Information Theoretic Secrecy

Parthajit Mohapatra

Dept. of ECE, Indian Institute of Science
Bangalore

21^{st} Jan 2012

Outline

- Introduction
- Shannon's secrecy system
- Secure communication over DMC
- Wiretap channel
- Problem of interest

Introduction

- Inherent openness in wireless communications channel: eavesdropping and jamming
- To overcome security threat at different layers
  - Cryptography
    - at higher layers of the protocol stack
    - based on limited computational power at Eve
  - Techniques like frequency hopping, CDMA
    - at the physical layer
    - based on limited knowledge at Eve
  - Information theoretic security
    - at the physical layer
    - no assumption on Eve's computational power
    - no assumption on Eve's available information

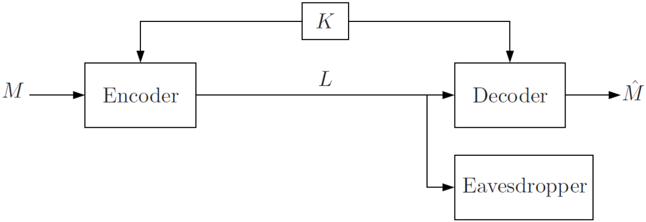
Notion of Secrecy

- How information can be communicated to the legitimate Rx, while keeping it secret from eavesdropper?
- How does such a secrecy constraint on communication affect the limits on information flow in the network?

System Model

- Eavesdropper listen through the same channel as that of legitimate Rx
  - Secret key sharing
- Eavesdropper listen through a different channel as that of legitimate Rx
  - Can channel be exploited in some way ?

Shannon's Secrecy System



- Message: M
- Key: $K \in \mathbb{Z}^+$
- Ciphered message: L

- **Problem:** How many key bits ($H(K)$) are needed so that Eve cannot obtain any information of the message
- $M \sim \text{Unif}[1:2^{nR}]$
- **Encoder:** assigns a ciphertext $l(m,k)$ to each message $m \in [1:2^{nR}]$
- **Decoder:** assigns a message $\hat{m}(l,k)$ to l and K
- **Perfect Secrecy:**
  1. $P\{M \neq \hat{M}(L(M,K),K)\} = 0$
  2. $I(L;M) = 0$ (Information Leakage)

Theorem

The sufficient and necessary condition for perfect secrecy is $H(K) \geq H(M)$.

Proof.

Proof of Necessity:

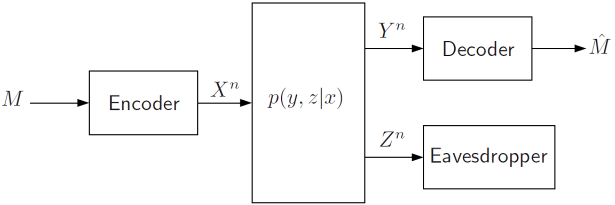
$$\begin{aligned} H(M) &= H(M|L) + I(M;L) \\ &\overset{(a)}{=} H(M/L) \\ &\leq H(M,K|L) \\ &= H(K|L) + H(M|K,L) \\ &\overset{(b)}{=} H(K|L) \\ &\leq H(K) \end{aligned}$$

where (a) follows by the secrecy constraint $I(M;L) = 0$ *and (b) follows from the communication constraint* $P\{M \neq \hat{M}\} = 0$ □

- Disadvantage: Need to share a key as long as that of the message
- How to overcome:
  1. Wiretap channel
  2. Secret key generation

Discrete Memoryless Wiretap Channel (DM-WTC)

- It is a DM-BC with sender X, legitimate receiver Y and eavesdropper Z



- A $(2^{nR}, n)$ secrecy code for the DM-WTC consists of
  - Message set $[1:2^{nR}]$ and $M \sim \mathrm{Unif}[1:2^{nR}]$
  - Randomized encoder: generates codeword $X^n(m)$ according to $p(x^n|m)$
  - Decoder: Assigns an estimate $\hat{m} \in [1:2^{nR}]$ or an error message
- Information leakage rate:

$$R_L^{(n)} = \frac{1}{n} I(M; Z^n)$$

- A rate-leakage pair (R, R_L) is said to be achievable if there exists a sequence of $(2^{nR}, n)$ codes such that

$$\lim_{n\to\infty} P_e^{(n)} = 0$$

$$\text{and} \qquad \lim_{n\to\infty} R_L^{(n)} \leq R_L$$

- Rate-leakage region $\mathbb{R}^*$: Closure of the set of achievable (R, R_L)

Recap

- Shannon's Secrecy System
- Information leakage rate:

$$R_L^{(n)} = \frac{1}{n} I(M; Z^n)$$

- DM-WTC:

$$C_S = \max_{p(u,x)} [I(U; Y) - I(U; Z)]$$

Secrecy Capacity

- Secrecy capacity: $C_S = \{R : (R, 0) \in \mathbb{R}^*\}$

Theorem

The secrecy capacity of the DM-WTC is

$$C_S = \max_{p(u,x)} [I(U;Y) - I(U;Z)]$$

- The secrecy capacity simplifies in degraded case i.e. $p(y,z|x) = p(y|x)p(z|y)$

$$C_S = \max_{p(x)} [I(X;Y) - I(X;Z)]$$

Gaussian Wiretap Channel

- Outputs:

$$
\begin{aligned}
Y &= X + Z_1 \\
Z &= X + Z_2
\end{aligned}
$$

  where $Z_1 \sim N(0, N_1)$ and $Z_2 \sim N(0, N_2)$
- Almost-sure average power constraint:

$$
P\left\{\sum_{i=1}^{n} X_i^2(m) \le nP\right\} = 1
$$

- The secrecy capacity of the Gaussian WTC is

$$
C_S = \left[C(\frac{P}{N_1}) - C(\frac{P}{N_2})\right]^+
$$

- Gaussian random codes achieve capacity

Gaussian Vector Wiretap Channel

- Consider a Gaussian vector WTC:

$$\mathbf{Y} = \mathbf{G}_1\mathbf{X} + \mathbf{Z}_1$$
$$\mathbf{Z} = \mathbf{G}_2\mathbf{X} + \mathbf{Z}_2$$

  with $\mathbf{K}_{\mathbf{Z}_1} = \mathbf{K}_{\mathbf{Z}_2} = \mathbf{I}$ and power constraint P

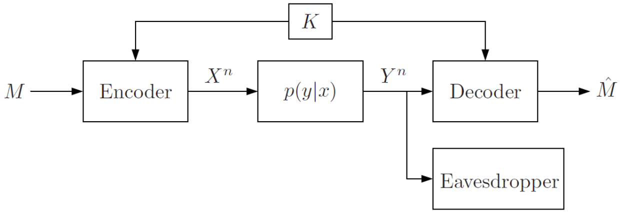
- Secrecy capacity:

$$C_S = \max_{\mathrm{Tr}(\mathbf{K}_\mathbf{X})} \log|\mathbf{I} + \mathbf{G}_1\mathbf{K}_\mathbf{X}\mathbf{G}_1^T| - \log|\mathbf{I} + \mathbf{G}_2\mathbf{K}_\mathbf{X}\mathbf{G}_2^T|$$

- Addition of spatial dimension helps to increase the secrecy

Confidential Communication Via Shared Key

- If the eavesdropper has a better channel than the receiver, then no secret communication can take place



- A $(2^{nR}, 2^{nR_K}, n)$ secrecy code for the DMC consists of
  - a message set $[1 : 2^{nR}]$ and a key set $[1 : 2^{nR_K}]$
  - randomized encoder: generates a codeword $X^n(m,k)$ according to $p(x^n|m,k)$ for each $(m,k) \in [1 : 2^{nR}] \times [1 : 2^{nR_K}]$
  - decoder: assigns an estimate or error to each of the received sequence
- Rate-leakage region $\mathbb{R}^*$: set of achievable rate triples (R, R_K, R_L)

- Secrecy capacity with key rate R_K is defined as

$$C_S(R_K) = \max\{R : (R, R_K, 0) \in \mathbb{R}^*\}$$

Theorem

The secrecy capacity of the DMC $p(y|x)$ with key rate R_K is

$$C_S(R_K) = \min\{R_K, \max_{p(x)} I(X;Y)\}$$

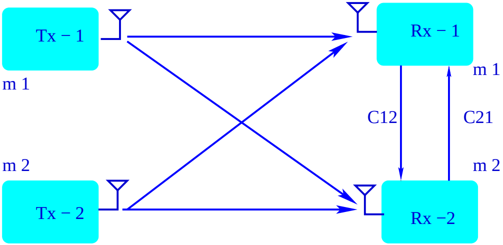
How to share the secret key ?

- Feedback link
- Possible to agree on a secret key if the sender and receiver has an access to correlated sources

Cooperation Vs Secrecy

- How do cooperation and secrecy interact
- Is there a trade-off or parallelism ?
- Cooperation can increase the throughput of the system
- Cooperation can also increase the secrecy
- Can we get both the benefits?

Interference Channel with Cooperation



- System model:

$$y_1 = h_{11}x_1 + h_{12}x_2 + z_1$$
$$y_2 = h_{21}x_1 + h_{22}x_2 + z_2$$

- Receiver Cooperative link:
  - Cooperative links are noiseless with capacity C_{ij} from Rx-i to Rx-j
  - Encoding must satisfy casuality constraints
    - $u_{21}[n]$: function of $\{y_2[1], \ldots, y_2[n-1], u_{12}[1], \ldots, u_{12}[n-1]\}$
    - $u_{12}[n]$: function of $\{y_1[1], \ldots, y_1[n-1], u_{21}[1], \ldots, u_{21}[n-1]\}$

- A $(2^{nR_1}, 2^{nR_2}, n)$ code has the following components
  - Secret message set $\mathbb{W}_k = \{1, \ldots, M_k\}$, $k = 1, 2$
  - Stochastic encoding function: $f_k : w_k \to x_k$, $w_k \in \mathbb{W}_k$, $k = 1, 2$
  - Decoding function: $\phi_k(y_k) = \hat{w}_k$, $k = 1, 2$
  - Encoding functions at each Rx
- Secrecy is measured as:

$$R_l^{(i)} = \frac{1}{n} I(w_j, y_i^n) \text{ and } i \neq j$$

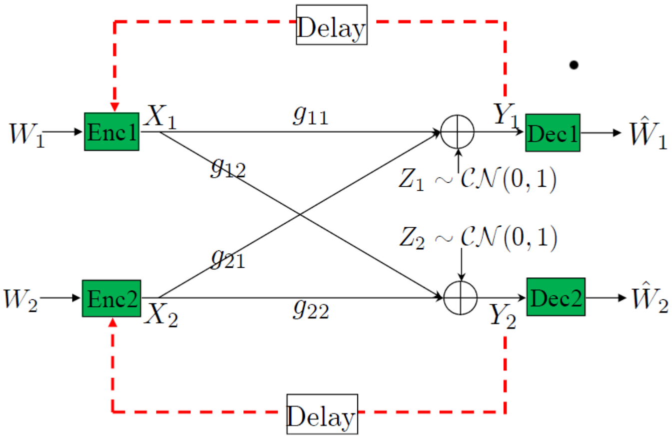
- A rate quadruple $(R_1, R_2, R_l^{(1)}, R_l^{(2)})$ is said to be achievable if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes such that

$$\lim_{n\to\infty} P_{e,j}^{(n)} = 0$$

$$\lim_{n\to\infty} R_l^{(j)} \le R_l^{(j)}$$

- To characterize the rate-leakage region

Other problem of interest



Achievability Proof in case of DM-WTC

Codebook Generation

- Assume that $C_s > 0$ and fix the pmf $p(u, x)$ that attains it.
- Randomly and independently generate $2^{n\bar{R}}$ sequences $u^n(l)$, $l \in [1 : 2^{n\bar{R}}]$ and according to $\prod_{i=1}^{n} p(u_i)$
- Partition the set of indices $[1 : 2^{n\bar{R}}]$ into 2^{nR} bins
- The codebook $\mathbf{B} = [\mathbf{B}(m) : m \in [1 : 2^{nR}]]$ is revealed to all parties

Encoding

- For sending $m \in [1 : 2^{nR}]$, the encoder picks an index $l \in [(m-1)2^{n(R-\bar{R})} + 1 : m2^{n(R-\bar{R})}]$, generate $X^n(m) \sim \prod_{i=1}^{n} p_{X|U}(x_i|u_i(l))$ and transmits it

Decoding

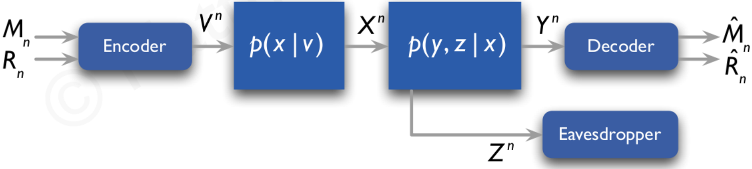
- Decoder declares that $\hat{l}$ is sent if $(u^n(\hat{l}), y^n) \in T_\epsilon^{(n)}$
- By the LLN and packing lemma, it can be shown that if

$$\overline{R} < I(U;Y) - \delta(\epsilon)$$

then $P(\text{error}) \to 0$ as $n \to \infty$

Information Leakage Rate

- For each $B(m)$, the eavesdropper has roughly $2^{n[\overline{R}-R-I(U;Z)]}$ $u^n(l)$ sequences such that $(u^n(l), z^n) \in T_\epsilon^n$
- If $\overline{R} - R > I(U;Z)$, then eavesdropper has almost no information about the actual message sent


M_n
R_n
Encoder
V^n
$p(x \mid v)$
X^n
$p(y, z \mid x)$
Y^n
Decoder
$\hat{M}_n$
$\hat{R}_n$
Z^n
Eavesdropper