Achievable Secrecy Sum-Rate in a Fading MAC-WT with Power Control and without CSI of Eavesdropper

Shahid Mehraj Shah
(Joint work with Vireshwar Kumar and Prof. Vinod Sharma)

ECE Dept., Indian Institute of Science
Bangalore, India

July 23, 2012

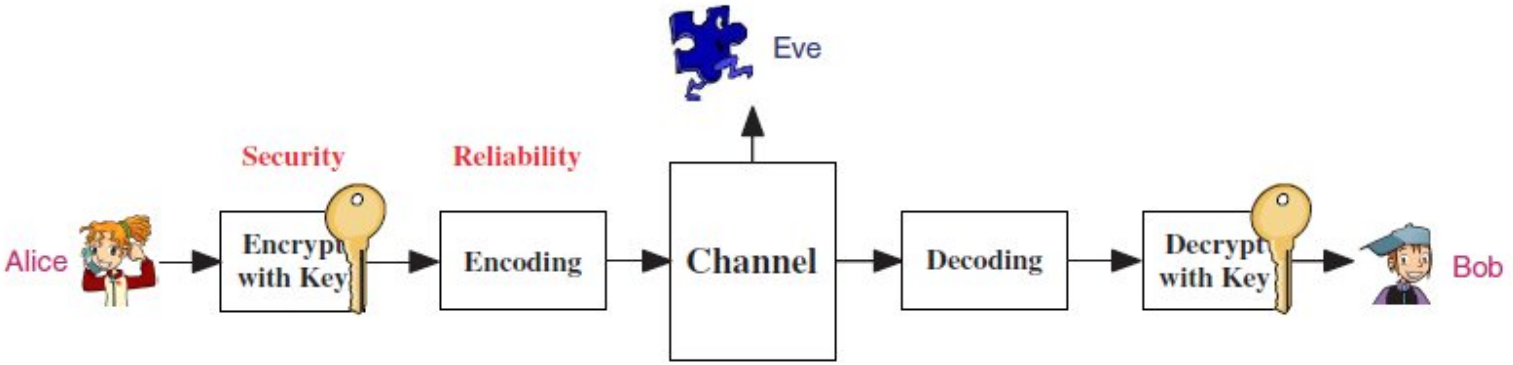
Outline

- Introduction
- Information Theoretic security
- Multiple Access Channel with Eavesdropper
- Fading MAC without CSI of eavesdropper
- Power control schemes with cooperative jamming
- Summary
- Future Work

Introduction

- Security is important in transmission of information
- Conventional technique is Cryptography
  - Assumes limited computational capacity of Eavesdropper.
- Information theoretic security.
  - Assumes unlimited computational capacity of Eavesdropper.
- Wyner introduced Wiretap channel in his seminal paper in 1974.

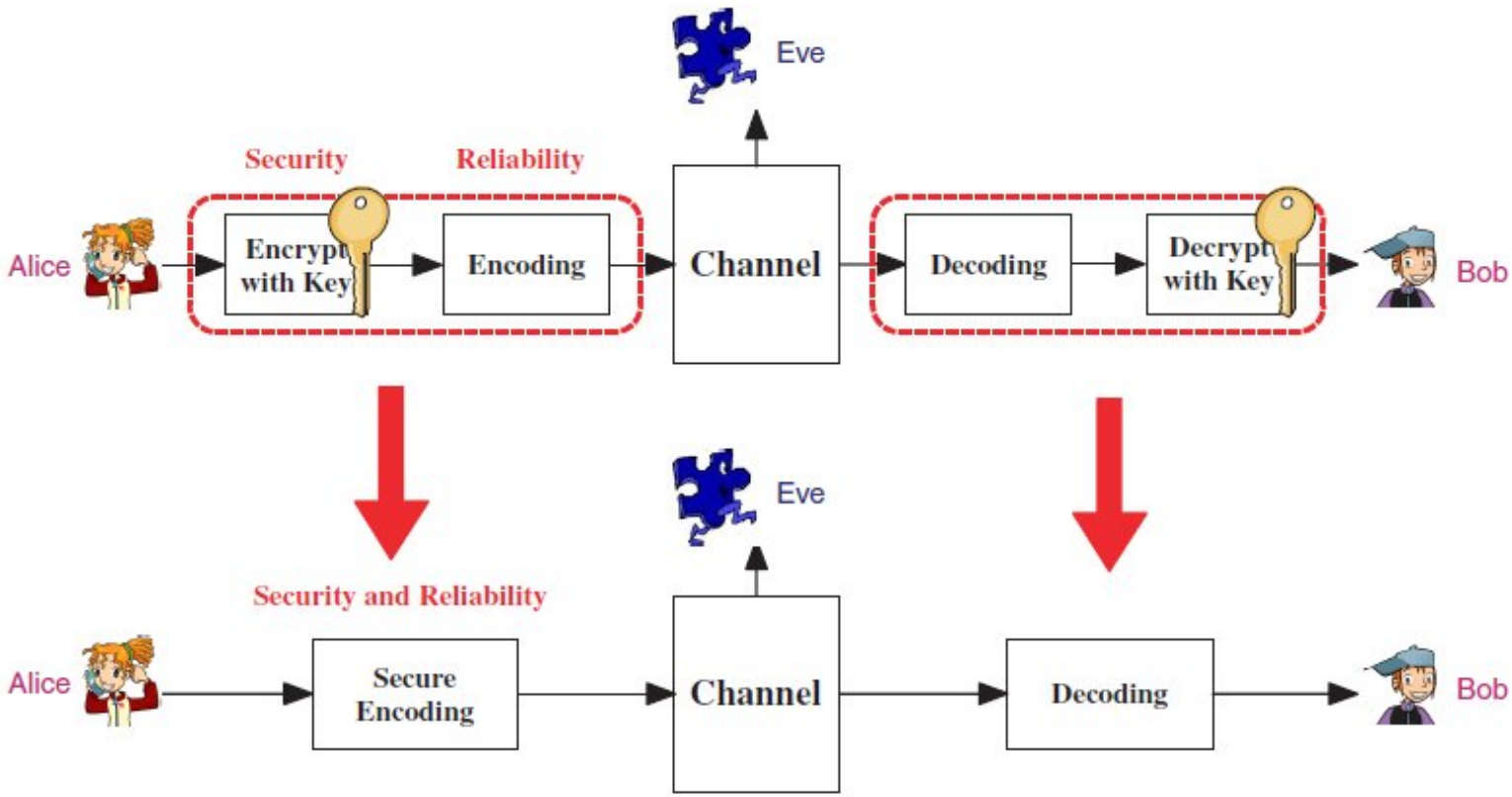
Model



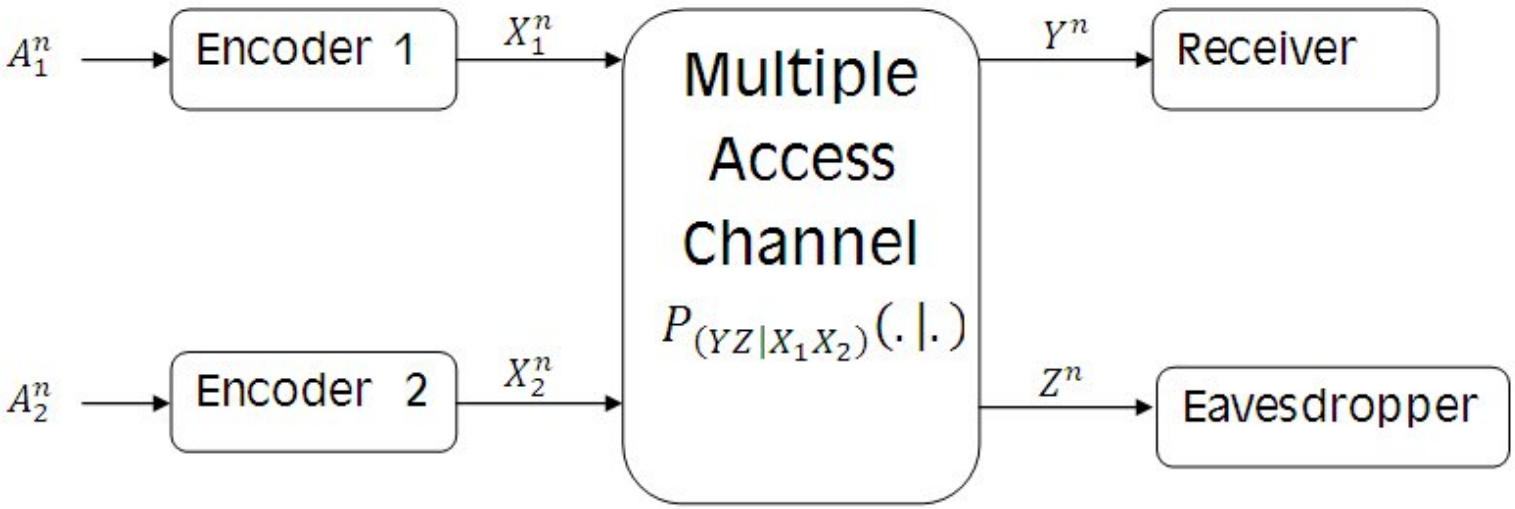
Encryption with channel coding

Information Theoretic Security

- Security issues include confidentiality, integrity, authentication, and non-repudiation
- Two basic types of attacks: passive attacks and active attacks.



Multiple Access Channel with Eve



Multiple Access Channel with Eve

- This model has been studied under the asumption of independent sources
- Gaussian MAC with eavesdropper studied by Yener and Tekin(IEEE trans 2008)
- Fading MAC with full CSI of eavesdropper studied by Yener and Tekin

Definitions

- Security if measured by the equivocation rate for each user
- $R_{1e}^{(n)} = \frac{1}{n} H(W_1|Z^n)$
- $R_{2e}^{(n)} = \frac{1}{n} H(W_2|Z^n)$
- $R_{1e}^{(n)} + R_{2e}^{(n)} = \frac{1}{n} H(W_1 W_2|Z^n)$
- Reliability: $P_{e1}^{(}n) = Pr\{\tilde{W}_1 \neq W_1\}, P_{e1}^{(}n) = Pr\{\tilde{W}_1 \neq W_1\}$
- A rate-equivocation pair $(R_1, R_2, R_{1e}, R_{2e})$ is achievable if $\exists$ a sequence of message sets $\mathcal{W}_{1n}$ and $\mathcal{W}_{2n}$ and encoder-decoder pairs (f_{1n}, f_{2n}, g_n) s.t. $P_e^{(n)} \to 0$ as $n \to \infty$ and equivocation rates satisfy $R_{1e} \leq \liminf_{n\to\infty} R_{1e}^{(n)}, R_{2e} \leq \liminf_{n\to\infty} R_{2e}^{(n)}$,

MAC with eavesdropper: Secrecy rate region

- The best known rate region for DM - MAC is as follows

$$R_1 \leq [I(U_1; Y \mid U_2) - I(U_1; Z)]^+$$
$$R_2 \leq [I(U_2; Y \mid U_1) - I(U_2; Z)]^+$$
$$R_1 + R_2 \leq [I(U_1, U_2; Y) - I(U_1, U_2; Z)]^+$$

  - where $p(x_1, x_2, u_1, u_2, y, z) = p(u_1)p(x_1 \mid u_1)p(u_2)p(x_2 \mid u_2)p(y, z \mid x_1, x_2)$
  - The rate region for Gaussian MAC and fading MAC can be obtained from this rate region.

Fading MAC: Secrecy rate region with perfect CSIT of Bob and Eve

- Rate region for fading MAC is as follows(Yener and Tekin)

$$R_1 \leq \mathrm{E}_{h,g}\left\{\left[log\frac{(1+h_1P_1(h,g))(1+g_2P_2(h,g))}{1+g_1P_1(h,g)+g_2P_2(h,g)}\right]^+\right\},$$

$$R_2 \leq \mathrm{E}_{h,g}\left\{\left[log\frac{(1+g_1P_1(h,g))(1+h_2P_2(h,g))}{1+g_1P_1(h,g)+g_2P_2(h,g)}\right]^+\right\},$$

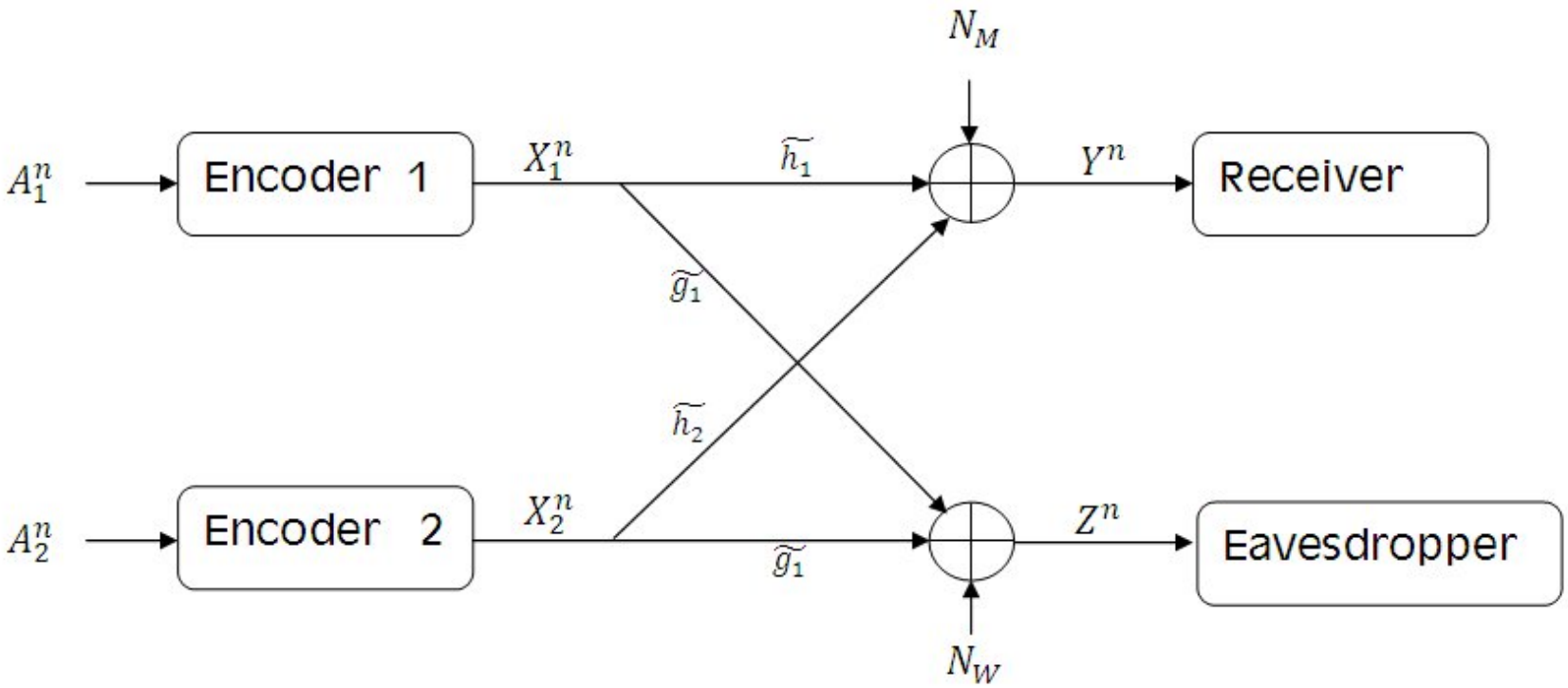
$$R_1+R_2 \leq \mathrm{E}_{h,g}\left\{\left[log\frac{1+h_1P_1(h,g)+h_2P_2(h,g)}{1+g_1P_1(h,g)+g_2P_2(h,g)}\right]^+\right\},$$

- where $h=(h_1,h_2), g=(g_1,g_2)$ are channel gains of Bob and Eve and $P_1(h,g)$ and $P_2(h,g)$ are the transmit powers satisfying power constraints and Gaussian signalling is used.

Fading MAC without CSI of eve

- In passive attack of Eavesdropper, CSI cannot be estimated
- Single user wiretap channel without CSI studied in H.E Elgamal(IEEE trans 2008)and Mathew Bloch et. al(IEEE trans 2008)
- We propose the power control scheme for fading MAC to optimize Secrecy sum-rate.

Fading MAC without CSI of eve: Channel Model



- $\tilde{h}_{k,i}$, $\tilde{g}_{k,i}$ Complex channel gains
- we define $|\tilde{h}_{k,i}|^2 = h_{k,i}$ and $|\tilde{g}_{k,i}|^2 = g_{k,i}$, for $k = 1, 2$.
- $\phi^s_{x_1,x_2} = 1 + s_1 x_1 + s_2 x_2$ where s is the channel state (h or g) and x_k is the power used.
- Let $A_1 \triangleq \{h_1 > \tau_1,\ h_2 < \tau_2\}$, $A_2 \triangleq \{h_1 < \tau_1,\ h_2 > \tau_2\}$ and $A_{12} \triangleq \{h_1 > \tau_1,\ h_2 > \tau_2\}$

Fading MAC without CSI of eve: Optimal power allocation

Theorem

For a given power control policy $\{P_k(h)\},\ k = 1, 2$, *the following secrecy sum-rate*

$$\mathrm{E}_{h,g}\left\{\left[log\left(\frac{\phi^{h}_{P_1,P_2}}{\phi^{g}_{P_1,P_2}}\right)\right]^{+}\right\} \tag{1}$$

is achievable, subject to power constraint
$\mathrm{E}_{h,g}[P_k(h)] \leq \bar{P}_k,\ k = 1, 2.$

- Optimal policy computed numerically.

Fading MAC without CSI of eve: Optimal power control with Cooperative Jamming

- A user when not transmitting information can jam the eve.
- $\{P_k(h)\},\ k=1,2$, power when transmitting information
  $\{Q_k(h)\},\ k=1,2$, power when jamming,

Theorem

With the above power control policies secrecy sum-rate

$$\mathrm{E}_{h,g}\left\{\left[log\left(\frac{\phi^{h}_{P_1,P_2}+\phi^{h}_{Q_1,Q_2}-1}{\phi^{g}_{P_1,P_2}+\phi^{g}_{Q_1,Q_2}-1}\right)\left(\frac{\phi^{g}_{Q_1,Q_2}}{\phi^{h}_{Q_1,Q_2}}\right)\right]^{+}\right\} \tag{2}$$

is achievable, subject to power constraint
$\mathrm{E}_{h,g}[P_k(h)+Q_k(h)]\leq \bar{P}_k,\ k=1,2.$

Without CSI of Eve: ON/OFF power control

- ON/OFF power control is a simple threshold based scheme as follows:
  - $h_1 > \tau_1$, $h_2 > \tau_2$: Both transmit;
  - $h_1 > \tau_1$, $h_2 < \tau_2$: User-1 transmits;
  - $h_1 < \tau_1$, $h_2 > \tau_2$: User-2 transmits;
  - $h_1 < \tau_1$, $h_2 < \tau_2$: No user transmits.
- Then secrecy sum-rate is given by:

$$R_B = \mathrm{E}_{h,g}\left\{\left[log\left(\frac{\phi^h_{P_1,P_2}}{\phi^g_{P_1,P_2}}\right)1_{A_{12}}\right]^+\right\} + \mathrm{E}_{h,g}\left\{\left[log\left(\frac{\phi^h_{P_1,0}}{\phi^g_{P_1,0}}\right)1_{A_1}\right]^+\right\} + \mathrm{E}_{h,g}\left\{\left[log\left(\frac{\phi^h_{0,P_2}}{\phi^g_{0,P_2}}\right)1_{A_2}\right]^+\right\} \quad (3)$$

where $1_{\{\}}$ is the indicator function.

- We then optimize the secrecy sum-rate over τ_1, τ_2

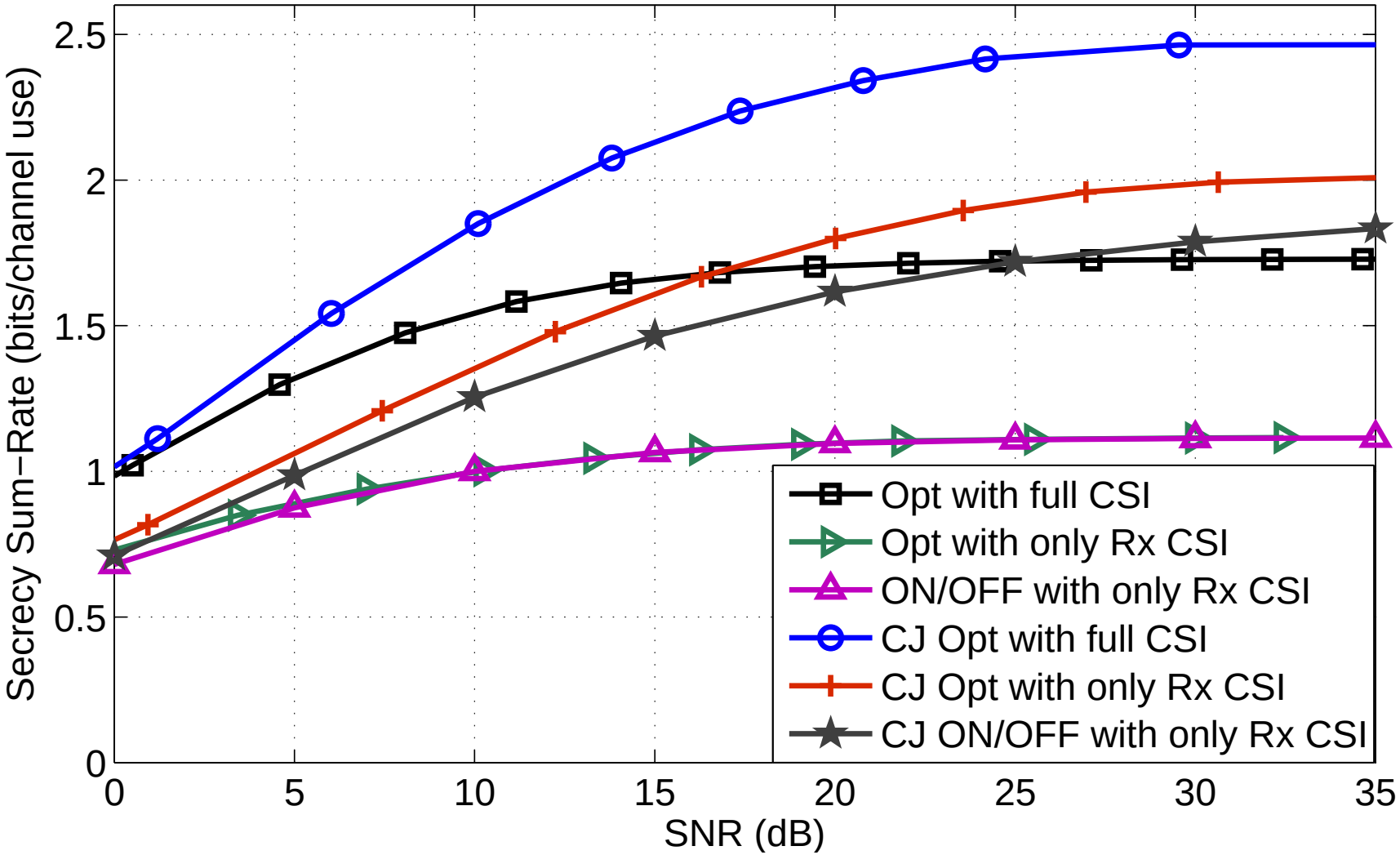
ON/OFF power control with cooperative Jamming

- Here we employ co-operative jamming over ON/OFF scheme
  - $h_1 > \tau_1$, $h_2 > \tau_2$: Both transmit with power P_{1a}, P_{2a};
  - $h_1 > \tau_1$, $h_2 < \tau_2$: User-1 transmits with power P_{1b}, user-2 jams with power Q_2;
  - $h_1 < \tau_1$, $h_2 > \tau_2$: User-2 transmits with power P_{2b}, user-1 jams with power Q_1;
  - $h_1 < \tau_1$, $h_2 < \tau_2$: None transmits or jams.

$$R_B^{CJ} = \mathrm{E}_{h,g}\left\{\left[log\left(\frac{\phi^h_{P_{1a},P_{2a}}}{\phi^g_{P_{1a},P_{2a}}}\right)1_{A_{12}}\right]^+\right\} + \mathrm{E}_{h,g}\left\{\left[log\left(\frac{\phi^h_{P_{1b},Q_2}}{\phi^g_{P_{1b},Q_2}}\right)1_{A_1}\right]^+\right\}$$
$$+ \mathrm{E}_{h,g}\left\{\left[log\left(\frac{\phi^h_{Q_1,P_{2b}}}{\phi^g_{Q_1,P_{2b}}}\right)1_{A_2}\right]^+\right\} \quad (4)$$

When $\tilde{h}_k$ and $\tilde{g}_k$ have Rayleigh distribution

Fading MAC Without CSI of Eve: Simulation results



Summary

- Studied optimal power control for fading Gaussian MAC when CSI of Eve not available.
- Obtained simple ON-OFF scheme
- Considered schemes with Cooperative Jamming

Future Work

- Correlated sources over Gaussian MAC with eavesdropper
- Fading MAC with eve: Fast and Slow fading
- Functions of correlated input sequences over MAC
- All above cases with side-information

Thanks !

References


A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355-1387, 1974.


I. Csiszàr and J.Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 82, no. 23, pp. 339–348, May 1978.


P. K. Gopala, L. Lai, H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Info. Theory*, vol. 54, no. 10, pp. 4687–4698, October 2008.

References- Contd.

- M. Bloch, J. Barros, M.R.D. Rodrigues, S.W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.
- E. Tekin, A. Yener, "The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54 , no. 6, pp. 2735-2751, June 2008.
- E. Tekin, A. Yener, "Secrecy sum-rates for the multiple-access wire-tap Channel *45th Annual Allerton Conference, UIUC, Illinois, USA*, Sep 26–28, 2007.

References- Contd.


Y. Liang, H.V. Poor, S. Shamai, "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5 (2008), pp. 355–580, 2009.