Distributed Beamforming in Adversarial Environments

Yagiz Savas and Ufuk Topcu

in collaboration with Abolfazl Hashemi, Abraham P. Vinod, Brian M. Sadler
Wireless Communications in the Presence of Adversaries

- Intended receiver (client)
- Unintended receiver (adversary)
- Robots with isotropic antennas
- Unintended receiver (adversary)

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**

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](https://en.wikipedia.org/wiki/Phased_array)
Beamforming as a Wireless Communication Technique: Main Idea

Adjust the phase and the amplitude

- Transmitted signal travels through the channel $h_i$

Superposition

Received signal

$y(t) = \sum_{i=1}^{m} w_i h_i s(t) + n(t)$

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

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

High SINR implies reliable communication
Beamforming as a Wireless Communication Technique: **Benefits**

- No directionality
- Low SINR

**Single robot equipped with an isotropic antenna**

**Two robots each equipped with an isotropic antenna**

- Improved directionality
- Improved SINR
Secure Communication Problem: An Informal Problem Statement

Data

Encoder

$S^K = (S_1, S_2, \ldots, S_K)$

$X^N = (X_1, X_2, \ldots, X_N)$

$N \geq K$

Wireless transmission

Decoder

Client

Conditional entropy of $S^K$

$S^K \rightarrow$ Decoder

$X^N \rightarrow$ Decoder

$Z_{N,1}^i = (Z_1^i, Z_2^i, \ldots, Z_N^i)$

$Z_t^i = \begin{cases} X_t & \text{if signal is received} \\ ? & \text{otherwise} \end{cases}$

Adversary $a_1$

$H(S^K | Z_{N,1}^i) = K$

Adversary $a_2$

$H(S^K | Z_{N,2}^i) = K$

$\vdots$

Adversary $a_L$

$H(S^K | Z_{N,L}^i) = K$
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 \[^3\]

\[ S^K \rightarrow \text{Wireless transmission} \]

\[ \text{Client} \rightarrow \text{Receives } S^K \]

\[ \text{Adversary} \rightarrow \text{Receives nothing} \]

\}\text{Stationary transmission strategy}

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

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

**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
\[^3\] 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 $N = K \cdot L$ 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

Encoded sequence $X^N$ from robots to the client at the known far-field direction $\theta_c$. 
Environment Model

Adversary $a_1$ at the unknown far-field direction
Possible directions: $I_1 \subseteq [-\pi, \pi)$

Adversary $a_2$ at the unknown far-field direction
Possible directions: $I_2 \subseteq [-\pi, \pi)$

Adversary $a_3$ at the unknown far-field direction
Possible directions: $I_3 \subseteq [-\pi, \pi)$

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

Encoded sequence $X^N$

Client at the known far-field direction $\theta_c$
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

\[
y_{transmit}[t] = w_t s_t + v_t
\]

Beamforming vector $w_t = [w_1, w_2, \ldots, w_m]'$

Artificial noise $v_t \sim \mathcal{CN}(0, \Sigma_t)$
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

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

 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 simultaneously

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

$$y_{transmit}[t] = w_t s_t + v_t$$

**Beamforming vector** $w_t = [w_1, w_2, \ldots, w_m]'$

**Artificial noise** $v_t \sim \mathcal{CN}(0, \Sigma_t)$

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 $\theta$ is

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

Channel matrix $H(\theta) = h(\theta)h(\theta)^H$

$Tr(M)$ 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 \( ((w_1, \Sigma_1), (w_2, \Sigma_2), \ldots, (w_N, \Sigma_N)) \) of pairs \( (w_t, \Sigma_t) \) such that

1. The client receives all transmitted symbols \( X_t \)
2. 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

\[
((w_1, \Sigma_1), (w_2, \Sigma_2), \ldots, (w_L, \Sigma_L), (w_1, \Sigma_1), (w_2, \Sigma_2), \ldots, (w_L, \Sigma_L), \ldots, (w_1, \Sigma_1), (w_2, \Sigma_2), \ldots, (w_L, \Sigma_L))
\]

First cycle    Second cycle    K-th cycle

\[
\min_{w_k \in \mathbb{C}^m, \Sigma_k \geq 0} \quad Tr(\Sigma_k) + \|w_k\|_2^2 
\]

Minimize total transmit power

subject to:

\[
SINR_k(\theta_c) \geq \gamma_c 
\]

Client’s SINR constraint

\[
\forall \theta \in I_k, \quad SINR_k(\theta) \leq \gamma_a 
\]

Adversary \( a_k \)’s SINR constraint

\[
\forall i \in [m], \quad w_k(i) + \Sigma_k(i, i) \leq P 
\]

Agents’ power constraints
Semi-Definite Program Relaxation and Probabilistic Approximation

Semi-infinite nonconvex optimization problem

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

Source of infiniteness

Source of nonconvexity
Semi-infinite convex optimization problem

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

Result: The convex relaxation is exact
Semi-Definite Program Relaxation and Probabilistic Approximation

Semi-infinite convex optimization problem

\[
\begin{align*}
\min_{W_k \geq 0, \Sigma_k \geq 0} & \quad Tr(\Sigma_k) + Tr(W_k) \\
\text{s.t.} & \quad Tr(H(\theta_c)W_k) \geq \gamma_c \left( Tr(H(\theta_c)\Sigma_k) + \sigma_k^2 \right) \\
\forall \theta \in I_k, & \quad Tr(H(\theta)W_k) \leq \gamma_a \left( Tr(H(\theta)\Sigma_k) + \sigma_k^2 \right) \\
\forall i \in [m], & \quad W_k(i, i) + \Sigma_k(i, i) \leq P
\end{align*}
\]

Source of infiniteness
Semi-Definite Program Relaxation and Probabilistic Approximation

Finite convex optimization problem

\[
\begin{align*}
\min_{W_k \geq 0, \Sigma_k \geq 0} & \quad Tr(\Sigma_k) + Tr(W_k) \\
\text{s.t.} & \quad Tr(H(\theta_c)W_k) \geq \gamma_c \left( Tr(H(\theta_c)\Sigma_k) + \sigma_k^2 \right) \\
& \quad \forall \theta \in \Theta, \quad Tr(H(\theta)W_k) \leq \gamma_a \left( Tr(H(\theta)\Sigma_k) + \sigma_k^2 \right) \\
& \quad \forall i \in [m], \quad W_k(i, i) + \Sigma_k(i, i) \leq P
\end{align*}
\]

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

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 \( 1 - \beta_1 \).

A Numerical Example

adversary $a_1$, unknown directions $I_1 = \left[ -\frac{\pi}{6}, \frac{4\pi}{6} \right]$

adversary $a_2$, unknown directions $I_2 = \left[ \frac{4\pi}{6}, \frac{7\pi}{6} \right]$

adversary $a_3$, unknown directions $I_3 = \left[ \frac{7\pi}{6}, \frac{11\pi}{6} \right]$

client ($\theta_c = 0$)
A Numerical Example

First time step:

Second time step:

Third time step:
Conclusions

- Distributed beamforming
- Physical-layer security
- Semi-definite programming

Diagram:
- Data → Encoder → Wireless transmission → Decoder

Graph and chart:
- The beam pattern of the pair \( (w_i, \Sigma_i) \)
- Possible directions for adversary \( a_i \)
- SNR \( (\theta) \)
- Far-field directions \( \theta \) (radians)
Thank you for listening

E-mail: yagiz.savas@utexas.edu