Effects of Cooperation on the Secrecy of Multiple Access Channels with Generalized Feedback

Ersen Ekrem and Şennur Ulukuş

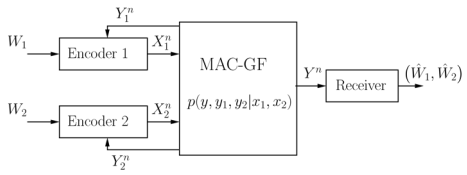
The Institute for Systems Research

University of Maryland 18 56

CSPL

Motivation

- Inherent openness of wireless medium brings two concepts:
  - Cooperation: Overheard information allows users to cooperate and increases rates
  - Secrecy: But it also decreases secrecy
- How do cooperation and secrecy interact?
- Our focus:
  - A two user multiple access channel with generalized feedback
  - Each user considers the other as a wire-tapper
  - Yet, they are still willing to cooperate through feedback
  - How does cooperation affect secrecy?
    - Feedback increases achievable rates, but what about secrecy?



MAC with Generalized Feedback

- Presence of feedback: Cooperation and/or Secrecy
- Cooperation:
  - Similar to the relay channel, basic schemes are decode-and-forward (DAF) and compress-and-forward (CAF) [Cover-El Gamal 1979]
  - DAF: Cover-Leung 1981, Willems *et al.* 1983, Carleial 1982
  - CAF: Khojastepour 2004, Ong-Motani 2007
- Secrecy:
  - Previous works did not utilize the feedback, i.e., no cooperation
  - The only effect of feedback: Leakage of confidential information
    - Liang-Poor 2008, Liu-Maric-Yates-Spasojevic 2006

Generalized MAC with Secrecy

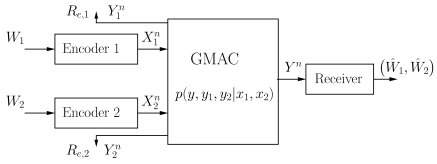


Figure 1: The channel model in Liang-Poor 2008, Liu *et. al.* 2006.

An Achievable Scheme

Theorem 1 *Rate tuples* $(R_1,R_2,R_{e,1},R_{e,2})$ *satisfying*

$$\begin{aligned} R_1 &\le R_1' &&\le I(X_1;Y,\hat{Y}_1|U,X_2) \\ R_2 &\le R_2' &&\le I(X_2;Y,\hat{Y}_1|U,X_1) \\ R_1+R_2 &\le R_1'+R_2' &&\le I(X_1,X_2;Y,\hat{Y}_1|U) \\ R_{e,1} &&&\le \min\left\{R_1'-\tilde{R}_{e,1},R_1\right\} \\ R_{e,2} &&&\le \min\left\{R_2'-I(X_2;Y_1|U,X_1),R_2\right\} \end{aligned}$$

where $\tilde{R}_{e,1}$ *is given by*

$$\tilde{R}_{e,1}=\begin{cases} I(X_1;Y_2,\hat{Y}_1|U,X_2) & \text{if } \mathcal{S}_1 \\ I(X_1;Y_2|U,X_2) & \text{otherwise} \end{cases}$$

are achievable for any distribution of the form

$$p(u)p(x_1|u)p(\hat{y}_1|u,x_1,y_1)p(x_2)p(y,y_1,y_2|x_1,x_2)$$

subject to the constraint

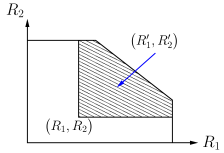
$$I(\hat{Y}_1;Y_1|U,X_1)\le I(U,\hat{Y}_1;Y)$$

where

$$\mathcal{S}_1=\left\{I(U;Y)\le I(U;Y_2|X_2),\quad I(\hat{Y}_1;Y|U)\le I(\hat{Y}_1;Y_2|U,X_2)\right\}$$

Comments on the Achievable Scheme

- It uses CAF for cooperation
- Stochastic encoding:
  - Embed your messages (R_1,R_2) to a larger codebook (R_1',R_2')
  - Additional redundancy is to confuse the other user



- User 1's observation can include self-interference
  - We eliminate user 1's signal, X_1, from Y_1 while compressing it to $\hat{Y}_1$
  - An alternative: Keep self-interference for a possible rate increase
- Channel prefixing can be employed, replace X_1 (resp. X_2) with V_1 (resp. V_2) and the PMF with

$$p(u)p(v_1|u)p(x_1|v_1)p(\hat{y}_1|u,v_1,y_1)p(v_2)p(x_2|v_2)p(y,y_1,y_2|x_1,x_2)$$

- User 2 may want to decode the compressed version of user 1's feedback, $\hat{Y}_1$
  - Depending on whether it can or not, different leakage expressions
- We can also extend this scheme to the case with two-sided cooperation [Ekrem-Ulukus CISS 2008]

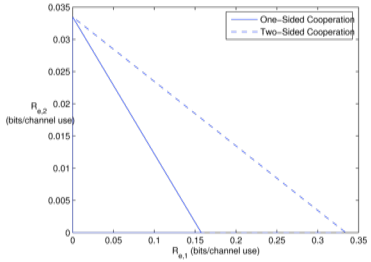
Gaussian Channels

- A Gaussian MAC-GF is

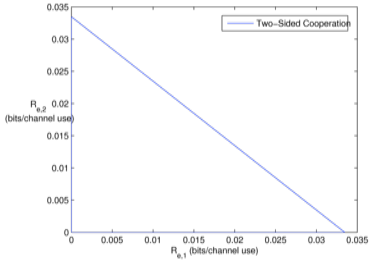
$$\begin{aligned} Y_i &= X_1+X_2+Z_i, \quad i=1,2 \\ Y &= X_1+X_2+Z \end{aligned}$$

where $Z\sim\mathcal{N}(0,N),Z_i\sim\mathcal{N}(0,N_i),i=1,2$. $E[X_1^2]\le P_1$ and $E[X_2^2]\le P_2$.

- For Gaussian channels without cooperation,
  - If $N_1<N$, then $R_{e,2}=0$ and if $N_2<N$, then $R_{e,1}=0$
- What is the effect of cooperation on secrecy?
  - **Case I:** No secrecy for user 2 if cooperation is not allowed, $N_1=0.75<N=1<N_2=1.25$



  - **Case II:** No secrecy for both users if cooperation is not allowed, $N_1=N_2=0.75<N=1$



Conclusions

- Cooperation can increase secrecy; even an untrusted party can help
- Since cooperation enlarges achievable rates, this might be expected
- Crucial point: Depends on how cooperation enlarges the achievable region
  - DAF or partial DAF cannot increase secrecy, but CAF can.
  - Via CAF, a user can increase the rate of the other user beyond its own decoding capability.