S@movar
Comelec

MIXING A COVERT AND NON COVERT USERS

Abdelaziz Bounhar - Michèle Wigger - Mireille Sarkiss

TELECOM SudParis · TELECOM Paris · IP PARIS · Institut Mines-Télécom

ABSTRACT

Covert communication refers to any communication setup where users wish to convey information while ensuring low probability of detection by other users, adversaries or network monitoring nodes. We show that:

- It is possible to remain covert while other non-covert users are present.
- The presence of the non-covert users allows us to improve the secret-key and message rates of the covert user.

SETUP OF COMMUNICATION

Define the message and key sets

$$\mathcal{M}_1 \triangleq \{1, \dots, M_1\}, \quad \mathcal{M}_2 \triangleq \{1, \dots, M_2\}, \quad \mathcal{K} \triangleq \{1, \dots, K\}, \tag{1}$$

for given numbers M_1, M_2, and K and let the messages W_1 and W_2 and the key S be uniform over $\mathcal{M}_1, \mathcal{M}_2$, and $\mathcal{K}$ respectively.

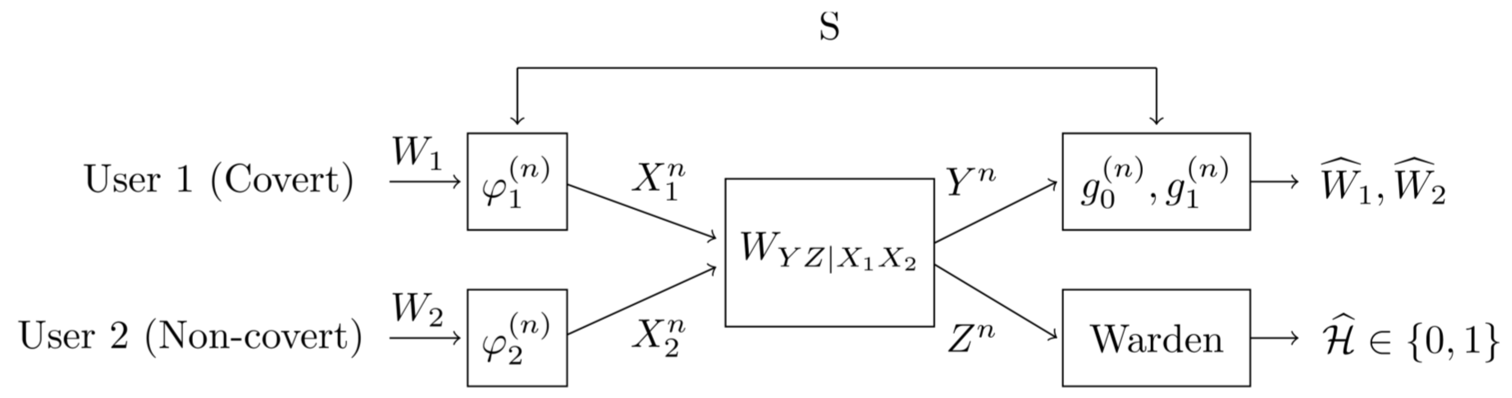


Fig. 1: Multi-access communication where communication of User 1 has to remain undetectable to an external warden.

Reliability:

$$P_{e0} \triangleq \Pr\left(\widehat{W}_2 \neq W_2 \middle| \mathcal{H} = 0\right) \tag{2}$$

$$P_{e1} \triangleq \Pr\left(\widehat{W}_2 \neq W_2 \text{ or } \widehat{W}_1 \neq W_1 \middle| \mathcal{H} = 1\right) \tag{3}$$

Covertness:
For each $w_2 \in \mathcal{M}_2$ and $W_2 = w_2$, define the warden's output distribution under $\mathcal{H} = 1$

$$\widehat{Q}^n_{\mathcal{C},w_2}(z^n) \triangleq \frac{1}{M_1 K} \sum_{(w_1,s)} W^{\otimes n}_{Z|X_1X_2}(z^n | x_1^n(w_1, s), x_2^n(w_2)), \tag{4}$$

and under $\mathcal{H} = 0$

$$W^{\otimes n}_{Z|X_1X_2}(z^n | 0^n, x_2^n(w_2)), \tag{5}$$

and the divergence between these two distributions:

$$\delta_{n,w_2} \triangleq \mathbb{D}\left(\widehat{Q}^n_{\mathcal{C},w_2} \middle\| W^{\otimes n}_{Z|X_1X_2}(\cdot | 0^n, x_2^n(w_2))\right), \quad w_2 \in \mathcal{M}_2. \tag{6}$$

Objective:
We aim to propose coding schemes such that:

$$\lim_{n\to\infty} \delta_{n,w_2} = 0, \qquad w_2 \in \mathcal{M}_2, \tag{7}$$

$$\lim_{n\to\infty} P_{ei} = 0, \qquad i \in \{0, 1\}. \tag{8}$$

Coding scheme:

Fix a large blocklength n and let $t^n = (t_1, \dots, t_n)$ be the time sequence.

Define a pmf P_T and two conditional pmfs $P_{X_{1,n}|T}$ and $P_{X_2|T}$.

Encoding: We use coded time-sharing for both users, i.e. the i-th entry of both users codebooks ($\mathcal{C}_1$ and $\mathcal{C}_2$) are generated (i.i.d.) according to the pmfs $P_{X_{1,n}|T}(\cdot|t_i)$ and $P_{X_2|T}(\cdot|t_i)$.

Decoding: We use successive decoding, i.e. decode message of user 2 then of user 1.

MAIN RESULT

THEOREM 1

A rate-triple (r_1, r_2, k) is achievable, if and only if, for some pmf P_{TX_2} over $\mathcal{T} \times \mathcal{X}_2$ and $\epsilon_1, \epsilon_2 \in [0, 1]$ the following three inequalities hold:

$$r_2 \leq \mathbb{I}(X_2; Y \mid X_1 = 0, T), \tag{9}$$

$$r_1 \leq \sqrt{2} \frac{\mathbb{E}_{P_{TX_2}}[\epsilon_T D_Y(X_2)]}{\sqrt{\mathbb{E}_{P_{TX_2}}[\epsilon_T^2 \cdot \chi_{2,Z}(X_2)]}}, \tag{10}$$

$$k \geq \sqrt{2} \frac{\mathbb{E}_{P_{TX_2}}[\epsilon_T (D_Z(X_2) - D_Y(X_2))]}{\sqrt{\mathbb{E}_{P_{TX_2}}[\epsilon_T^2 \cdot \chi_{2,Z}(X_2)]}}, \tag{11}$$

where for the right-hand sides of (10) and (11) we define $0/0 = 0$ and for any $x_2 \in \mathcal{X}_2$

$$D_Y(x_2) \triangleq \mathbb{D}\left(W_{Y|X_1X_2}(\cdot|1, x_2) \,||\, W_{Y|X_1X_2}(\cdot|0, x_2)\right) \tag{12}$$

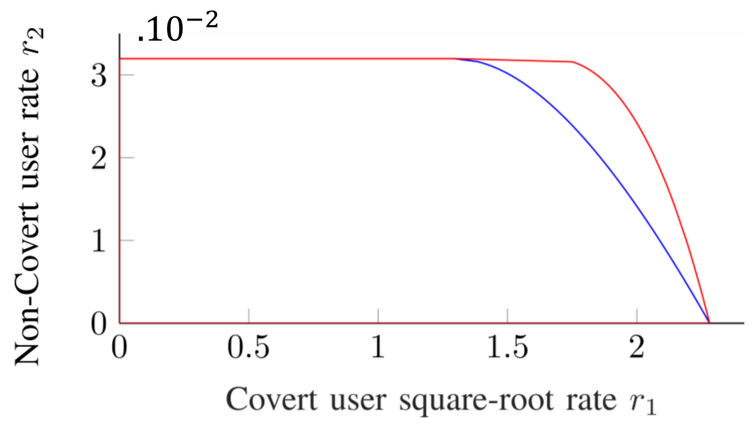
$$D_Z(x_2) \triangleq \mathbb{D}\left(W_{Z|X_1X_2}(\cdot|1, x_2) \,||\, W_{Z|X_1X_2}(\cdot|0, x_2)\right) \tag{13}$$

$$\chi_{2,Z}(x_2) \triangleq \chi_2\left(W_{Z|X_1X_2}(\cdot|1, x_2) \,||\, W_{Z|X_1X_2}(\cdot|0, x_2)\right). \tag{14}$$

SIMULATION

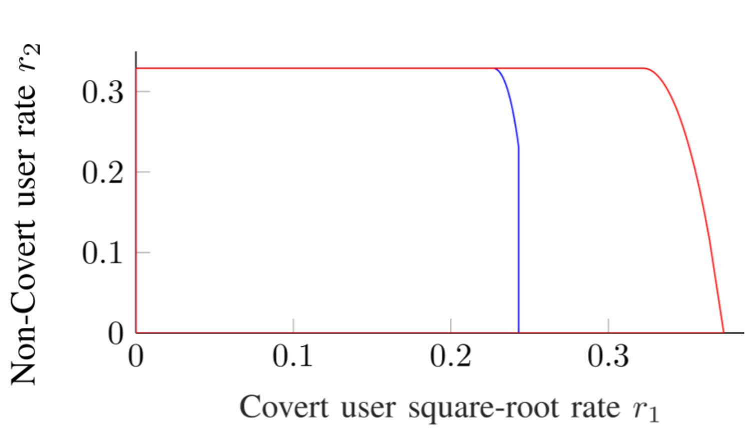
Consider input alphabets $\mathcal{X}_1 = \mathcal{X}_2 = \{0, 1\}$ and randomly generated channel matrices.

Time-sharing improves the rates



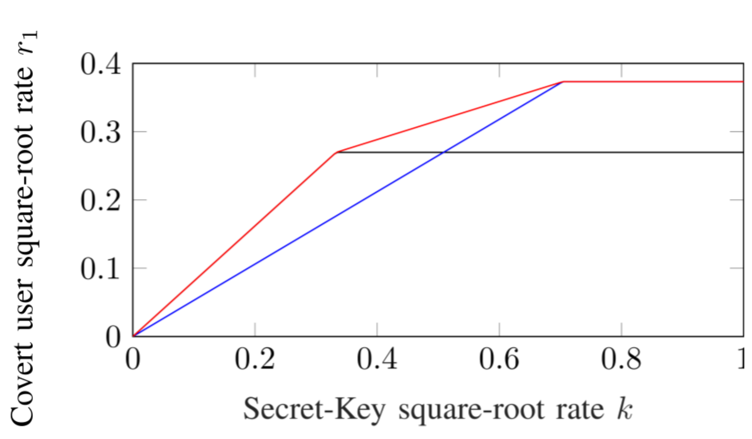
- With time-sharing $|\mathcal{T}| = 2$ (in red).
- Without time-sharing $|\mathcal{T}| = 2$ (in blue).

Higher secret-key rates k increase the rate-region of Theorem 1



- Key-rates $k \leq 0.8$ (in red).
- Key-rates $k \leq 0.3$ (in blue).

The non covert user simulates channel states



- Non constant channel inputs X_2 at User 2 (in red).
- Constant channel inputs $X_2 = 0$ at User 2 (in blue).
- Constant channel inputs $X_2 = 1$ at User 2 (in black).

OUTLOOKS

Generalize to the setup where many covert users are mixed with many non covert users.

Samovar PhD day 23 mars 2023

Contact abdelaziz.bounhar@telecom-paris.fr