Capacity of a Broadcast Channel with Gaussian Jamming and a Friendly Eavesdropper

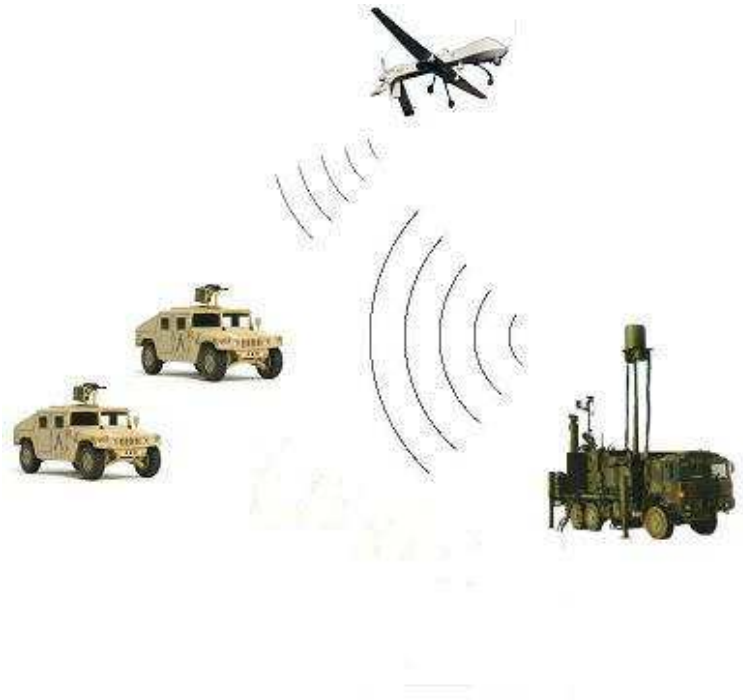
Kevin Luo, Ramy Gohary, Halim Yanikomeroglu

Carleton University, Ottawa, ON, Canada

Oct 2015

A Battlefield Communication Scenario

- a drone sends common information to two ground troops
- a malicious jammer transmits high power Gaussian signal to disrupt the communication



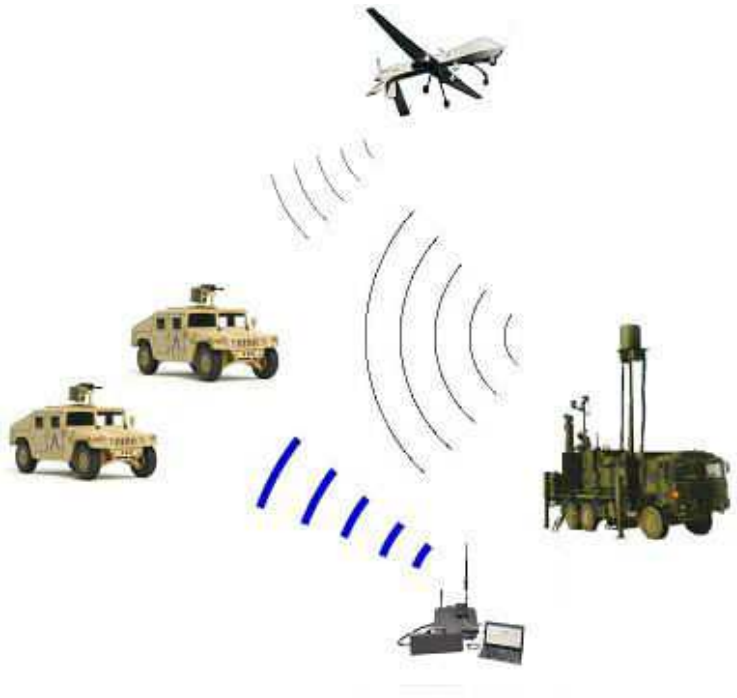
Literature Review (related work)

- Basar, Gaussian channel with jamming, 1983;
- Kashyap, Basar and Srikant, correlated jamming on MIMO Gaussian fading channels, 2004;
- Tekin and Yener, Gaussian multiple access channel with two-way wiretap, 2008;
- Shafie and Ulukus, mutual information games in multiuser channels with correlated jamming, 2009;
- Lai and H. E. Gamal, relay-eavesdropper channel, 2008. In particular, the relay can be seen as a "friendly jammer" who forwards noise to the malicious eavesdropper to improve secrecy.

Eavesdropper

We introduce a “friendly eavesdropper" who

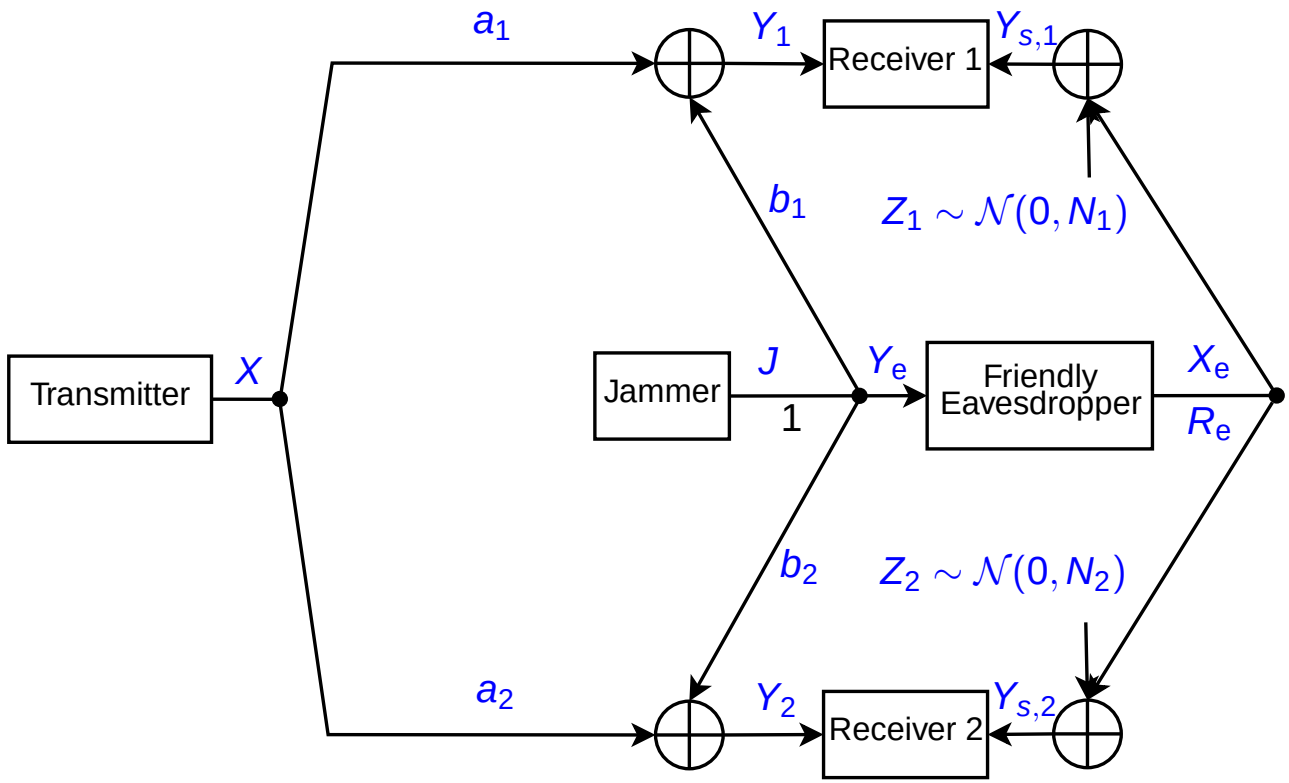
- picks up the jammer’s signal
- assists the communication on an orthogonal channel



System Model-1

We conceive the role of the eavesdropper as a relay

- drone $\rightarrow$ source
- troops $\rightarrow$ receivers
- jammer $\rightarrow$ noise or interference
- eavesdropper $\rightarrow$ relay



System Model-2

Model details of the eavesdropper as a relay:

- The eavesdropper has average power constraint
- The eavesdropper-to-receiver links are noisy links
- The eavesdropper's transmission is rate-limited by the higher capacity of the two eavesdropper-to-receiver links
- The jammer does not cooperate with the eavesdropper, i.e., the jammer's codebook is not exposed to the eavesdropper

What is the eavesdropper's optimal strategy to enable the maximum rate to be reliably communicated between the source and the receivers?

Relaying Schemes

Two types of relaying schemes:

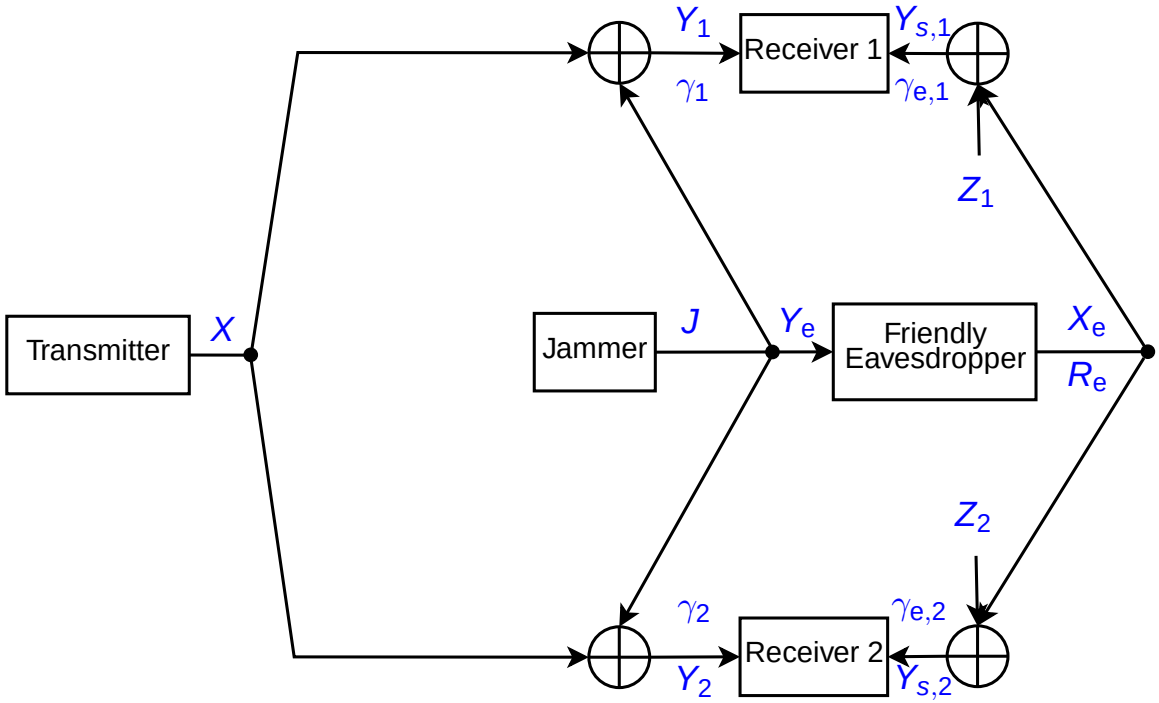
- Relaying schemes that require the eavesdropper (relay) to know the the jammer's codebook:
  - decode-and-forward (DF) and hash-and-forward (HF)
  - DF and HF are not suitable for this channel
- Relaying schemes that do not require the eavesdropper (relay) to know the the jammer's codebook:
  - amplify-and-forward (AF)
  - compress-and-forward (CF) and variants

Cut-set Bound

- We first show a capacity upper bound by deriving the cut-set bound:

$$C \leq \min\left\{\mathcal{C}(\gamma_1) + \mathcal{C}(\gamma_{e,1}), \mathcal{C}(\gamma_2) + \mathcal{C}(\gamma_{e,2})\right\}.$$

where γ_i is the signal-to-jamming ratio of the source-to-receiver i link and $\gamma_{e,i}$ is the signal-to-noise ratio of the eavesdropper-to-receiver i link.



AF: Suboptimal

- The achievable rate expression of the AF scheme can be obtained by

$$R_{\mathrm{AF}} = \min_{i=1,2} \{\mathcal{C}\left(\gamma_i(1+\gamma_{\mathrm{e},i})\right)\}.$$

  which is below the cut-set bound in general.
- AF does not achieve the cut-set bound in general.

CF with Standard Decoding: Suboptimal

- Conventional CF
  - The relay bin index is recovered by finding a unique codeword representing the bin index in the joint typicality set with the received signal at the receiver.
- The achievable rate expression of the conventional CF can be obtained by

$$R_{\mathrm{CF}} \leq \min_{i=1,2} \mathcal{C}(\gamma_i) + \min_{i=1,2} \mathcal{C}(\gamma_{\mathrm{e},i}),$$

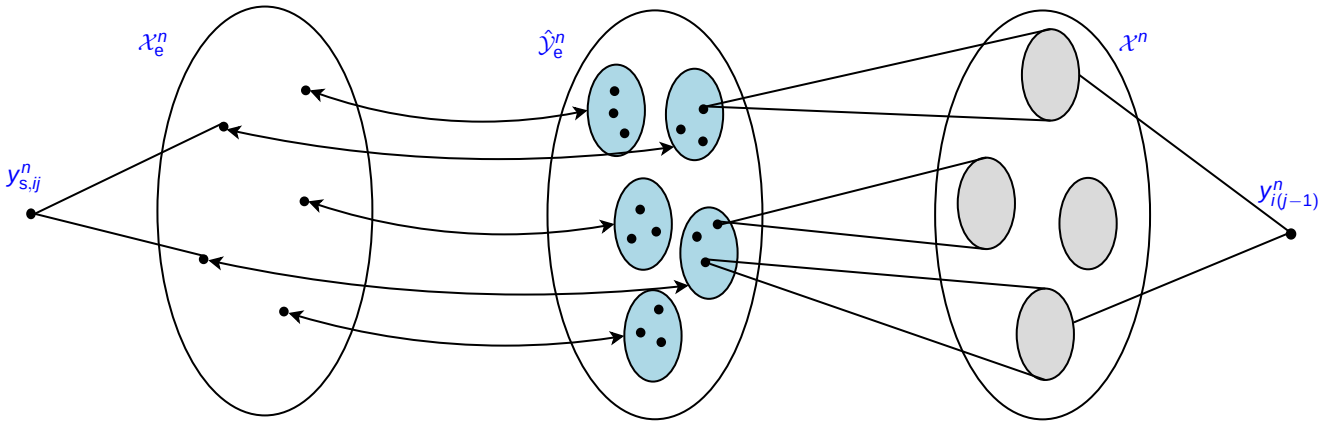
  which is also below the cut-set bound in general.
- CF with standard decoding does not achieve the cut-set bound in general either.

CF with List Decoding: Capacity Achieving

- Modified CF
  - Use the same codebook structure and encoding as conventional CF.

CF with List Decoding: Capacity Achieving

- Modified CF (continued)
  - In decoding block j, receiver i finds unique $(\hat{y}^n_{\mathrm{e},j-1}, x^n_{j-1}, x^n_{\mathrm{e},j})$ such that
    - $\{(\hat{y}^n_{\mathrm{e},j-1}, x^n_{j-1})\}$ jointly typical with $y^n_{i(j-1)}$ (not necessarily unique); and
    - $x^n_{\mathrm{e},j}$ jointly typical with $y^n_{s,ij}$, $i = 1, 2$. ($x^n_{\mathrm{e},j}$ is the eavesdropper codeword corresponding to $\hat{y}^n_{\mathrm{e},j-1}$)



CF with List Decoding: Capacity Achieving

- The eavesdropper uses
  - Standard CF encoding, with
  - Gaussian codebook.

This signaling strategy is able to achieve the cut-set bound and hence

$$C = \min\left\{\mathcal{C}(\gamma_1) + \mathcal{C}(\gamma_{e,1}), \mathcal{C}(\gamma_2) + \mathcal{C}(\gamma_{e,2})\right\}.$$

Benefit of Eavesdropper

- Capacity without eavesdropper

$$C_{\text{No Eavesdropper}} = \min_{i=1,2} \mathcal{C}(\gamma_i).$$

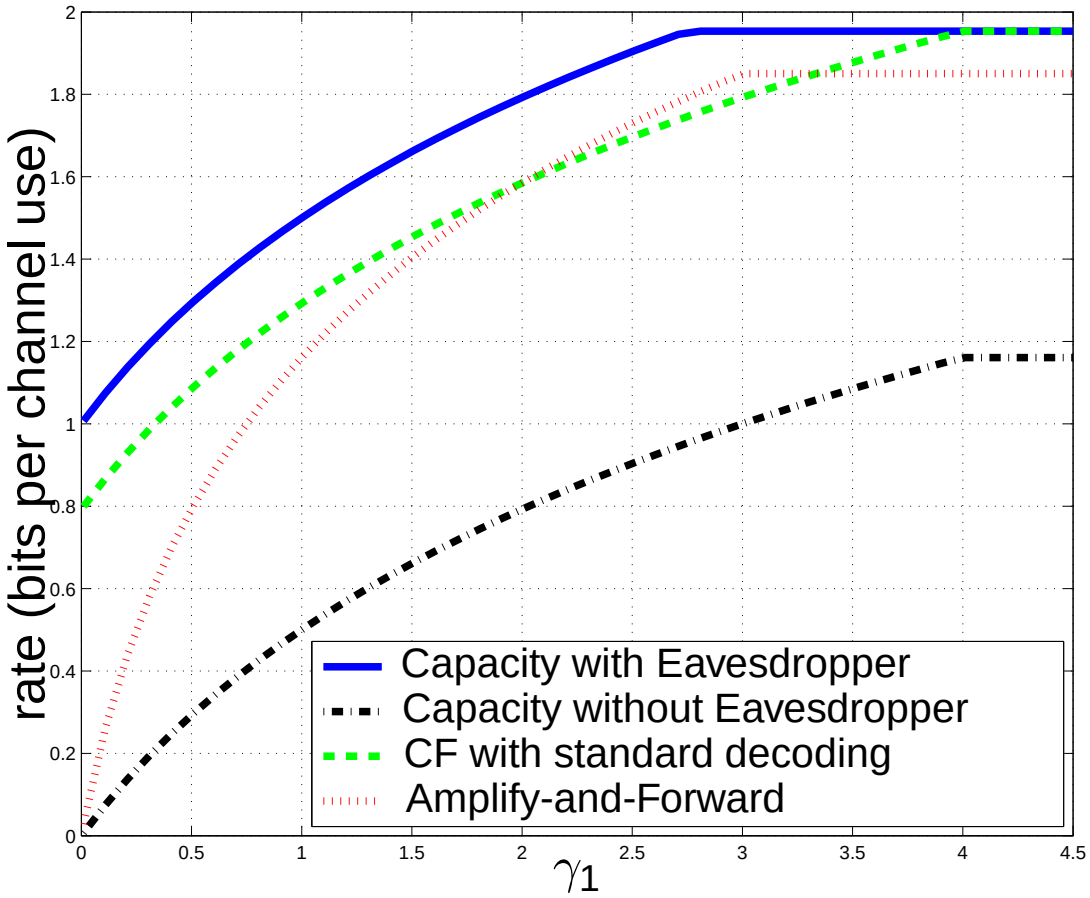
- The rate gain provided by the friendly eavesdropper is given by

$$\begin{aligned} &\min\left\{\Delta + \mathcal{C}(\gamma_{e,1}), \mathcal{C}(\gamma_{e,2})\right\}, && \gamma_1 \geq \gamma_2, \\ &\min\left\{\mathcal{C}(\gamma_{e,1}), \Delta + \mathcal{C}(\gamma_{e,2})\right\}, && \gamma_1 < \gamma_2, \end{aligned}$$

where $\Delta \triangleq |\mathcal{C}(\gamma_1) - \mathcal{C}(\gamma_2)|$.

Numerical Result

- Consider the instance $\gamma_2 = 4$, $\gamma_{e,1} = 3$, $\gamma_{e,2} = 2$ and $\gamma_1 \in [0, 4.5]$.



Summary and Conclusions

- Channel with multiple receivers, a jammer and a friendly eavesdropper.
- AF and conventional CF with Gaussian codebooks do not achieve cut-set bound.
- CF with list decoding and Gaussian codebooks achieves cut-set bound.

Comments on NNC and SNNC

- NNC and SNNC uses a 1-to-1 mapping between the codewords in $\hat{\mathcal{Y}}_{\mathsf{e}}$ and in $\mathcal{X}_{\mathsf{e}}$.
- This is in contrast with conventional CF and modified CF, both of which use the N-to-1 mapping from Wyner-Ziv binning.
- The 1-to-1 mapping induces an additional constraint on the estimation noise at the eavesdropper since $\mathcal{X}_{\mathsf{e}}$ is rate limited in the considered channel.
- This constraint results in a rate loss in general.

Comments on HF

- In HF, the relay constructs a mapping from $\mathcal{J}$ to the bins ($\mathcal{X}_e$).
- Mapping available at receivers. Hence, not applicable in jamming case.