Enhancing Wireless Security with Physical Layer Network Cooperation

Amitav Mukherjee, Ali Fakoorian, A. Lee Swindlehurst
University of California Irvine

The “Physical” Layer
Outline

• Background

• Game Theory for Dual-Mode Adversaries
  ➢ Adversary can act as either link eavesdropper or jammer
  ➢ Transmitter can allocate power to jamming as well
  ➢ Derived conditions for Nash equilibria in resulting two-player game
  ➢ Examples

• Transmitter Cooperation for Secrecy in Interference Channels
  ➢ Maintain secrecy of co-channel links
  ➢ Cooperation through CSI sharing and “artificial noise alignment”
  ➢ Examples

• Impact of Malicious Feedback in the Physical Layer
  ➢ Fair downlink resource allocation schemes susceptible to malicious users
  ➢ Fraudulent feedback from a single user can cause significant degradation
  ➢ Example

• Future directions
Background – The MIMO Wiretap Channel

Two possible scenarios:

1. **CSI for Eve is known**: Generalized Singular Value Decomposition (GSVD)

   \[
   H_{ba} T = \Phi_b \Sigma_b \\
   H_{ea} T = \Phi_e \Sigma_e
   \]

   \(x_a\) transmitted along columns of \(T\) for which \(\Sigma_{b,ii} > \Sigma_{e,ii}\)

2. **CSI for Eve is unknown**: Artificial noise (jamming)

   \[
   x_a = T s_a + T' z_a
   \]

   transmit power allocated to jamming \(z_a\) in addition to information signal \(s_a\)
Suppose Eve can either eavesdrop or jam.

Which should she do to minimize the secrecy rate? What should Alice do in response, transmit artificial interference of her own or not?

Is there an equilibrium strategy for Alice and Eve?
Dual-Mode Adversary – Strategic Game Theory Formulation

- Two-player matrix, use secrecy rate as utility function
- Zero-sum formulation, where Eve’s payoff is negative of Alice’s
- CSI assumptions: Alice knows $H_{ba}$, Eve knows $H_{ea}$, all other channels assumed to be zero-mean i.i.d. Gaussian
**Strategic Game Theory Formulation (cont.)**

<table>
<thead>
<tr>
<th></th>
<th>EVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eavesdrop</td>
<td>Full power</td>
</tr>
<tr>
<td>Jam</td>
<td>Artificial noise</td>
</tr>
</tbody>
</table>

**ALICE**

- Clearly, we have:
  - \( R_{FJ} \geq R_{AJ} \) (Eve cannot simultaneously jam and eavesdrop)
  - \( R_{AE} \geq R_{FE} \) (artificial noise helps w/ eavesdroppers)

- \((A,E)\) is Nash equilibrium if \( R_{AJ} \geq R_{AE} \)
Strategic Game Theory Formulation (cont.)

**ALICE**

<table>
<thead>
<tr>
<th></th>
<th>Eavesdrop</th>
<th>Jam</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full power</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Artificial noise</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**EVE**

<table>
<thead>
<tr>
<th></th>
<th>Eavesdrop</th>
<th>Jam</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full power</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Artificial noise</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Clearly, we have $R_{FJ} \geq R_{AJ}$ (Eve cannot simultaneously jam and eavesdrop)
- $R_{AE} \geq R_{FE}$ (artificial noise helps with eavesdroppers)

- $(A,E)$ is Nash equilibrium if $R_{AJ} \geq R_{AE}$
- $(F,J)$ is Nash equilibrium if $R_{FE} \geq R_{FJ}$
Strategic Game Theory Formulation (cont.)

Clearly, we have

\[ R_{FJ} \geq R_{AJ} \]  (Eve cannot simultaneously jam and eavesdrop)

\[ R_{AE} \geq R_{FE} \]  (artificial noise helps with eavesdroppers)

\( (A,E) \) is Nash equilibrium if \( R_{AJ} \geq R_{AE} \)

\( (F,J) \) is Nash equilibrium if \( R_{FE} \geq R_{FJ} \)

We have derived the conditions under which these equilibria occur.
Example – Nash Equilibrium for Dual-Mode Adversary

Eve closer to Alice than Bob in this scenario, equal background noise power, thus equilibrium for $R_{FE} \geq R_{FJ}$ never occurs.

Theoretical prediction accurately matches conditions for equilibrium when $R_{AJ} \geq R_{AE}$.
Extensive Game Theory Formulation

In the **strategic** formulation of the game, both players move simultaneously. In the **extensive** formulation, one player moves first and the other then responds. For example, in a two-step game, we have two possible decision trees:

Solution found by working upwards, the player at a given level choosing the best strategy for each subtree on that level. For example:
Extensive Game Theory Formulation

In the *strategic* formulation of the game, both players move simultaneously. In the *extensive* formulation, one player moves first and the other then responds. For example, in a two-step game, we have two possible decision trees:

Solution found by working upwards, the player at a given level choosing the best strategy for each subtree on that level. For example:
Extensive Game Theory Formulation

In the **strategic** formulation of the game, both players move simultaneously. In the **extensive** formulation, one player moves first and the other then responds. For example, in a two-step game, we have two possible decision trees:

![Decision Trees](image_url)

Solution found by working upwards, the player at a given level choosing the best strategy for each subtree on that level. For example:
Example – Nash Equilibrium and Extensive Game Results

As before, theory accurately predicts situation for Nash equilibrium.

In equilibrium region, extensive game results in equilibrium solution.

Outside equilibrium region, advantage of moving second is evident.

\[ N_a = N_b = N_e = 4 \quad P_a = 100 \]
Outline

• Background

• Game Theory for Dual-Mode Adversaries
  ➢ Adversary can act as either link eavesdropper or jammer
  ➢ Transmitter can allocate power to jamming as well
  ➢ Derived conditions for Nash equilibria in resulting two-player game
  ➢ Examples

• Transmitter Cooperation for Secrecy in Interference Channels
  ➢ Maintain secrecy of co-channel links
  ➢ Cooperation through CSI sharing and “artificial noise alignment”
  ➢ Examples

• Malicious Feedback in the MIMO Downlink
  ➢ Fair downlink resource allocation schemes susceptible to malicious users
  ➢ Fraudulent feedback from a single user can cause significant degradation
  ➢ Examples

• Future directions
Secrecy in Interference Channels

- two co-channel wireless links
- receiver for link 1 is a potential eavesdropper for link 2, and vice versa
- can be thought of as two wiretap channels in parallel
- we examine both cooperative and non-cooperative transmission strategies for secrecy in the general MIMO case
- “cooperation” here includes (1) the sharing of CSI between transmitters, (2) the design of beamformers for artificial noise alignment, and (3) bargaining between transmitters to determine noise levels
Non-Cooperative Jamming (NCJ)

• in this non-cooperative approach, transmitters only know the direct channel to their desired receiver, either $H_1$ or $H_2$

• only option in this case is for both transmitters to employ artificial noise

• secrecy rate region found by calculating rate points for all possible transmit power allocations (including fraction of power devoted to noise)
GSVD-Based Beamforming

- both direct and cross channels assumed to be known; transmitter 1 knows $(H_1, G_1)$, transmitter 2 knows $(H_2, G_2)$. Each implements GSVD approach independent of the other

- also non-cooperative, since algorithm cannot account for interference of transmitter 1’s signal with transmitter 2’s signal at receiver 2, and vice versa

- secrecy rate region found by calculating rate points for all possible transmit power allocations (no jamming in this case)
Cooperative Interference Alignment

Idea: Calculate GSVD beamformers, then allocate power to artificial noise that will be (approximately) aligned with information signal from other transmitter. Transmitters must share information signal subspaces.
GSVD + Artificial Noise Alignment (ANA) Algorithm

Algorithm for Transmitter 1

(1) Calculate GSVD for generalized singular values > 1

\[ H_1 T = \Phi_h \Sigma_h \]
\[ G_1 T = \Phi_g \Sigma_g \]

(2) Find beamformers for artificial noise that is approximately aligned with transmitter 2’s information signal and orthogonal to transmitter 1’s signal:

\[ T' = \arg \min_{T'} \text{Tr} \left( T'^H H_1^H (I - \Phi_g \Phi_g^H + \Phi_h \Phi_h^H) H_1 T' \right) \]

(3) Transmitters now “negotiate” to determine how much power each will devote to artificial interference. Here we use a game-theoretic bargaining approach.

\[ x_1 = T s_1 + T' z_1 \]
\[ E \left( s_1^H T^H T s_1 \right) = (1 - \alpha_1) P_1 \]
\[ E \left( z_1^H T'^H T' z_1 \right) = \alpha_1 P_1 \]
Two-User Bargaining Games – Graphical Interpretation

Convex hull of rate points obtained for all possible \((\alpha_1, \alpha_2)\) yields the set of achievable secrecy rates. Goal is to find an acceptable operating point on the “Pareto” frontier.

Operating point should be an acceptable trade-off between overall performance (sum sec. rate) and fairness (min sec. rate).

K-S solution provides each user the same fraction of their max secrecy rate.
Example – Secrecy Rates for Interference Channel

Link 1 is slightly handicapped, with one fewer transmit antennas.

Cooperation provides significant gains in secrecy rate, especially for link 1.

![Graph](image-url)

Parameters:
- $n_1=2$, $m_1=n_2=m_2=3$, $p_1=p_2=20$, $\sigma_d^2=\sigma_c^2=1$

- NCJ
- GSVD
- GSVD+ANA

K-S Point: $(R_{1K-S}, R_{2K-S})=(2.61, 2.55)$
Outline

• Background

• Game Theory for Dual-Mode Adversaries
  ➢ Adversary can act as either link eavesdropper or jammer
  ➢ Transmitter can allocate power to jamming as well
  ➢ Derived conditions for Nash equilibria in resulting two-player game
  ➢ Examples

• Transmitter Cooperation for Secrecy in Interference Channels
  ➢ Maintain secrecy of co-channel links
  ➢ Cooperation through CSI sharing and “artificial noise alignment”
  ➢ Examples

• Malicious Feedback in the MIMO Downlink
  ➢ Fair downlink resource allocation schemes susceptible to malicious users
  ➢ Fraudulent feedback from a single user can cause significant degradation
  ➢ Examples

• Future directions
MIMO Downlink Resource Allocation

- downlink power/beamformer assignment to guarantee fair network QoS based on feedback (---) from user terminals

- a user terminal may attempt to degrade network performance by sending fraudulent feedback, forcing the basestation to allocate more resources to it, and hence reducing those available for others

- in this initial study, we focus on fraudulent feedback mechanisms a malicious user may employ in a multicast scenario
Problem Setup

- Transmitter has $N$ antennas
- $K$ single-antenna users, assume user 1 is malicious
- $h_k$ denotes $1 \times N$ channel for user $k$, this information is fed back to transmitter
- Multicast scenario: unit power symbol $s$ is to be transmitted to all users
- Transmitter uses $N \times 1$ beamformer $w$ to transmit $s$
- Total power constraint must be satisfied: $\|w\|^2 \leq P$
- User $k$ observes received signal is AWGN of power $\sigma_k^2$
  \[ y_k = h_k w s + n_k \]
- Performance metric is SNR (or equivalently rate) for each link:
  \[ \text{SNR}_k = \frac{\|h_k w\|^2}{\sigma^2}, \ k = 1, \cdots, K \]
Example: Max-Min Transmitter Strategy

• Suppose transmitter’s strategy is to maximize minimum link SNR:

\[
\mathbf{w} = \arg \max_{\mathbf{w}} \min_k \| \mathbf{h}_k \mathbf{w} \|^2 \\
\| \mathbf{w} \|^2 \leq P
\]

• While falsely reporting \( \mathbf{h}_1 \rightarrow 0 \) would be sufficient, such a naïve approach is easily detected

• Instead, assume malicious user adopts the following approach:

\[
\min_{\mathbf{h}_1} \max_{\mathbf{w}} \min_k \| \mathbf{h}_k \mathbf{w} \|^2 \\
\text{s.t. } \| \mathbf{w} \|^2 \leq P \\
\| \mathbf{h}_1 \|^2 \geq \beta
\]

• Solution can be found a series of sequential quadratic programs
Example: Max-Min Transmitter Strategy

![Graph showing the Max-Min Transmitter Strategy]

- **Accurate**
- **Open-loop**
- ** Poisoned**

The graph illustrates the maximum minimum information rate (b/s/Hz) against the number of receivers. The data shows a decreasing trend with an increasing number of receivers for all strategies.
Future Directions

• Strategies for detecting fraudulent feedback in the physical layer
  - exploiting channel temporal correlation
  - channel tracking/prediction
  - multiuser diversity, variations in channel norm

• Sensitivity and robustness of interference channel algorithms, effects of imperfect CSI and development of robust beamformers

• Secrecy for one- and two-way relay channels, benefit of inactive nodes providing jamming support

• Dual-adversary scenarios for more complicated network topologies (interference channels, relay & helper configurations, etc.)

• Experimental evaluation of point-to-point and cooperative jamming approaches (joint with Michael Jensen)


