# Physical-Layer Security via Distributed Beamforming in the Presence of Adversaries with Unknown Locations

Yagiz Savas, Abolfazl Hashemi, Abraham P. Vinod, Brian M. Sadler, Ufuk Topcu

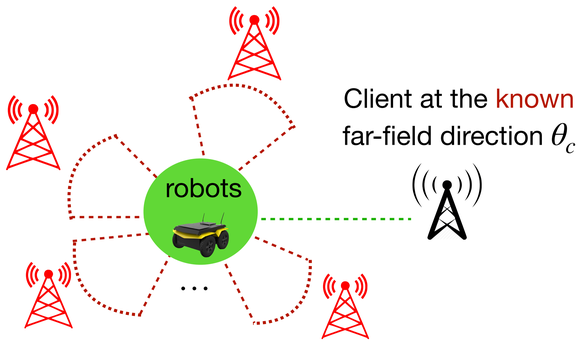
TEXAS The University of Texas at Austin

DEVCOM ARMY RESEARCH LABORATORY

aUTonomous SYSTEMS GROUP

## Motivation

How can a group of robots securely communicate with a client in the presence of multiple adversaries that eavesdrop on the transmission?




Adversary $a_i$ at the unknown far-field direction
Possible directions: $I_i \subseteq [-\pi, \pi)$

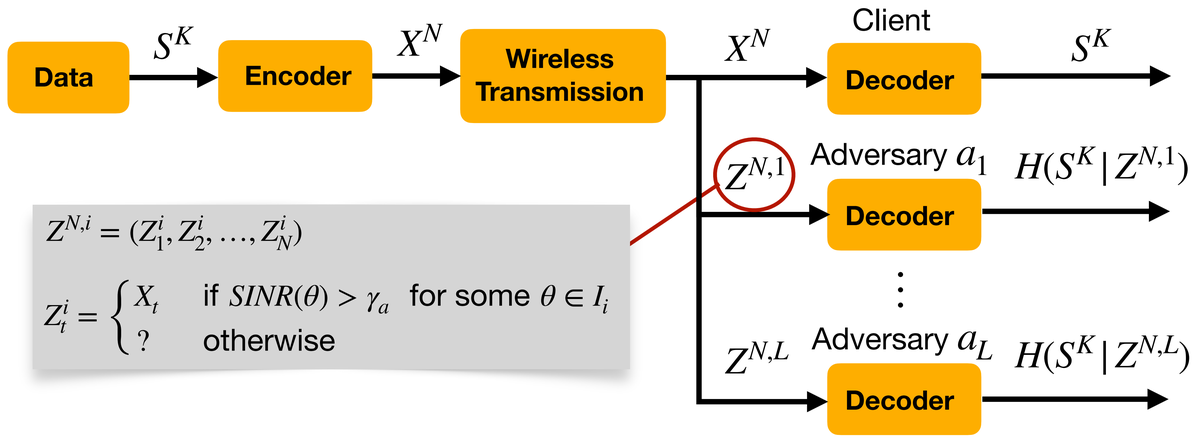
### Key challenges:

- Unknown adversary locations
- Limited individual transmission power

### Assumptions:

- Free space propagation
- $L$ adversaries in the environment
- Communication to far-field region
- Possible adversary directions are expressed by direction intervals

## Problem Statement




$$Z^{N,i} = (Z_1^i, Z_2^i, \ldots, Z_N^i)$$

$$Z_t^i = \begin{cases} X_t & \text{if } SINR(\theta) > \gamma_a \text{ for some } \theta \in I_i \\ ? & \text{otherwise} \end{cases}$$

**Design a transmission strategy such that the client receives the transmitted symbols while we have $H(S^K \mid Z^{N,i}) = K$ for all adversaries**

## Proposed Approach

- Design a periodic transmission strategy such that the client receives all transmitted symbols while each adversary receives at most $K$ symbols
- Linear MDS codes ensure security, i.e., $H(S^K \mid Z^{N,i}) = K$ [Ozarow '84]

Transmit each symbol $X_k$ using the pair $(\mathbf{w}_k, \mathbf{\Sigma}_k)$:

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

$$\text{subject to:} \quad SINR_k(\theta_c) \geq \gamma_c$$

$$\forall \theta \in I_{k \mod L}, \quad SINR_k(\theta) \leq \gamma_a$$

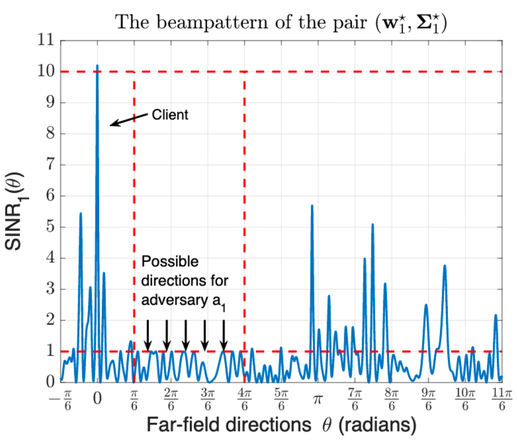
$$\forall i \in [m], \quad \mathbf{w}_k(i) + \mathbf{\Sigma}_k(i,i) \leq P$$

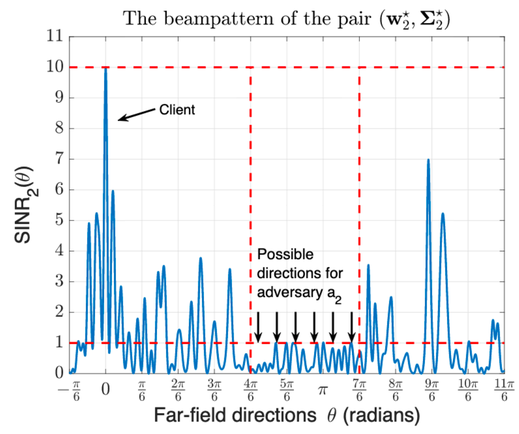
**Semi-infinite non-convex** program!

We present a **finite convex** program whose solution coincides with this program **with probabilistic guarantees**

## Main Contribution

**We ensure security in scenarios in which all existing strategies fail**




**Acknowledgement:**
This work is supported by the grant ARL DCIST CRA W911NF-17-2-0181.