Secure Broadcasting with Uncertain Channel State Information

Amal Hyadi*, Zouheir Rezki*, Ashish Khisti† and Mohamed-Slim Alouini*

* Computer, Electrical, and Mathematical Sciences & Engineering (CEMSE) Division, King Abdullah University of Science and Technology (KAUST), Saudi Arabia.

† Electrical and Computer Engineering Department, University of Toronto, Canada.

Abstract

We investigate the problem of secure broadcasting over fast fading channels with imperfect main channel state information (CSI) at the transmitter. In particular, we analyze the effect of the noisy estimation of the main CSI on the throughput of a broadcast channel where the transmission is intended for multiple legitimate receivers in the presence of an eavesdropper. Besides, we consider the realistic case where the transmitter is only aware of the statistics of the eavesdropper's CSI and not of its channel's realizations. First, we discuss the common message transmission case where the source broadcasts the same information to all the receivers, and we provide an upper and a lower bounds on the ergodic secrecy capacity. For this case, we show that the secrecy rate is limited by the legitimate receiver having, on average, the worst main channel link and we prove that a non-zero secrecy rate can still be achieved even when the CSI at the transmitter is noisy. Then, we look at the independent messages case where the transmitter broadcasts multiple messages to the receivers, and each intended user is interested in an independent message. For this case, we present an expression for the achievable secrecy sum-rate and an upper bound on the secrecy sum-capacity and we show that, in the limit of large number of legitimate receivers K, our achievable secrecy sum-rate follows the scaling law $\log((1-\alpha)\log(K))$, where α is the estimation error variance of the main CSI. The special cases of high SNR, perfect and no-main CSI are also analyzed. Analytical derivations and numerical results are presented to illustrate the obtained expressions for the case of independent and identically distributed Rayleigh fading channels.

System Model

We consider a broadcast wiretap channel where a transmitter T communicates with K legitimate receivers $(\mathsf{R}_1, \cdots, \mathsf{R}_K)$ in the presence of an eavesdropper E as depicted in Fig.1.

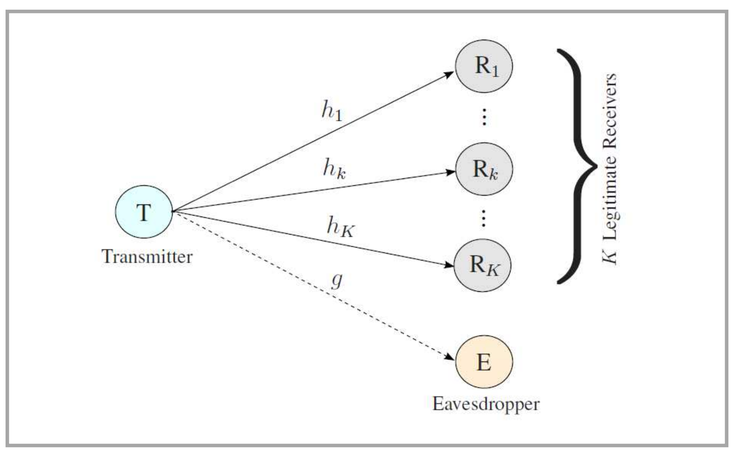


Figure 1: The fading wiretap channel with multiple receivers and one eavesdropper.

- Each terminal is equipped with a single antenna for transmission and reception.
- During every coherence interval $i \in \{1, \cdots, n\}$, the received signals by each legitimate receiver $\mathsf{R}_k, k \in \{1, \cdots, K\}$, and the eavesdropper are, respectively, given by

$$\begin{cases} Y_k(i) = h_k(i)X(i) + v_k(i) \\ Z(i) = g(i)X(i) + w(i), \end{cases} \tag{1}$$

  where $h_k(i) \in \mathbb{C}$, $g(i) \in \mathbb{C}$ are zero-mean, unit-variance complex Gaussian channel gains corresponding to each legitimate channel and the eavesdropper's channel, respectively; and $v_k(i) \in \mathbb{C}$, $w(i) \in \mathbb{C}$ represent zero-mean, unit-variance circularly symmetric white Gaussian noises at R_k and E, respectively; and $X(i)$ is the transmitted message to all the receivers.
- An average transmit power constraint is imposed at the transmitter such that

$$\mathbb{E}[|X(i)|^2] \leq P_{\mathsf{avg}},$$

  where the expectation is over the input distribution.
- The channel gains h_k and g are independent, ergodic and stationary.
- We consider that the transmitter is only aware of the statistics of the eavesdropper's CSI and not of its channel's realizations $g(i)$. Also, we assume that the transmitter is only provided with a noisy version of each $h_k(i)$, say $\hat{h}_k(i) \sim \mathcal{CN}(0,1)$, such that the main channel estimation model can be written as

$$h_k(i) = \sqrt{1-\alpha}\hat{h}_k(i) + \sqrt{\alpha}\tilde{h}_k(i),$$

  where α is the estimation error variance $(\alpha \in [0,1])$ and $\tilde{h}_k(i) \sim \mathcal{CN}(0,1)$ is the zero-mean unit-variance channel estimation error. We assume that $\hat{h}_k(i)$ and $\tilde{h}_k(i)$ are uncorrelated and hence independent.
- We assume that each receiver R_k has a perfect knowledge of its channel gain $h_k(i)$, and that the eavesdropper is aware of its channel gain $g(i)$, and of all the legitimate receivers' channel gains $h_k(i), k \in \{1, \cdots, K\}$. The estimated channel gains $\hat{h}_k(i), k \in \{1, \cdots, K\}$, are known globally.
- We denote $|h_k|^2$, $|\hat{h}_k|^2$, $|\tilde{h}_k|^2$ and $|g|^2$ by γ_k, $\hat{\gamma}_k$, $\tilde{\gamma}_k$ and γ_e, respectively.

Broadcasting a Common Message

In this part, we consider the common message transmission case when a unique confidential information is broadcasted to all the legitimate receivers.

Theorem 1

The common message secrecy capacity, $\mathcal{C}_\mathsf{s}$, of the fast fading broadcast channel under imperfect main channels estimation at the transmitter is bounded by

$$\mathcal{C}_\mathsf{s}^- \leq \mathcal{C}_\mathsf{s} \leq \mathcal{C}_\mathsf{s}^+, \tag{2}$$

such as

$$\mathcal{C}_\mathsf{s}^- = \max_{P(\tau)} \min_{1\leq k\leq K} \mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma_k,\\ \hat{\gamma}_k \geq \tau}} \left[\log\left(\frac{1+\gamma_k P(\tau)}{1+\gamma_e P(\tau)}\right)\right], \tag{3a}$$

and

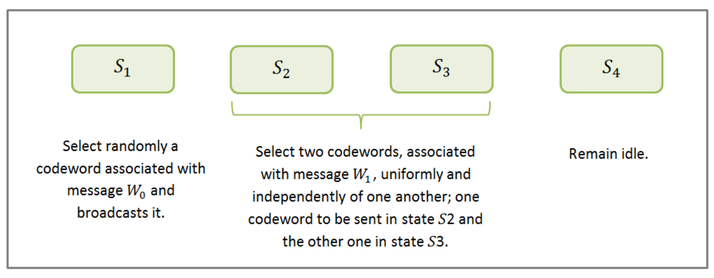
$$\mathcal{C}_\mathsf{s}^+ = \min_{1\leq k\leq K} \max_{P(\hat{h}_k)} \mathop{\mathbb{E}}_{\hat{h}_k,\tilde{h}_k} \left[\left\{\log\left(\frac{1+|\sqrt{1-\alpha}\hat{h}_k+\sqrt{\alpha}\tilde{h}_k|^2 P(\hat{h}_k)}{1+|\tilde{h}_k|^2 P(\hat{h}_k)}\right)\right\}^+\right], \tag{3b}$$

with $P(\tau) = P_{\mathsf{avg}} / \left(1 - F_{\hat{\gamma}_k}(\tau)\right)$ and $\mathbb{E}[P(\hat{h}_k)] \leq P_{\mathsf{avg}}$.

Achievability Scheme in Theorem 1: We consider a probabilistic model where the transmission is constrained by the quality of the legitimate channels.

To illustrate, let us consider the case $K=2$.

- We use two independent Gaussian codebooks C_0 and C_1 constructed similarly to the standard wiretap codes. Codebook C_0 is a $(n_0, 2^{n_0\mathcal{R}_k})$ code, with $2^{n_0(\mathcal{R}_k+\mathcal{R}_w)}$ codewords randomly partitioned into $2^{n_0\mathcal{R}_k}$ bins, and codebook C_1 is a $(n_1, 2^{n_1\mathcal{R}_k})$ code, with $2^{n_1(\mathcal{R}_k+\mathcal{R}_w)}$ codewords randomly partitioned into $2^{n_1\mathcal{R}_k}$ bins.
- The transmitted common message is given in the form $W=(W_0, W_1)$, where W_0 and W_1 are uniformly distributed over the indices $\{1, 2, \cdots, 2^{n_0\mathcal{R}_k}\}$ and $\{1, 2, \cdots, 2^{n_1\mathcal{R}_k}\}$, respectively.
- Next, we define the events: $S_1 = \{\hat{\gamma}_1 \geq \tau, \hat{\gamma}_2 \geq \tau\}$, $S_2 = \{\hat{\gamma}_1 \geq \tau, \hat{\gamma}_2 < \tau\}$, $S_3 = \{\hat{\gamma}_1 < \tau, \hat{\gamma}_2 \geq \tau\}$ and $S_4 = \{\hat{\gamma}_1 < \tau, \hat{\gamma}_2 < \tau\}$. That is, the transmitter selects randomly a codeword $U_0^{n_0}$ associated with message W_0 and broadcasts it when he experiences event S_1. For message W_1, the transmitter selects two codewords uniformly and independently of one another; one codeword $U_1^{n_1}$ to be sent in state S_2 and the other one $U_2^{n_1}$ to be sent in state S_3. The source remains idle when experiencing event S_4.



The randomness and the independence in the choice of the two codewords for message W_1 ensures that the eavesdropper does not take advantage of this repetition.

Sketch of the Proof of the Upper Bound in Theorem 1:

- Suppose that the transmitter sends message X to only one legitimate receiver R_k.
- Upper bound the secrecy capacity in this case.
- Since the choice of the receiver to transmit to is arbitrary, we choose the legitimate receiver that minimizes the upper bound.

Broadcasting Independent Messages

In this part, we consider the independent messages case when multiple confidential messages are transmitted to the legitimate receivers.

Theorem 2

The secrecy sum-capacity, $\widetilde{\mathcal{C}}_\mathsf{s}$, of the fast fading broadcast channel with imperfect main CSI is bounded by

$$\widetilde{\mathcal{C}}_\mathsf{s}^- \leq \widetilde{\mathcal{C}}_\mathsf{s} \leq \widetilde{\mathcal{C}}_\mathsf{s}^+, \tag{4}$$

such as

$$\widetilde{\mathcal{C}}_\mathsf{s}^- = \max_{P(\tau)} \mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma_{\mathsf{max}}^{\mathsf{est}},\\ \hat{\gamma}_{\mathsf{max}} \geq \tau}} \left[\log\left(\frac{1+\gamma_{\mathsf{max}}^{\mathsf{est}} P(\tau)}{1+\gamma_e P(\tau)}\right)\right], \tag{5a}$$

with $\gamma_{\mathsf{max}}^{\mathsf{est}} = |\sqrt{1-\alpha}\hat{h}_{\mathsf{max}} + \sqrt{\alpha}\tilde{h}|^2$ and $P(\tau) = P_{\mathsf{avg}} / \left(1 - F_{\hat{\gamma}_{\mathsf{max}}}(\tau)\right)$,

and

$$\widetilde{\mathcal{C}}_\mathsf{s}^+ = \min\left\{\max_{P(\hat{\Gamma})} \mathop{\mathbb{E}}_{\gamma_{\mathsf{max}},\hat{\Gamma},\tilde{\gamma}} \left[\left\{\log\left(\frac{1+\gamma_{\mathsf{max}} P(\hat{\Gamma})}{1+\tilde{\gamma} P(\hat{\Gamma})}\right)\right\}^+\right], K \max_{P(\hat{\gamma})} \mathop{\mathbb{E}}_{\gamma,\hat{\gamma},\tilde{\gamma}} \left[\left\{\log\left(\frac{1+\gamma P(\hat{\gamma})}{1+\tilde{\gamma} P(\hat{\gamma})}\right)\right\}^+\right]\right\}, \tag{5b}$$

with $\hat{\Gamma} = (\hat{\gamma}_1, \hat{\gamma}_2, \cdots, \hat{\gamma}_K)$, $\mathbb{E}[P(\hat{\Gamma})] \leq P_{\mathsf{avg}}$ and $\mathbb{E}[P(\hat{\gamma})] \leq P_{\mathsf{avg}}$.

Achievability Scheme in Theorem 2: The lower bound on the secrecy capacity is achieved using a time division multiplexing scheme that selects instantaneously one receiver to transmit to. That is, at each time, the source only transmits to the user with the best estimated channel gain $\hat{h}_{\mathsf{max}}$. Since we are transmitting to only one legitimate receiver at a time, the achieving coding scheme consists on using independent standard single user wiretap codebooks with power $P(\hat{\gamma}_{\mathsf{max}})$ satisfying the constraint $\mathbb{E}[P(\hat{\gamma}_{\mathsf{max}})] \leq P_{\mathsf{avg}}$.

A Note on the Upper Bound in Theorem 2: We represent the upper bound on the secrecy sum-capacity as the minimum between two upper bounds, i.e., $\widetilde{\mathcal{C}}_\mathsf{s}^+ = \min\left\{\widetilde{\mathcal{C}}_1^+, \widetilde{\mathcal{C}}_2^+\right\}$ with

$$\widetilde{\mathcal{C}}_1^+ = \max_{P(\hat{\Gamma})} \mathop{\mathbb{E}}_{\gamma_{\mathsf{max}},\hat{\Gamma},\tilde{\gamma}} \left[\left\{\log\left(\frac{1+\gamma_{\mathsf{max}} P(\hat{\Gamma})}{1+\tilde{\gamma} P(\hat{\Gamma})}\right)\right\}^+\right] \quad \text{and} \quad \widetilde{\mathcal{C}}_2^+ = K \max_{P(\hat{\gamma})} \mathop{\mathbb{E}}_{\gamma,\hat{\gamma},\tilde{\gamma}} \left[\left\{\log\left(\frac{1+\gamma P(\hat{\gamma})}{1+\tilde{\gamma} P(\hat{\gamma})}\right)\right\}^+\right]. \tag{6}$$

The reason behind choosing this particular representation was to ensure having the tightest possible upper bound for all the values of the error variance α.

- $\widetilde{\mathcal{C}}_2^+$ is a loose upper bound for the secrecy sum-rate for most values of α, especially when the number of users K is large.
- When the CSI available at the transmitter gets very noisy, i.e., $\alpha \to 1$, $\widetilde{\mathcal{C}}_2^+$ becomes tighter then $\widetilde{\mathcal{C}}_1^+$.
- For $\alpha = 1$, $\widetilde{\mathcal{C}}_2^+$ vanishes, reflecting the fact that the secrecy capacity is zero for the no CSI case, while $\widetilde{\mathcal{C}}_1^+$ does not.

Sketch of the Proof of the Upper Bound $\widetilde{\mathcal{C}}_1^+$:

- To prove that $\widetilde{\mathcal{C}}_1^+$ is an upper bound on the secrecy sum-capacity, we consider a new channel where the eavesdropper is listening to the transmission between the source and a selection combining receiver equipped with a number of antennas equivalent to the number of legitimate receivers K.
- The new channel can be modelled as

$$\begin{cases} Y(i) = h_{\mathsf{max}}(i)X(i) + v(i) \\ Z(i) = g(i)X(i) + w(i). \end{cases} \tag{7}$$

- The proof is conducted in two steps:
  - Prove that the secrecy capacity of the new channel upper bounds the secrecy sum-capacity of the K-receivers channel with imperfect CSI.
  - Prove that $\widetilde{\mathcal{C}}_1^+$ upper bounds the secrecy capacity of the genie-aided channel.

Scaling Law:

Corollary 1

The secrecy sum-capacity when broadcasting independent messages to a large number of legitimate receivers, i.e., $K \to \infty$, with an infinite average power constraint, i.e., $P_{\mathsf{avg}} \to \infty$, is bounded by

$$\log((1-\alpha)\log(K)) \leq \widetilde{\mathcal{C}}_s \leq \log\log K, \qquad \text{for all} \quad \alpha \neq 1. \tag{8}$$

Numerical Results

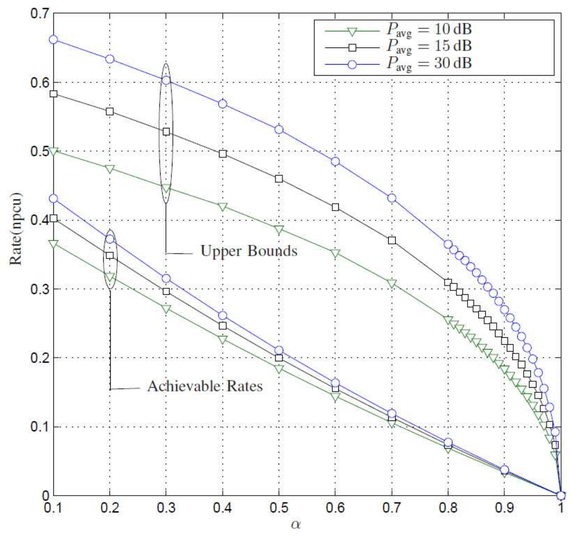


Figure 2: Lower and upper bounds on the common message secrecy capacity in function of α.

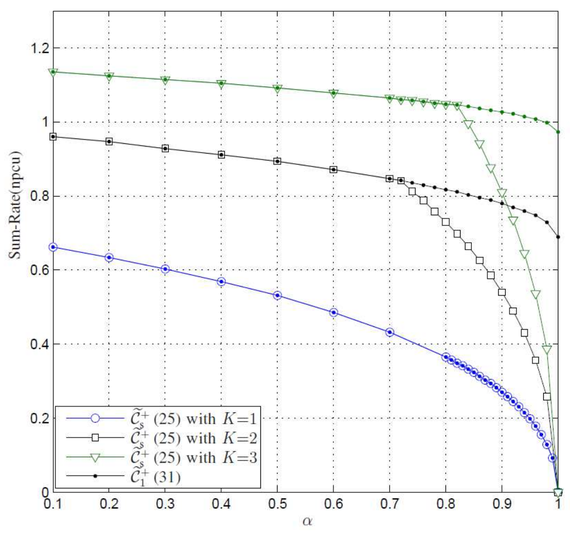


Figure 3: Comparison between the upper bounds $\widetilde{\mathcal{C}}_\mathsf{s}^+$ and $\widetilde{\mathcal{C}}_1^+$ for the independent messages case, in terms of α.

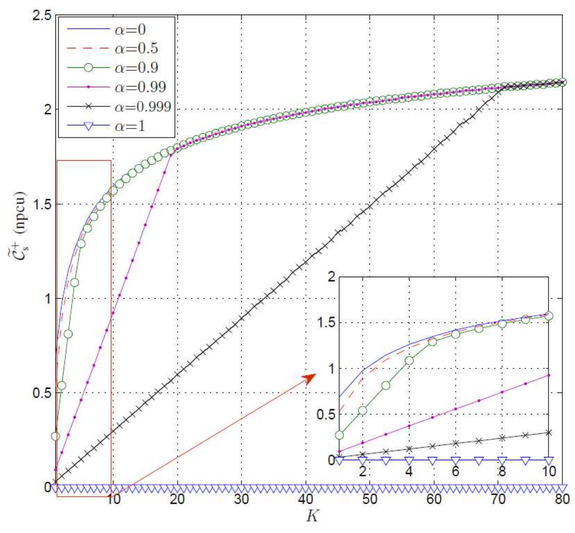


Figure 4: Upper bound on the secrecy capacity versus the number of legitimate receivers K for the independent messages case with different values of α.

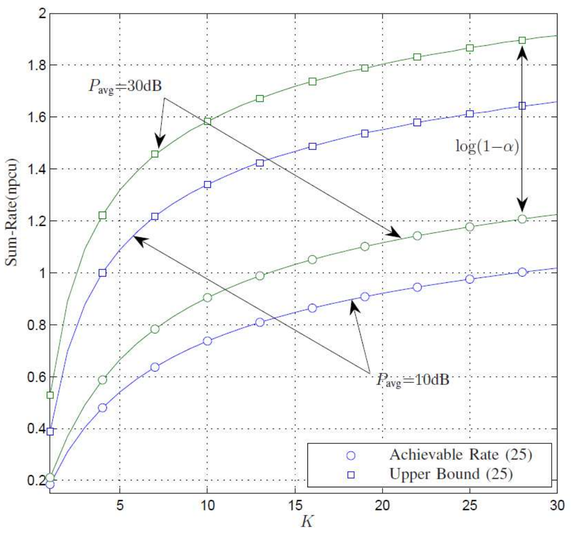


Figure 5: Upper and Lower bounds on the secrecy sum-rate versus the number of users K with α=0.5 and two values of P_{avg}.

References

1. A. Hyadi, Z. Rezki, A. Khisti and M.-S. Alouini, "On the secrecy capacity of the broadcast wiretap channel with imperfect channel state information", in Proceedings of IEEE Global Communications Conference (Globecom'2014), Austin, TX, USA, Dec. 2014.

2. A. Hyadi, Z. Rezki, A. Khisti and M.-S. Alouini, "Secure Broadcasting with Imperfect Channel State Information at the Transmitter", accepted for publication in IEEE Transactions on Wireless Communications.