Enhancing Secrecy Rates and Resourse Allocation in Single-User & Multi-User Fading Wiretap Channels

(Thesis Colloqium)

Shahid Mehraj Shah *

*Dept. of ECE, Indian Institute of Science, Bangalore

June 22nd 2015

Outline

Outline

How it began

- Conventional security measure taken at higher layer
- Cryptographic techniques depend on finiteness of computational power while Information theoretic security (ITS) promises provable security
- Wyner in 1975 Proposed a wiretap coding scheme for degraded Wiretap Channel[1]
- Security achieved at the cost of *rate loss*
- Wyner's result extended in several ways: BCC, MAC, IC, RC [2]
- Cost paid in each channel model is: *Rate Loss*
- In most of the work in ITS, Eve's complete channel knowledge is assumed
- Because of passive nature of Eve, this assumption not practical

[1] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, 1974.

[2] Y. Liang, H.V. Poor, S. Shamai, "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, 2009.

Motivation

- We try to address these two issues in our work
- To mitigate rate loss we propose alternate measure of secrecy and novel coding scheme.
- We use optimization techniques to allocate power with No CSI of Eve in MAC
- We also use Game theoretic learning to allocate resources with less information about Eve's channel state.

Outline

Channel Model: AWGN Wiretap Channel[1]

- Message $W \in \{1, \ldots, 2^{nR}\}$ to be transmitted securely & is encoded to $X^n = \{X_1, \ldots, X_n\}$.
- Bob receives $Y_i = X_i + N_{1i}$, $N_{1i} \sim \mathcal{N}(0, \sigma_1^2)$, *iid*, Eve receives $Z_i = X_i + N_{2i}$, $N_{2i} \sim \mathcal{N}(0, \sigma_2^2)$, *iid*, and $\sigma_1^2 < \sigma_2^2$
- Let $C_1 = 0.5 \log(1 + P/\sigma_1^2)$ and $C_2 = 0.5 \log(1 + P/\sigma_2^2)$
- Equivocation Based definition:
  - (R, R_e) is achievable if $\exists\ \mathcal{W}_n$ with $\mid \mathcal{W}_n \mid = 2^{nR}$ and encoder - decoder pairs (f_n, g_n) such that $P_e^{(n)} \to 0$, and the equivocation rate $lim_{n\to\infty} \frac{1}{n} H(W|Z^n) \geq R_e$
- Code design to satisfy equivocation rate is difficult. [2]
- To confuse Eve random messages are sent, which decreases the rate.

[2] Klinc, D., Ha, J., McLaughlin, S. W., Barros, J., & Kwak, B. J. "LDPC codes for the Gaussian wiretap channel." *IEEE Trans. on Info. Forensics and Sec., (2011)*

[1] Part of this work has been presented in IEEE ICCS 2012, Singapore

New Notion

- Natural Definition of secrecy: Probability of error for receiver $\rightarrow 0$ and that for eavesdropper $\rightarrow 1$.
- Strong converse: $R > C$, probability of error of decoding $\rightarrow 1$.
- Will use strong converse to formulate coding schemes.
- Eve is confused with the messages which are useful for Intended receiver,and Eve getting no message, i.e. no common information.
- Each message for Eve confused with same number of codewords as in Equivocation based approach

New Notion: Achieving Shannon Capacity

Proposition

All rates $R < C_1$ are achievable such that $P_e^n(B) \to 0$, $P_e^n(E) \to 1$ as $n \to \infty$.

- where $P_e^n(B)$ = Probability of decoding error at Bob, $P_e^n(E)$ = Probability of decoding error at Eve

Coding Scheme

- Region $C_2 < R < C_1$: generate n length *iid* Gaussian codewords with $X \sim \mathcal{N}(0, P)$
- $R < C_1$ ensures $P_e^n(B) \to 0$
- $R > C_2$, by strong converse, $P_e^n(E) \to 1$.
- To achieve rate $R < C_2$, select Gaussian P_X with power $< P$ such that $I(X;Y) > R > I(X;Z)$

Performance (via AEP decoder at Eve)

- N be the number of codewords other than that of message 1 that are jointly typical with Z^n
- $\mathrm{E}[N] = (2^{nR} - 1)2^{-nI(X;Z)}$ and $P_e^n(E) \approx 2^{n(R-I(X;Z))}$
- $P_e^n(E) \leq 2^{-n(C_1-C_2)}$ possible, maximum decay rate for equivocation based secrecy also.
- Higher R means more confusion for Eve.
- ML Decoding at Eve: If $x_1(1), ..., x_n(1)$ is transmitted, decode as message $\hat{m}$ if

$$\hat{m} = \arg\min \sum_{k=1}^{n} (Z_k - x_k(\hat{m}))^2 . \tag{1}$$

- Eve will confuse with $2^{n(R-C_2)}$ codewords . Max confusion as in AEP decoder.
- AEP and ML decoder best for Eve.

New Notion: Relation with Equivocation

- When $C_2 < R < C_1$, $P_e^n(B) \to 0$, and $P_e^n(E) \to 1$. Fano's Inequality gives: For Bob

$$\frac{1}{n} H(W|Y^n) \leq \frac{H(P_e^n(B))}{n} + P_e^n(B)R \tag{2}$$

- Lower bound: For Eve

$$H(W \mid Z^n) \geq \phi^*(\pi(W \mid Z^n)) \tag{3}$$

where ϕ^* is a piecewise linear, continuous, non-decreasing, convex function.[2]. $\pi(W \mid Z^n)$ is the average probability of error for the MAP decoder at Eve.

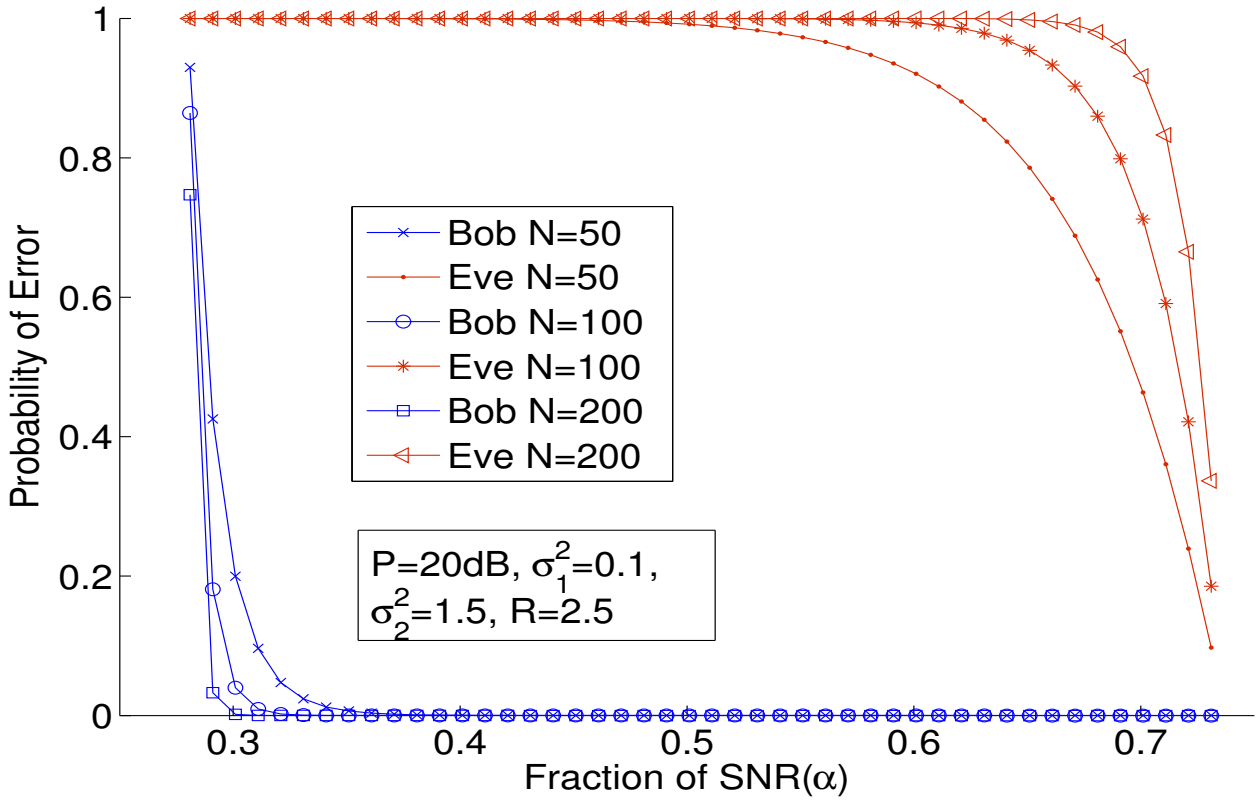
- From Arimoto's lower bound

$$\pi(W \mid Z^n) \geq 1 - e^{-n(E_0(\rho,p)-\rho R)}, \quad 0 \geq \rho \geq -1. \tag{4}$$

[2] M. Feder and N. Merhav, "Relations Between Entropy and Error Probability," *IEEE Trans. Inform. Theory. Jan. 1994*

Numerical Example

- For $\sigma_1^2 = 0.1$, $\sigma_2^2 = 1.5$, and $P = 20dB$, $P_e^n(B)$ and $P_e^n(E)$ are plotted for $n = 50, 100$ and 200.
- For $P_e^n(B)$ Gallagers random coding bound and for $P_e^n(E)$ Arimoto's lower bound are plotted



Fading Channel

- For the fading channel

$$Y_i = h_i X_i + N_{1i}, \quad Z_i = g_i X_i + N_{2i}, \tag{5}$$

,

- The capacity is ([gopala2008]):

$$C_s = \int_0^\infty \int_r^\infty [\log(1 + qP^*(q,r)) - \log(1 + rP^*(q,r))] f(q) f(r) dq dr \tag{6}$$

where $q(i) = |h(i)|^2$ and $r(i) = |g(i)|^2$ $E[P^*(q,r)] = P$,

Proposition

All rates $R < C_1$ are achievable such that $P_e^n(B) \to 0$ and $P_e^n(E) \to 1$ where

$$C_1 = \sup_{P(q,r)} \int_0^\infty \int_r^\infty [\log(1 + qP(q,r))] f(q) f(r) dq dr. \tag{7}$$

.

Outline

Discrete Memoryless Wiretap Channel[1]

- Yamamoto in 1997 used Wiretap coding and secret key to enhance secrecy rate in degraded Wiretap channel. [1]
- Kang and Liu (2010) extended Yamamoto's work to general broadcast channel [2].
- E. Ardestanizadeh et. al. (2008) used feedback from Bob to Alice to enhance secrecy rate [3].
- In this work we use previous secret messages as secret key to enhance the secrecy rate.

[1] H. Yamamoto, "Rate-distortion Theory For The Shannon Cipher System," *IEEE Trans. on Info. Theory*,May 1997.

[2] W. Kang, N. Liu,"Wiretap Channel with Shared Key," *2010 Info. theory Workshop, Dublin, 2010.*

[3] E. Ardestanizadeh et. al., "Wiretap Channel With Secure Rate-Limited Feedback," *IEEE Trans. on Info. Theory Dec. 2009.*

[1] Part of this work has been presented in IEEE ICC 2013 workshop on Physical Layer Security, Hungary

Channel Model

- $W \in \mathcal{W} = \{1, 2, \ldots, 2^{nR_s}\}$ is message set, where

$$R_s = \max_{p(x)} \left[I(X;Y) - I(X;Z) \right]. \tag{8}$$

- $\{W_m, m \geq 1\}$ is an independent sequence of messages to be transmitted.
- At time i: X_i the channel input, Y_i Channel O/P at Bob & Z_i Channel O/P at Eve.
- A mini-slot consists of n channel uses
- Each slot, upto λ, consists of 2 mini-slots where

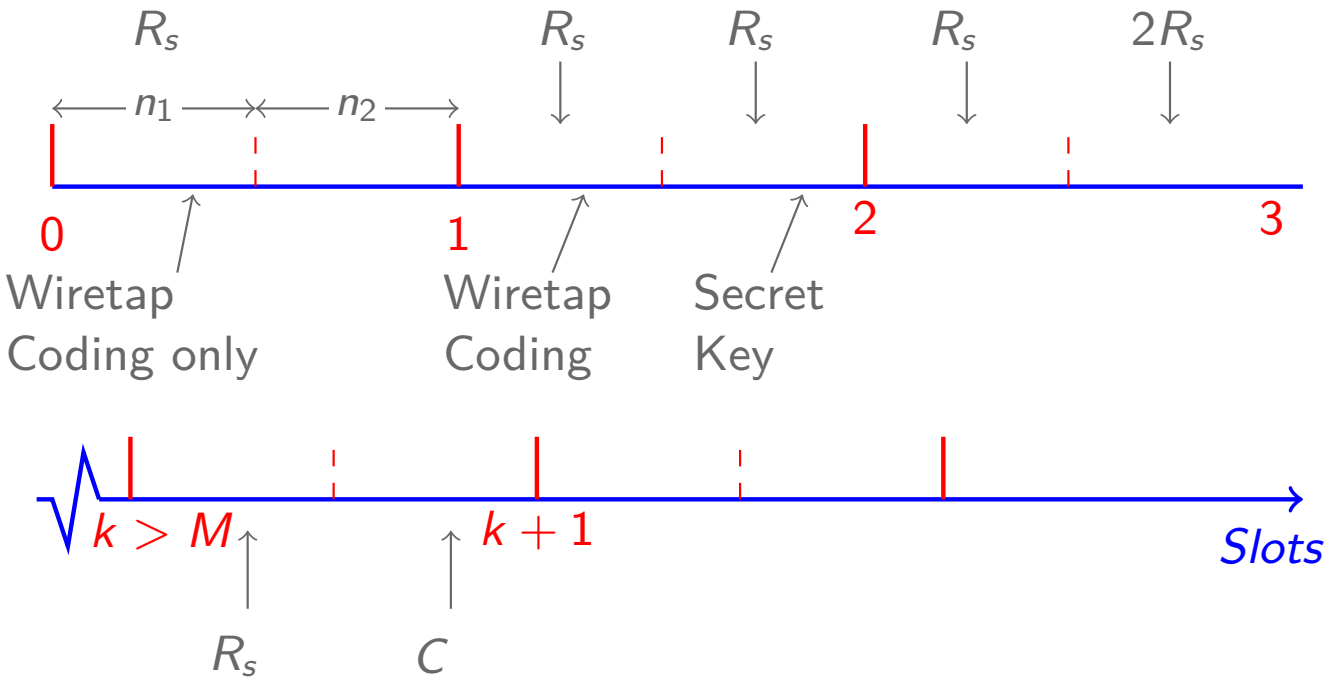
$$\lambda \triangleq \left\lceil \frac{C}{R_s} \right\rceil, \tag{9}$$

- After λ slots each slot has only one mini-slot.

Channel Model

- $\overline{W_k}$ to be transmitted in slot k consists of one or more messages W_m.
- Codeword for $\overline{W}_k$: $X_k^{2n} = \{X_{k1}, \ldots, X_{2kn}\}$ or X_k^n depending on the length of the slot.
- Transmitter uses the secret message $\overline{W}_k$ transmitted in slot k as the key for transmitting the message in slot $k+1$.

Encoder/Decoder



- Encoder: To transmit $\overline{W}_k$ in slot k, encoder has two parts

$$f_s : \mathcal{W} \to \mathcal{X}^n, f_d : \mathcal{W} \times \mathcal{K} \to \mathcal{X}^n, \tag{10}$$

  where $X \in \mathcal{X}$, and $\mathcal{K}$ set of secret keys generated and f_s is the Wiretap encoder
- Deterministic Encoder f_d: Encode *XOR* of message and binary version of the key optimal usual channel encoder.
- Slot 1:Message encoded using the wiretap code only.
- Slot k: $(1 < k \leq \lambda)$, both f_s and f_d used simultaneously.

Encoder/Decoder

- Slot 1: Decoder function at Bob is

$$\phi_1 : \mathcal{Y}^{2n} \to \mathcal{W}. \tag{11}$$

- Slot k: $(k > 1)$, decoder is

$$\phi_i : \mathcal{Y}^n \times \mathcal{K} \to \mathcal{W}^j \tag{12}$$

for time slot i, with $j = \min(i, \frac{C}{R_s})$.

- Probability of error:

$$P_e^{(n)} = Pr\{\widehat{W} \neq \overline{W}\} \tag{13}$$

where $\widehat{W}$ is the decoded message.

Achievable Rate

- Leakage rate is $R_L^n = \frac{1}{n} I(\overline{W}; Z^{2n})$.

Definition

A Leakage-rate pair (R_L, R) is said to be achievable if there exists a sequence of $(2^{nR}, n)$-codes such that $P_e^{(n)} \to 0$ and $\limsup_{n\to\infty} R_L^n \leq R_L$ as $n \to \infty$.

Theorem

Any rate $< \ C$ is achievable for all slots $k \geq \lambda$.

- Slot 1: Alice picks message W_1 from $\mathcal{W}$ and transmits this message using $(n, 2^{nR_s})$-Code.
- Slot 2: *using the previous message*, $\overline{W}_1 = W_1$, as a key (with key rate $R_k = R_s$) Alice transmits message $\overline{W}_2 = (W_{21}, W_{22})$, where $W_{21} = W_2, W_{22} = W_3$ are taken from the *iid* sequence $\{W_k, k \geq 1\}$.

Coding Scheme Contd.

- 1st message W_{21} is encoded to X_{21}^n using wiretap code.
- 2nd message W_{22} is first encrypted to produce the cipher using one-time pad with the previous message as secret key, i.e., $\widetilde{W}_{22} = W_{22} \bigoplus W_1$
- We encode this encrypted message to X_{22}^n using a point-to-point optimal channel code
- We continue this till $\lambda - 1$ slots. In slot $\lambda - 1$, we transmit message $(W_{\lambda-1,1}, W_{\lambda-1,2}, ..., W_{\lambda-1,\lambda-1})$.
- Total rate:

$$\frac{1}{2}\left(R_s + (\lambda - 1)R_s\right) = \frac{1}{2}\left(R_s + C\right). \tag{14}$$

- Bob (Decoder): In slot k, (for $1 < k < \lambda$) Y_{k1}^n is decoded via usual wiretap decoding while Y_{k2}^n is decoded first by the channel decoder and then XORed with $\widehat{W}_{k-1}$

Error Analysis

- ϵ_n = message error probability for the wiretap encoder and δ_n = message error probability due to the channel encoder for W_k
- Slot k: $(1 < k < \lambda - 1)$, $P(\overline{W}_k \neq \widehat{W}_k) \leq Pr(\text{Error in decoding } W_{k1}) + Pr(\text{Error in decoding } \widetilde{W}_{k2}) + Pr(\text{Error in decoding } \overline{W}_{k-1}) \leq k\epsilon_n + (k-1)\delta_n$.
- Error upper bound increases with k
- Restarting (as in slot 1) after some k slots ($> \lambda$) will ensure that $P(\overline{W}_k \neq \widehat{W}_k) \to 0$ as $n \to \infty$.

Leakage Rate Analysis

- We show
$$\frac{1}{n} I(\overline{W}_k; Z_1^n, Z_2^{2n}, ..., Z_k^{2n}) \to 0 \tag{15}$$
as $n \to \infty$
- Slot 1: Wire-tap coding is used, hence $\frac{1}{n} I(\overline{W}_1; Z_1^n) \to 0$, as $n \to \infty$.
- slot 2:
$$\frac{1}{n} I(\overline{W}_1; Z_1^n, Z_2^{2n}) \to 0 \tag{16}$$
- We use mathematical induction to show that $\frac{1}{n} I(\overline{W}_m; Z_1^n, Z_2^{2n}, ..., Z_{k+1}^{2n}) \to 0$ for all $m \leq k+1, k \geq 1$

Strong Secrecy

- Same secrecy rate can be achieved even with *strong secrecy*.
- Use *Resolvability based codes*[4] in the first slot.
- In the subsequent blocks we use both the stochastic encoder and the deterministic encoder

[4] Bloch, M and Laneman, N, "Strong Secrecy from Channel Resolvability," *IEEE Transactions on Information Theory*, vol. 51, no. 1, pp. 44–55, May 2011.

Wiretap Channel with Secret Key Buffer

- We now consider the following model

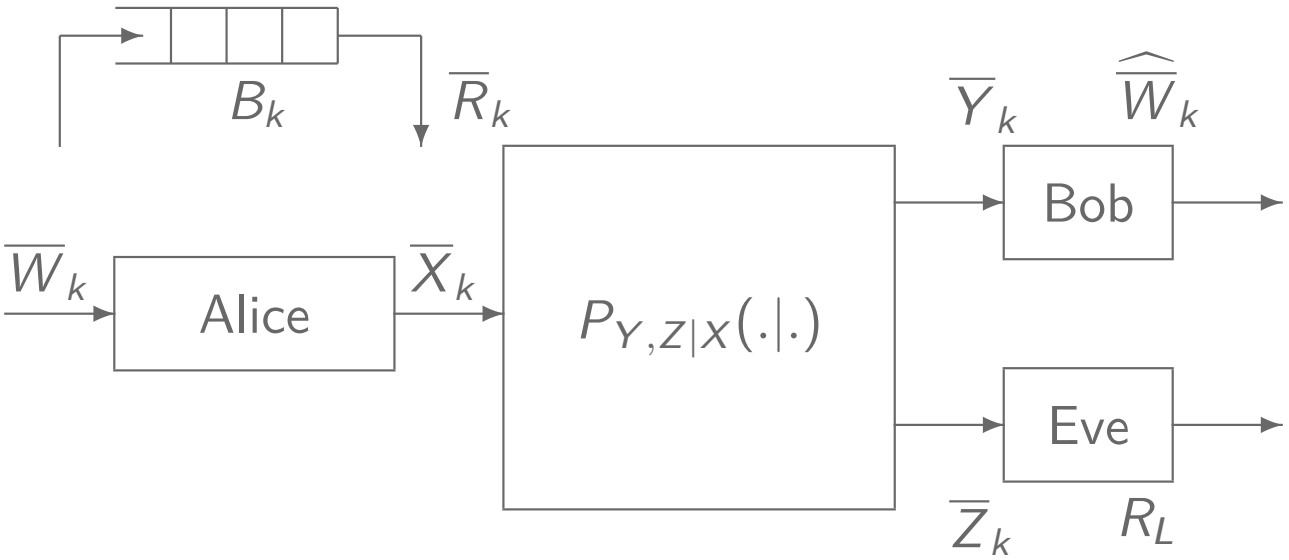


Figure : Wiretap Channel with secret key buffer

- In slot k message $\overline{W}_k$ is stored in key buffer.
- B_k=# of bits in buffer in beginning of slot k,
- $\overline{R}_k$=# of bits used as secret key in slot k, then

$$B_{k+1} = B_k + |\overline{W}_k| - \overline{R}_k, \text{ where } |\overline{W}_k| = \# \text{ of bits in} |\overline{W}_k|. \quad (17)$$

- In slot k, $(k-1)R_s n$ bits from buffer removed, $kR_s n$ bits added.
- Message $\overline{W}_k = (\overline{W}_{k,1}, \overline{W}_k, 2)$ transmitter s.t. $\overline{W}_{k,1}$ via wiretap coding, $\overline{W}_{k,2}$ via secret key.
- Key buffer used as a FIFO queue, also $B_k \infty$ as $k \to \infty$.

- Aim is to make secrecy criterion stronger:

$$\frac{1}{n} I\left(\overline{W}_k, \ldots, \overline{W}_{k-N_1}; \overline{Z}_1, \ldots, \overline{Z}_k\right) \to 0 \text{ as } n \to \infty. \tag{18}$$

  for some $k > N_1$, N_1 is arbitrarily large integer.
- We now have the following result

Theorem

The secrecy capacity of our coding-decoding scheme is C and it satiafies (18) for any $N_1 \geq 0$, for all k large enough.

- We use the oldest key bits in buffer (not more than MC bits), after $k \geq N_2$ we use key bits from $\overline{W}_1, \overline{W}_2, \ldots, \overline{W}_{k-N_1-1}$ for messages $\overline{W}_k, \overline{W}_{k-1}, \ldots, \overline{W}_{k-N_1}$.
- can extend to strong secrecy by using resolvability based coding.

AWGN Slow Fading Wiretap Channel

- We consider Fading channel

$$Y_i = \widetilde{H}\, X_i + N_{1i}, \;\; Z_i = \widetilde{G}\, X_i + N_{2i}, \tag{19}$$

- X_i channel i/p, $N_{ki} \sim \mathcal{N}(0, \sigma_k^2)$, $k = 1, 2$ and $H = |\widetilde{H}|^2$, $G = |\widetilde{G}|^2$.
- we define $C(P(H,G)) = \frac{1}{2}\log\left(1 + \frac{HP(H,G)}{\sigma_1^2}\right)$, $C_e(P(H,G)) = \frac{1}{2}\log\left(1 + \frac{GP(H,G)}{\sigma_2^2}\right)$,
- Now we have following result

Theorem

The secrecy rate

$$C_s = \mathrm{E}_H\left[C(P(H))\right] \tag{20}$$

is achievable if $Pr(H_k > G_k) > 0$, where $P(H) = P(H,G)$ is the water-filling power policy for Alice $\rightarrow$ Bob channel.

Fading Wiretap Channel: No CSI of Eve

- Here we assume the coherence time of (H_k, G_k) is much smaller than the duration n of a minislot
- We use the coding-decoding scheme developed earlier in first minislot with secrecy rate R_s, where $R_s = \frac{1}{2}\mathrm{E}_{H,G}\left[C(P(H,G)) - C_e(P(H,G))\right].$
- We have the following proposition

Proposition

Secrecy capacity equal to the main channel capacity without CSI of Eve at the transmitter

$$C = \frac{1}{2}\mathrm{E}_H\left[\log\left(1 + \frac{HP(H)}{\sigma_1^2}\right)\right] \tag{21}$$

is achievable subject to power constraint $\mathrm{E}_H\left[P(H)\right] \leq \bar{P}$, where $P(H)$ is the waterfilling policy.

Outline

Multiple Access Channel with Eve[1]

- Gaussian MAC with eavesdropper studied by Yener and Tekin(IEEE trans 2008)
- Co-operative jamming improves secrecy sum-rate
- Fading MAC with full CSI of eavesdropper studied by Yener and Tekin
- In general, Secrecy Capacity region for MAC not known.

[1] Part of this work has been presented in IEEE SPCOM 2012, Bangalore, India

Multiple Access Channel with Eve

- 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

$$R_1 \leq [I(U_1; Y \mid U_2) - I(U_1; Z)]^+ \tag{22}$$

$$R_2 \leq [I(U_2; Y \mid U_1) - I(U_2; Z)]^+ \tag{23}$$

$$R_1 + R_2 \leq [I(U_1, U_2; Y) - I(U_1, U_2; Z)]^+ \tag{24}$$

- 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

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

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

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

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

- $\mathrm{E}\left[P_i(h,g)\right] \leq \bar{P}_i, i=1,2.$ Gaussian signalling is used.

Fading MAC without CSI of eve

- In passive attack of Eavesdropper, CSI cannot be estimated
- In single user wiretap channel, H.E Elgamal(IEEE trans 2008) reports secrecy capacity with optimal power control with main channel CSI only
- Mathew Bloch et. al(IEEE trans 2008) studied outage analysis of single user slow fading channel with imperfect CSI of eve.
- We study fading MAC which achieve secrecy sum rate without knowing CSI of eve.

Fading MAC without CSI of eve: Optimal power allocation

- $\phi^{s}_{x_1,x_2} = 1 + s_1 x_1 + s_2 x_2$ where s is the channel state (h or g) and x_k is the power used.

Theorem

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

$$\mathrm{E}_{h,g}\left\{\left[\log\left(\frac{\phi^{h}_{P_1,P_2} + \phi^{h}_{Q_1,Q_2} - 1}{\phi^{g}_{P_1,P_2} + \phi^{g}_{Q_1,Q_2} - 1}\right)\left(\frac{\phi^{g}_{Q_1,Q_2}}{\phi^{h}_{Q_1,Q_2}}\right)\right]^{+}\right\} \tag{25}$$

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

- Optimal policy is not available in closed form. Can be computed numerically.

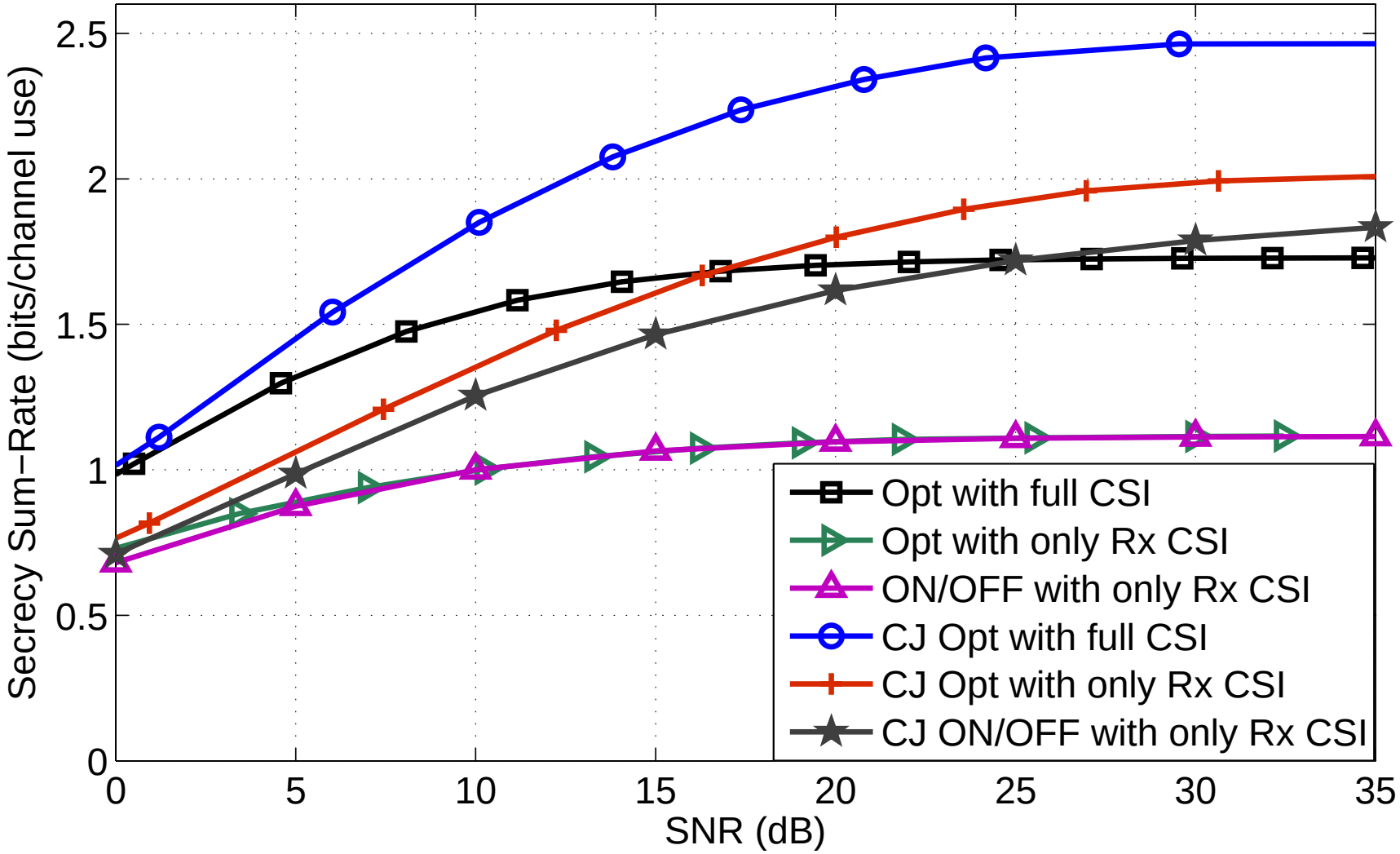
Fading MAC without CSI of eve: Optimal power control with Cooperative Jamming

- $\{P_k(h)\}$, $k = 1, 2$, policy when users transmit and $\{Q_k(h)\}$,when users jam
- Cooperative Jamming substantially improves secrecy sum-rate.

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;
  - $h_i > \tau_i$, $h_j < \tau_j$, $j \neq i$: User-i transmits;
  - $h_1 < \tau_1$, $h_2 < \tau_2$: No user transmits.
- Optimize the secrecy sum-rate over τ_1, τ_2
- We also employ co-operative jamming over ON/OFF scheme

Fading MAC Without CSI of Eve: Simulation results



Outline

Fading MAC without security constraint

- Power allocation in Fading MAC well known
- Tse & Hanly assumes Global CSI available at Tx
- They use Polymatroid theory
- H El Gamal et al use Game theory for distributed power control
- They also assume Global CSI
- Altman et al assume partial CSI, use Bayesian Game theory

- We consider K- user fading, discrete time MAC

$$Y(t) = \sum_{i=1}^{K} H_i(t) X_i(t) + \eta(t), \tag{26}$$

- $X_i(t)$ channel i/p, $\eta(t)$ is WGN $\sim \mathcal{N}(0, \sigma^2)$
- Fading process $H_i(t) \in \mathcal{H}_i \triangleq \{h_i^{(1)}, \ldots, h_i^{(M)}\}$ for user i with pmf $\{\rho_i^{(1)}, \ldots, \rho_i^{(M)}\}$

- User i transmits at fixed rate r_i
- Receiver uses succesive decoding in following order
- Arranges users in increasing order of channel gains
- Let π be permutation on $\mathcal{K}$ s.t. $h_{\pi(1)} \geq h_{\pi(2)} \geq \ldots, fh_{\pi(K)}$
- Receiver sends ACK to user $\pi(i)$ if

$$r_{\pi(i)} \leq \frac{1}{2} \log \left(1 + \frac{h_{\pi(i)} P_{\pi(i)}(h_\pi(i))}{\sigma^2 + \sum_{j=i+1}^{K} h_{\pi(j)} P_{\pi(j)}(h_\pi(j))} \right) \tag{27}$$

$$\tag{28}$$

- Reward of user i in time slot t

$$\omega_i^{(t)}\left(a_i^{(t)}, h_i(t)\right) = \begin{cases} 1, & \text{If user } i \text{ receives ACK} \\ 0, & \text{else} \end{cases}$$

- Average utility is

$$\nu_i\left(P_i, P_{-i}\right) \triangleq \limsup_{T\to\infty} \frac{1}{T}\sum_{t=1}^{T} \omega_i^{(t)}\left(P_i, H_i(t)\right) = \mathrm{E}\left[\omega_i^{(t)}\left(P_i, H_i\right)\right], \tag{29}$$

- By WLLN Probability of successful transmission $= \nu_i\left(P_i, P_{-i}\right)$.

- Goal of each user

$$\max_{a_i} \nu_i \left(P_i, P_{-i}\right) \tag{30}$$

$$\text{subject to } a_i \in \mathcal{P}_i \tag{31}$$

- This is a stochastic game $\mathfrak{G} = \langle \mathcal{K}, \mathcal{P}_i, \{\nu_i\} \rangle$.
- We would like to find ϵ-Coarse Correlated Equilibrium (CCE), defined as

Definition

If a distribution ψ on $\mathcal{P}$ satisfy the following inequality

$$\mathrm{E}_{a\sim\psi}\left[C_{\pi(i)}\left(a\right)\right] \leq \mathrm{E}_{a\sim\psi}\left[C_{\pi(i)}\left(\hat{a}_{\pi(i)}, a_{-\pi(i)}\right)\right] + \epsilon \tag{32}$$

then it is called $\epsilon-$*coarse correlated equilibrium* for each user $\pi(i), i \in \{1, \ldots, K\}$, and every action $a_{\pi(i)}, \hat{a}_{\pi(i)} \in \mathcal{P}_{\pi(i)}$.

- We use Multiplicative Weight No-regret algorithm to obtain CCE

1: $\omega_i^{(t)} \leftarrow 1, \; i = 1, 2, \ldots, K$

2: User i: Choose action $w.p.$ $\Phi_i^{(t)} = \frac{\omega_i^{(t)}(a_i)}{\sum_{\hat{a} \in \mathcal{P}_i} \omega_i^{(t)}(\hat{a}_i)}$

3: Time t: User i receives average utility for choosing a_i
$\nu_i^{(t)} = \mathrm{E}_{a_{-i} \sim \; _{-i}}[C(a_i, a_{-1})]$

4: Update the weight

5: $\omega_i^{(t+1)} = \omega_i^{(t)}(a_i)(1-\epsilon)^{c_i^{(t)(a_i)}}$

6: Time $t+1$: Calculate $\psi_t = \prod_{i=1}^{K} \Phi_i^{(t)}$

Pareto Optimal Points

- We first define

$$\Omega(a) = \sum_{i=1}^{K} \gamma_i \nu_i(a) \tag{33}$$

- Goal is to obtain

$$\max_{a} \quad \Omega(a)$$
$$\text{subject to } a \in \mathcal{P}. \tag{34}$$

- The equilibrium obtained is Pareto optimal, defined as

Pareto optimality

An action profile $a \in \mathcal{P}$ is Pareto optimal if there does not exist another profile $\tilde{a}$ such that $\nu_i(\tilde{a}) \geq \nu_i(a)$, $\forall\ i \in \mathcal{K}$ and $\nu_j(\tilde{a}) > \nu_i(a)$ for $j \neq i$.

- We use distributed algorithm to obtain Pareto points

Distributed Algorithm I

$OUTER\_ITER = 1$,User i: choose $a_i \in \mathcal{P}_i$ uniformly.
Use a_i for T time slots.
Update weight of each user i
$\hat{\Omega}(a) \leftarrow \sum_{i=1}^{K} \gamma_i \left(\frac{1}{T} \sum_{t=1}^{T} \omega_i^{(t)}(a_i, H_i(t)) \right)$
After T slots: $INNER\_ITER = 1$, User i experiments $w.p.$ P_{exp}
    $w.p$ ϵ choose $a_i' \neq a_i$, $a_i' \in \mathcal{P}_i$
    $w.p.$ $1 - \epsilon$
        choose $a_i' \neq a_i$ s.t. h_i with high α_i gets higher power level
        If α_i same for all h_i, then higher value of channel state gets higher
        power level.
        Call new action $\hat{a}_i$
        User i: use $\hat{a}_i$ for T time slots.

Distributed Algorithm II

12: User j: use a_j for T time slots, $j \neq i$.
13: User i: find $\hat{\Omega}(\hat{a}_i, a_{-i})$
14: **if** $\hat{\Omega}(\hat{a}_i, a_{-i}) > \hat{\Omega}(a_i, a_{-i})$ **then**
15: $\quad a_i \leftarrow \hat{a}_i$
16: $\quad P_{benchmark} = \hat{\Omega}(\hat{a}_i, a_{-i})$
17: **else**
18: $\quad$ Randomly select another action
19: **end if**
20: $INNER\_ITER = INNER\_ITER + 1$, **goto** step 5 till $INNER\_ITER = MAX$
21: $OUTER\_ITER = OUTER\_ITER + 1$, **goto** step 1 till $OUTER\_ITER = M$

Nash Bargaining Solution

- consider the strategic game $\mathfrak{G} = \langle \mathcal{K}, \mathcal{P}_i, \{\nu_i\} \rangle$ where users cooperate.
- we need to specify *disagreement* outcome
- We define the set of all possible utulities as

$$\mathcal{V} = \{(\nu_1(a), \ldots, \nu_K(a)) : a \in \mathcal{P}\} \tag{35}$$

- disagreement action vector as $\delta = (\delta_1, \ldots, \delta_K)$ where $\delta_i = \xi_i(\Delta), i = 1, \ldots, K$, and where Δ is disagreement action.
- Bargaining problem is $(\mathcal{V}, \delta)$
- Aim is to find some function, ξ, that specifies a bargaining outcome $\xi(\mathcal{V}, \delta)$ for every bargaining problem $(\mathcal{V}, \delta)$ that satisfies the following axioms.

A-1 *Pareto efficiency*:

A-2 *Symmetry*:

A_3 *Invariance*:

A-4 *Independence of irrelevant alternatives*:

Existence of Nash Equilibrium

There exists a unique bargaining solution (provided feasible region is non-empty) that satisfy $A1 - A4$ and it is given by the solution of the following optimization problem[a]

$$\begin{aligned} &\max \ (\nu_1 - \delta_1)(\nu_2 - \delta_2) \\ &\text{subject to } \nu_i \geq \delta_i, i = 1, 2 \\ &(\nu_1, \nu_2) \in \mathcal{V} \end{aligned} \tag{36}$$

[a] Nash Jr, John F, "The bargaining problem," *Econometrica*, 1950.

- Generalized to $K-$player

$$\max \prod_{i=1}^{K}(\nu_i - \delta_i) \text{ subject to } \nu_i \geq \delta_i, i = 1, \ldots, K \ (\nu_1, \ldots, K) \in \mathcal{V}. \tag{37}$$

- Since the set $\mathcal{V}$ is convex, hence NBS is proportionally fair also.

Fading MAC-WT

- The channel model is

$$Y(t) = \sum_{i=1}^{K} \widetilde{H}_i(t) X_i(t) + \eta_b(t) \tag{38}$$

$$Z(t) = \sum_{i=1}^{K} \widetilde{G}_i(t) X_i(t) + \eta_e(t) \tag{39}$$

- $\eta_b(t), \eta_e(t) \sim \mathcal{N}(0,1)$, $H_i(t) \triangleq |\widetilde{H}_i(t)|$ and $G_i(t) \triangleq |\widetilde{G}_i(t)|$
- $H_i(t) \in \mathcal{H}_i \triangleq \{h_i^{(1)}, \ldots, h_i^{(M_i^{(H)})}\}$ with probabilities $(w.p.)$ $\{\alpha_i^{(1)}, \ldots, \alpha_i^{(M_i^{(H)})}\}$
- $G_i(t) \in \mathcal{G} \triangleq \{g_i^{(1)}, \ldots, g_i^{(M_i^{(G)})}\}$ $w.p.$ $\{\beta_i^{(1)}, \ldots, \beta_i^{(M_i^{(G)})}\}$

- Power can be choosen from $\mathcal{P}_i \triangleq \{P_i^{(1)}, \ldots, P_i^{(M)}\}$ subject to

$$\sum_{j=1}^{K} \alpha_i^{(j)} \beta_i^{(j)} P_i^{(j)} \leq \overline{P}_i. \tag{40}$$

- Receiver decodes via succesive decoding in the increasing order of main channel gain.
- We define

$$C_b\left(P_{\pi(i)}, H_{\pi(i)}\right) \triangleq \frac{1}{2}\log\left(1 + \frac{H_{\pi(i)} P_{\pi(i)}(H_{\pi(i)}, G_{\pi(i)})}{1 + \sum_{j=i+1}^{K} H_{\pi(j)} P_{\pi(j)}(H_{\pi(j)}, G_{\pi(j)})}\right) \tag{41}$$

$$C_e\left(P_{\pi(i)}, G_{\pi(i)}\right) \triangleq \frac{1}{2}\log\left(1 + \frac{G_{\pi(i)} P_{\pi(i)}(H_{\pi(i)}, G_{\pi(i)})}{1 + \sum_{j\neq i}^{K} G_{\pi(j)} P_{\pi(j)}(H_{\pi(j)}, G_{\pi(j)})}\right) \tag{42}$$

- Receiver sends ACK to user $\pi(i)$ if

$$r_{\pi(i)} \leq \left(C_b(P_{\pi(i)}, h_{\pi(i)}, g_{\pi(i)}) - C_e(P_{\pi(i)}, h_{\pi(i)}, g_{\pi(i)})\right)^+ \tag{43}$$

- Feasible Action Space

$$\mathcal{P}_i = \left\{ \mathbf{P}_i = (P_i^{(1)}, \ldots, P_i^{(M)}) : P_i^{(k)} \in \{p_i^{(1)}, \ldots, p_i^{(M)}\}, \sum_{j=1}^{M} \alpha_i(j)\beta_i^{(j)} P_i^{(j)} \leq \overline{P}_i \right\} \tag{44}$$

Fading-MAC without CSI of Eve

- Outage based metric

$$P_O^S \triangleq Pr\left\{r_i > C_b\left(P_{\pi(i)}, H_{\pi(i)}\right) - C_e\left(P_{\pi(i)}, G_{\pi(i)}\right)\right\} \tag{45}$$

- We define

$$\Gamma = \frac{1}{2^{r_{\pi(i)}}}\left(1 + \frac{h_{\pi(i)}p_{\pi(i)}}{1 + \sum_{j=i+1}^{K} h_{\pi(j)}p_{\pi(j)}}\right) \tag{46}$$

- Hence

$$P_O^S = Pr\left\{1 + \frac{g_{\pi(i)}p_{\pi(i)}}{1 + \sum_{j\neq i}^{K} g_{\pi(j)}p_{\pi(j)}} > \Gamma\right\} \tag{47}$$

- Now the receiver send ACK if $P_o^S < \epsilon$, else NACK.
- Utility is now defined as

$$\omega_{\pi(i)}\left(a_{\pi(i)}^{(t)}, h_{\pi(i)}(t)\right) = 1_{\{P_O^S < \epsilon\}} \tag{48}$$

Simulation Results: MAC without Eve

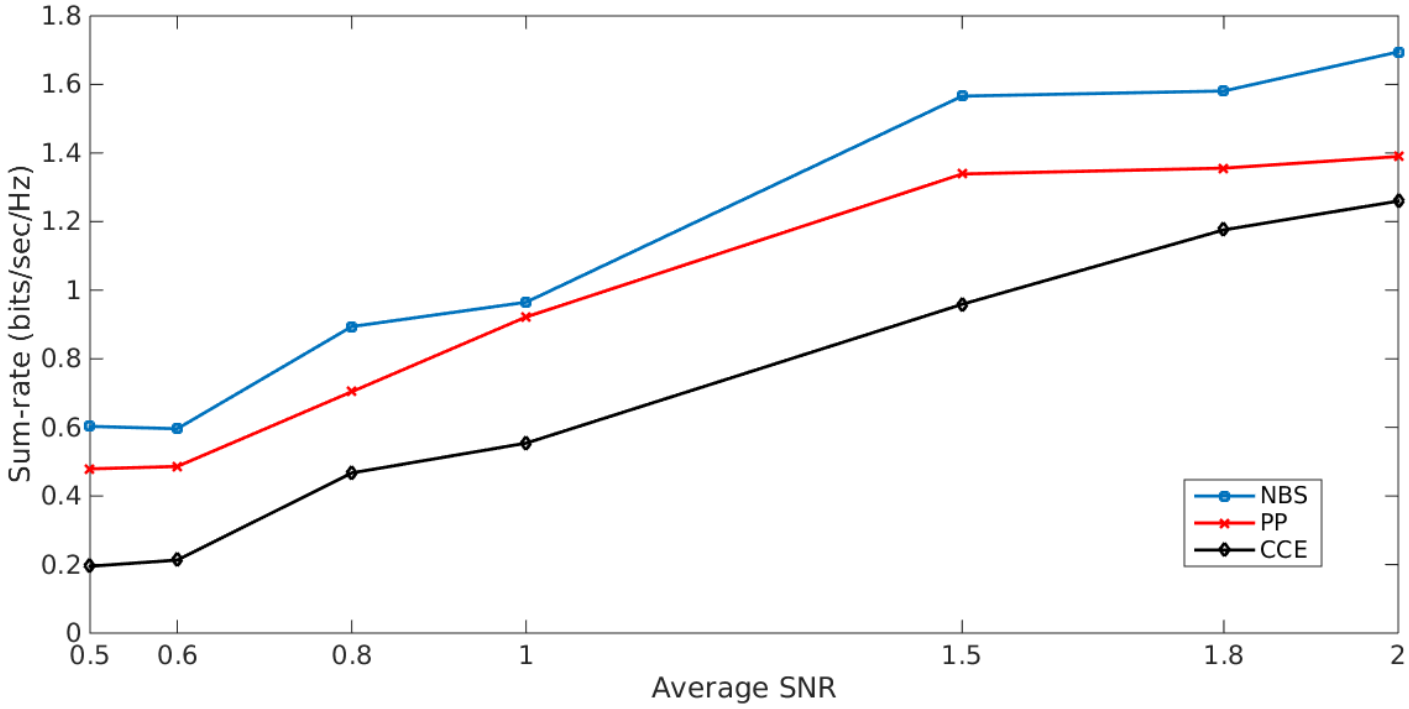


Figure : Comparision of Sum-Rate in Fading MAC without Eve: Fixed rate transmission

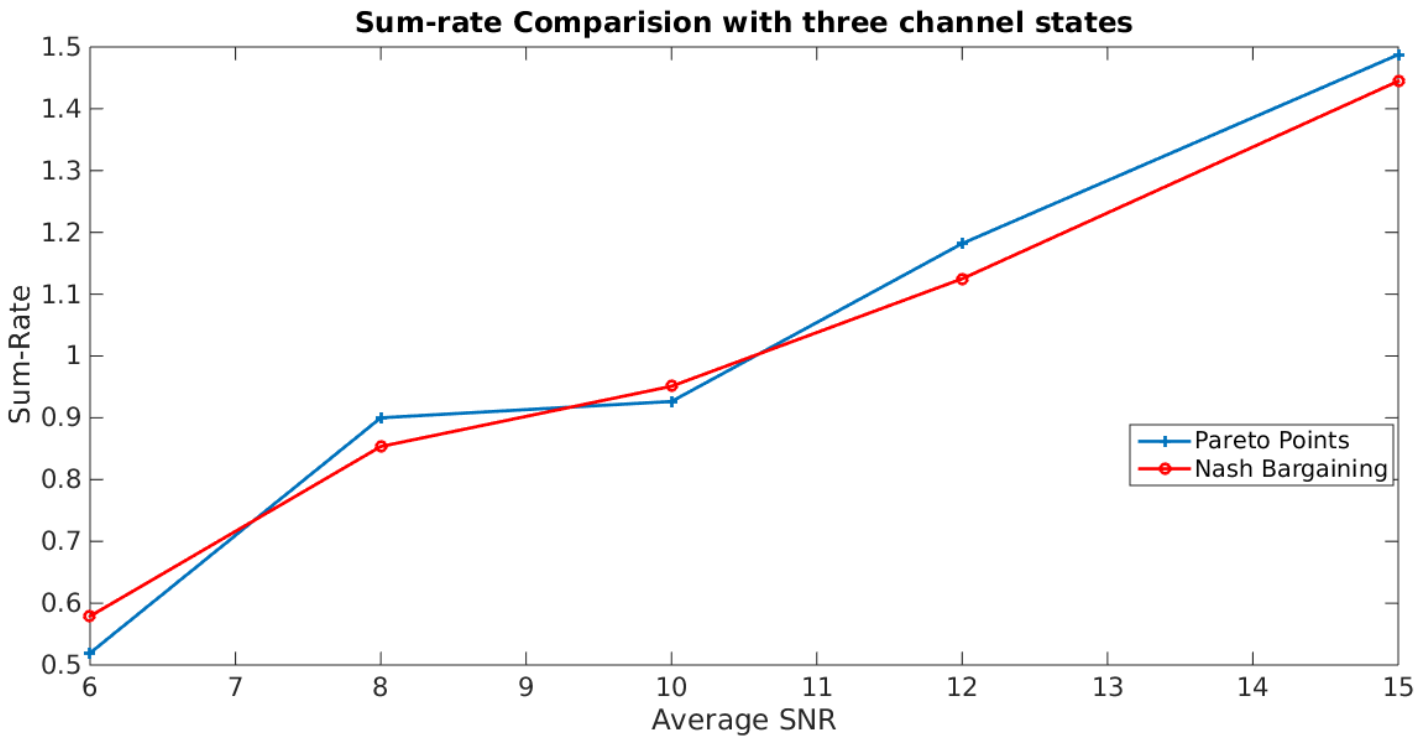


Figure : Sum-rate comparision: Multiple rate (3 states)

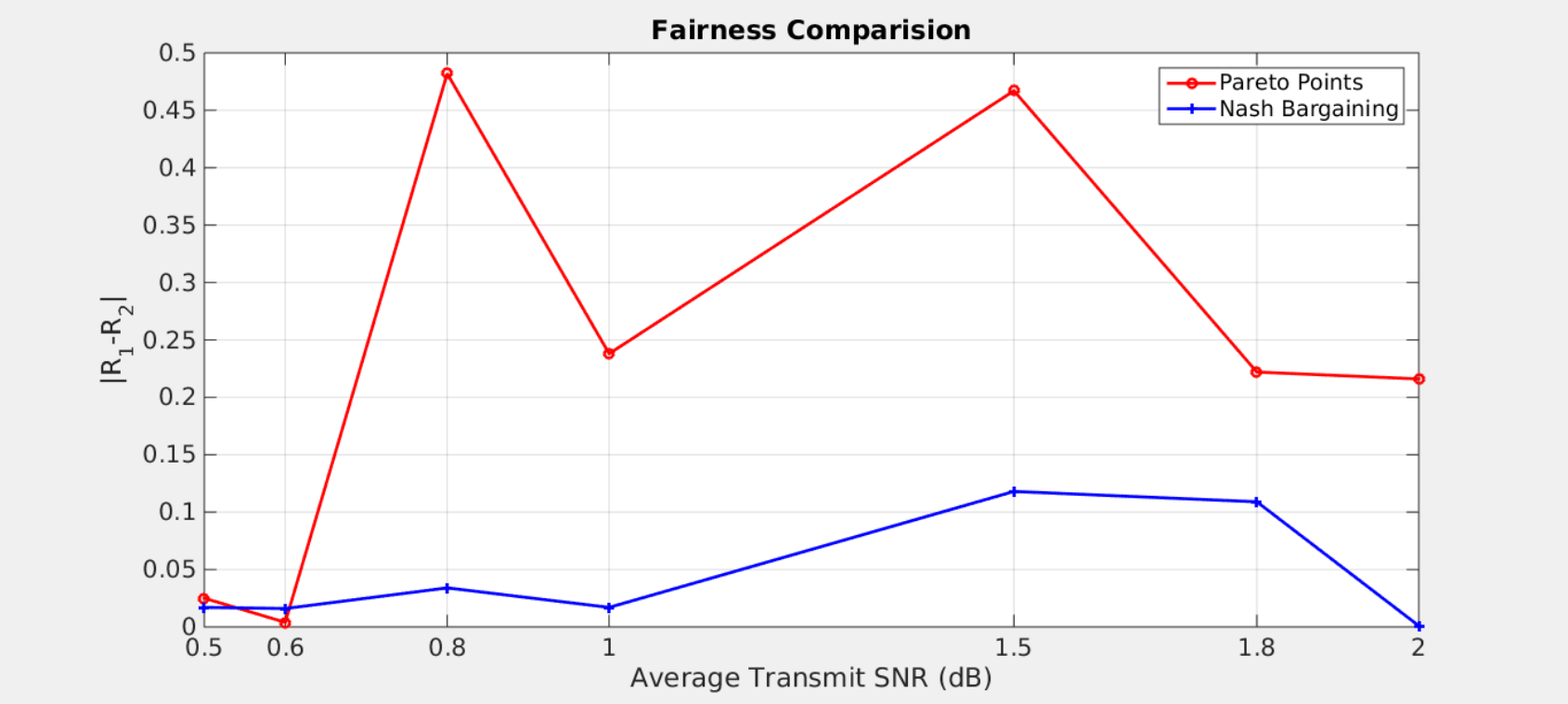


Figure : Comparision of Fairness b/w NBS and PP

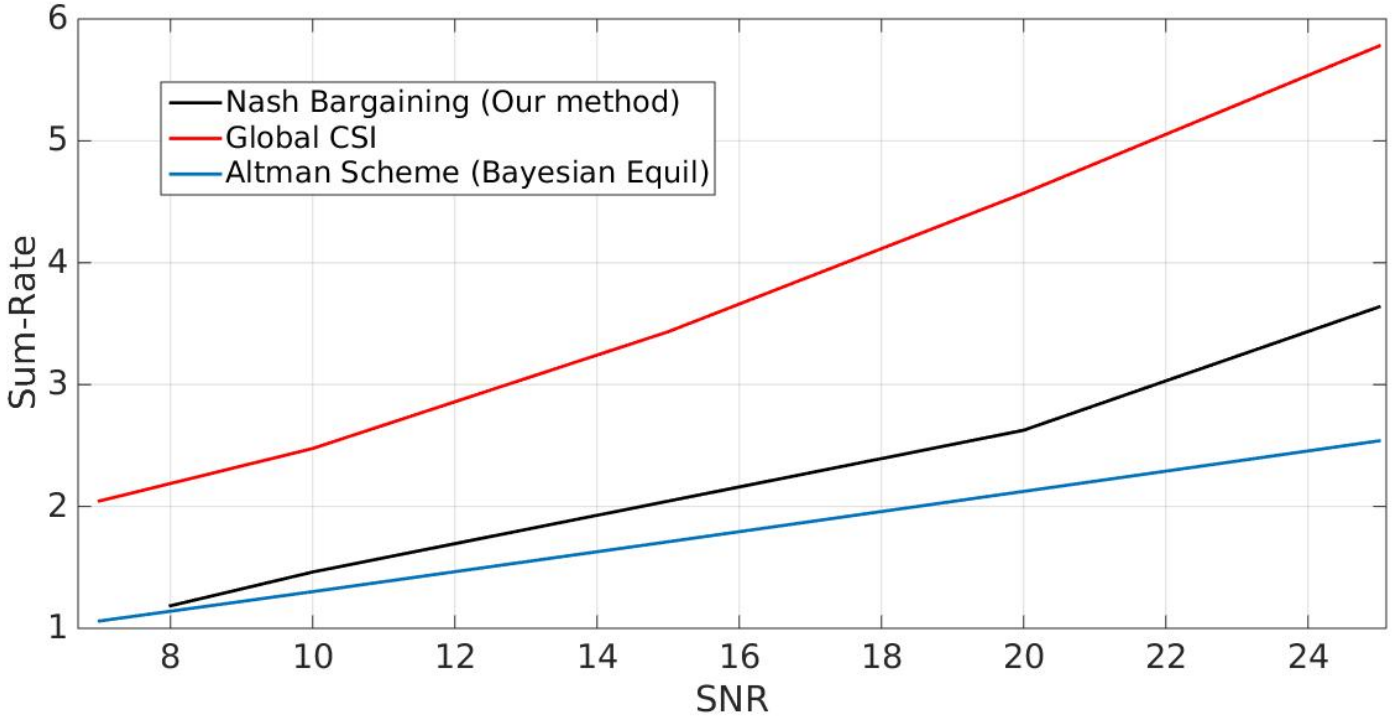


Figure : Fading MAC without Eve: Comparision with other schemes (Multiple rate transmission)

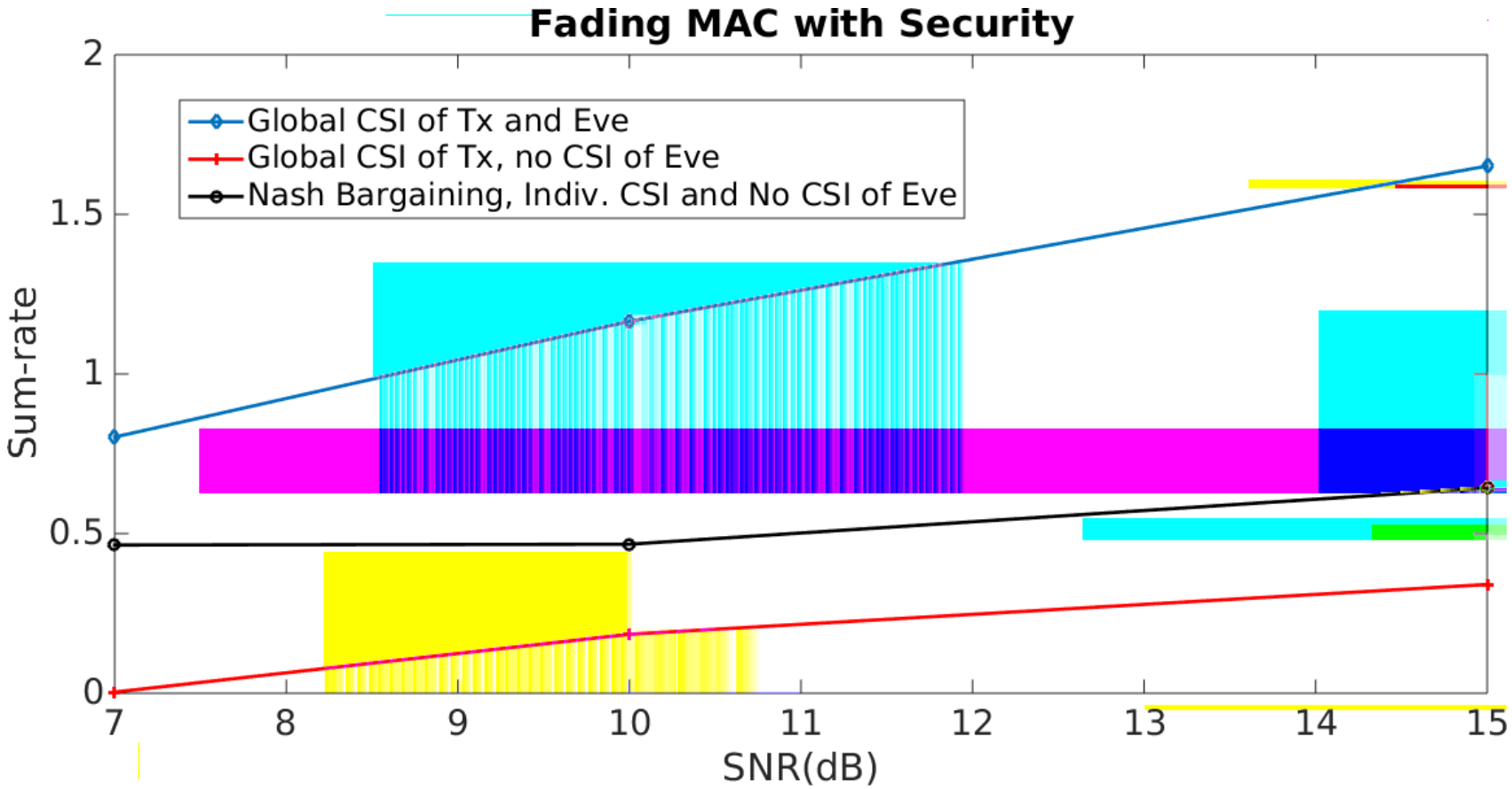


Figure : Fading MAC-WT: Comparision with full CSI and other scheme (Multiple rate)

Outline

Discrete Memoryless Wiretap Channel[1]

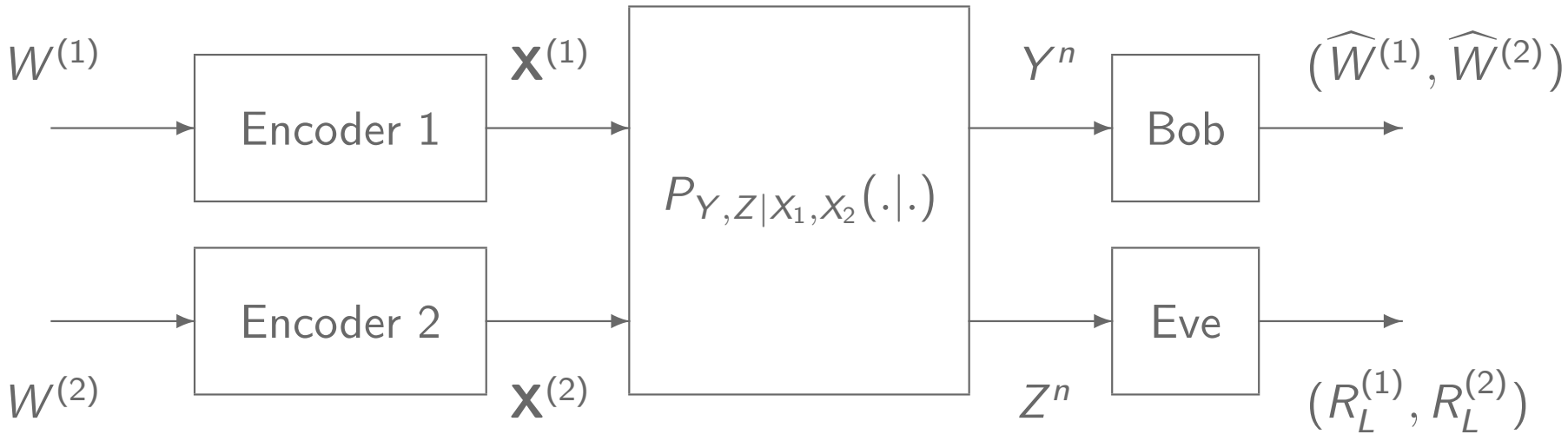


Figure : Discrete Memoryless Multiple Access Wiretap Channel

[1] Part of this work has been presented in IEEE WCNC 2015, New Orleans, USA

Codebook for MAC-WT

MAC-WT

- 2-user MAC-WT $(\mathcal{X}_1 \times \mathcal{X}_2, p(y,z|x_1,x_2), \mathcal{Y}, \mathcal{Z})$, $\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}, \mathcal{Z}$ are finite sets and $p(y,z|x_1,x_2)$ is the collection of t.p.m
- 2 users want to send messages $W^{(1)}$ and $W^{(2)}$ to Bob reliably, keeping Eve ignorant
- $(2^{nR_1}, 2^{nR_2}, n)$ codebook consists of
  - Message sets $\mathcal{W}^{(1)}$ and $\mathcal{W}^{(2)}$ of cardinality 2^{nR_1} and 2^{nR_2}
  - Two independent Messages $W^{(1)}$ and $W^{(2)}$, uniformally distributed over $\mathcal{W}^{(1)}$ and $\mathcal{W}^{(2)}$
  - stochastic encoders,

$$f_i : \mathcal{W}^{(i)} \to \mathcal{X}_i^n \quad i = 1, 2, \tag{49}$$

Codebook for MAC-WT

MAC-WT

- 4) Decoder at Bob:

$$g : \mathcal{Y}^n \to \mathcal{W}^{(1)} \times \mathcal{W}^{(2)}. \tag{50}$$

- average probability of error at Bob is

$$P_e^{(n)} \triangleq P\left\{\left(\widehat{W}^{(1)}, \widehat{W}^{(2)}\right) \neq \left(W^{(1)}, W^{(2)}\right)\right\}. \tag{51}$$

- *Leakage Rate* is

$$R_L^{(n)} = \frac{1}{n} I(W^{(1)}, W^{(2)}; Z^n), \tag{52}$$

Discrete Memoryless MAC

Capacity region

- Capacity region of DM-MAC

Capacity Region for DM-MAC

Closure of convex hull of all rate pair (R_1, R_2) satisfying

$$\begin{aligned} R_1 &\leq I(X_1; Y|X_2), \\ R_2 &\leq I(X_2; Y|X_1), \\ R_1 + R_2 &\leq I(X_1, X_2; Y), \end{aligned} \tag{53}$$

for some X_1, X_2 independent.

Discrete Memoryless MAC-WT

Inner Bound

- Secrecy Capacity region *not known* for DM-MAC-WT
- Inner bound was proposed by Tekin and Yener [1]

Secrecy-Rate Region for MAC

Rates (R_1, R_2) are achievable with $\limsup_{n\to\infty} R_L^{(n)} = 0$, if there exist independent random variables (X_1, X_2) satisfying

$$\begin{aligned} R_1 &\leq I(X_1; Y|X_2) - I(X_1; Z), \\ R_2 &\leq I(X_2; Y|X_1) - I(X_2; Z), \\ R_1 + R_2 &\leq I(X_1, X_2; Y) - I(X_1; Z) - I(X_2; Z). \end{aligned} \tag{54}$$

[1] Tekin, Ender and Yener, Aylin, "The Gaussian multiple access wire-tap channel," *IEEE Transactions on Information Theory*, 2008.

Notation

- $\overline{W}_k^{(i)}$ denotes message of user i in slot k.
- $\mathbf{X}^{(i)}$ denotes n-length codeword transmitted by user i.
- $\overline{W}_k^{(i)} = (\overline{W}_{k,1}^{(i)}, \overline{W}_{k,2}^{(i)})$, $\overline{W}_{k,1}^{(i)}$ being first part and $\overline{W}_{k,2}^{(i)}$ the second part.
- $\mathbf{X}^{(i)} = (\mathbf{X}_1^{(i)}, \mathbf{X}_2^{(i)})$, $\mathbf{X}_1^{(i)}$ is n_1-length codeword for $\overline{W}_{k,1}^{(i)}$ and $\mathbf{X}_2^{(i)}$ is codeword for $\overline{W}_{k,2}^{(i)}$

Encoder modified

- Also the encoders will now be defined as

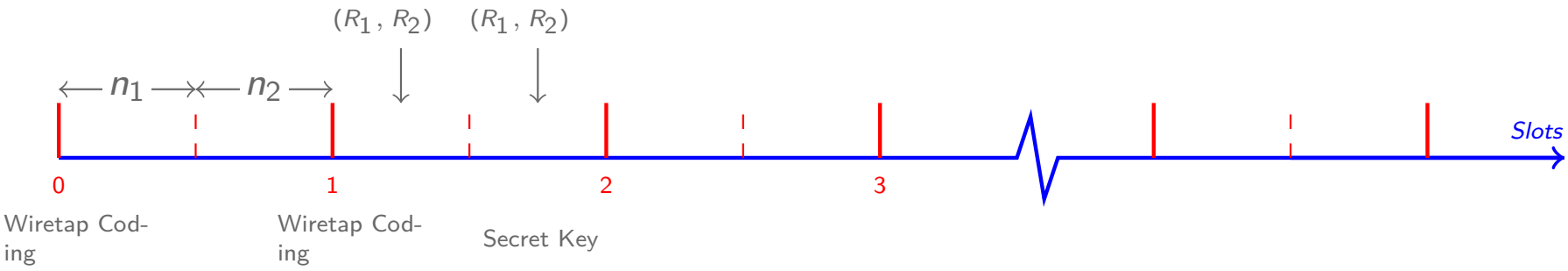
Encoders

$$f_1^s : \mathcal{W}^{(1)} \to \mathcal{X}_1^{n_1}, \quad f_1^d : \mathcal{W}^{(1)} \times \mathcal{K}_1 \to \mathcal{X}_1^{n_2} \tag{55}$$

$$f_2^s : \mathcal{W}^{(2)} \to \mathcal{X}_2^{n_1}, \quad f_2^d : \mathcal{W}^{(2)} \times \mathcal{K}_2 \to \mathcal{X}_2^{n_2}, \tag{56}$$

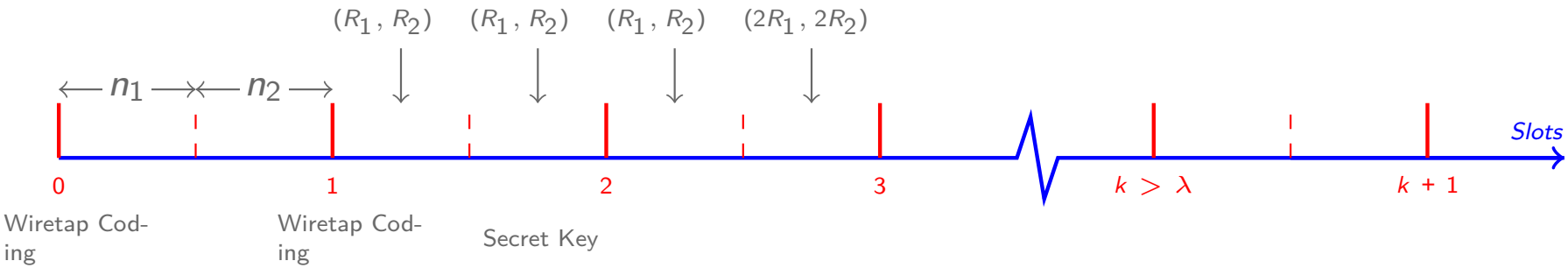
- where $X_i \in \mathcal{X}_i, i = 1, 2,$
- $\mathcal{K}_i, i = 1, 2$ are the sets of secret keys generated for the respective user, $f_i^s, i = 1, 2$ are the wiretap encoders,
- $f_i^d, i = 1, 2$ are the deterministic encoders , $n_1 + n_2 = n$

Coding Scheme



- Fix distributions p_{X_1}, p_{X_2}& consider time slotted system
- Initialization: Take $n_1 = n_2 = n/2$ & in Slot 1 User i transmits $\overline{W}_1^{(i)}$ via *Wiretap Coding*
- Slot 2: Each user selects two messages $(\overline{W}_{21}^{(i)}, \overline{W}_{22}^{(i)}) \equiv \overline{W}_2^{(i)}$, $i = 1, 2$
  - $(\overline{W}_{21}^{(1)}, \overline{W}_{21}^{(2)})$ transmitted via Wiretap coding
  - For $\overline{W}_{22}^{(i)}$, first take *XOR* with *previous message*, then transmit $\overline{W}_{22}^{(i)} \oplus \overline{W}_1^{(i)}$ via usual *MAC coding*

Coding Scheme



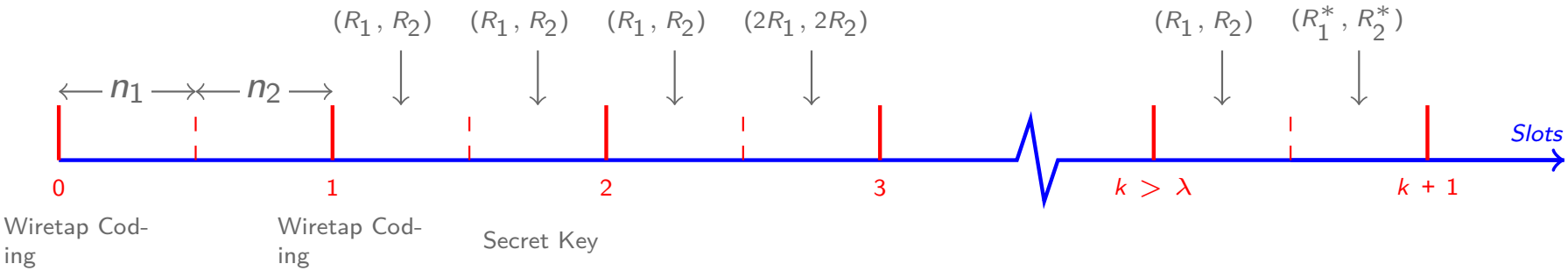
- Slot 3: Transmit first part of message via Wiretap coding (WTC)
- 2nd part by $\bigoplus$ with previous message, hence *rate doubled*.
- Slot λ: We define

Time slot of Saturation

$$\lambda_i \triangleq \left\lceil \frac{I(X_i; Y|X_j)}{I(X_i; Y|X_j) - I(X_i; Z)} \right\rceil, (i \neq j, i, j \in \{1, 2\})$$

$$\lambda \triangleq \max\{\lambda_1, \lambda_2\} + 1 \tag{57}$$

Coding Scheme



- After some slot $\lambda^* > \lambda$ sum-rate will get saturated

$$R_1 + R_2 \leq I(X_1, X_2; Y). \tag{58}$$

- Slot k ($k > \lambda$): For $\overline{W}_k^{(i)} = (\overline{W}_{k,1}^{(i)}, \overline{W}_{k,2}^{(i)})$, $i = 1, 2$, use WTC for $(\overline{W}_{k,1}^{(1)}, \overline{W}_{k,1}^{(2)})$ & for the 2nd part, encode $\overline{W}_{k,2}^{(i)} \oplus \overline{W}_{k-1}^{(i)}$ & transmit at *Shannon rate* (R_1^*, R_2^*).
- Then we make n_2/n_1 large enough to achieve close to *Shannon Capacity* for the *whole slot*.

Secrecy Measures

- We consider the following Secrecy measure

Secrecy Measure

$$I(W^{(1)}, W^{(2)}; Z^n) \leq n\epsilon. \tag{59}$$

- We note that $I(W^{(1)}, W^{(2)}; Z^n) \leq I(W^{(1)}; Z^n | X_2^n) + I(W^{(2)}; Z^n | X_1^n)$

k^{th} slot

Let the leakage rate inequality

$$I(\overline{W}_l^{(1)}, \overline{W}_l^{(2)}; Z_1^n, \ldots, Z_k^n) \leq 2n_1\epsilon, \text{ for } l = 1, \ldots, k \tag{60}$$

hold for k, then it holds for $k+1$ slot also (Mathematical Induction).

Enhancing rate in Strong Sense

- The same rate region can be achieved in *Strong Secrecy* sense.
- We use *resolvability* based coding scheme in slot 1 .
- In subsequent slots use *resolvability coding* scheme instead of wiretap coding.
- We can achieve Shannon capacity region as secrecy rate region satisfying

Strong Secrecy

$$\limsup_{n\to\infty} I(\overline{W}_k^{(1)}, \overline{W}_k^{(2)}; Z_1^n, Z_2^n, \ldots, Z_k^n) = 0, \tag{61}$$

as $n \to \infty$.

MAC with Secret Key Buffer

- We consider the following model

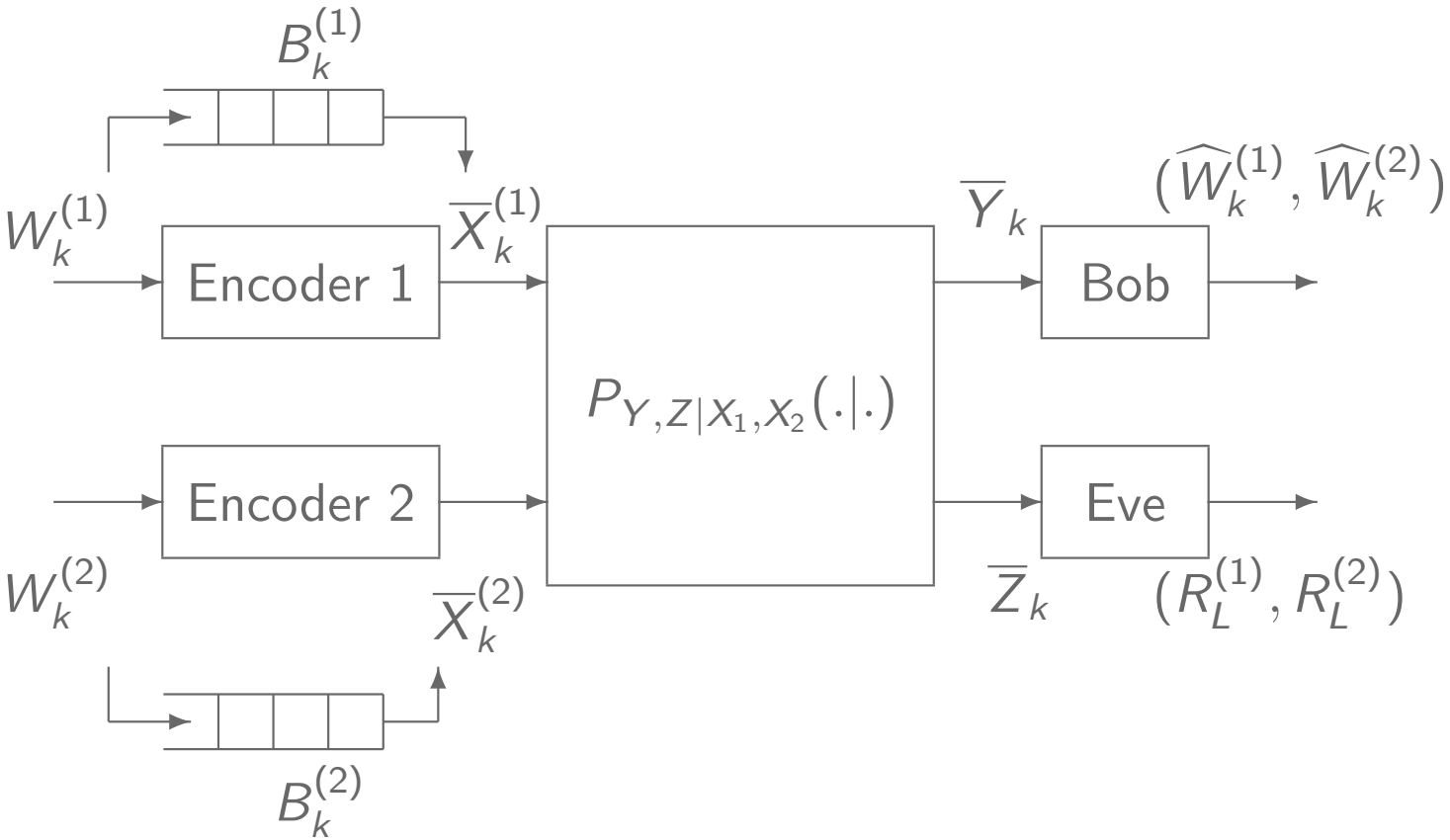


Figure : Discrete Memoryless Multiple Access Wiretap Channel with secret key buffers

MAC with Secret key buffer

- By using very old messages as keys we have the following result

Theorem

The secrecy-rate region of a DM-MAC-WT equals the usual Shannon capacity region of the MAC while satisfying

$$\begin{aligned} I(\overline{W}_k^{(1)}, \overline{W}_{k-1}^{(1)}, \ldots, \overline{W}_{k-N_1}^{(1)}; \overline{Z}_1, \ldots, \overline{Z}_k | \overline{X}_k^{(2)}) &\leq n_1 \epsilon, \\ I(\overline{W}_k^{(2)}, \overline{W}_{k-1}^{(2)}, \ldots, \overline{W}_{k-N_1}^{(1)}; \overline{Z}_1, \ldots, \overline{Z}_k | \overline{X}_k^{(1)}) &\leq n_1 \epsilon, \\ I(\overline{W}_k^{(1)}, \overline{W}_k^{(2)}, \ldots, \overline{W}_{k-N_1}^{(1)}, \overline{W}_{k-N_1}^{(2)}; \overline{Z}_1, \ldots, \overline{Z}_k) &\leq 2n_1 \epsilon. \end{aligned} \tag{62}$$

Fading MAC-WT

- Channel model

$$Y = \widetilde{H}_1 X_2 + \widetilde{H}_2 X_2 + N_1 \;\; Z = \widetilde{G}_1 X_1 + \widetilde{G}_2 X_2 + N_2, \tag{63}$$

- Notation

$$\begin{aligned}
C_1(P_1(H,G)) &\triangleq \frac{1}{2}\log\left(1+\frac{H_1 P_1(H,G)}{\sigma_1^2}\right)\\
C_2(P_2(H,G)) &\triangleq \frac{1}{2}\log\left(1+\frac{H_2 P_1(H,G)}{\sigma_1^2}\right)\\
C_1^e(P_1(H,G)) &\triangleq \frac{1}{2}\log\left(1+\frac{G_1 P_1(H,G)}{\sigma_2^2+G_2 P_2(H,G)}\right)\\
C_2^e(P_2(H,G)) &\triangleq \frac{1}{2}\log\left(1+\frac{G_2 P_2(H,G)}{\sigma_2^2+G_1 P_1(H,G)}\right)\\
C(P_1(H,G),P_2(H,G)) &\triangleq \frac{1}{2}\log\left(1+\frac{H_1 P_1(H,G)+H_2 P_2(H,G)}{\sigma_1^2}\right)
\end{aligned} \tag{64}$$

- We have the following result If $Pr(H_{ik} > G_{ik}) > 0, i = 1, 2$, and all the channel gains are available at all the transmitters, then the following long term average rates that maintain the leakage rates (62), are achievable:

$$\begin{aligned} R_1 &\leq \frac{1}{2}\mathrm{E}_{H,G}\left[C_1\left(P_1(H)\right)\right], \\ R_2 &\leq \frac{1}{2}\mathrm{E}_{H,G}\left[C_2\left(P_2(H)\right)\right], \\ R_1 + R_2 &\leq \frac{1}{2}\mathrm{E}_{H,G}\left[C\left(P_1(H), P_2(H)\right)\right]. \end{aligned} \tag{65}$$

where P is any policy that satisfies avg. power constraint. If only Bob knows all the channel states but not the transmitters, then (R_1, R_2) satisfies (65) with $P_i(H, G) \equiv \overline{P}_i,\ i = 1, 2$.

Outline

Conclusions

- Proposed Probability of error as metric of security
- Achieved Shannon capacity in wiretap channel via previous messages
- Power allocation in fading MAC-WT without CSI of Eve
- Extended CJ to enhance secrecy sum-rate in fading MAC-WT
- Used Algorithmic Game theory to allocate resources in fading MAC with individual CSI only
- Extended the same algorithms to fading MAC-WT
- Extended coding scheme of using previous messages as key to MAC to achieve Shannon Capacity region

Future Work

- Develop practical codes based on probability of error at Eve as security metric
- Develop practical codes for using previous messages as secret key to enhance secrecy rates
- Resource allocation with continous state space

References I

Thanks

Questions ?

Shahid M Shah
shahid.nit@gmail.com