Enhancing Secrecy Rates for Wiretap Channels

Shahid Mehraj Shah

ECE Dept., Indian Institute of Science
Bangalore, India

November 06, 2013

Outline

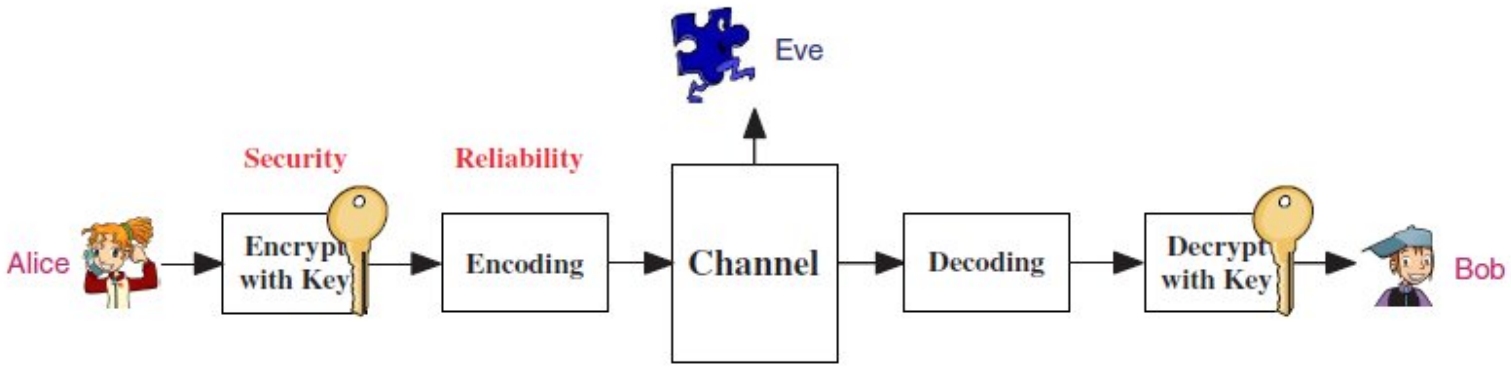
- Introduction
- Information Theoretic security
- The Wiretap Channel
- Fading Wiretap Channel
- Fading MAC with Eve
- Alternative notion of Security
- Dual encoder scheme
- Conclusions

Introduction

- Security is one of the most important considerations in transmission of information from one user to another
- Conventional technique is Cryptography
  - Transmitter uses key to encrypt source information.
  - Eve is assumed to be ignorant of the key.
  - Assumes limited computational capacity of Eavesdropper.
- Information theoretic security.
  - Does not require key for securing the message.
  - Assumes unlimited computational capacity of Eavesdropper.
- Wyner introduced Wiretap channel in his seminal paper in 1974.

- Key distribution and storage adds complexity to the network design.
- Various Cryptographic encryption algorithms are vulnerable to Man-in-the middle attack
- Open nature of Wireless networks and lack of infrastructure in decentralized networks makes further makes key distribution/management difficult.
- Information theoretic security Promises new direction toward solving security problems.

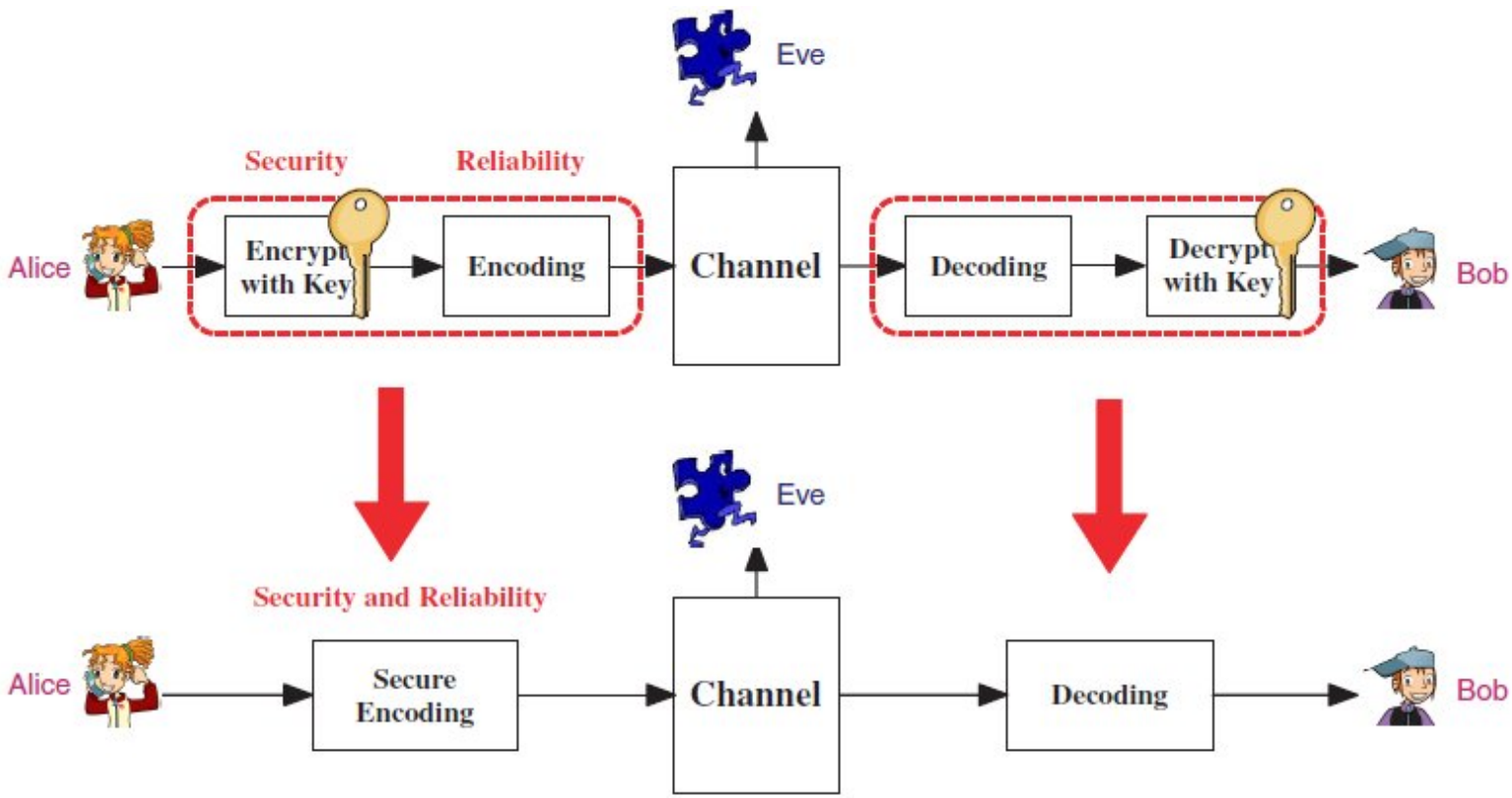
Model



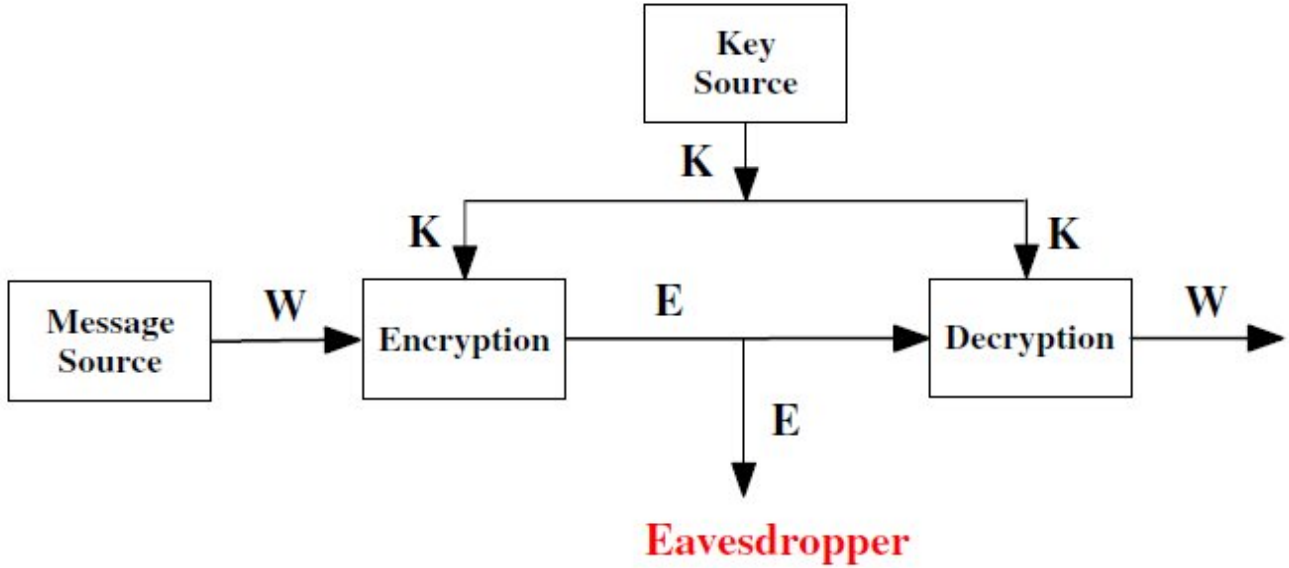
Encryption with channel coding

Information Theoretic Security

- Security issues include confidentiality, integrity, authentication, and non-repudiation
- Attacks on the security of communication networks can be divided into two basic types: passive attacks and active attacks.

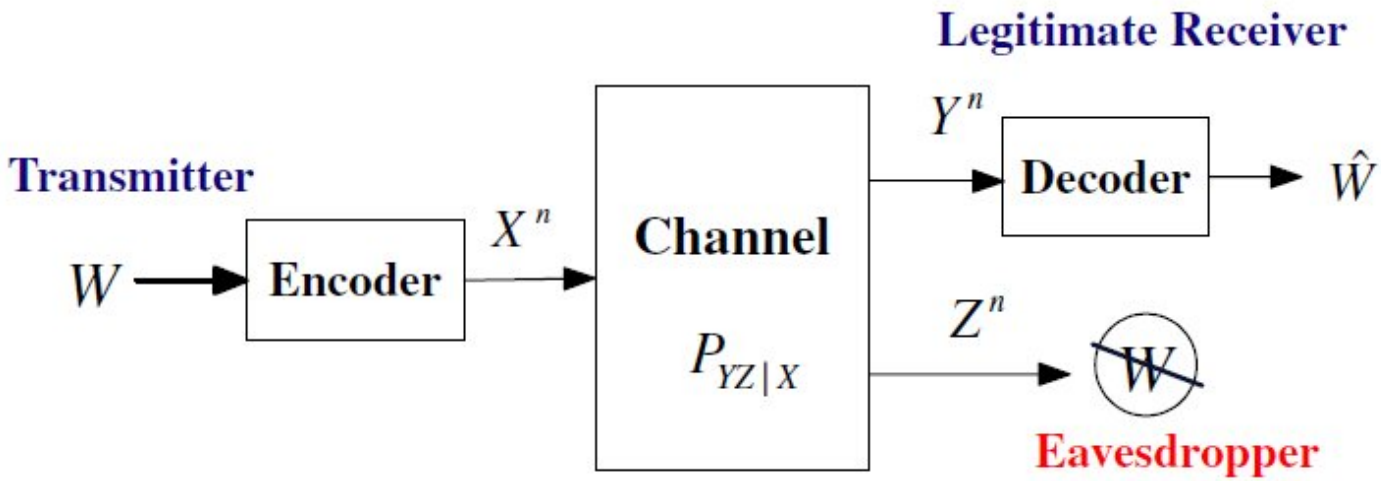


Information Theoretic Security: Shannon's Model



- A source message W is encrypted to a ciphertext E by a key K shared by the transmitter and receiver
- System is perfectly secure if the a posteriori probabilities of W given E are equal to the a priori probabilities of W for all E, i.e., $P_{W|E} = P_W$
- Shannon also showed that we need $H(K) \geq H(W)$ for perfect secrecy.

Wyner's Wiretap Model



- Security, i.e., the secrecy level of the confidential message W at the eavesdropper, is measured by the equivocation rate defined as
- $R_e^{(n)} = \frac{1}{n} H(W \mid Z^n)$
- The reliability is average block probability of error, for a length n code:
- $P_e^{(n)} = Pr\{\tilde{W} \neq W\} = \frac{1}{|\mathcal{W}|} \sum_{w=1}^{|\mathcal{W}|} Pr\{\tilde{w} \neq w\}$

- A $rate - equivocationpair(R, R_e)$ is achievable if $\exists$ message sets $\mathcal{W}_n$ with $\mid \mathcal{W}_n \mid = 2^{nR}$ and encoder - decoder pairs (f_n, g_n) such that $P_e^{(n)} \to 0$, $Re \leq liminf_{n\to\infty} R_e^{(n)}$
- The capacity-equivocation region $\mathcal{C}$ is defined to be the closure

$$\mathscr{C} = \bigcup_{P_{QU}P_{X|U}P_{YZ|X}} \left\{ \begin{array}{l} (R, R_e): \\ 0 \leq R \leq I(U;Y) \\ 0 \leq R_e \leq R \\ R_e \leq I(U;Y\,|\,Q) - I(U;Z\,|\,Q) \end{array} \right\}$$

- $Q \to U \to X \to (Y, Z)$.

The Wiretap Channel: Coding Scheme

- Wiretap Coding is basically random binning.
- The codebook is divided into subcode books.
- The message to be sent is selected according to the subcodebook, from which a message is choosen randomly and transmitted.
- The codebook is constructed such that, Eve can successfully decode message but could not decode from which sub-codebook the message was selected.
- Where as legitimate reciever can decode the sub-codebook also.

The Wiretap Channel: Coding Scheme

- The Codebook is constructed as

$$\mathcal{C} = \left\{ x_{ab}^{n}, a = 1, 2, \ldots 2^{n(I(X;Y)-I(X;Z))}; b = 1, 2 \ldots, 2^{nI(X;Z)} \right\} \quad (1)$$

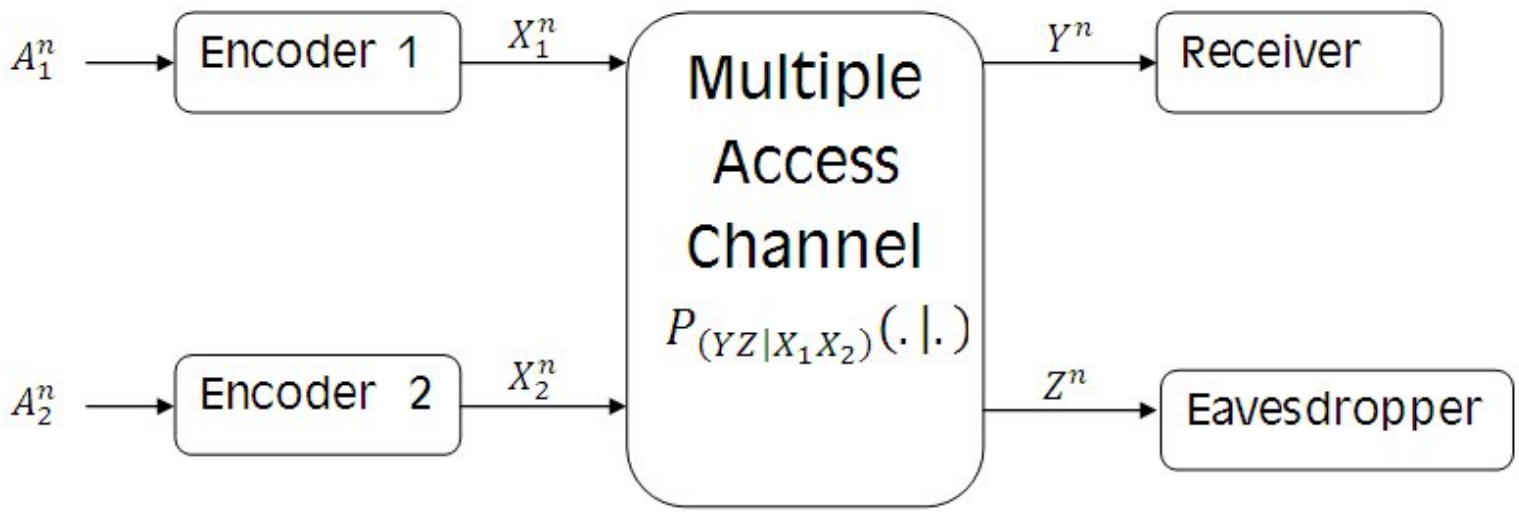
a \ b	1	2	•	•	•	B
1	x_{i11}^{n}	x_{i12}^{n}	•	•	•	
2	x_{i21}^{n}	•	•	•	•	
3	•	•	•	•	•	
	•	•	•	•	•	
•	•	•	•	•	•	
•	•	•	•	•	•	
•	•	•	•	•	•	
A	•	•	•	•	•	

Gaussian Wiretap Channel

- The Gaussian Wiretap Channel was studied by Cheong and Hellman in 1978
- The Channel model is
- $Y = X + N_1$, $Z = X + N_2$, where X is the input, $N_1 \sim \mathcal{N}(0, \sigma_1^2)$ and $N_2 \sim \mathcal{N}(0, \sigma_2^2)$
- The secrecy capacity for the degraded Gaussian Channel(i.e. $\sigma_1 < \sigma_2$) is
- $C_s = \frac{1}{2}\log\left(1 + \frac{P}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1 + \frac{P}{\sigma_2^2}\right)$, where $\mathcal{E}(X^2) \leq P$

Multiple Access Channel with Eve

- Model 2: Eavesdropper at the receiving end
- We follow this model in our work



- $\{X_1^n\}$ independent of $\{X_2^n\}$

Multiple Access Channel with Eve

- 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.

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

$$R_1 \leq [I(U_1; Y \mid U_2) - I(U_1; Z)]^+ \tag{2}$$

$$R_2 \leq [I(U_2; Y \mid U_1) - I(U_2; Z)]^+ \tag{3}$$

$$R_1 + R_2 \leq [I(U_1, U_2; Y) - I(U_1, U_2; Z)]^+ \tag{4}$$

- 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)

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

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

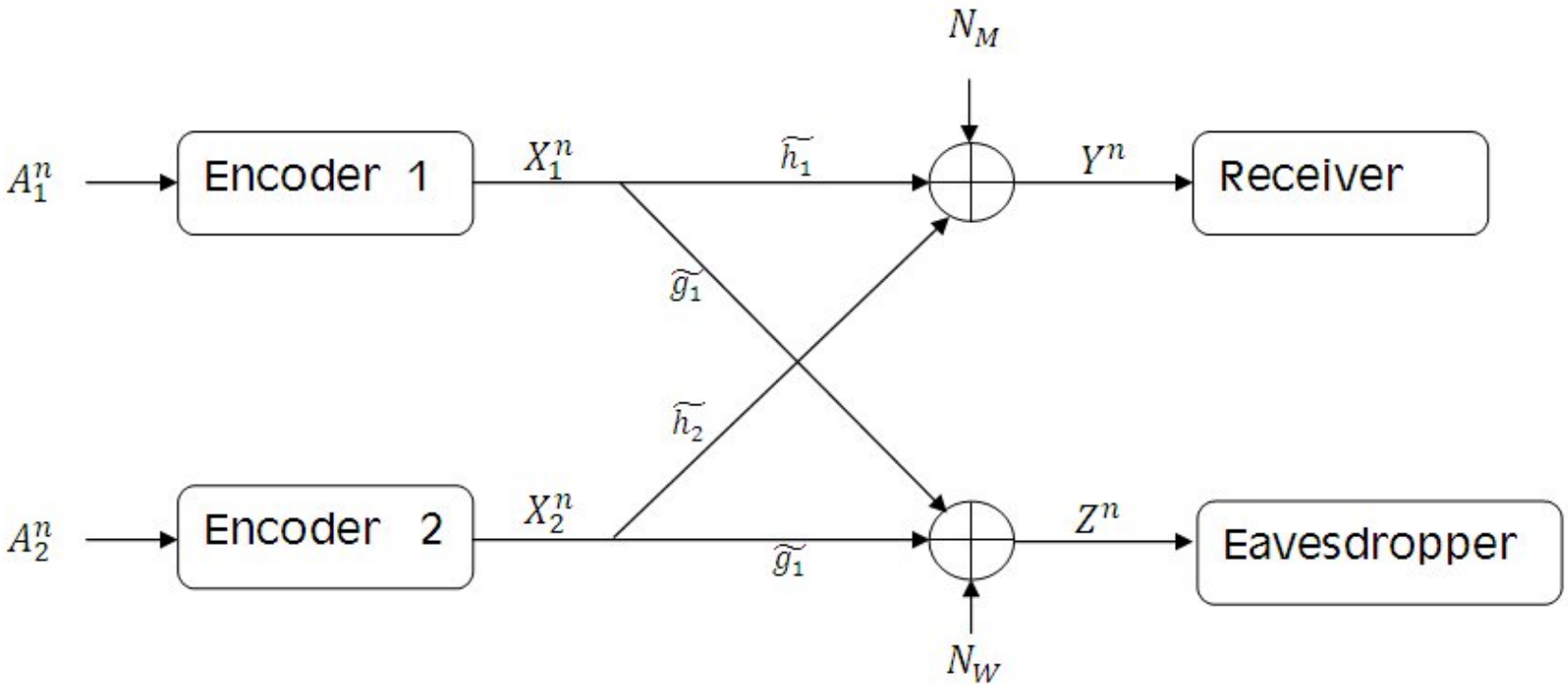
$$R_1+R_2 \leq \mathrm{E}_{h,g}\left\{\left[log\frac{1+h_1P_1(h,g)+h_2P_2(h,g)}{1+g_1P_1(h,g)+g_2P_2(h,g)}\right]^+\right\},$$

- $\mathrm{E}\left[P_i(h,g)\right] \leq \bar{P}_i, i = 1,2.$ 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: Channel Model



- $\phi^s_{x_1,x_2} = 1 + s_1x_1 + s_2x_2$ where s is the channel state (h or g) and x_k is the power used.

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*

$$\mathrm{E}_{h,g}\left\{\left[log\left(\frac{\phi^{h}_{P_1,P_2}}{\phi^{g}_{P_1,P_2}}\right)\right]^{+}\right\} \tag{5}$$

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.

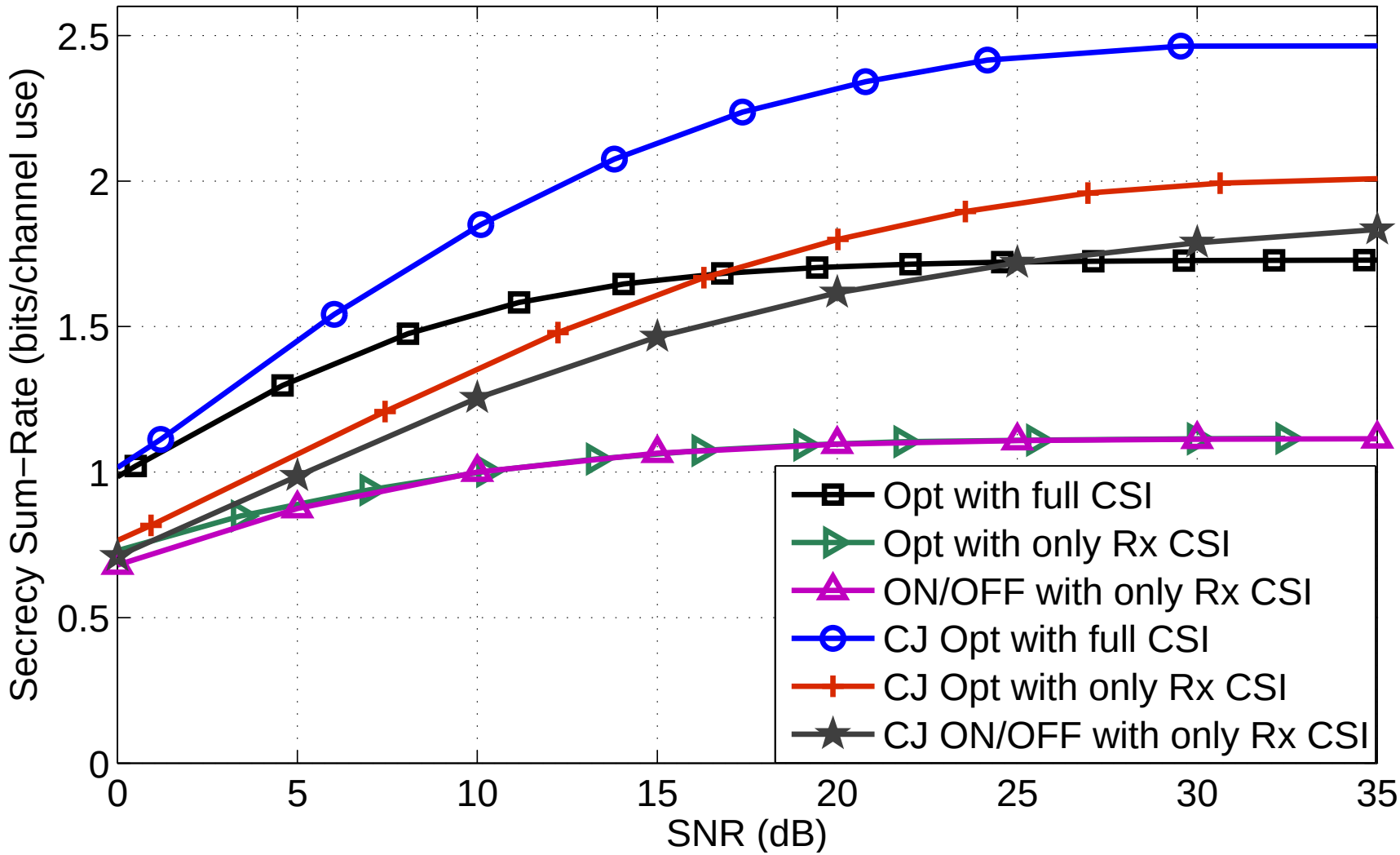
Without CSI of Eve: ON/OFF power control

- ON/OFF power control is a simple threshold based scheme as follows:
  - $h_1 > \tau_1$, $h_2 > \tau_2$: Both transmit;
  - $h_1 > \tau_1$, $h_2 < \tau_2$: 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.
- 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.

Fading MAC Without CSI of Eve: Simulation results



New Notion

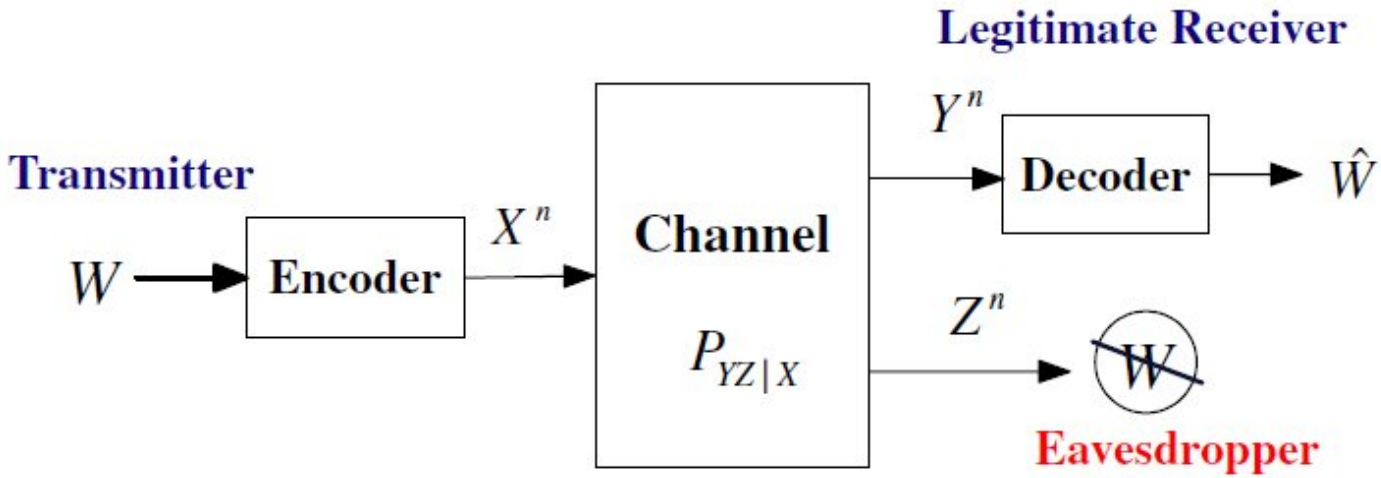
- Equivocation Based definition:
  - (R, R_e) is achievable if $\exists\ \mathcal{W}_n$ with $\mid \mathcal{W}_n \mid = 2^{nR}$ and encoder - decoder pairs (f_n, g_n) such that $P_e^{(n)} \to 0$, and the equivocation rate $lim_{n\to\infty} \frac{1}{n} H(W|Z^n) \geq R_e$
- Code design to satisfy equivocation rate is difficult.([**?**])
- To confuse Eve random messages are sent, which decreases the rate.

New Notion

- Natural Definition of secrecy: Probability of error for receiver $\to 0$ and that for eavesdropper $\to 1$. ([1])
- Strong converse: $R > C$, probability of error of decoding $\to 1$.
- 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 Capacity

Gaussian Wiretap Channel



C_1 = Capacity of main channel, C_2 = Capacity of Eve's channel,
$P_e^n(B)$ = Probability of decoding error at Bob,
$P_e^n(E)$ = Probability of decoding error at Eve

Proposition

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

New Notion: 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
- $\mathrm{E}[N] = (2^{nR} - 1)2^{-nI(X;Z)}$.
- $P_e^n(E) \approx 2^{n(R-I(X;Z))}$
- $P_e^n(E) \leq 2^{-n(C_1-C_2)}$ possible, maximum decay rate for equivocation based secrecy also.
- Higher R means more confusion for Eve.

ML Decoding at Eve

- ML Decoding at Eve: If $x_1(1), ..., x_n(1)$ is transmitted, decode as message $\hat{m}$ if

$$\hat{m} = argmin \sum_{k=1}^{n} (Z_k - x_k(\hat{m}))^2 . \tag{6}$$

- 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

$$\frac{1}{n} H(W|Y^n) \leq \frac{H(P_e^n(B))}{n} + P_e^n(B)R \tag{7}$$

- Lower bound: For Eve

$$H(W \mid Z^n) \geq \phi^*(\pi(W \mid Z^n)) \tag{8}$$

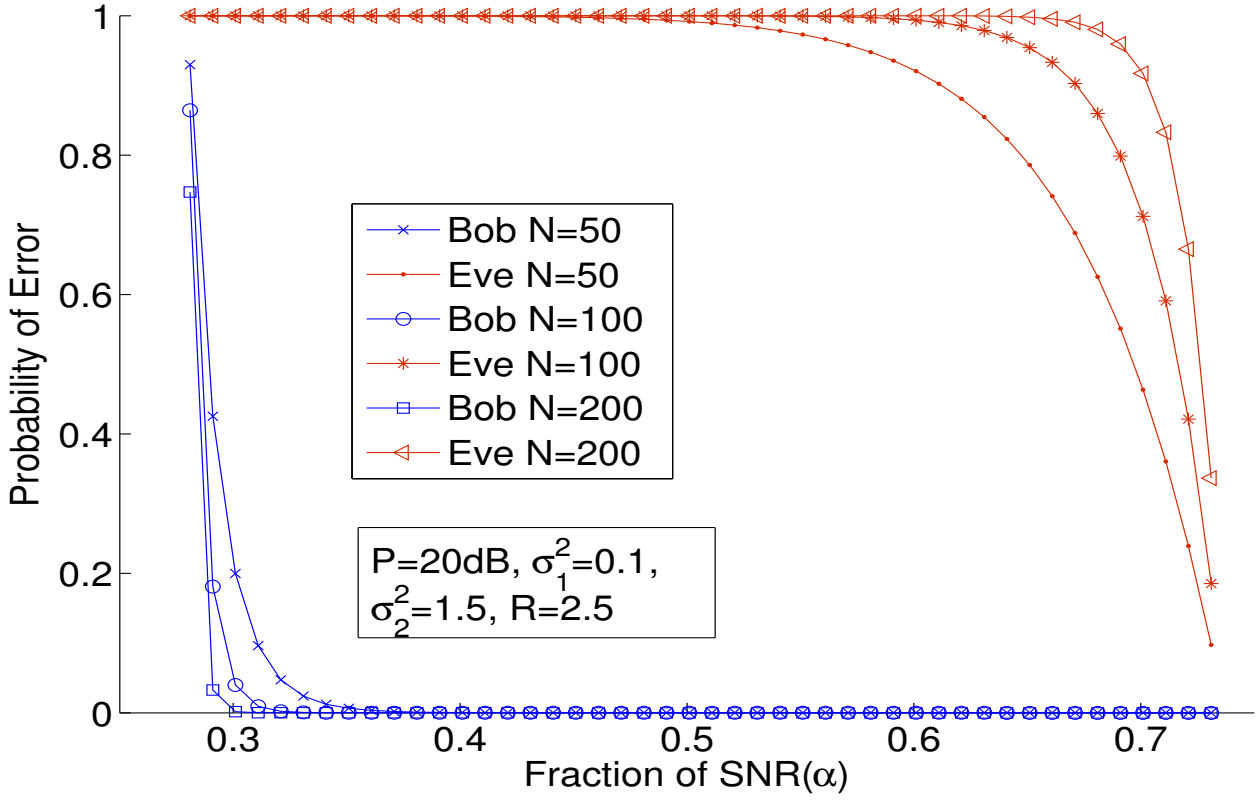
where ϕ^* is a piecewise linear, continuous, non-decreasing, convex function.([2]). $\pi(W \mid Z^n)$ is the average probability of error for the MAP decoder at Eve.

- From Arimoto's lower bound

$$\pi(W \mid Z^n) \geq 1 - e^{-n(E_0(\rho,p)-\rho R)}, \quad 0 \geq \rho \geq -1. \tag{9}$$

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

$$Y_i = h_i X_i + N_{1i}, \tag{10}$$

$$Z_i = g_i X_i + N_{2i}, \tag{11}$$

,

- The capacity is ([gopala2008]):

$$\begin{aligned} C_s &= \int_0^\infty \int_r^\infty [\log(1 + qP^*(q,r)) - \\ &\qquad \log(1 + rP^*(q,r))] f(q) f(r) dq dr \end{aligned} \tag{12}$$

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

$$\begin{aligned} P^*(q,r) &= 0.5[\sqrt{(1/r - 1/q)^2 + 4/\lambda(1/r - 1/q)} + \\ &\qquad (1/r + 1/q)]^+ \end{aligned} \tag{13}$$

Secrecy Capacity for fading Channel

Proposition

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

$$C_1 = \sup_{P(q,r)} \int_0^\infty \int_r^\infty [\log(1 + qP(q,r))] f(q) f(r) dq dr. \qquad (14)$$

.

Channel Model

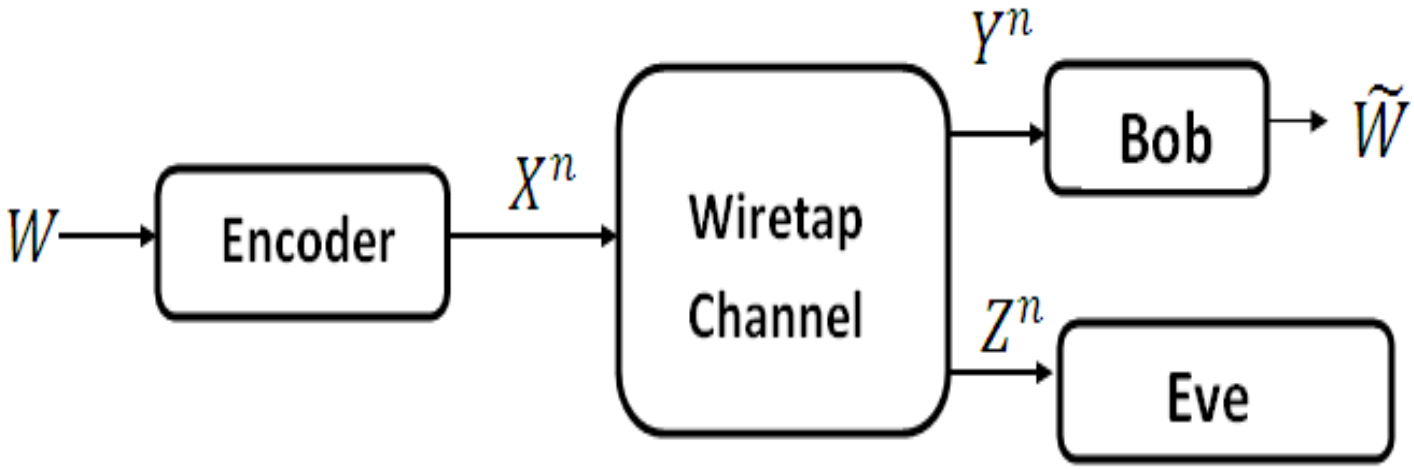


Figure : The Wiretap channel

Literature Survey

- 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.

Channel Model

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

$$R_s = \max_{p(x)} [I(X;Y) - I(X;Z)]. \tag{15}$$

- $\{W_m, m \geq 1\}$ 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.

Channel Model

- A mini-slot consists of n channel uses
- Each slot, upto λ, consists of 2 mini-slots where

$$\lambda \triangleq \left[\frac{C}{R_s}\right], \tag{16}$$

- 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 $k+1$.

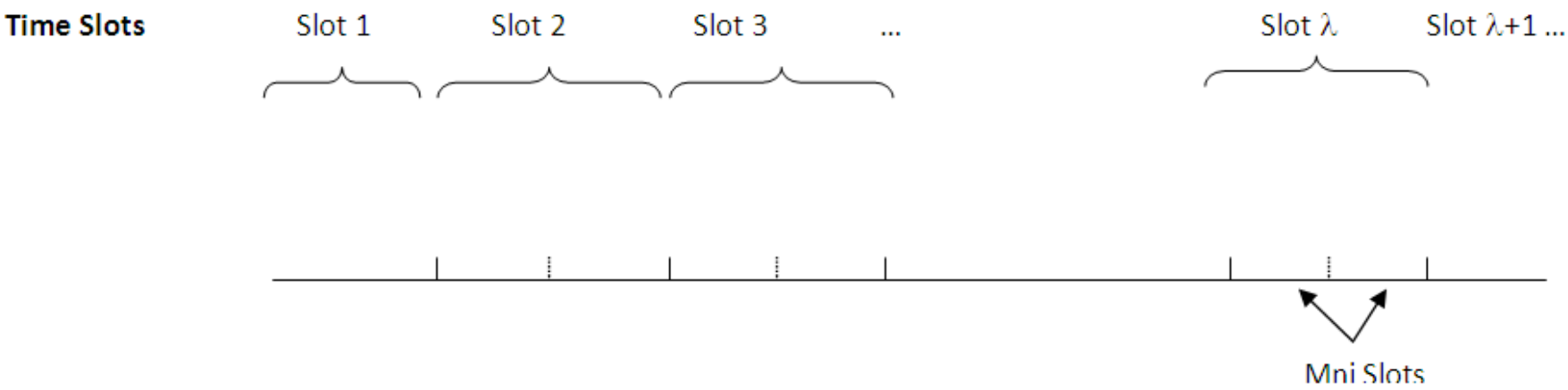
Encoder/Decoder

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

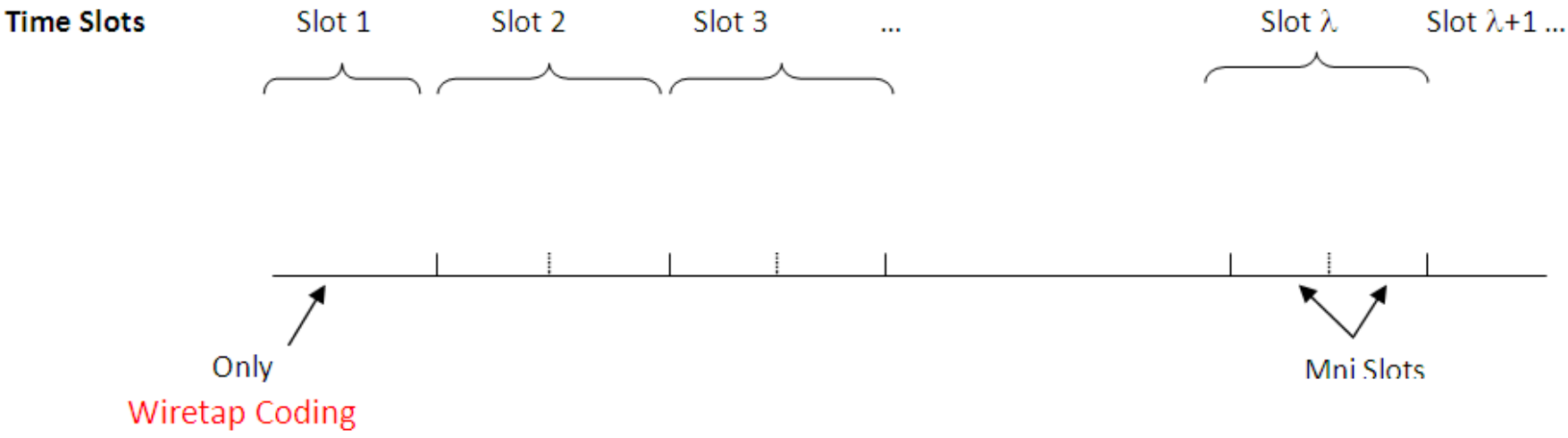
$$f_s : \mathcal{W} \to \mathcal{X}^n, f_d : \mathcal{W} \times \mathcal{K} \to \mathcal{X}^n, \tag{17}$$

  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.

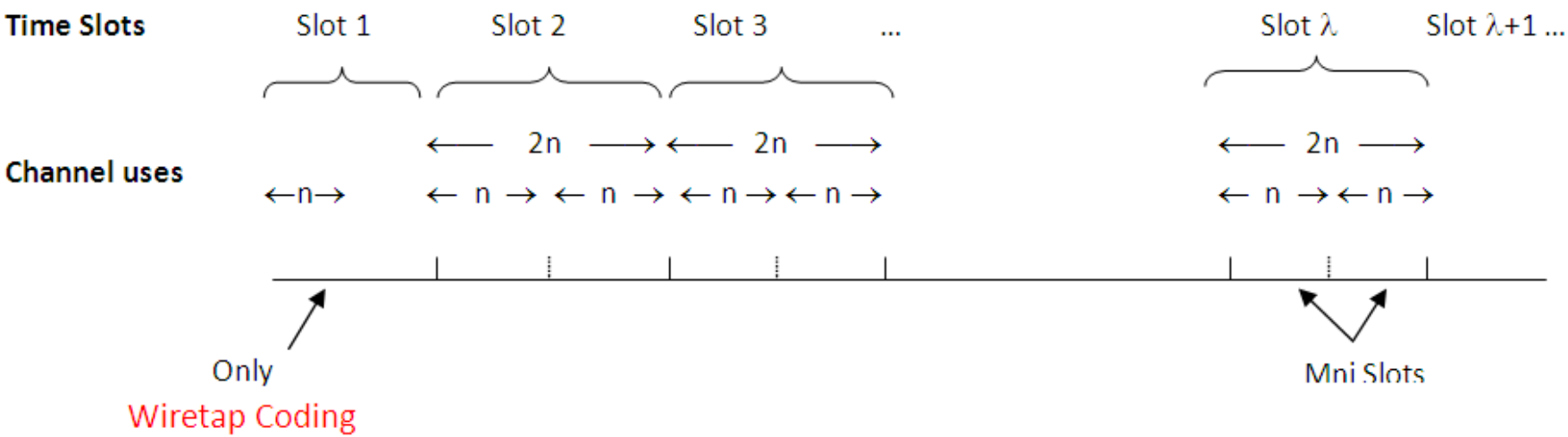
Encoder/Decoder



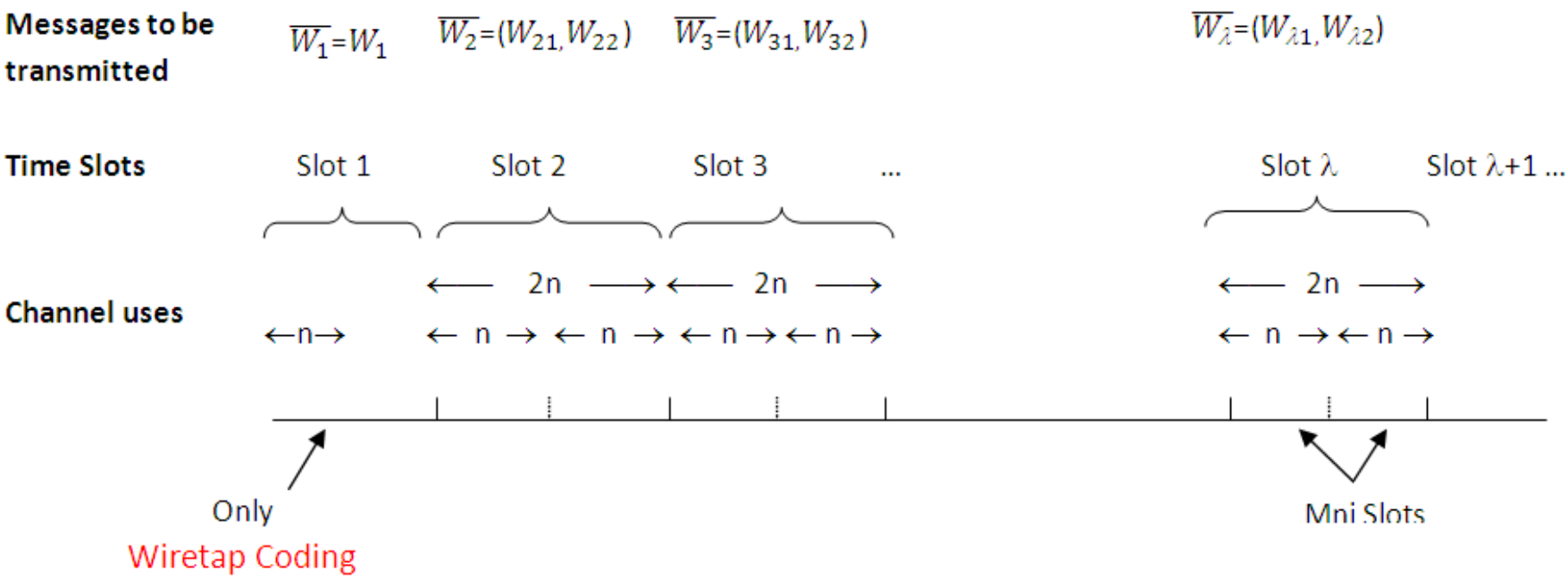
Encoder/Decoder



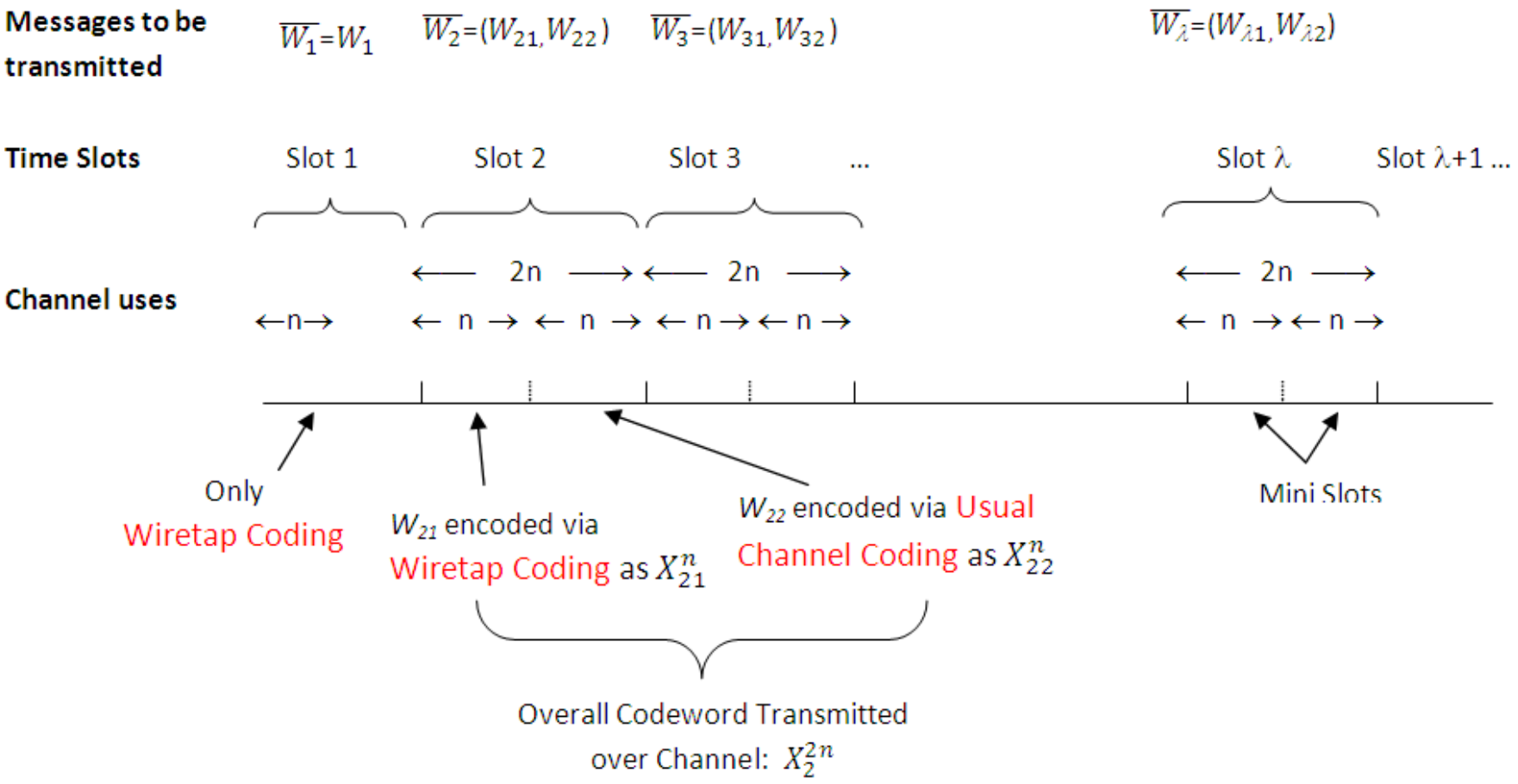
Encoder/Decoder



Encoder/Decoder



Encoder/Decoder



Encoder/Decoder

- Slot 1: Decoder function at Bob is

$$\phi_1 : \mathcal{Y}^{2n} \rightarrow \mathcal{W}. \tag{18}$$

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

$$\phi_i : \mathcal{Y}^n \times \mathcal{K} \rightarrow \mathcal{W}^j \tag{19}$$

  for time slot i, with $j = \min(i, \frac{C}{R_s})$.
- Probability of error:

$$P_e^{(n)} = Pr\{\widehat{W} \neq \overline{W}\} \tag{20}$$

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

Achievable Rate

- Leakage rate is $R_L^n = \frac{1}{n} I(\overline{W}; Z^{2n})$.
- *Definition 1*: 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* $k \geq \lambda$.

Coding Scheme

- 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.

- First message W_{21} is encoded to X_{21}^n using wiretap code.
- Second message W_{22} is first encrypted to produce the cipher using one-time pad with the previous message as secret key, i.e., $K = W_1$ and the cipher is $\widetilde{W}_{22} = W_{22} \bigoplus W_1$
- 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 $(W_{\lambda-1,1}, W_{\lambda-1,2}, ..., W_{\lambda-1,\lambda-1})$.

Decoding Scheme

- Total rate:

$$\frac{1}{2}\left(R_s + (\lambda - 1)R_s\right) = \frac{1}{2}\left(R_s + C\right). \tag{21}$$

- 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
$$\frac{1}{n} I(\overline{W}_k; Z_1^n, Z_2^{2n}, ..., Z_k^{2n}) \to 0 \tag{22}$$
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:
$$\frac{1}{n} I(\overline{W}_1; Z_1^n, Z_2^{2n}) \to 0 \tag{23}$$
- 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 *information reconciliation* and *privacy amplification* in the first slot after transmitting message $\overline{W}_1$ using wiretap coding
- In the subsequent blocks we use both the stochastic encoder and the deterministic encoder

Fading Wiretap Channel

- We consider Slow fading AWGn model

$$Y = \tilde{H}X + N_1 \tag{24}$$

$$Z = \tilde{G}X + N_2 \tag{25}$$

  - N_1 and $N_2 \sim \mathcal{N}(0, \sigma_1^2)$ and $(0, \sigma_1^2)$.
  - $\tilde{H}$ and $\tilde{G}$ are Rayleigh distributed channel gains.
  - $H = |\tilde{H}|^2$ and $G = |\tilde{G}|^2$, are exponentially distributed with mean μ_1 and μ_2 respectively.

Fading Wiretap Channel

- H_k = fading in slot k of Bob's channel
- G_k = fading in slot k of Eve's channel
- B_k = Total key capacity in key buffer
- P_k = Average power to be used in slot k
- $\bar{P}$ = Long term average power constraint
- n = Number of channel uses in a slot
- r_k = rate of transmission of message in slot k and R_k = secret key rate from buffer.

Fading Wiretap Channel

- Buffer size evolves as follows

$$B_{k+1} = B_k - R_k + r_k \tag{26}$$

- Let

$$R_{sec} = \frac{1}{2}\left[\log(1+\frac{H_k P_k}{\sigma_1^2}) - \log(1+\frac{G_k P_k}{\sigma_2^2})\right]^+ \tag{27}$$

- If we use P_k in slot k then the secret rate in slot k, using B_k the key rate

$$R_k = \min\left\{B_k, \frac{1}{2}\log(1+\frac{G_k P_k}{\sigma_2^2})\right\}. \tag{28}$$

- the secrecy rate that is achieved is

$$r_k = \left[\frac{1}{2}\log\frac{\left(1+\frac{H_k P_k}{\sigma_1^2}\right)}{\left(1+\frac{G_k P_k}{\sigma_2^2}\right)}\right] + R_k. \tag{29}$$

Fading Wiretap Channel

- Some notation

$$C_k^b = \frac{1}{2}\log\left(1 + \frac{H_k P_k}{\sigma_1^2}\right) \tag{30}$$

$$C_k^e = \frac{1}{2}\log\left(1 + \frac{G_k P_k}{\sigma_2^2}\right) \tag{31}$$

- $H_1 > G_1$: First Slot of communication.
- Case 1: $H_2 < G_2$, No wiretap coding. Use previous secret key from buffer.
- secret key rate that we can get from the buffer is

$$R_2 = min(B_2, C_2^b) \tag{32}$$

- Power P_k will use water-filling with average power $\bar{P}$

Fading Wiretap channel: Infinite Buffer

- Case 2: $H_2 > G_2$, Use both wiretap coding and secret key from buffer.
- the total secret rate we will get is

$$r_2 = C_2^b - C_2^e + \min(B_2, C_2^e) \tag{33}$$

- use power control policy as in [3]
- From the evolution of buffer (26) we have $r_k \geq R_k$ hence $B_k \to \infty$ *a.s.* as $k \to \infty$
- Hence when k is large

$$\min(B_k, C_k^b) = B_k \tag{34}$$

and as well as

$$\min(B_k, C_k^b) = B_k \tag{35}$$

- the secret key rate that we will get from the buffer will be

$$R_k = C_k^b = \frac{1}{2}\log(1 + \frac{H_k P_k}{\sigma_1^2}) \tag{36}$$

Finite Buffer

- The queue process will evolve as

$$B_{k+1}^{(F)} = \min(\overline{B}, B^{(F)} + r_k - R_k) \tag{37}$$

- for any initial B_0, if $P(H_k > G_k) > 0$, then eventually $B_k = \overline{B}$
- we can get rate

$$r_k\left(P_k(h,g)\right) =$$

$$\begin{cases} \max\left\{(C_k^b - C_k^e)^+ + \min(\overline{B}, C_k^e), \min(\overline{B}, C_k^b)\right\}, & \text{if} \frac{h}{\sigma_1^2} \geq \frac{g}{\sigma_2^2} \\ \min(\overline{B}, C^b) & \text{if} \frac{h}{\sigma_1^2} < \frac{g}{\sigma_2^2} \end{cases}$$

- long term average power constraint

$$\limsup_{m\to\infty} \frac{1}{m} \sum_{k=1}^{m} P_k \leq \bar{P} \tag{38}$$

Finite Buffer: Power Control

- we obtain power policy $P(h, g)$ that maximizes

$$\mathrm{E}\left[r(H, G)\right], \tag{39}$$

subject to

$$\mathrm{E}\left[P(H, G)\right] \leq \overline{P}. \tag{40}$$

Using Lagrange multipliers we can convert this problem to minimize

$$F(P) = \mathrm{E}\left[r(H, G)\right] + \gamma\left(\mathrm{E}\left[P(H, G)\right] - \overline{P}\right) \tag{41}$$

Finite Buffer

- The resulting equation is,
  $\frac{\partial F}{\partial P} =$

$$\begin{cases} \frac{1}{2}\frac{1}{1+\frac{hP(h,g)}{\sigma_1^2}}\frac{h}{\sigma_1^2}+\gamma, & \text{if} \frac{h}{\sigma_1^2} \geq \frac{g}{\sigma_2^2}, C^e < \overline{B}, \\ \frac{1}{2}\left[\frac{1}{1+\frac{hP(h,g)}{\sigma_1^2}}\frac{h}{\sigma_1^2}-\frac{1}{1+\frac{gP(h,g)}{\sigma_2^2}}\frac{g}{\sigma_2^2}+\gamma\right], & \text{if} \frac{h}{\sigma_1^2} \geq \frac{g}{\sigma_2^2}, C^e > \overline{B}, \\ \frac{1}{2}\frac{1}{1+\frac{hP(h,g)}{\sigma_1^2}}\frac{h}{\sigma_1^2}+\gamma & \text{if} \frac{h}{\sigma_1^2} < \frac{g}{\sigma_2^2} \& \overline{B} > C^b. \end{cases}$$

Finite Frame: Numerical result

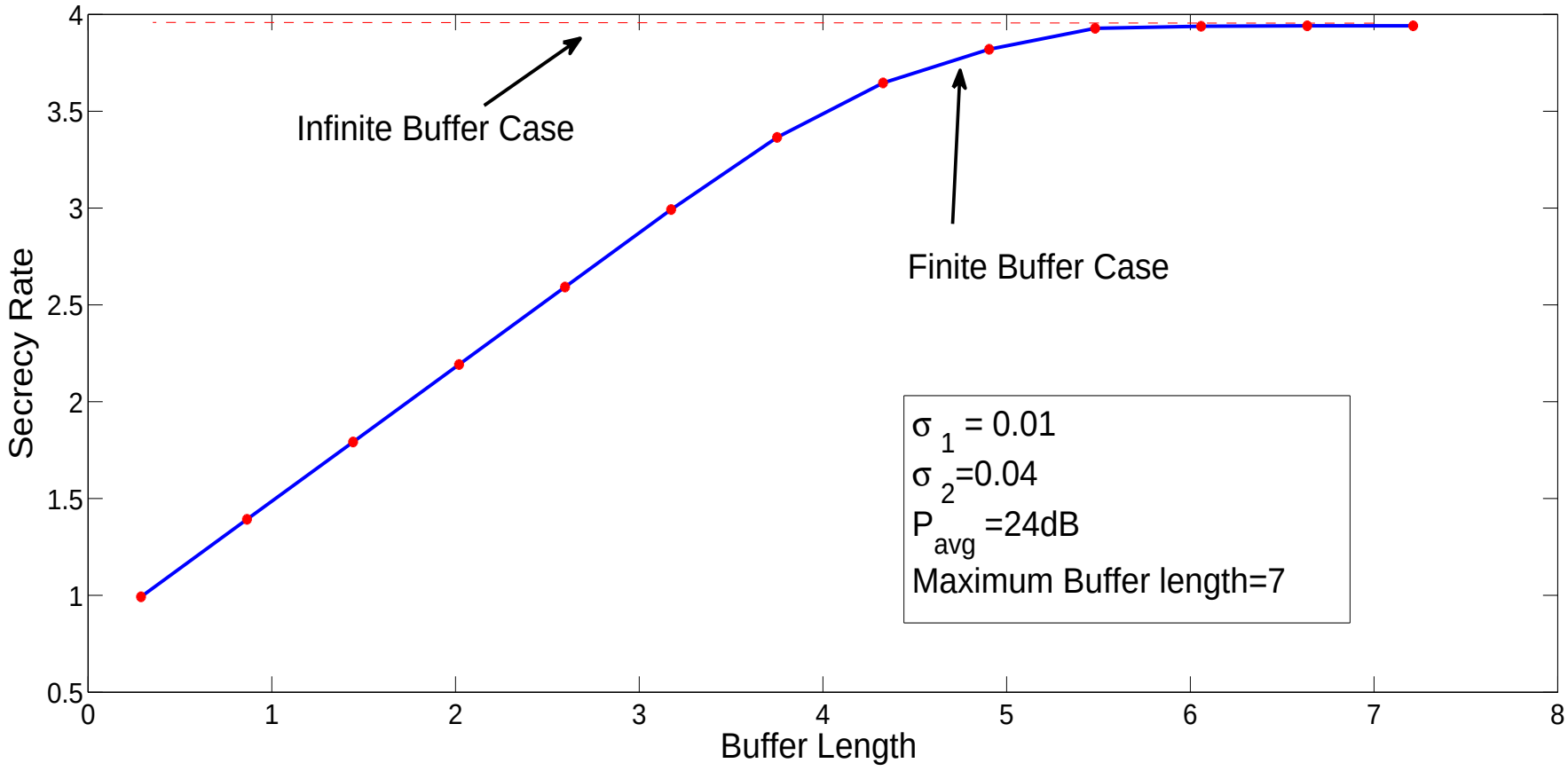


Figure : The Wiretap channel

References

- C.E. Shannon, "Communication of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656-715, October 1949.
- 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.
- Y. Liang, H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 54, no. 3, pp. 35–45, March 2008. 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.
- J Villard, P Piantanida and Shlomo Shamai (Shitz), "Secure Lossy Source-Channel Wiretapping with Side Information at the Receiving Terminals", *ISIT 2011*, St. Pittsburgh, Russia.
- J Villard, P Piantanida , "Secure Lossy Source-Channel Wiretapping with Side Information at the Receiving Terminals", *Submitted to IEEE transactions on Information Theory*, To appear in september 2011

References- Contd.


Jean-Claude Belfiore and F. Oggier, "Secrecy Gain: a Wiretap Lattice Code Design," *ISITA 2010*


M. Feder and N. Merhav, "Relations Between Entropy and Error Probability," *IEEE Trans. Inform. Theory.*, VOL. 40, NO. 1, Jan. 1994.


E. Ardestanizadeh, M. Franceschetti, T. Javidi, Y. H. Kim, "Wiretap Channel With Secure Rate-Limited Feedback," *IEEE Transactions on Information Theory*, vol. 55, No. 12 pp. 5353–5361, December 2009.

References- Contd.

- H. Yamamoto, "Rate-distortion Theory For The Shannon Cipher System," *IEEE Transactions on Information Theory*, vol. 43, No. 3 pp. 827–835, May 1997.
- W. Kang, N. Liu, "Wiretap Channel with Shared Key," *2010 Information theory Workshop*, Dublin, 2010.
- 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.