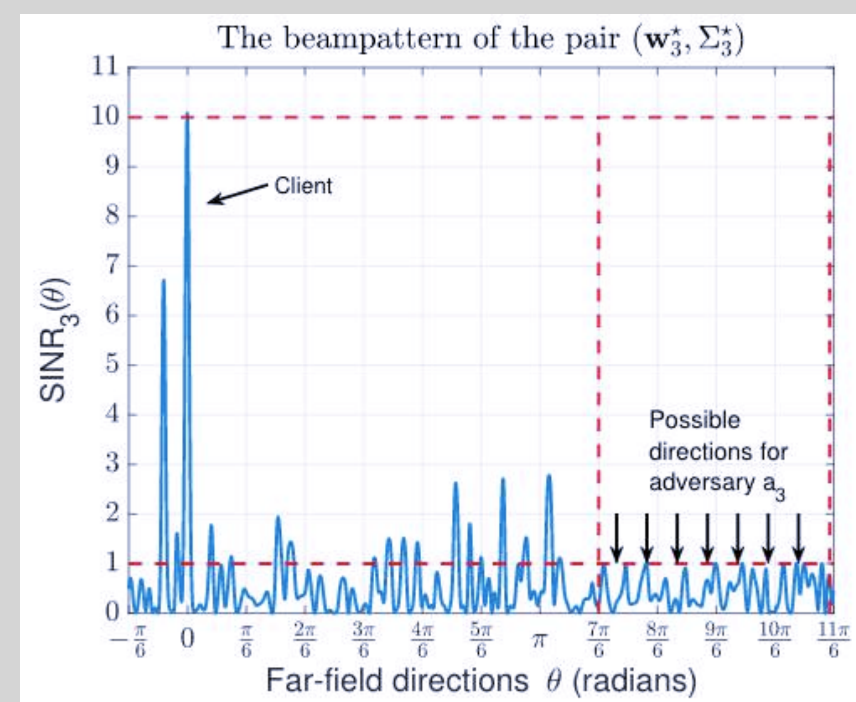
[1] Campi, M.C., Garatti, S., and Prandini, M., `` The scenario approach for systems and control design", Annual Reviews in Control, 2009

A Numerical Example



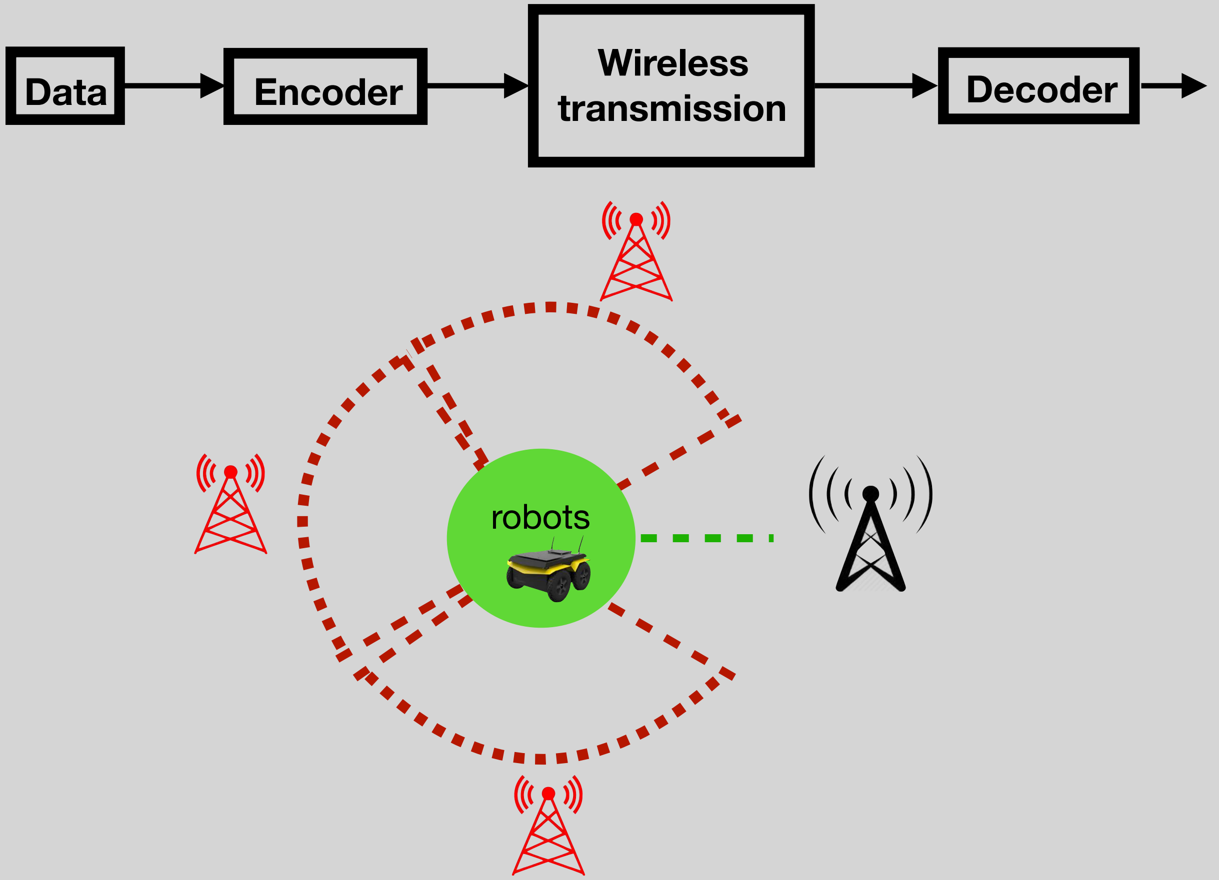




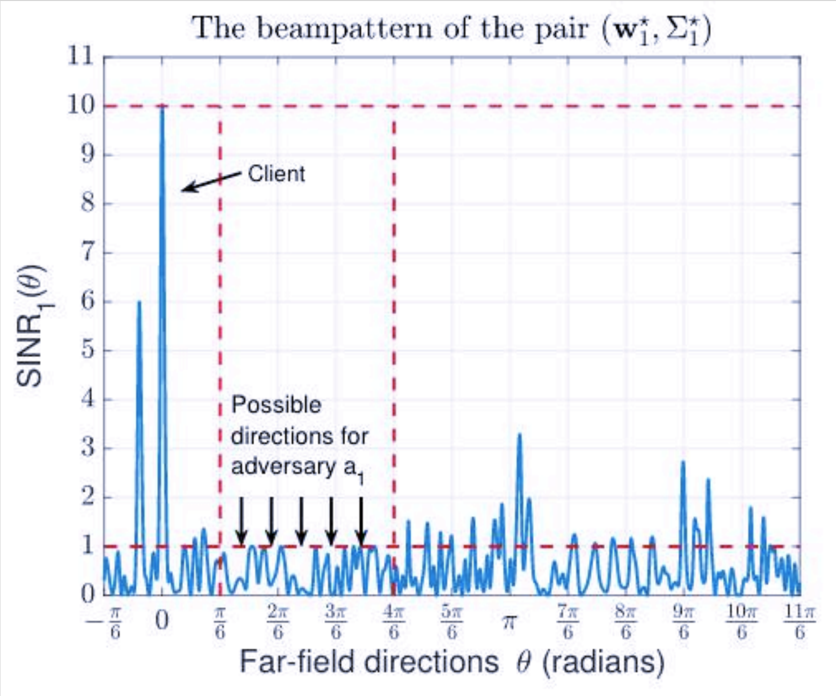


Conclusions and Future Work

- Distributed beamforming techniques improve the signal strength and the directionality of the signal.
- By approaching the wireless communications problem from a sequential-decision making perspective, we can improve the security of communication.
- We can synthesize a transmission strategy, based on a semi-definite program, that enables a robot group to securely communicate with a client in the presence of adversaries with unknown locations in the environment.



- What is the optimal strategy to group the adversaries that will minimize the redundancy in communication?
- How can we modify the proposed algorithms for scenarios in which the perfect channel state information is unavailable?



Thank you for listening

E-mail: yagiz.savas@utexas.edu

autonomous SYSTEMS GROUP

TEXAS
The University of Texas at Austin