

## Motivation and Model

- ◇ In a multi-terminal network, it is possible that a relay is captured by an adversary.
- ◇ We study the problem of achieving secrecy when a jammer relay helps the eavesdropper.
- ◇ Model and assumptions:
  - Four-terminal Gaussian network as shown in Fig. 1
  - All channel gains fixed and known at all nodes
  - Source (S) and Jammer relay (JR) have average power constraints  $P_S$  and  $P_R$
  - Legitimate destination D, eavesdropper E
  - S wants to increase secrecy rate  $R_s$  while JR wants to decrease it

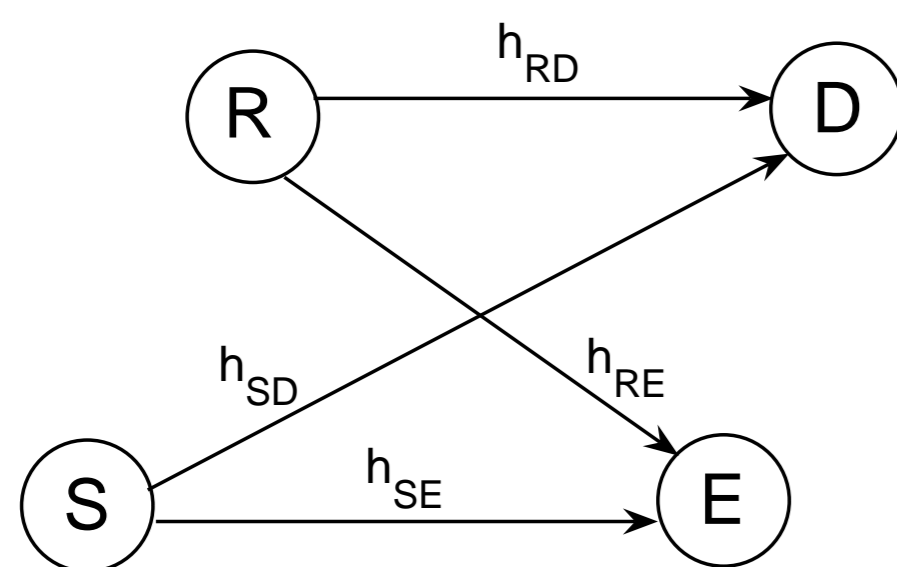


Fig. 1 Four-terminal Gaussian network.

- Assume JR does not listen to S transmission. Two options for JR are: send unstructured noise or structured codewords.
  - \* Unstructured noise harms D as well as E;
  - \* Structured codewords have the potential to help E more provided that E can decode;
  - \* When S sends Gaussian codewords, the JR distribution that helps E most is also Gaussian.

## Game Theoretic Formulation

- ◇ Assume both S and R choose codebooks i.i.d. Gaussian, with zero mean and variances  $P_S$  and  $P_R$  respectively.
- ◇ Source strategy: Choose information rate  $\xi$
- ◇ Relay strategy: Choose dummy information rate  $\eta$
- ◇ D can decode both S and R's codewords if  $(\xi, \eta)$  is in  $\mathcal{R}_{MAC}^{[D]}$  where
$$\mathcal{R}_{MAC}^{[D]} = \left\{ (\xi, \eta) \left| \begin{array}{l} \xi \leq \log(1 + \gamma_{SD}) \\ \eta \leq \log(1 + \gamma_{RD}) \\ \xi + \eta \leq \log(1 + \gamma_{SD} + \gamma_{RD}) \end{array} \right. \right\} \quad (1)$$
- ◇ If D fails to decode R's codeword, it treats it as noise. All rates in  $\mathcal{R}_N^{[D]}$  are also achievable.
$$\mathcal{R}_N^{[D]} = \left\{ \xi \left| \xi \leq \log\left(1 + \frac{\gamma_{SD}}{1 + \gamma_{RD}}\right) \right. \right\} \quad (2)$$
- ◇ D can decode source message with arbitrarily small  $P_e$  if  $(\xi, \eta) \in \mathcal{R}^{[D]} = \mathcal{R}_{MAC}^{[D]} \cup \mathcal{R}_N^{[D]}$ .  $\mathcal{R}_{MAC}^{[E]}$ ,  $\mathcal{R}_N^{[E]}$  and  $\mathcal{R}^{[E]}$  can be defined similarly.

## Playing the Game

- ◇ Two-user zero-sum game with secrecy rate  $R_s$  being the payoff.
- ◇ For a fixed S and R rate pair  $(\xi, \eta)$ , S's payoff is given by
$$R_s(\xi, \eta) = \begin{cases} 0, & \text{if } (\xi, \eta) \in \mathcal{R}^{[E]} \text{ or } (\xi, \eta) \notin \mathcal{R}^{[D]} \\ \max_{R_{S,d}}(\xi - R_{S,d}), & \text{if } (\xi, \eta) \in \mathcal{R}^{[D]} \text{ and } (R_{S,d}, \eta) \notin \mathcal{R}^{[E]} \end{cases} \quad (3)$$
- ◇ Fig. 2(a) shows one example for the boundary regions  $\mathcal{R}^{[D]}$  and  $\mathcal{R}^{[E]}$ , where the positions of the corner points depend on  $\gamma_{kl}$ 's,  $k = S, R, l = D, E$ .

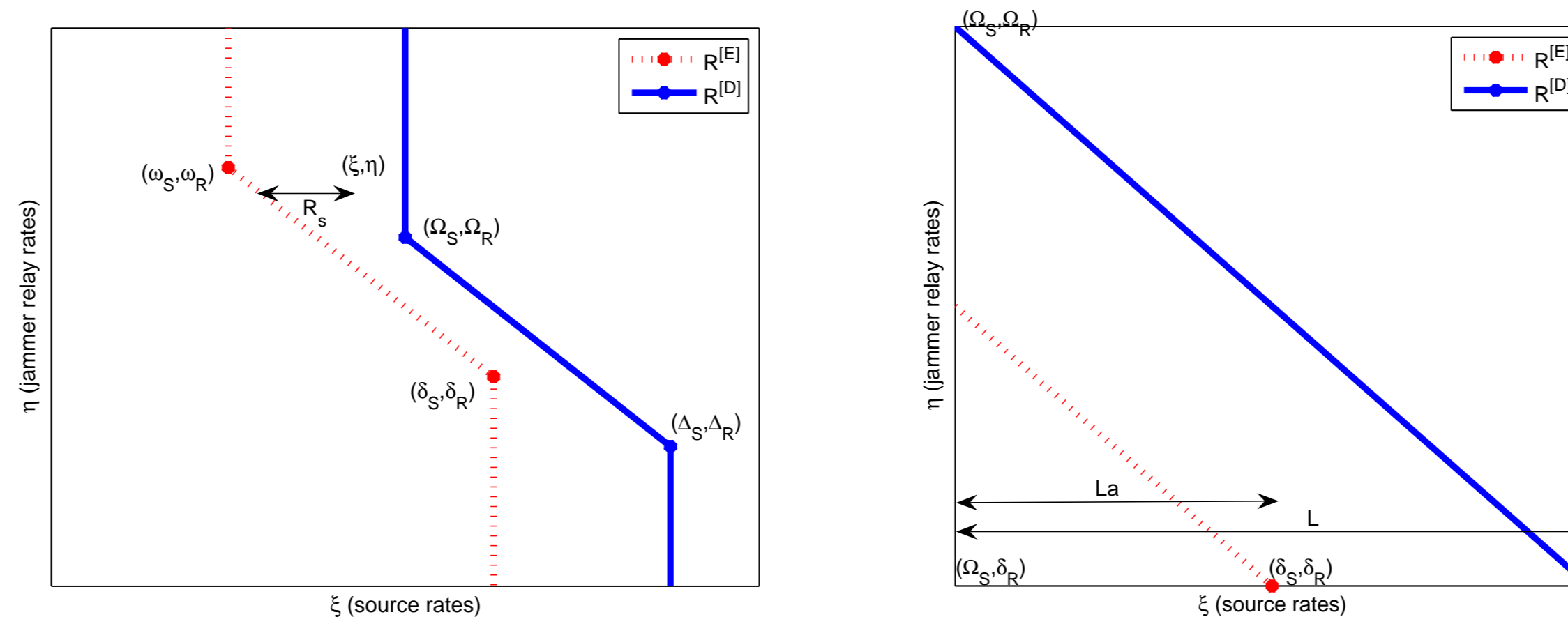


Fig. 2 (a) Boundaries for  $\mathcal{R}^{[D]}$  and  $\mathcal{R}^{[E]}$ ; (b) The equivalent game.

**Lemma 1** For the regions considered in Fig.2(a), the game does not have a pure strategy solution.

**Lemma 2** The game defined in Lemma 1 is equivalent to one played over the square with "discontinuous" payoff as in Fig.2(b), where the S and JR strategies are respectively restricted to compact intervals  $\xi \in [\Omega_S, \Omega_S + L]$  and  $\eta \in [\delta_R, \delta_R + L]$ . Here  $L = \Omega_R - \delta_R$  and  $a = (\delta_S - \Omega_S)/L$ .

**Theorem 1** Suppose  $a \in [k/(k+1), (k+1)/(k+2)]$ , for some integer  $k \geq 0$ . Then the equivalent game has the Nash Equilibrium secrecy rate  $R_s^* = L\alpha(1-a)$ , where  $\alpha = g_k(a)$ , and is achieved with c.d.f. for S and JR  $F_\xi(\xi)$  and  $F_\eta(\eta)$ , respectively.

- ◇ For instance, when  $0 \leq a \leq 1/2$ ,  $\alpha = g_0(a) = \frac{e^{-1/(1-a)}}{1 - \frac{a}{1-a}e^{-1}}$ ; and optimal c.d.f. for S is
$$F_\xi(\xi) = \begin{cases} \alpha e^{\frac{\xi - \Omega_S}{L(1-a)}}, & \Omega_S \leq \xi \leq \Omega_S + L(1-a) \\ \alpha \left[ (1 + e^{-1})e^{\frac{\xi - \Omega_S}{L(1-a)}} - \frac{\xi - \Omega_S}{L(1-a)} e^{\frac{\xi - \Omega_S}{L(1-a)}} \right], & \Omega_S + L(1-a) \leq \xi \leq \Omega_S + L \end{cases} \quad (4)$$
- ◇ However, a general analytical expression does not exist for any  $a$ .

## Contact information:

e-mail: xliu02@students.poly.edu

## The Discrete Game

- ◇ A more practical way to compute game value is discrete approximation:
  - Take  $(T + 1)^2$  samples by dividing the square into a uniform grid, i.e.,  $\xi_l = \omega_s + Ll/T$ ,  $\eta_l = \delta_R + Ll/T$ ,  $R_s(l) = R_s(\xi_l, \eta_l)$ ,  $l = 0, 1, \dots, T$ .
  - The value of the discrete game can be easily obtained using linear programming.
  - Difference between values of the discrete and the continuous games is at most  $2\sqrt{2}L/T$ .
- ◇ A numerical example:
  - $|h_{SD}| = 1$ ,  $|h_{SR}| = 1/3$ ,  $|h_{RD}| = 1/2$ ,  $|h_{SE}| = |h_{RE}| = 2/3$ ,  $P_S = P_R = 10$ .
  - Thus, we have  $a = 0.5255$  ( $1/2 < a < 1$ ),  $L = 0.946$ ,  $\alpha = 0.20484$ .
  - Equilibrium secrecy rate of the continuous game is 0.092 bits/channel use while that of the discrete game is 0.0923 bits/channel use ( $T = 400$ ). Optimal c.d.f.'s for S in both cases are plotted in Fig. 3.
  - In the case of no JR,  $R_s = 1.0146$  bits/ channel use.

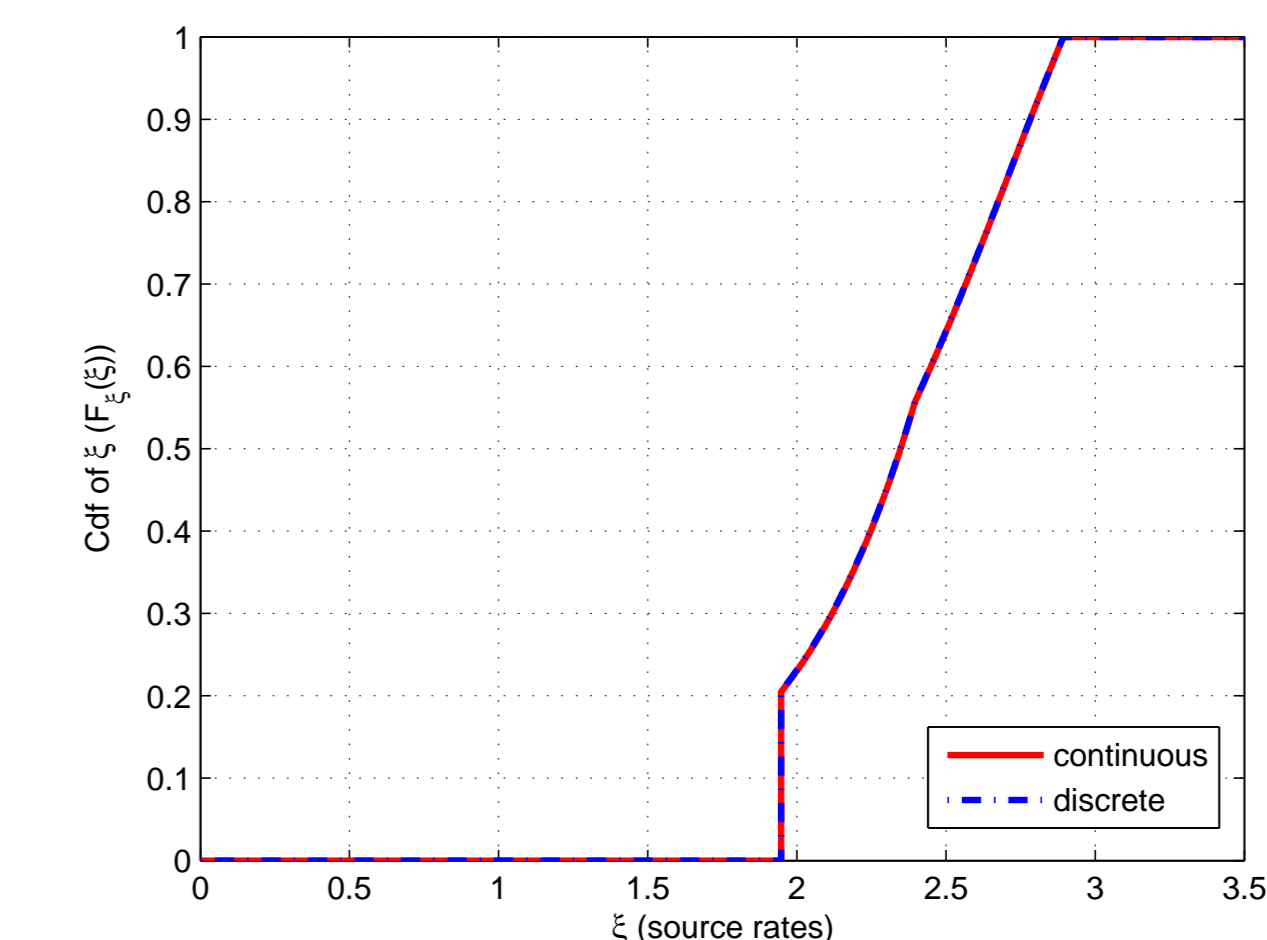


Fig. 3 Optimal c.d.f. for S, for the continuous and discrete games when  $a = 0.5255$ .

## Conclusion and Future Work

- ◇ We formulate the problem of achieving secrecy when a jammer relay helps eavesdropper as a two-user zero-sum continuous game and find the optimal solution for S and JR to be mixed strategies. A discrete approximation to the continuous game is also provided to compute the game value (equilibrium secrecy rate) more easily.
- ◇ Results show presence of JR decreases secrecy rates significantly.
- ◇ The cases in which JR hears S transmission remain open.
- ◇ More details can be found in the paper: M. Yuksel, X. Liu, and E. Erkip, "A secure communication game with a relay helping the eavesdropper", to be presented in ITW Taormina 09.