Covert Communication with Channel-State Information at the Transmitter

Si-Hyeon Lee

Joint Work with Ligong Wang, Ashish Khisti, and Gregory W. Wornell

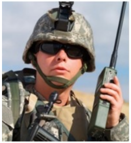
POSTECH
POHANG UNIVERSITY OF SCIENCE AND TECHNOLOGY

July 27, 2017

Covert Communication

- Transmitter and receiver wish to communicate reliably, while ensuring that their communication is not detected by the warden.

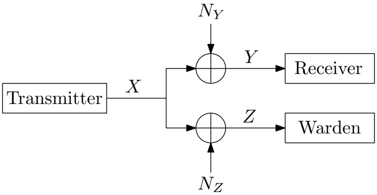
Covert Communication



Warden

- Hypothesis test by the warden
  - Probability of false alarm: α
  - Probability of missed detection: β
- Covertness guaranteed if $D(P_{Z,\text{Sending}} \| P_{Z,\text{Not sending}})$ is small
  - Blind test: $\alpha + \beta = 1$
  - Optimal test: $\alpha + \beta \geq 1 - \sqrt{D(P_{Z,\text{Sending}} \| P_{Z,\text{Not sending}})}$

Square Root Law



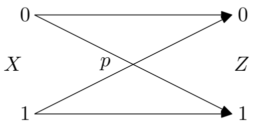
- Maximum amount of information scales like the square root of the blocklength
  - AWGN channel [Bash-Goekel-Towsley 13]
  - A broad class of DMC [Bloch 16], [Wang-Wornell-Zheng 16]

When We Beat the Square Root Law?

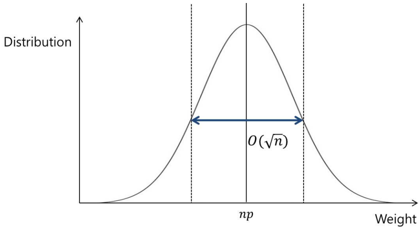
- Unknown channel statistics at the warden
  - BSCs with unknown cross over probability [Che-Bakshi-Chan-Jaggi 14]
  - AWGN with unknown noise power [Lee-Baxley-Weitnauer-Walkenhorst 15]

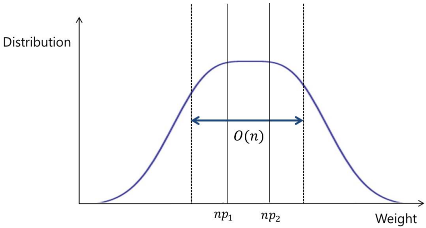
- This talk: State-dependent channel with CSI at the transmitter

Binary Symmetric Channel

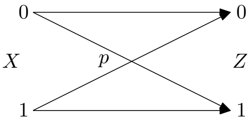


- p fixed and known: Zero capacity [Bloch 16], [Wang-Wornell-Zheng 16]
- p random and unknown: Positive capacity [Che-Bakshi-Chan-Jaggi 14]
- p fixed and known, realizations known to the transmitter
  - Our model
  - Positive capacity by pre-cancellation



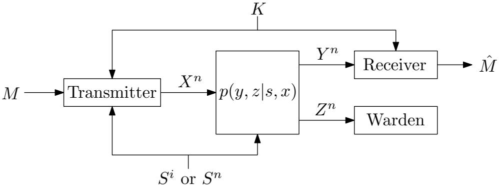


Binary Symmetric Channel



- p fixed and known: Zero capacity [Bloch 16], [Wang-Wornell-Zheng 16]
- p random and unknown: Positive capacity [Che-Bakshi-Chan-Jaggi 14]
- p fixed and known, realizations known to the transmitter
  - Our model
  - Positive capacity by pre-cancellation

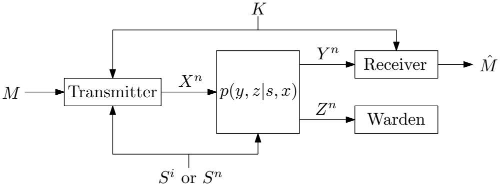
Model



- State-dependent DMC $(\mathcal{X}, \mathcal{S}, \mathcal{Y}, \mathcal{Z}, P_S, P_{Y,Z|S,X})$
- Transmitter and receiver share a secret key $K \in [1 : 2^{nR_0}]$
- Input cost function $b(x^n) = \frac{1}{n}\sum_{i=1}^{n} b(x_i)$
- State sequence known to the transmitter causally or noncausally

- (R, R_K, n) code for causal CSI
  - Encoding function at time i: $(M, K, S^i) \to X_i$
  - Decoding function $(Y^n, K) \to \hat{M}$

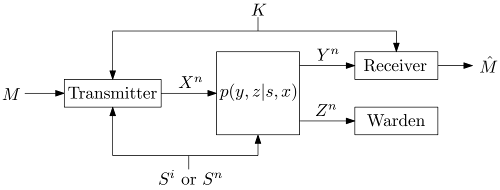
Model



- State-dependent DMC $(\mathcal{X}, \mathcal{S}, \mathcal{Y}, \mathcal{Z}, P_S, P_{Y,Z|S,X})$
- Transmitter and receiver share a secret key $K \in [1 : 2^{nR_0}]$
- Input cost function $b(x^n) = \frac{1}{n} \sum_{i=1}^{n} b(x_i)$
- State sequence known to the transmitter causally or noncausally

- (R, R_K, n) code for noncausal CSI
  - Encoding function: $(M, K, S^n) \to X^n$
  - Decoding function $(Y^n, K) \to \hat{M}$

Model



- Covert communication:
  - $x_0 \in \mathcal{X}$: "no input" symbol, $Q_0(\cdot) = \sum_{s \in \mathcal{S}} P_S(s) P_{Z|S,X}(\cdot|s, x_0)$
  - Small $D(\widehat{P}_{Z^n} \| Q_0^{\times n})$ ensures the warden's best hypothesis test performs not much better than a blind test.

- A covert rate of R is achievable if $\exists$ a sequence of (R, R_K, n) codes that simultaneously satisfies
  - input cost constraint $\limsup_{n\to\infty} E_{M,K,S^n}[b(X^n)] \leq B$
  - reliability constraint $\lim_{n\to\infty} P(\hat{M} \neq M) = 0$
  - covertness constraint $\lim_{n\to\infty} D(\widehat{P}_{Z^n} \| Q_0^{\times n}) = 0$

- Covert capacity C: Supremum of all achievable covert rates

Main Results: Causal CSI

Theorem 1 (Upper Bound)

For $R_K \geq 0$ and $B \geq 0$, the covert capacity is upper-bounded as

$$C \leq \max_{\substack{P_V,\ x(v,s): \\ P_Z = Q_0,\ \mathsf{E}[b(X)] \leq B}} I(V;Y).$$

Theorem 2 (Lower Bound)

For $R_K \geq 0$ and $B \geq 0$, the covert capacity is lower-bounded as

$$C \geq \max_{\substack{P_V,\ x(v,s): \\ P_Z = Q_0,\ \mathsf{E}[b(X)] \leq B,\ I(V;Z) - I(V;Y) < R_K}} I(V;Y).$$

Main Results: Causal CSI

Theorem 1 (Upper Bound)

For $R_K \geq 0$ and $B \geq 0$, the covert capacity is upper-bounded as

$$C \leq \max_{\substack{P_V,\ x(v,s): \\ P_Z = Q_0,\ \mathrm{E}[b(X)] \leq B}} I(V;Y).$$

Theorem 2 (Lower Bound)

For $R_K \geq 0$ and $B \geq 0$, the covert capacity is lower-bounded as

$$C \geq \max_{\substack{P_V,\ x(v,s): \\ P_Z = Q_0,\ \mathrm{E}[b(X)] \leq B,\ I(V;Z) - I(V;Y) < R_K}} I(V;Y).$$

Main Results: Causal CSI

Theorem 1 (Upper Bound)

For $R_K \geq 0$ and $B \geq 0$, the covert capacity is upper-bounded as

$$C \leq \max_{\substack{P_V,\ x(v,s): \\ P_Z = Q_0,\ \ \mathsf{E}[b(X)] \leq B}} I(V;Y).$$

Theorem 2 (Lower Bound)

For $R_K \geq 0$ and $B \geq 0$, the covert capacity is lower-bounded as

$$C \geq \max_{\substack{P_V,\ x(v,s): \\ P_Z = Q_0,\ \ \mathsf{E}[b(X)] \leq B,\ \ I(V;Z) - I(V;Y) < R_K}} I(V;Y).$$

Main Results: Noncausal CSI

Theorem 3 (Upper Bound)

For $R_K \geq 0$ and $B \geq 0$, the covert capacity is upper-bounded as

$$C \leq \max_{\substack{P_{U|S},\ x(u,s): \\ P_Z = Q_0,\ \mathrm{E}[b(X)] \leq B}} I(U;Y) - I(U;S).$$

Theorem 4 (Lower Bound)

For $R_K \geq 0$ and $B \geq 0$, the covert capacity is lower-bounded as

$$C \geq \max_{\substack{P_{U|S},\ x(u,s): \\ P_Z = Q_0,\ \mathrm{E}[b(X)] \leq B,\ I(U;Z) - I(U;Y) < R_K}} I(U;Y) - I(U;S).$$

Main Results: Noncausal CSI

Theorem 3 (Upper Bound)

For $R_K \geq 0$ and $B \geq 0$, the covert capacity is upper-bounded as

$$C \leq \max_{\substack{P_{U|S},\ x(u,s): \\ P_Z = Q_0,\ \mathsf{E}[b(X)] \leq B}} I(U;Y) - I(U;S).$$

Theorem 4 (Lower Bound)

For $R_K \geq 0$ and $B \geq 0$, the covert capacity is lower-bounded as

$$C \geq \max_{\substack{P_{U|S},\ x(u,s): \\ P_Z = Q_0,\ \mathsf{E}[b(X)] \leq B,\ I(U;Z) - I(U;Y) < R_K}} I(U;Y) - I(U;S).$$

Main Results: Noncausal CSI

Theorem 3 (Upper Bound)

For $R_K \geq 0$ and $B \geq 0$, the covert capacity is upper-bounded as

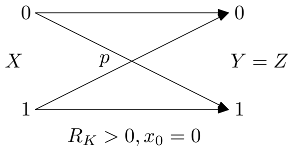
$$C \leq \max_{\substack{P_{U|S},\ x(u,s): \\ P_Z = Q_0,\ \mathbb{E}[b(X)] \leq B}} I(U;Y) - I(U;S).$$

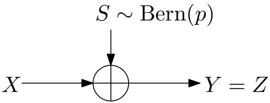
Theorem 4 (Lower Bound)

For $R_K \geq 0$ and $B \geq 0$, the covert capacity is lower-bounded as

$$C \geq \max_{\substack{P_{U|S},\ x(u,s): \\ P_Z = Q_0,\ \mathbb{E}[b(X)] \leq B,\ I(U;Z) - I(U;Y) < R_K}} I(U;Y) - I(U;S).$$

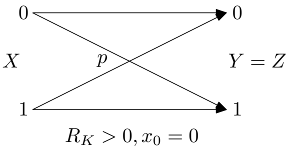
Example: Binary Symmetric Channels

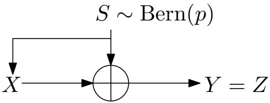




- Without CSI at the transmitter: $C = 0$
- With CSI at the transmitter: $C = H_b(p)$ for both causal and noncausal cases
  - $X = V \oplus S$, $V \sim \mathrm{Bern}(p)$ independent with S

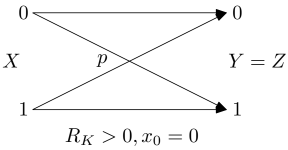
Example: Binary Symmetric Channels

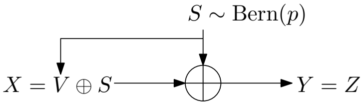




- Without CSI at the transmitter: $C = 0$
- With CSI at the transmitter: $C = H_b(p)$ for both causal and noncausal cases
  - $X = V \oplus S$, $V \sim \mathrm{Bern}(p)$ independent with S

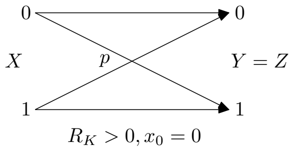
Example: Binary Symmetric Channels





- Without CSI at the transmitter: $C = 0$
- With CSI at the transmitter: $C = H_b(p)$ for both causal and noncausal cases
  - $X = V \oplus S$, $V \sim \mathrm{Bern}(p)$ independent with S

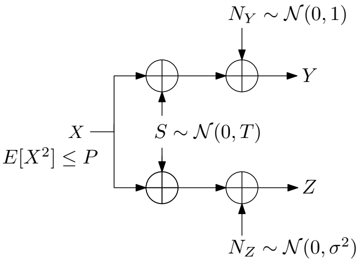
Example: Binary Symmetric Channels



$$V = Y = Z$$

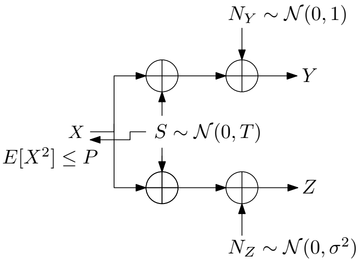
- Without CSI at the transmitter: $C = 0$
- With CSI at the transmitter: $C = H_b(p)$ for both causal and noncausal cases
  - $X = V \oplus S$, $V \sim \text{Bern}(p)$ independent with S

Example: AWGN Channels



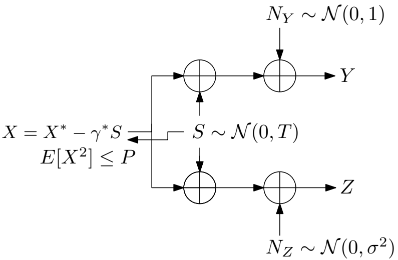
- Without CSI at the transmitter: $C = 0$
- With CSI at the transmitter: $C > 0$
  - Make room for message transmission by reducing the interference power, i.e., $X = X^* - \gamma^* S$
  - Choose P^* and γ^* to simultaneously satisfy the covertness constraint and the input power constraint, i.e., $\gamma^* = \min\left\{1, \frac{P}{2T}\right\}$, $T^* = (1-\gamma^*)^2 T$, $P^* = T - T^*$

Example: AWGN Channels



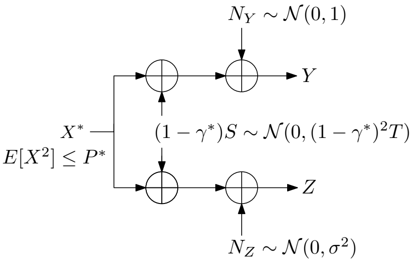
- Without CSI at the transmitter: $C = 0$
- With CSI at the transmitter: $C > 0$
  - Make room for message transmission by reducing the interference power, i.e., $X = X^* - \gamma^* S$
  - Choose P^* and γ^* to simultaneously satisfy the covertness constraint and the input power constraint, i.e., $\gamma^* = \min\left\{1, \frac{P}{2T}\right\}$, $T^* = (1-\gamma^*)^2 T$, $P^* = T - T^*$

Example: AWGN Channels



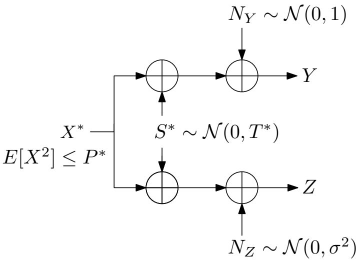
- Without CSI at the transmitter: $C = 0$
- With CSI at the transmitter: $C > 0$
  - Make room for message transmission by reducing the interference power, i.e., $X = X^* - \gamma^* S$
  - Choose P^* and γ^* to simultaneously satisfy the covertness constraint and the input power constraint, i.e., $\gamma^* = \min\left\{1, \frac{P}{2T}\right\}$, $T^* = (1-\gamma^*)^2 T$, $P^* = T - T^*$

Example: AWGN Channels



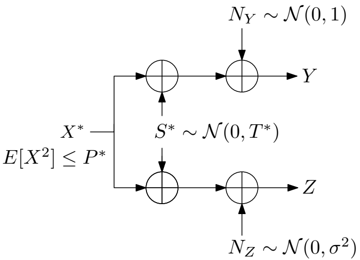
- Without CSI at the transmitter: $C = 0$
- With CSI at the transmitter: $C > 0$
  - Make room for message transmission by reducing the interference power, i.e., $X = X^* - \gamma^* S$
  - Choose P^* and γ^* to simultaneously satisfy the covertness constraint and the input power constraint, i.e., $\gamma^* = \min\left\{1, \frac{P}{2T}\right\}$, $T^* = (1-\gamma^*)^2 T$, $P^* = T - T^*$

Example: AWGN Channels



- Without CSI at the transmitter: $C = 0$
- With CSI at the transmitter: $C > 0$
  - Make room for message transmission by reducing the interference power, i.e., $X = X^* - \gamma^* S$
  - Choose P^* and γ^* to simultaneously satisfy the covertness constraint and the input power constraint, i.e., $\gamma^* = \min\left\{1, \frac{P}{2T}\right\}$, $T^* = (1-\gamma^*)^2 T$, $P^* = T - T^*$

Example: AWGN Channels



- Causal CSI at the transmitter
  - Choose $V = X^*$ and treat interference as noise at the receiver

Example: AWGN Channels

- $\gamma^* = \min\left\{1, \frac{P}{2T}\right\},\ T^* = (1-\gamma^*)^2 T,\ P^* = T - T^*$

Theorem 5 (Causal CSI)

If

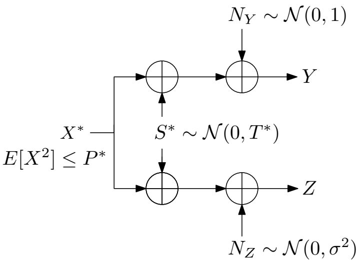
$$R_K > \frac{1}{2}\log\left(1 + \frac{P^*}{T^* + \sigma^2}\right) - \frac{1}{2}\log\left(1 + \frac{P^*}{T^* + 1}\right),$$

the covert capacity with causal CSI at the transmitter is lower-bounded as

$$C_{\mathrm{c}} \geq \frac{1}{2}\log\left(1 + \frac{P^*}{T^* + 1}\right).$$

- If the warden's channel is degraded, i.e., $\sigma^2 > 1$, a secret key is not needed to achieve the rate

Example: AWGN Channels



- Noncausal CSI at the transmitter
  - Choose U as in the dirty paper coding with input power constraint P^* and interference power T^*

Example: AWGN Channels

- $\gamma^* = \min\left\{1, \frac{P}{2T}\right\}$, $T^* = (1-\gamma^*)^2 T$, $P^* = T - T^*$

Theorem 6 (Noncausal CSI)

If

$$R_K > \frac{1}{2}\log\left(1 + \frac{(P^* + \frac{P^*}{P^*+1}T^*)^2}{(P^* + (\frac{P^*}{P^*+1})^2 T^*)(P^* + T^* + \sigma^2) - (P^* + \frac{P^*}{P^*+1}T^*)^2}\right) - \frac{1}{2}\log\left(1 + \frac{(P^* + \frac{P^*}{P^*+1}T^*)^2}{(P^* + (\frac{P^*}{P^*+1})^2 T^*)(P^* + T^* + 1) - (P^* + \frac{P^*}{P^*+1}T^*)^2}\right),$$

the covert capacity with noncausal CSI at the transmitter is given by

$$C_{\mathrm{nc}} = \frac{1}{2}\log\left(1 + P^*\right).$$

- If the warden's channel is degraded, i.e., $\sigma^2 > 1$, a secret key is not needed to achieve the capacity

Example: AWGN Channels

- For R_K sufficiently large,

$$C_{\mathrm{c}} \geq \frac{1}{2}\log\left(1+\frac{P^*}{T^*+1}\right)$$
$$C_{\mathrm{nc}} = \frac{1}{2}\log\left(1+P^*\right).$$

- If $T^*=0$, i.e., $T \leq \frac{P}{2}$, $C_{\mathrm{c}} = C_{\mathrm{nc}}$.
- As $T \to \infty$, $P^* \to P$ and hence C_{nc} approaches to the capacity without a covertness constraint

Achievability with Noncausal CSI

- Key idea: Gelfend-Pinsker coding, except that likelihood encoding by [Song-Cuff-Poor 16], [Goldfeld-Kramer-Permuter-Cuff 17] is used instead of joint-typicality encoding.

- Codebook generation:
  - Fix $P_{U|S}$ and $x(u, s)$ such that $P_Z = Q_0$ and $\mathrm{E}[b(X)] \le \frac{B}{1+\epsilon'}$.
  - For each $k \in [1:2^{nR_K}]$ and $m \in [1:2^{nR}]$, randomly generate a subcodebook $\mathcal{C}(k, m) = \{u^n(k, m, l) : l \in [1:2^{nR'}]\}$ according to $\prod_{i=1}^n P_U(u_i)$.

- Encoding: Given state sequence s^n, secret key k, and message m, evaluate the likelihood

$$g(l|s^n, k, m) = \frac{P_{S|U}^{\times n}(s^n|u^n(k, m, l))}{\sum_{l' \in [1:2^{nR'}]} P_{S|U}^{\times n}(s^n|u^n(k, m, l'))}.$$

  The encoder randomly generates l according to the above and transmits x^n where $x_i = x(u_i(k, m, l), s_i)$.

Achievability with Noncausal CSI

- Decoding: Upon receiving y^n, with access to the secret key k, the decoder declares that $\hat{m}$ is sent if it is the unique message such that

$$(u^n(k, \hat{m}, l), y^n) \in \mathcal{T}_\epsilon^{(n)}$$

for some $l \in [1 : 2^{nR'}]$; otherwise it declares an error.

- Covertness analysis:
  - Γ: Joint distribution when the codeword index in the subcodebook is uniformly chosen and then the state sequence is generated in an iid manner according to $P_{S|U}$.
  - $\widehat{P}_{Z^n} \approx \Gamma_{Z^n}$, if $R' > I(U; S)$
  - $\Gamma_{Z^n} \approx Q_0^{\times n}$, if $R_K + R + R' > I(U; Z)$

- Reliability analysis:
  - Done by packing lemma
  - $R + R' < I(U; Y)$

Converse with Noncausal CSI

- Step (a): Bounding techniques for channels with noncausal CSI without covertness constraint, where $U_i := (M, K, Y^{i-1}, S_{i+1}^n)$.
- Step (b): Characterization of capacity function

$$C(A,B) := \max_{\substack{P_{U|S}, P_{X|U,S}: \\ \mathsf{E}[b(X)]\leq B,\ D(P_Z\|Q_0)\leq A}} (I(U;Y) - I(U;S))$$

  - The function $C(A,B)$ is non-decreasing in each of A and B, and concave and continuous in (A,B).
- Step (c): Application of covertness and input cost constraints

$$\begin{aligned}
R &\overset{(a)}{\leq} \frac{1}{n}\sum_{i=1}^{n}(I(U_i;Y_i) - I(U_i;S_i)) + \epsilon_n \\
&\overset{(b)}{\leq} \frac{1}{n}\sum_{i=1}^{n} C(D(\widehat{P}_{Z_i}\|Q_0), \mathsf{E}[b(X_i)]) + \epsilon_n \\
&\overset{(b)}{\leq} C\left(\frac{1}{n}\sum_{i=1}^{n} D(\widehat{P}_{Z_i}\|Q_0), \frac{1}{n}\sum_{i=1}^{n}\mathsf{E}[b(X_i)]\right) + \epsilon_n \\
&\overset{(c)}{\to} C\,(0,B)
\end{aligned}$$

Conclusion

- Considered state dependent channel with state information at the transmitter
- Characterized the covert capacity when a sufficiently long secret key is shared between the transmitter and the receiver
- Derived lower bounds on the rate of the secret key that is needed to achieve the covert capacity
- For certain channel models, showed that the covert capacity is positive with CSI at the transmitter, but is zero without CSI
- Full version will be uploaded on arXiv soon