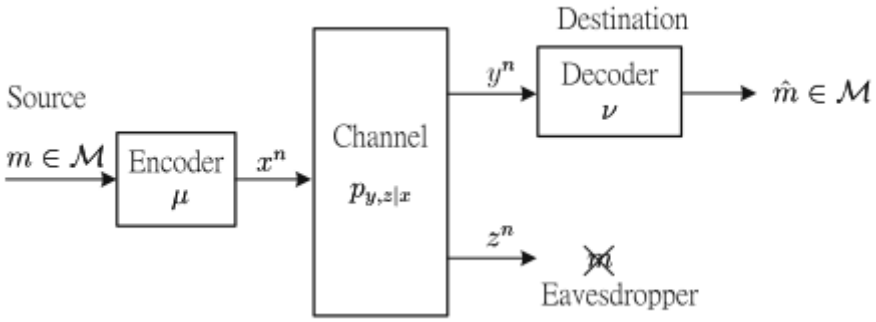
11/5/2020 信息论物理层安全背景

The basic Wiretap Channel

基本模型：basic discrete memoryless wiretap channel



模型描述：

Suppose that a confidential message m chosen from the message set $\mathcal{M} \triangleq \{1, \ldots, 2^{nR_s}\}$ is to be transmitted to the destination over n channel uses. Let $x^n \triangleq [x_1, \ldots, x_n]$ be the channel input over the n channel uses and let $y^n \triangleq [y_1, \ldots, y_n]$ and $z^n \triangleq [z_1, \ldots, z_n]$ be the corresponding channel outputs at the destination and the eavesdropper, respectively. A $(2^{nR_s}, n)$ wiretap code consists of a (stochastic) encoder $\mu : \mathcal{M} \to \mathcal{X}^n$ that maps a message $m \in \mathcal{M}$ into a length-n codeword $x^n \in \mathcal{X}^n$ and a decoder $\nu : \mathcal{Y}^n \to \mathcal{M}$ that maps the received sequence $y^n \in \mathcal{Y}^n$ to an estimated message $\hat{m} \in \mathcal{M}$. Note that the stochastic encoder maps each message $m \in \mathcal{M}$ randomly to a codeword $x^n \in \mathcal{X}^n$ according to a set of conditional probabilities, i.e., $\{p_{x^n|m}, \forall m \in \mathcal{M}, x^n \in \mathcal{X}^n\}$. The reception performance at the destination is measured by the average error probability defined as

m: binary number

Average error probability

$$P_e^{(n)} \triangleq \frac{1}{2^{nR_s}} \sum_{m=1}^{2^{nR_s}} \sum_{x^n \in \mathcal{X}^n} \Pr\left(\nu(y^n) \neq m | x^n\right) p_{x^n|m}. \tag{2.1}$$

窃听者的安全水平：equivocation rate

$$\frac{1}{n} H(m|z^n).$$

Entropy(definition) (where X is a discrete random variable)

$$H(X) = -\sum_{x \in \mathcal{X}} p(x) \log p(x).$$

Joint Entropy of a pair of discrete random variables (X,Y)

$$H(X, Y) = -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log p(x, y).$$

conditional entropy (Given (X, Y) has p(x,y))

$$\begin{aligned} H(Y|X) &= \sum_{x \in \mathcal{X}} p(x) H(Y|X = x) \\ &= -\sum_{x \in \mathcal{X}} p(x) \sum_{y \in \mathcal{Y}} p(y|x) \log p(y|x) \\ &= -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log p(y|x) \\ &= -E \log p(Y|X). \end{aligned}$$

rate-equivocation pair achievable (given a tolerance epsilon)

average error probability at bob: $P_e^{(n)} \leq \epsilon,$

equivocation rate at eve: $\frac{1}{n} H(m|z^n) \geq R_e - \epsilon.$

random variables: Markov property

Definition Random variables X, Y, Z are said to *form a Markov chain in that order* (denoted by $X \to Y \to Z$) if the conditional distribution of Z depends only on Y and is conditionally independent of X. Specifically, X, Y, and Z form a Markov chain $X \to Y \to Z$ if the joint probability mass function can be written as

$$p(x, y, z) = p(x) p(y|x) p(z|y). \tag{2.117}$$

Mutual information $I(X,Y)$

$$\begin{aligned} I(X; Y) &= \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log \frac{p(x, y)}{p(x) p(y)} \\ &= D(p(x, y) || p(x) p(y)) \\ &= E_{p(x,y)} \log \frac{p(X, Y)}{p(X) p(Y)}. \end{aligned}$$

Conditional Mutual information

Definition The *conditional mutual information* of random variables X and Y given Z is defined by

$$I(X;Y|Z) = H(X|Z) - H(X|Y,Z) \tag{2.60}$$

$$= E_{p(x,y,z)} \log \frac{p(X,Y|Z)}{p(X|Z)p(Y|Z)}. \tag{2.61}$$

窃听信道的rate-equivocation region由下面的公式给出：

$$\mathcal{R} = \bigcup_{p_u, p_{v|u}, p_{x|v}} \left\{ (R_s, R_e) : \begin{array}{c} 0 \le R_e \le I(v;y|u) - I(v;z|u) \\ \text{and } R_e \le R_s \le I(v;y) \end{array} \right\} \tag{2.3}$$

where $I(x;y)$ represents the mutual information between x and y, and u and v are auxiliary random variables that satisfy the Markov relation $u \to v \to x \to (y,z)$.

perfect secrecy scenario达到当：

$$R_e = R_s$$

推论：窃听信道的(perfect) secrecy capacity:

$$C_s = \max_{p_v, p_{x|v}} [I(v;y) - I(v;z)] \tag{2.4}$$

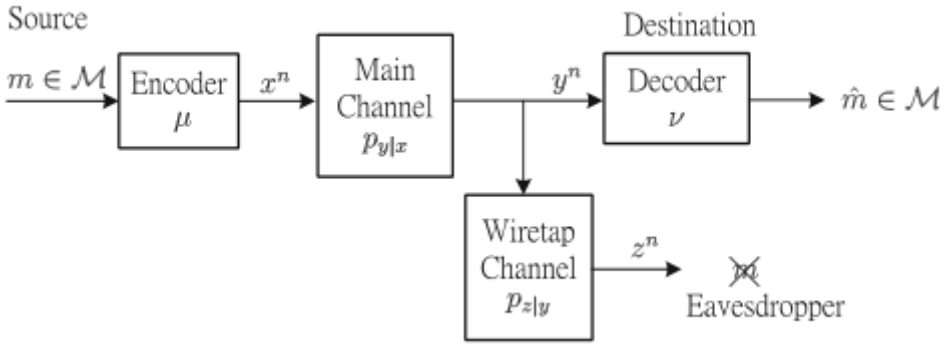
where v is an auxiliary random variable that satisfies the Markov relation $v \to x \to (y,z)$.

secrecy capacity 定义为 maximum achievable secrecy rate

$$C_s = \max_{p_u, p_{v|u}, p_{x|v}} [I(v;y|u) - I(v;z|u)]$$

Channel prefixing : if v is regarded as the effective channel input, this is called channel prefixing.

模型：The degraded wiretap channel



定义一个窃听信道是**degraded if**

[2]. Specifically, as mentioned previously, a wiretap channel is said to be *degraded* if the channel input and output variables satisfy the Markov relation $x \to y \to z$, i.e., when the output at the eavesdropper is a degraded version of that at the destination.

定义一个窃听信道是 **less noisy** if for every auxiliary random variable v

$$I(v; y) \geq I(v; z).$$

定义一个窃听信道是**more capable** if

$$I(x; y) \geq I(x; z), \text{ for every channel input } x.$$

对于 more capable 的窃听信道， secrecy capacity 的表达式可以简化为：

$$\begin{aligned} C_s &= \max_{p_v, p_{x|v}} [I(v; y) - I(v; z)] \\ &= \max_{p_v, p_{x|v}} \{I(x; y) - I(x; z) - [I(x; y|v) - I(x; z|v)]\} \\ &= \max_{p_x} [I(x; y) - I(x; z)]. \end{aligned}$$

一般的带有加密信息的广播信道(**general broadcast channel with confidential message**)：一个公共信息t ,一个私密信息m ,公共信息是被Eve, Bob解码，而私密信息则只被Bob解码，此时我们有三元组(R_s, R_t, R_e)

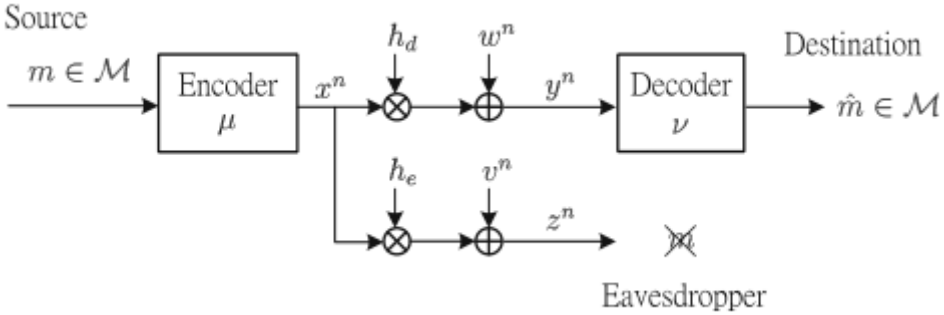
对于general broadcast channel with confidential message，rate-equivocation region可以用下面的给出：

$$\mathcal{R} = \bigcup_{p_u, p_{v|u}, p_{x|v}} \left\{ \begin{array}{l} (R_s, R_t, R_e): \\ 0 \leq R_e \leq R_s, \quad R_e \leq I(v; y|u) - I(v; z|u), \\ R_s + R_t \leq I(v; y|u) + \min[I(u; y), I(u, z)], \\ 0 \leq R_t \leq \min[I(u; y), I(u; z))] \end{array} \right\}$$

where u and v are auxiliary random variables that satisfy the Markov relation $u \to v \to x \to (y, z)$.

如果$R_t = 0$, 则三元组的rate-equivocation region退化为之前的情景。

模型：单输入-单输出高斯窃听信道



其中的数学关系为：

$$y = h_d x + w$$
$$z = h_e x + v$$

参数需要满足如下的性质：

where h_d and h_e are the channel coefficients and $w \sim \mathcal{CN}(0, \sigma_w^2)$ and $v \sim \mathcal{CN}(0, \sigma_v^2)$ are the AWGN at the destination and the eavesdropper, respectively. The codeword transmitted over n channel uses, i.e., $x^n = [x_1, \ldots, x_n]$, must satisfy the average power constraint

$$\frac{1}{n}\sum_{i=1}^{n} \mathrm{E}[|x_i|^2] \leq \bar{P} \tag{2.14}$$

SISO Gaussian wiretap channel 的安全速率下面可以给出：

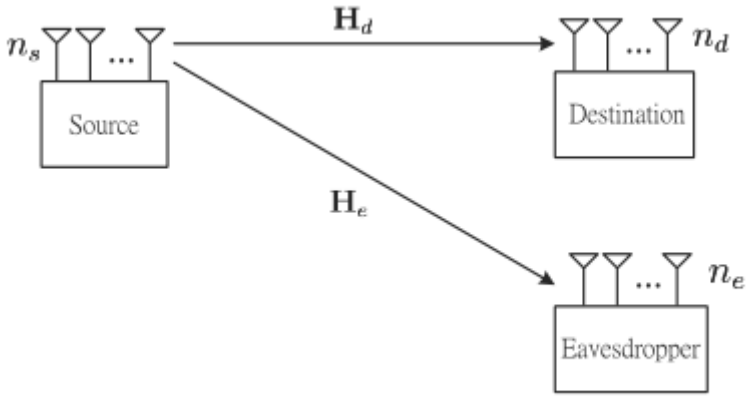
$$C_s = \left[\log\left(1 + \frac{|h_d|^2 \bar{P}}{\sigma_w^2}\right) - \log\left(1 + \frac{|h_e|^2 \bar{P}}{\sigma_v^2}\right)\right]^+ \tag{2.15}$$

where $[\cdot]^+ = \max(0, \cdot)$ *and* $\bar{P}$ *is the average power constraint.*

如果 $|h_d|^2/\sigma_w^2 > |h_e|^2/\sigma_v^2$，则高斯窃听信道可以视为(stochastically) degraded wiretap channel

如果 $|h_d|^2/\sigma_w^2 \leq |h_e|^2/\sigma_v^2$，则主信道可以当作一个窃听信道的degraded version，然后安全速率为负.

模型：多输入-多输出高斯窃听信道



数学关系为：

$$\mathbf{y} = \mathbf{H}_d\mathbf{x} + \mathbf{w},$$
$$\mathbf{z} = \mathbf{H}_e\mathbf{x} + \mathbf{v},$$

参数需要满足如下性质：

where $\mathbf{H}_d \in \mathbb{C}^{n_d \times n_s}$ and $\mathbf{H}_e \in \mathbb{C}^{n_e \times n_s}$ are the channel matrices corresponding to the main and the eavesdropper channels, respectively, and $\mathbf{w} \in \mathbb{C}^{n_d \times 1}$ and $\mathbf{v} \in \mathbb{C}^{n_e \times 1}$ are the AWGN vectors at the destination and the eavesdropper, respectively. The AWGN vectors are assumed to have i.i.d. entries with zero-mean and unit-variance, i.e., $\mathbf{w} \sim \mathcal{CN}(0, \mathbf{I}_{n_d})$ and $\mathbf{v} \sim \mathcal{CN}(0, \mathbf{I}_{n_e})$. The channel matrices $\mathbf{H}_d$ and $\mathbf{H}_e$ are assumed to be known at all terminals and remain constant over the transmission of a codeword. Let $\mathbf{x}^n = [\mathbf{x}_1, \ldots, \mathbf{x}_n]$ be the transmitted codeword, where $\mathbf{x}_i$ is the $n_s \times 1$ channel input vector during the ith channel use. The codeword transmitted over n

码字(codeword)需要满足平均功率限制：

$$\mathrm{E}\left[\frac{1}{n}\sum_{i=1}^{n}||\mathbf{x}_i||^2\right] \le \bar{P},$$

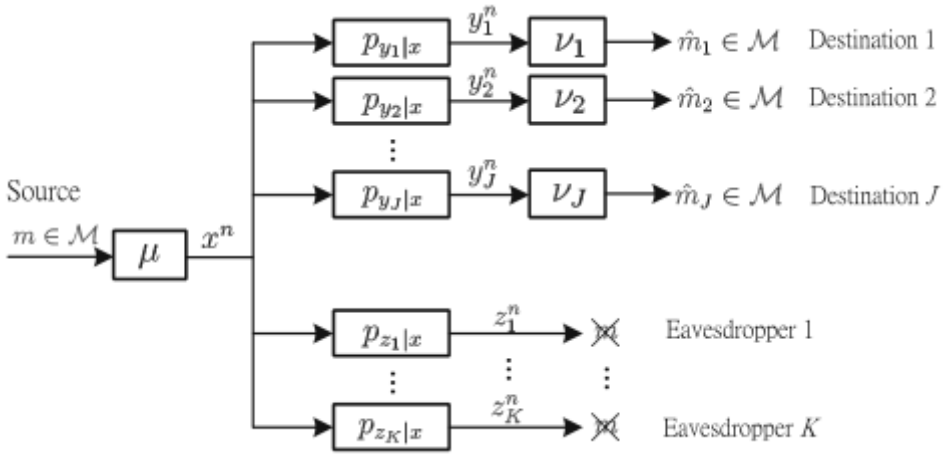
MIMO的Gaussian wiretap channel由下列给出：

$$C_s = \max_{\mathbf{K_x}\succeq\mathbf{0},\mathrm{tr}(\mathbf{K_x})\le\bar{P}} \log\frac{\det(\mathbf{I}_{n_d}+\mathbf{H}_d\mathbf{K_x}\mathbf{H}_d^H)}{\det(\mathbf{I}_{n_e}+\mathbf{H}_e\mathbf{K_x}\mathbf{H}_e^H)}, \tag{2.18}$$

where $\mathbf{K_x} \triangleq \mathrm{E}[\mathbf{x}\mathbf{x}^H]$ *is the input covariance matrix.*

！注意事项：对于K_x来说，这是non-convex的

模型：复合窃听信道(Compound Wiretap Channel)，一个发射器，多合法用户，多窃听者



参数需要满足下列性质：

Let us consider a compound wiretap channel that consists of a source, J destinations, and K eavesdroppers, as illustrated in Fig. 2.6. Let $x \in \mathcal{X}$ be the channel input and let $y_j \in \mathcal{Y}_j$ and $z_k \in \mathcal{Z}_k$ be the channel output at the jth destination and the kth eavesdropper, where $\mathcal{X}$, $\mathcal{Y}_j$, for $j = 1, \ldots, J$, and $\mathcal{Z}_k$, for $k = 1, \ldots, K$, are the channel input and output alphabets. The channel input and output relations are described by the conditional probabilities $p_{y_j|x}$, for $j = 1, \ldots, J$, and $p_{z_k|x}$, for $k = 1, \ldots, K$. A $(2^{nR_s}, n)$ code consists of a (stochastic) encoder $\mu : \mathcal{M} \to \mathcal{X}^n$, where $\mathcal{M} \triangleq \{1, \ldots, 2^{nR_s}\}$ is the message, that maps the message into a length-n codeword and J decoders $\nu_j : \mathcal{Y}_j^n \to \mathcal{M}$, for $j = 1, \ldots, J$, that maps the received

对复合信道来说，很多东西需要重新定义：

- Average error probability for destination j:

$$P_{e,j}^{(n)} \triangleq \frac{1}{2^{nR_s}}\sum_{m=1}^{2^{nR_s}}\sum_{x^n\in\mathcal{X}^n}\Pr\left(\nu_j(y_j^n)\neq m|x^n\right)p_{x^n|m}$$

- equivocation rate at eve k:

$$\frac{1}{n}H(m|z_k^n).$$

- secrecy rate R_s is achievable

A secrecy rate R_s is achievable if, for any $\epsilon \geq 0$, there exists $n'(\epsilon)$ and a sequence of $(2^{nR_s}, n)$ codes such that, for all $n \geq n'(\epsilon)$, the average error probabilities at the J destinations are all less than ϵ, i.e.,

$$P_{e,j}^{(n)} \leq \epsilon,$$

for $j = 1, \ldots, J$, and the equivocation rate at the K eavesdroppers are all ϵ close to R_s, i.e.,

$$\frac{1}{n} H(m|z_k^n) \geq R_s - \epsilon,$$

for $k = 1, \ldots, K$. The secrecy capacity is the maximum achievable secrecy rate. The secrecy capacity of the compound wiretap channel is not known in general, but

复合窃听信道的安全速率的一般公式未知，但是上下界可以给出

Theorem 2.5 ([17]) *The secrecy capacity of the compound wiretap channel is lower bounded by the achievable secrecy rate*

$$R_{s,\text{lower}} = \max_{p_u, p_{x|u}} \left\{ \min_{j,k} \left[I(u; y_j) - I(u; z_k) \right] \right\}, \tag{2.21}$$

where the maximization is taken over the distributions of u and x that satisfy $u \to x \to (y_j, z_k)$, for $j = 1, \ldots, J$ and $k = 1, \ldots, K$, and is upper bounded by

$$R_{s,\text{upper}} = \min_{j,k} \left\{ \max_{p_u, p_{x|u}} \left[I(u; y_j) - I(u; z_k) \right] \right\}. \tag{2.22}$$

下界可以当作在最差的Bob和最好的Eve下的可达的安全速率。此时，the compound channel is degraded.

此时secrecy capacity is

$$C_s = \max_{p_x} \left\{ \min_{j,k} \left[I(x; y_j) - I(x; z_k) \right] \right\},$$

若Destination的数目只有一个，则

$$C_s = \min_k \left[\log\left(1 + \frac{P|h_d|^2}{\sigma_w^2}\right) - \log\left(1 + \frac{P|h_{e,k}|^2}{\sigma_{v,k}^2}\right) \right]^+.$$

Compound wiretap channel可以拓展为MIMO Gaussian compound wiretap channel,则对应的数学关系为：

$$\mathbf{y}_j = \mathbf{H}_{d,j}\mathbf{x} + \mathbf{w}_j,$$
$$\mathbf{z}_k = \mathbf{H}_{e,k}\mathbf{x} + \mathbf{v}_k,$$

for $j = 1, \ldots, J$ and $k = 1, \ldots, K$, where $\mathbf{w}_j \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ and $\mathbf{v}_k \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$. The secrecy capacity(最大的安全可达安全速率未知)，但是可达的安全速率是：

$$R_s = \max_{\mathbf{K_x} \succeq \mathbf{0}, \mathrm{tr}(\mathbf{K_x}) \leq \bar{P}} \min_{j,k} \log \frac{\det(\mathbf{I}_{n_d} + \mathbf{H}_{d,j}\mathbf{K_x}\mathbf{H}_{d,j}^H)}{\det(\mathbf{I}_{n_e} + \mathbf{H}_{e,k}\mathbf{K_x}\mathbf{H}_{e,k}^H)},$$

Ergodic Secrecy Capacity 遍历安全速率

模型：SISO wiretap channel

数学关系：

$$y = h_d x + w,$$
$$z = h_e x + v,$$