3-Receivers Broadcast Channels with Common and Confidential Messages

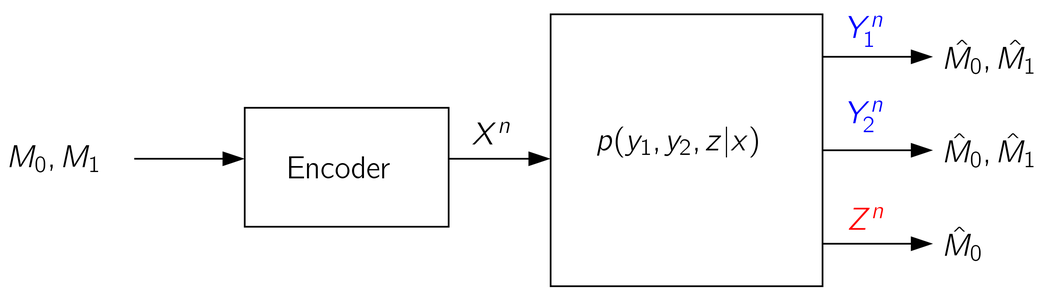
Yeow-Khiang Chia and Abbas El Gamal
Department of Electrical Engineering, Stanford University

Abstract

- Extend wiretap channel with confidential messages to:
  I. 2 receivers and 1 eavesdropper
  II. 1 receiver and 2 eavesdroppers
- Establish inner bounds using subcode generation and indirect decoding
- Bounds are shown to be optimal for some special cases

3-Receiver Wiretap Channel I

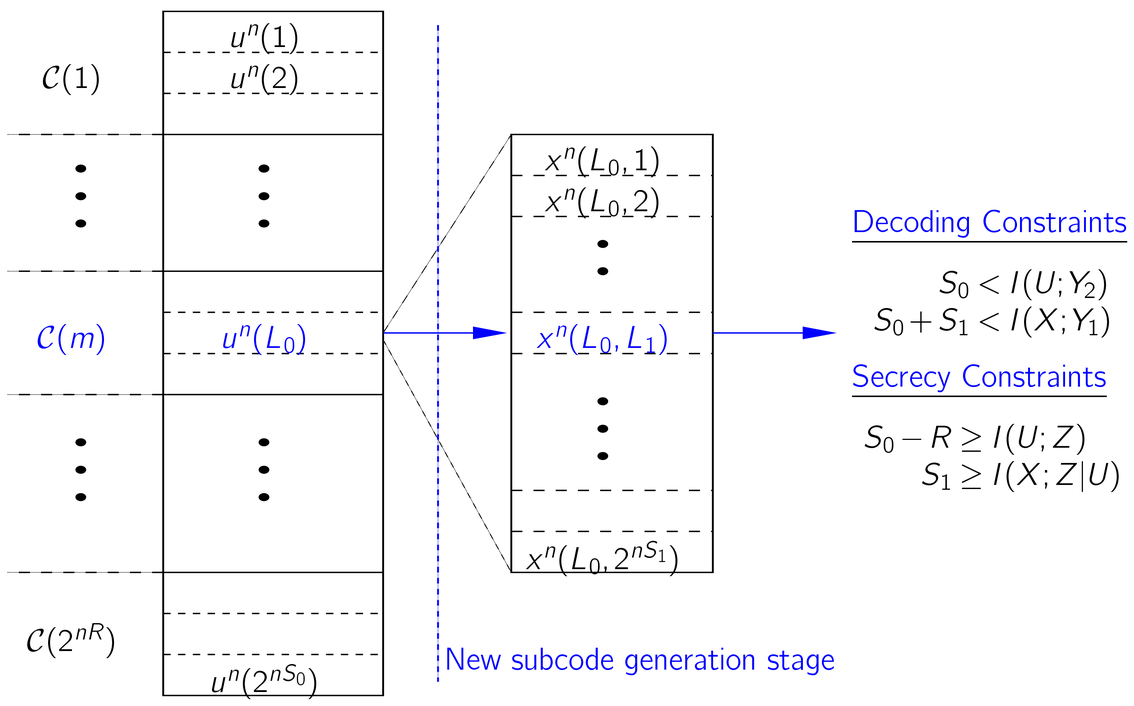
- Common message to all receivers. Confidential message to Y_1 and Y_2



- Equivocation constraint: $R_e \leq H(M_1|Z^n)/n$
- Secrecy capacity region: Set of all achievable rate tuples (R_0, R_1, R_e)

Outline of Achievability

- Consider example with $R_0 = 0$ and $X \to Y_1 \to Z$



- New coding strategy: Generate second subcode of X^n sequences for each $u^n(l_0)$. To send message m, pick random L_0, L_1 such that $u^n(L_0) \in \mathcal{C}(m)$ and transmit $x^n(L_0, L_1)$
- Decoding: Y_2 decodes L_0 (and hence m) directly through U. Y_1 decodes L_0 indirectly [1] through X. It looks for unique L_0 such that $(x^n(L_0, L_1), Y_1^n) \in \mathcal{T}_\epsilon^{(n)}$
- Secrecy Constraint: To confuse eavesdropper Z, require enough codewords in both the u^n and x^n subcodes
- Fourier-Motzkin elimination, we obtain:

$$R < \max_{p(u)p(x|u)} \min\{I(X;Y_1) - I(X;Z), I(U;Y_2) - I(U;Z)\}$$

- New achievable rate can be shown to be strictly larger than extension of (optimum) achievable schme for 1 receiver and 1 eavesdropper [2]

New Inner Bound I

- Inner bound for general case obtained by combining new coding strategy with Marton binning and superposition coding

  An inner bound to the secrecy capacity region of the 2-receiver, 1-eavesdropper broadcast channel with one common and one confidential messages is given by the set of non-negative rate tuples (R_0, R_1, R_e) such that

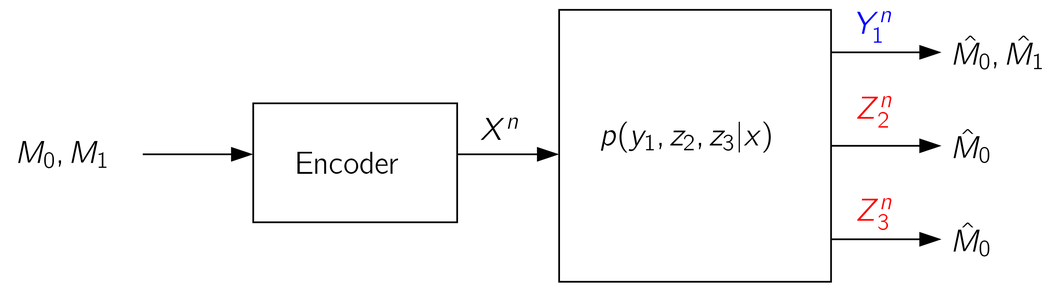
$$\begin{aligned}
R_0 &< I(U;Z)\\
R_1 &< \min\{I(V_1;Y_1|U) - I(V_1;Z|V_0), I(V_2;Y_2|U) - I(V_2;Z|V_0)\}\\
2R_1 &< I(V_1;Y_1|U) + I(V_2;Y_2|U) - I(V_1;V_2|V_0)\\
R_0 + R_1 &< \min\{I(V_1;Y_1) - I(V_1;Z|V_0), I(V_2;Y_2) - I(V_2;Z|V_0)\}\\
R_0 + 2R_1 &< I(V_1;Y_1) + I(V_2;Y_2|U) - I(V_1;V_2|V_0)\\
R_0 + 2R_1 &< I(V_2;Y_2) + I(V_1;Y_1|U) - I(V_1;V_2|V_0)\\
2R_0 + 2R_1 &< I(V_1;Y_1) + I(V_2;Y_2) - I(V_1;V_2|V_0)\\
R_e &\leq [R_1 - I(V_0;Z|U)]^+
\end{aligned}$$

for some $p(u, v_0, v_1, v_2, x) = p(u)p(v_0|u)p(v_1, v_2|v_0)p(x|v_1, v_2)$ such that $I(V_1, V_2; Z|V_0) \leq I(V_1;Z|V_0) + I(V_2;Z|V_0) - I(V_1;V_2|V_0)$, where $[x]^+ := \max\{0, x\}$

- Bound is optimum when
  - Both Y_1 and Y_2 are less noisy than Z
  - Channel is reversely degraded [3] and asymptotic perfect secrecy is required ($R_e = R_1$ and $R_0 = 0$)

3-Receiver Wiretap Channel II

- Common message to all receivers. Confidential message to Y_1 only



- Equivocation constraint: $R_{e2} \leq H(M_1|Z_2^n)/n$; $R_{e3} \leq H(M_1|Z_3^n)/n$
- Secrecy capacity region: Set of all achievable rate tuples $(R_0, R_1, R_{e2}, R_{e3})$
- Focus on case of Multi-level Broadcast Channel with degraded message sets [4]

Inner and Outer Bounds II

Inner bound:

An inner bound to the secrecy capacity region of the 1-receiver, 2-eavesdropper multi-level broadcast channel with one common message and one confidential message is given by the set of non-negative rate tuples $(R_0, R_1, R_{e2}, R_{e3})$ such that

$$\begin{aligned}
R_0 &< \min\{I(U;Z_2), I(U_3;Z_3)\},\\
R_1 &< I(V;Y_1|U),\\
R_0 + R_1 &< I(U_3;Z_3) + I(V;Y_1|U_3),\\
R_{e2} &\leq \min\{R_1, I(V;Y_1|U) - I(V;Z_2|U)\},\\
R_{e2} &\leq [I(U_3;Z_3) - R_0 - I(U_3;Z_2|U)]^+ + I(V;Y_1|U_3) - I(V;Z_2|U_3),\\
R_{e3} &\leq \min\{R_1, [I(V;Y_1|U_3) - I(V;Z_3|U_3)]^+\}
\end{aligned}$$

for some $p(u, u_3, v, x) = p(u)p(u_3|u)p(v|u_3)p(x|v)$

Outer bound:

$$\begin{aligned}
R_0 &\leq \min\{I(U;Y_2), I(U_3;Y_3)\},\\
R_1 &\leq I(V;Y_1|U),\\
R_0 + R_1 &\leq I(U_3;Y_3) + I(V;Y_1|U_3),\\
R_{e2} &\leq I(X;Y_1|U) - I(X;Y_2|U),\\
R_{e2} &\leq [I(U_3;Z_3) - R_0 - I(U_3;Z_2|U)]^+ + I(X;Y_1|U_3) - I(X;Z_2|U_3),\\
R_{e3} &\leq [I(V;Y_1|U_3) - I(V;Z_3|U_3)]^+
\end{aligned}$$

for some $p(u, u_3, v, x) = p(u)p(u_3|u)p(v|u_3)p(x|v)$

Bounds are optimum when (i) Y_1 is *more capable* than Z_3; and (ii) when one of the eavesdroppers can be considered *neutral*; i.e. we can set R_{e2} or R_{e3} to zero

References

[1] Chandra Nair and Abbas El Gamal. An outer bound to the capacity region of the broadcast channel. *IEEE Trans. Inf. Theory*, 53(1):350–355, January 2007.

[2] Yeow-Khiang Chia and Abbas El Gamal. 3-receivers broadcast channels with common and confidential messages. In *Proc. IEEE International Symposium on Information Theory*, Seoul, Korea, July 2009.

[3] Ashish Khisti, Aslan Tchamkerten, and Gregory W. Wornell. Secure broadcasting over fading channels. *IEEE Trans. Inf. Theory*, 54(6):2453–2469, 2008.

[4] Shashi Borade, Lizhong Zheng, and Mitchell Trott. Multilevel broadcast networks. In *Proc. IEEE International Symposium on Information Theory*, pages 1151–1155, Nice, France, June 2007.