Secure Communications over Wireless Networks Even 1-Bit Feedback Helps to Achieve Secrecy

Zouheir Rezki

Computer, Electrical and Mathematical Sciences & Engineering Division
King Abdullah University of Science and Technology (KAUST)
Thuwal, Mekkah Province, Saudi Arabia
zouheir.rezki@kaust.edu.sa

January 6, 2016

Outline

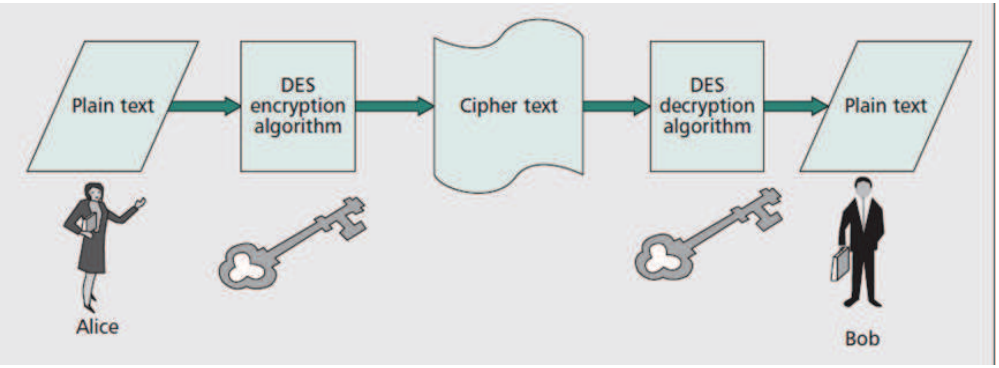
- ✔ Introduction
- ✔ Motivation
- ✔ System Model
- ✔ Capacity Results
- ✔ Asymptotic Analysis
- ✔ Conclusion
- ✔ Future Research Directions

Introduction

- ✔ With the tremendous progress of wireless communication technologies, security is a natural concern that could be related to ethical, social, or financial issues.
- ✔ Security is a critical issue in most military applications.
- ✔ Security is critical in many civilian applications: Credit card transactions, banking related data communications.
- ✔ Adversary attacks: Gain unauthorized access to and modify the information, or even disrupt the information flows.
- ✔ Therefore, the ability to share secret information reliably in presence of adversaries is extremely important.

Cryptography

- ✔ Traditionally, security has been addressed above the physical layer, through cryptographic encryption.



Symmetric Cryptographic Technique.

- ✔ Alice and Bob share a common private key.
- ✔ Message is encrypted using the key and Alice and Bob can decipher the message.
- ✔ Even if the message is intercepted, no key, no deciphered message.
- ✔ If these two users do not have this private key, a secure channel is required for the key exchange.

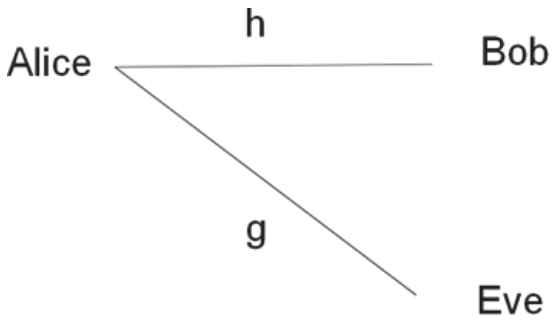
Limitations of Existing Techniques

- ✔ However, with the emergence of adhoc and decentralized networks, such encryption techniques are complex and difficult to implement.
- ✔ Dedicated secure channels are very expensive.
- ✔ Vulnerability to adversary attacks: Eavesdropping, denial-of-service (DOS), intrusion, message modification, localization through traffic analysis, etc.
- ✔ Security level relies on computation limitations of the adversary: cloud computing, quantum computers may compromise security.

Physical Layer Security (PLS)

- ✔ Introducing physical layer security as a new approach to achieve secure communications is a potential opportunity to complement and significantly improve security of wireless networks.
- ✔ The principle behind wireless physical layer security relies on exploiting the characteristics of the wireless channel, such as fading or noise, to provide secrecy for wireless transmissions.
- ✔ Instead of using a dedicated channel for key exchange, PLS provides tools to distribute secret keys or to transmit secret messages by exploiting the randomness of the channel (noise, fading).
- ✔ Once a key is shared, upper-layer security algorithms can finish the job (one-time pad encryption).

Example: Wireless Channels



- ✔ Alice is communicating with Bob through a fading channel h.
- ✔ Bob is listening to their communication through another fading g.
- ✔ h and g are constant over each coherence block (block fading model) and we can code over many such coherence blocks (delay-tolerant applications).
- ✔ The average noise level on both channels is the same.
- ✔ The average channel gain power of both channels is the same.
- ✔ Alice and Bob know h perfectly; Eve is a super-listener and thus knows both h and g.
- ✔ In this case, secure communication can be guaranteed at the PL and the capacity is known.

Motivation

- ✔ Perfect CSI is a bit too strong assumption.
- ✔ Quantized side information is a step forward to deploy PLS in practical systems.
- ✔ The role of feedback on fading channels without secrecy constraint has been widely studied, e.g., [Jindal, IT-06;Kim & Skoglund, TW-07;Love et al., JSAC-08].
- ✔ Feedback is incorporated in most emerging wireless standards.
- ✔ We are curious to understand how (already deployed) feedback mechanisms can help to enhance security of existing systems.

System Model

- ✔ Consider a discrete-time memoryless wire-tap channel: a transmitter, a legitimate receiver and an eavesdropper.
- ✔ Each terminal is equipped with a single antenna.
- ✔ At time coherence period i, $i = 1, \ldots, L$, we have

$$\begin{cases} Y(i,j) = h(i)\, X(i,j) + U(i,j) \\ Z(i,j) = g(i)\, X(i,j) + V(i,j), \end{cases} \tag{1}$$

  where $j = 1, \ldots, m$, with m representing the number of symbols in each coherence block. Average power constraint: $\mathbb{E}[|\mathbf{x}(i,j)|^2] \leq P_{avg}$.
- ✔ **h** and **g** are i.i.d., with bounded and continuous PDF.
- ✔ Legitimate Rx knows $\mathbf{h}(i)$'s, eavesdropper Rx knows both $\mathbf{h}(i)$'s and $\mathbf{g}(i)$'s.
- ✔ Transmitter only knows statistic CSI and is given q-bit feedback at the beginning (or at the end) of each coherence block, through an error-free feedback channel with limited capacity that is available to Alice and tracked by Eve.

Ergodic Secrecy Capacity with Finite-Rate Feedback

Theorem 1. *Let $\Pi^{(N)}$ be the set of all discrete power policies $\{P_k\}_{k=1}^{N}$ that satisfy the STPC (resp. LTPC). Let $\Theta^{(N)}$ be the set of all reconstruction points $\{\tau_k \mid 0 \leq \tau_1 \leq \ldots \leq \tau_N\}_{k=1}^{N}$ describing γ_h. For the discrete-time memoryless channel described by (1), with an error-free q-bit feedback link at the beginning of each coherence block, the following rates are achievable:*

$$R_{-1} = \max_{\substack{\{P_k\}_{k=1}^{N} \in \Pi^{(N)} \\ \{\tau_k\}_{k=1}^{N} \in \Theta^{(N)}}} \sum_{k=1}^{N} Pr\{\tau_k \leq \gamma_h < \tau_{k+1}\} \cdot \mathop{\mathbb{E}}_{\gamma_g} \left[\left[\log \left(\frac{1+\tau_k P_k}{1+\gamma_g P_k} \right) \right]^{+} \right]$$

$$R_{-2} = \max_{\substack{\{P_k\}_{k=1}^{N} \in \Pi^{(N)} \\ \{\tau_k\}_{k=1}^{N} \in \Theta^{(N)}}} \sum_{k=1}^{N} Pr\{\tau_k \leq \gamma_h < \tau_{k+1}\} \mathop{\mathbb{E}}_{\gamma_h, \gamma_g} \left[\log \left(\frac{1+\gamma_h P_k}{1+\gamma_g P_k} \right) \middle| \gamma_h \in [\tau_k, \tau_{k+1}] \right],$$

where for convenience, we set $\tau_{N+1} = \infty$.

Proof: Achievability of R_{-1}

- ✔ $\{0 = R_0 \leq R_1 \leq R_2, \ldots \leq R_N\}$ selected in advance.
- ✔ $\Delta_p = \mathsf{Pr}(R_p \leq \log(1 + P|\mathbf{h}|^2) < R_{p+1})$ for $p = 0, \ldots, N-1$.
- ✔ We establish that $R_s = \sum_{p=0}^{N-1} \Delta_p E[R_p - \log(1 + |\mathbf{g}|^2 P)]^+ + \epsilon$ is achievable.
- ✔ Let $R = \sum_{p=0}^{N-1} \Delta_p R_p - 2\epsilon$.
- ✔ We uniformly partition all 2^{nR} sequences of length nR into 2^{nR_s} bins, $n = mL$.
- ✔ To transmit W, select the corresponding bin index and choose a binary sequence $\mathbf{v}$ uniformly at random from all of the sequences in that bin.
- ✔ In each coherence block of length m, we transmit $m \cdot R_p$ information bits using a Gaussian codebook.
- ✔ By weak law of large numbers, when $L \gg 1$, the entire $\mathbf{v}$ is transmitted with high probability.
- ✔ Since in each block $R_p \leq \log(1 + |\mathbf{h}|^2 P)$ holds, the receiver can decode the sequence $\mathbf{v}$ with high probability.

Achievability of R_{-1} (cont'd.)

- ✔ Secrecy Analysis:

$$\begin{aligned} nR_e &\geq H(X^n|Z^n,h^L,g^L) - H(X^n|Z^n,h^L,g^L,W) \\ &\geq \sum_{i=1}^{L} m[R^i - \log(1+|g_i|^2P)]^+ - H(X^n|Z^n,h^L,g^L,W) \qquad (2) \end{aligned}$$

where (2) follows from $X(1), X(2), \ldots X(L)$ is independent sequence and from the analysis of a Gaussian wiretap code.

- ✔ By W.L.L.N., we have:

$$\frac{1}{L}\sum_{i=1}^{L}[R^i - \log(1+|g_i|^2P)]^+ \overset{L\to\infty}{\longrightarrow} \sum_{p=0}^{N-1}\Delta_p E[R_i - \log(1+|g|^2P)]^+.$$

- ✔ By a list decoding argument, we show that $H(X^n|Z^n,h^L,g^L,W) \leq n\epsilon$.

Achievability of R_{-2}

- ✔ Think of feedback as a deterministic mapping: $\kappa(\gamma_h) = k$ if $\gamma_h \in [\tau_k, \tau_{k+1})$.
- ✔ Construct a new main channel with output $\tilde{Y}(i,j) = \tilde{h}(i)\ X(i,j) + U(i,j)$, where $\tilde{h}(i) = \sqrt{P(\kappa(\gamma_h(i)))}\, h(i)$.
- ✔ This is a specific use of CSI-T and thus the capacity of the new channel is not higher than the original one.
- ✔ The new channel has no CSI-T and perfect CSI-R at the legitimate receiver.
- ✔ The rate R_{-2} follows then from [C&K, IT-78] by taking $V = X \sim \mathcal{CN}(0,1)$.
- ✔ With this choice, the rate $\left[I\left(X;\tilde{Y},\tilde{h}\right) - I\left(X;Z,\tilde{h},g\right)\right]$ is achievable.
- ✔ Evaluating the above rate and maximizing over all P_k's and τ_k's subject to the power constraint completes the proof.

Upper Bound

Theorem 2. *Let $\Pi_{(0)}^{(N)}$ be the set of all power policies $\{P_k\}_{k=0}^{N}$ that satisfy the STPC (resp. LTPC). Let $\Theta_{(0)}^{(N)}$ be the set of all reconstruction points $\{\tau_k \mid 0 = \tau_0 \leq \tau_1 \leq \ldots \leq \tau_N\}_{k=0}^{N}$ describing γ_h. For the discrete-time memoryless channel described by (1), with an error-free q-bit feedback link at the beginning of each coherence block, an upper bound on the secrecy capacity is given by:*

$$R_+ = \max_{\substack{\{P_k\}_{k=0}^{N} \in \Pi_{(0)}^{(N)} \\ \{\tau_k\}_{k=0}^{N} \in \Theta_{(0)}^{(N)}}} \sum_{k=0}^{N} Pr\{\tau_k \leq \gamma_h < \tau_{k+1}\} \underset{\gamma_h,\gamma_g}{\mathbb{E}} \left[\left[\log\left(\frac{1+\gamma_h P_k}{1+\gamma_g P_k} \right) \right]^+ \middle| \gamma_h \in [\tau_k, \tau_{k+1}] \right], \tag{3}$$

where for convenience, we set $\tau_{N+1} = \infty$. Furthermore, R_{-1} in Theorem 1 coincides with R_+ as $N \to \infty$.

Proof of the Upper Bound:

- ✔ We assume that the transmitter has CSI $u_i = \kappa(h_i)$ at time instant i, whereas the legitimate receiver knows $\gamma_{h,i}$.
- ✔ We upper bound the equivocation rate as follows:

$$
\begin{aligned}
n\,R_e &= H\left(W \,\middle|\, \boldsymbol{Z}^n, \boldsymbol{h}^L, \boldsymbol{g}^L\right) && (4)\\
&= H\left(W \,\middle|\, \boldsymbol{Z}^n, \boldsymbol{h}^L, \boldsymbol{g}^L, \boldsymbol{u}^L\right) && (5)\\
&\leq \sum_{i=1}^{n} I\left(X_i; Y_i \,\middle|\, Z_i, h_i, g_i, \boldsymbol{u}^L\right) + n\,\delta_n && (6)\\
&\leq \sum_{i=1}^{n} \mathbb{E}\left[\left[\log\left(\frac{1+\gamma_{h,i}\,P_i\left(\boldsymbol{u}^i\right)}{1+\gamma_{g,i}\,P_i\left(\boldsymbol{u}^i\right)}\right)\right]^+\right] + n\,\delta_n, && (7)
\end{aligned}
$$

- ✔ Then we prove that the above upper bound is maximized by a power allocation $P_i\left(\boldsymbol{u}^i\right) = \lambda(u_i)$, a time-invariant function of u_i only.
- ✔ It remains to show that the lower and the upper bounds coincide as $N \to \infty$.
- ✔ Choose $\tau_k = \left(F_{\gamma_h}(\tau_{k+1}) - F_{\gamma_h}(\tau_k)\right) = \frac{1}{N}$ and let $N \to \infty$ completes the proof.

What If the Feedback Is of Type ARQ?

Theorem 3. *A lower bound on the secrecy capacity of the discrete-time memoryless channel described by (1), with an error-free* 1*-bit ARQ feedback at the end of each coherence block, is given by:*

$$R_{--} = \max_{\substack{\{P\} \in \Pi^{(1)} \\ \{\tau\} \in \Theta^{(1)}}} \theta^2 \cdot \mathop{\mathbb{E}}_{\gamma_g} \left[\left[\log \left(\frac{1+\tau\, P}{1+\gamma_g\, P} \right) \right]^+ \right], \tag{8}$$

where θ *is the probability of success defined by* $\theta = Pr\{\gamma_h \geq \tau\}$*. The upper bound in* (3)*, with* $N = 1$*, still holds.*

- ✔ Alice keeps retransmitting the same block until she gets an ACK.
- ✔ Repetition leaks information to the eavesdropper.
- ✔ Worst case scenario: All repeated blocks are revealed to the eavesdropper.

Proof of Th. 3:

✔ Reliability is guaranteed by a random coding argument.

✔ For secrecy analysis:

$$
\begin{aligned}
n\,R_e &= H\left(W \mid \boldsymbol{Z}^n, h^L, \boldsymbol{g}^L, \boldsymbol{s}^L\right) && (9)\\
&\geq I\left(W; \boldsymbol{X}^{m\,L_0} \mid \boldsymbol{Z}^n, \boldsymbol{h}^L, \boldsymbol{g}^L, \boldsymbol{s}^L\right) && (10)\\
&= h\left(\boldsymbol{X}^{m\,L_0} \mid \boldsymbol{Z}^n, \boldsymbol{h}^L, \boldsymbol{g}^L, \boldsymbol{s}^L\right) - h\left(\boldsymbol{X}^{m\,L_0} \mid W, \boldsymbol{Z}^n, \boldsymbol{h}^L, \boldsymbol{g}^L, \boldsymbol{s}^L\right) && (11)\\
&= h\left(\boldsymbol{X}^{m\,L_0} \mid \boldsymbol{Z}^{m\,L_0}, \boldsymbol{h}^{L_0}, \boldsymbol{g}^{L_0}\right) - h\left(\boldsymbol{X}^{m\,L_0} \mid W, \boldsymbol{Z}^n, \boldsymbol{h}^L, \boldsymbol{g}^L, \boldsymbol{s}^L\right) && (12)\\
&\geq \sum_{i=1}^{L_0} m \left\{\left[R - \epsilon - \log\left(1 + \gamma_g\left(i\right)\, P\right)\right]^+\right\} - h\left(\boldsymbol{X}^{m\,L_0} \mid W, \boldsymbol{Z}^n, \boldsymbol{h}^L, \boldsymbol{g}^L, \boldsymbol{s}^L\right) && (13)
\end{aligned}
$$

where L_0 is the number of blocks that have not been repeated.

✔ By a list decoding argument, the second term in (13) is vanishing.

✔ As $L_0 \to \infty$, $\frac{L_0}{L}$ can be computed as follows:

$$
\begin{aligned}
\lim_{L_0 \to \infty} \frac{L_0}{L} &= \lim_{L_0 \to \infty} \frac{1}{L} \sum_{i=1}^{L} \mathbb{1}_i && (14)\\
&= \Pr\left\{\text{no repetition}\right\}\\
&= \Pr\left\{\text{blocks } i \text{ and } (i-1) \text{ not repeated, } \forall i \geq 2\right\}\\
&= \Pr(\text{success})^2.
\end{aligned}
$$

Few Comments

- ✔ The rate in **Th**. 3 only accounts for the contribution of the blocks that have not been repeated into the secrecy rate.
- ✔ It can be immediately improved by accounting for the contribution of the blocks that have been repeated more than once into the secrecy rate.

Corollary 1. *A lower bound on the secrecy capacity of the discrete-time memoryless channel described by (1), with an error-free* 1*-bit ARQ feedback at the end of each coherence block, is given by:*

$$\begin{aligned} R_{--}^{+} \quad = \quad & \max_{\substack{\{P\} \in \Pi^{(1)} \\ \{\tau\} \in \Theta^{(1)}}} \left\{ \theta^2 \underset{\gamma_g}{\mathbb{E}} \left[\left[\log \left(\frac{1+\tau\, P}{1+\gamma_g\, P} \right) \right]^{+} \right] \right. \\ & \left. + \theta^2 \ (1-\theta) \underset{\gamma_g^{(2)}}{\mathbb{E}} \left[\left[\log \left(\frac{1+\tau\, P}{1+\gamma_g^{(2)}\, P} \right) \right]^{+} \right] \right\}, \end{aligned} \tag{15}$$

where $\gamma_g^{(2)}$ *is a random variable distributed as the sum of two independent* γ_g*'s.*

Proof of Corollary. 1:

✔ We only outline the secrecy analysis.

$$
\begin{aligned}
n\,R_e \;\geq\;& h\left(\boldsymbol{X}^{m\,L_0}, \boldsymbol{X}^{m\,L_1} \mid \boldsymbol{Z}^n, \boldsymbol{h}^L, \boldsymbol{g}^L, \boldsymbol{s}^L\right) \\
& -h\left(\boldsymbol{X}^{m\,L_0}, \boldsymbol{X}^{m\,L_1} \mid W, \boldsymbol{Z}^n, \boldsymbol{h}^L, \boldsymbol{g}^L, \boldsymbol{s}^L\right) && (16) \\
=\;& h\left(\boldsymbol{X}^{m\,L_0} \mid \boldsymbol{Z}^n, \boldsymbol{h}^L, \boldsymbol{g}^L, \boldsymbol{s}^L\right) \\
& +h\left(\boldsymbol{X}^{m\,L_1} \mid \boldsymbol{Z}^n, \boldsymbol{h}^L, \boldsymbol{g}^L, \boldsymbol{s}^L, \boldsymbol{X}^{m\,L_0}\right) \\
& -h\left(\boldsymbol{X}^{m\,L_0}, \boldsymbol{X}^{m\,L_1} \mid W, \boldsymbol{Z}^n, \boldsymbol{h}^L, \boldsymbol{g}^L, \boldsymbol{s}^L\right) && (17) \\
=\;& h\left(\boldsymbol{X}^{m\,L_0} \mid \boldsymbol{Z}^{m\,L_0}, \boldsymbol{h}^{L_0}, \boldsymbol{g}^{L_0}\right) \\
& +h\left(\boldsymbol{X}^{m\,L_1} \mid \boldsymbol{Z}^{2\,m\,L_1}, \boldsymbol{h}^{2\,L_1}, \boldsymbol{g}^{2\,L_1}\right) \\
& -h\left(\boldsymbol{X}^{m\,L_0}, \boldsymbol{X}^{m\,L_1} \mid W, \boldsymbol{Z}^n, \boldsymbol{h}^L, \boldsymbol{g}^L, \boldsymbol{s}^L\right) && (18) \\
\geq\;& \sum_{i=1}^{L_0} m \left\{\left[R - \epsilon - \log\left(1 + \gamma_g\left(i\right)\, P\right)\right]^+\right\} \\
& + \sum_{i=1}^{L_1} m \left\{\left[R - \epsilon - \log\left(1 + \gamma_g^{(2)}\left(i\right)\, P\right)\right]^+\right\} \\
& -h\left(\boldsymbol{X}^{m\,L_0}, \boldsymbol{X}^{m\,L_1} \mid W, \boldsymbol{Z}^n, \boldsymbol{h}^L, \boldsymbol{g}^L, \boldsymbol{s}^L\right), && (19)
\end{aligned}
$$

Proof of Corollary. 1 (cont'd.):

- ✔ To obtain (19), we expand the first term in (18) exactly as in the case of no repetition.
- ✔ The second term in (18) is obtained as follows:

$$h\left(\boldsymbol{X}^{m\,L_1} \mid \boldsymbol{Z}^{2\,m\,L_1}, \boldsymbol{h}^{2\,L_1}, \boldsymbol{g}^{2\,L_1}\right)$$

$$= \sum_{\substack{\text{blocks } i \\ \text{repeated once}}} h\left(\boldsymbol{X}^m(i) \mid \boldsymbol{Z}^m(i), \boldsymbol{Z}^m(i+1), h(i), h(i+1), g(i), g(i+1)\right) \tag{20}$$

$$= \sum_{\substack{\text{blocks } i \\ \text{repeated once}}} \left[h\left(\boldsymbol{X}^m(i)\right) - I\left(\boldsymbol{X}^m(i); \boldsymbol{Z}^m(i), \boldsymbol{Z}^m(i+1), h(i), h(i+1), g(i), g(i+1)\right)\right]^+ \tag{21}$$

$$= \sum_{\substack{\text{blocks } i \\ \text{repeated once}}} \left[h\left(\boldsymbol{X}^m(i)\right) - I\left(\boldsymbol{X}^m(i); \boldsymbol{Z}^m(i), \boldsymbol{Z}^m(i+1) \mid h(i), h(i+1), g(i), g(i+1)\right)\right]^+ \tag{22}$$

$$\geq \sum_{i=1}^{L_1} \left\{ m \left[R - \epsilon - \log\left(1 + \gamma_g^{(2)}\, P\right)\right]^+ \right\}, \tag{23}$$

- ✔ The third term on the RHS of (19) can be made arbitrary small using a list decoding argument.
- ✔ As $L_0 \to \infty$ and $L_1 \to \infty$, $\frac{L_0}{L} \to \theta^2$ and $\frac{L_1}{L} \to \theta^2\,(1-\theta) = \Pr\{\text{blocks } i \text{ and } (i-2) \text{ are not repeated and } (i-1) \text{ repeated}\}$

Bounds Evaluation

- ✔ The previous results hold for both short term power constraint (STPC) and long term power constraint (LTPC).
- ✔ STPC: $\mathbb{E}\left[\frac{1}{m}\sum_{j=1}^{m}|X(i,j)|^2\right] \leq P_{max}$.
- ✔ LTPC: $\mathbb{E}\left[\frac{1}{L}\sum_{i=1}^{L}\frac{1}{m}\sum_{j=1}^{m}|X(i,j)|^2\right] \leq P_{max}$.
- ✔ Next, we only focus on LTPC.
- ✔ Consider, for instance, the rate R_{-1}. We formulate the problem as:

$$\bar{\mathcal{P}}_1 : \begin{cases} \max\limits_{0\leq\tau_1\leq\ldots\leq\tau_N} \sum\limits_{k=1}^{N} \mathsf{Pr}\left\{\tau_k \leq \gamma_h < \tau_{k+1}\right\} \cdot \mathop{\mathbb{E}}_{\gamma_g}\left[\left[\log\left(\frac{1+\tau_k P_k}{1+\gamma_g P_k}\right)\right]^+\right] \\ \text{s.t.} \sum\limits_{k=1}^{N} \mathsf{Pr}\left\{\tau_k \leq \gamma_h < \tau_{k+1}\right\} P_k \leq P_{max}, \end{cases} \tag{24}$$

- ✔ $\bar{\mathcal{P}}_1$ is convex in P_k's, not convex in τ_k's and hence is non-convex.
- ✔ The KKT conditions provide necessary conditions.
- ✔ Note that there is no loss of optimality by taking $0 < \tau_1 \ldots < \tau_N$.
- ✔ it can be shown that the power constraint is satisfied with equality.

Bounds Evaluation (cont'd.)

- ✔ We present below an iterative algorithm that attempts to find the optimal solution using the KKT conditions.
- ✔ Initialize $i = 0$, $P_k^{(0)} = P_{max}, \quad \forall\, i$, set $\mu^{(0)}$ arbitrarily;
- ✔ Repeat:
- ✔ Fix $\left\{P_k^{(i)}\right\}$ and $\mu^{(i)}$, solve for $\left\{\tau_k^{(i)}\right\}$ using KKT;
- ✔ Compute R^i;
- ✔ Fix $\left\{\tau_k^{(i)}\right\}$, find $\left\{P_k^{(i+1)}\right\}$ and $\mu^{(i+1)}$ using KKT;
- ✔ $i \leftarrow i + 1$;
- ✔ Until Convergence: $\frac{R^{(i+1)} - R^{(i)}}{R^{(i+1)}} \leq \epsilon$;

Asymptotic Analysis: High-SNR

Corollary 2. *At high-SNR ($P_{max} \to \infty$), the secrecy capacity is bounded, i.e., does not grow with P_{max}. Furthermore, the following rates are achievable:*

$$R_{-1}^{\infty} = \max_{0 \le \tau_1 \le \ldots \le \tau_N} \sum_{k=1}^{N} Pr\{\tau_k \le \gamma_h < \tau_{k+1}\} \cdot \mathop{\mathbb{E}}_{\gamma_g} \left[\left[\log\left(\frac{\tau_k}{\gamma_g}\right) \right]^+ \right] \tag{25}$$

$$R_{-2}^{\infty} = \max_{\tau \ge 0} \mathop{\mathbb{E}}_{\substack{\gamma_h \ge \tau \\ \gamma_g}} \left[\log\left(\frac{\gamma_h}{\gamma_g}\right) \right]. \tag{26}$$

An upper bound on the secrecy capacity is given by:

$$R_{+}^{\infty} = \mathop{\mathbb{E}}_{\gamma_h, \gamma_g} \left[\left[\log\left(\frac{\gamma_h}{\gamma_g}\right) \right]^+ \right]. \tag{27}$$

- ✔ At high-SNR, likewise without secrecy constraint, power adaptation does not provide any additional capacity gain under secrecy constraint.
- ✔ STPC and LTPC have the same asymptotic behavior.

Asymptotic Analysis: Low-SNR

- ✔ At low-SNR, power adaptation drastically increases the achievable secrecy rate.
- ✔ More interestingly, under LTPC, the secrecy capacity is asymptotically equal to the capacity as if there is no secrecy constraint, for fading channels with unbounded support.
- ✔ Moreover, 1-bit feedback is enough to achieve this capacity.

Theorem 4. *For fading channels with infinite support, the secrecy capacity at low-SNR, $C_s\left(P_{max}\right)$, of the channel described by (1), with an error-free q-bit feedback link at the beginning of each coherence block is given by:*

$$C_s\left(P_{max}\right) \overset{0}{\approx} C_{w.s}\left(P_{max}\right), \tag{28}$$

where $C_{w.s}\left(\cdot\right)$ stands for the capacity of the main channel without secrecy constraint and with perfect CSI at both the transmitter (CSI-T) and the receiver (CSI-R). Furthermore, 1-bit feedback at the beginning of each coherence block is enough to achieve this capacity.

Few Comments

- ✔ Recall that with no CSI-T, the secrecy capacity is equal to zero.
- ✔ Theorem 4 highlights the fact that even with 1-bit feedback, not only one can achieve secrecy at low-SNR, but this secrecy is obtained "for free".
- ✔ Nevertheless, we still need a wiretap code to bin the secret message.
- ✔ The encoding scheme related to R_{-2} exploits the advantage that the legitimate receiver has over the eavesdropper through the feedback link: If the main channel is "good", it is more unlikely that the eavesdropper's channel be better.
- ✔ While this scheme is not the best strategy at an arbitrary P_{max}, it is enough to achieve the secrecy capacity at asymptotically low-SNR.
- ✔ **Th**. 4 holds if the main channel fading has an infinite support, otherwise it does not (proof via a counter example).

Counter Example

- ✔ Consider fading channels with PDF defined on $[0, a]$ by: $f_{\boldsymbol{\gamma}_h}(x) = f_{\boldsymbol{\gamma}_g}(x) = \frac{1}{a}$.
- ✔ The capacity of the main channel can be evaluated as:

$$C_{w.s}(P_{max}) = -1 - \frac{1}{W\left(-e^{-1-a\,P_{max}}\right)} + \log\left(-W\left(-e^{-1-a\,P_{max}}\right)\right) \quad (29)$$

$$= a\,P_{max} + \mathsf{o}(P_{max}) \quad (30)$$

- ✔ Next, we show that the secrecy capacity of this channel is at most asymptotically equal to $\frac{a}{2}\,P_{max}$.
- ✔ We upper-bound the secrecy capacity with perfect main CSI to obtain:

$$R_{++} \leq \mathop{\mathbb{E}}_{\boldsymbol{\gamma}_g}\left[\log\left(\frac{1+a\,P_{max}}{1+\gamma_g\,P_{max}}\right)\right] \quad (31)$$

$$\approx P_{max}\mathop{\mathbb{E}}_{\boldsymbol{\gamma}_g}[a-\gamma_g] \quad (32)$$

$$= \frac{a}{2}\,P_{max}, \quad (33)$$

Numerical Results

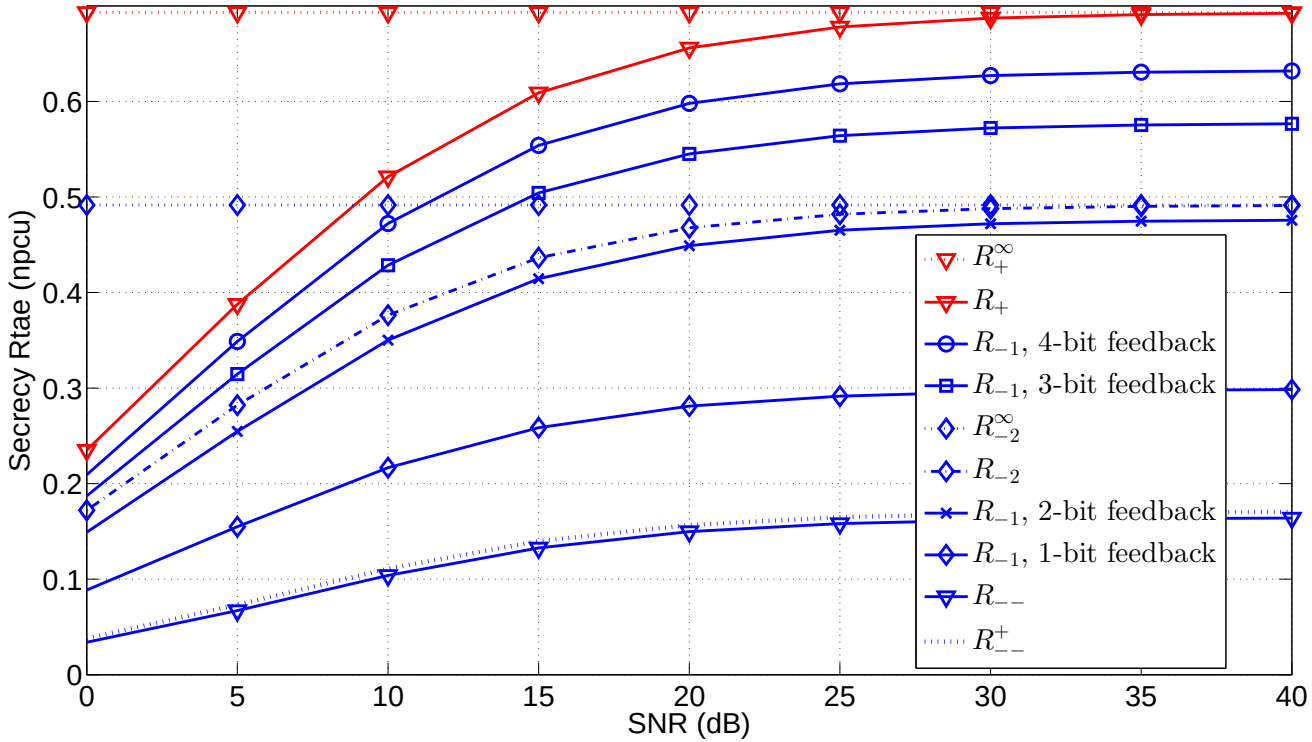


Figure 1: Achievable rates and the upper bound under STPC, for Rayleigh fading channels, with various q-bit feedback, $q = 1, 2, 3, 4$.

Numerical Results

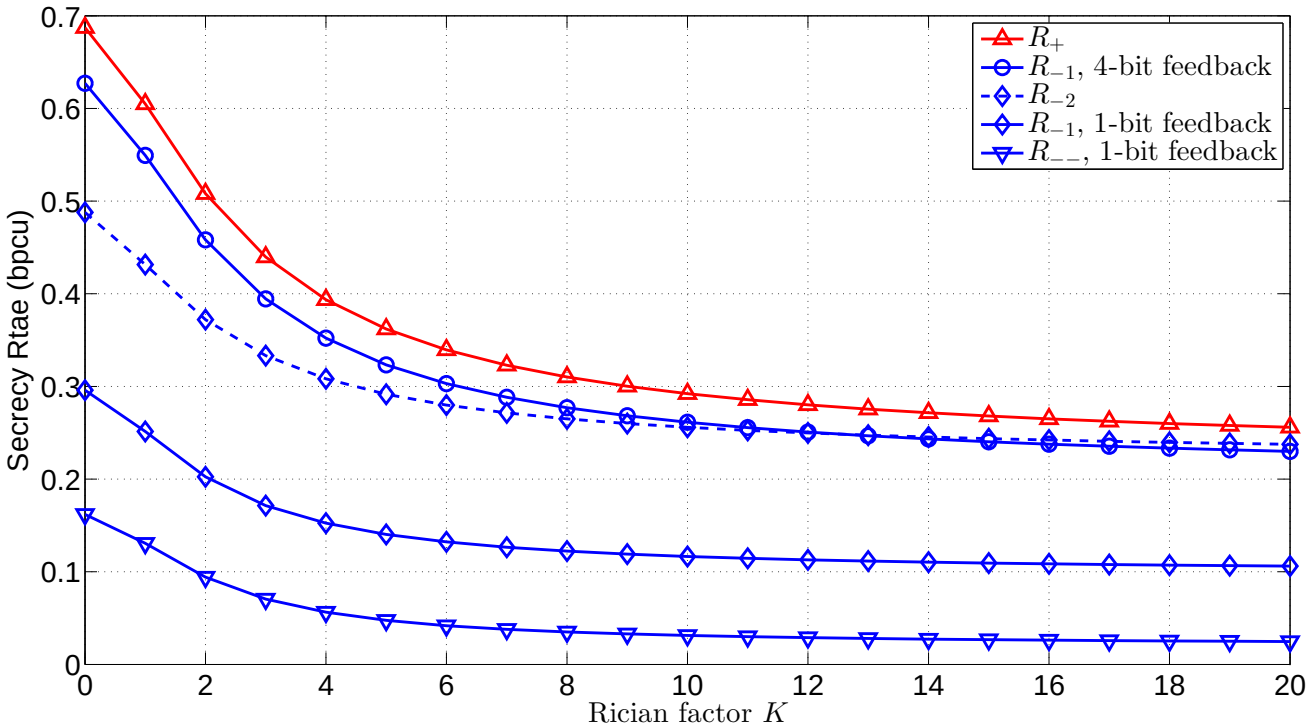


Figure 2: Achievable rates and the upper bound under STPC versus the Rician factor K, for q-bit feedback, $q = 1, 4$. The main channel is a normalized Rayleigh fading channel, whereas the eavesdropper's channel is a normalized Rician fading with factor K. The transmit power is equal to $P_{max} = 30$ dBs

Numerical Results

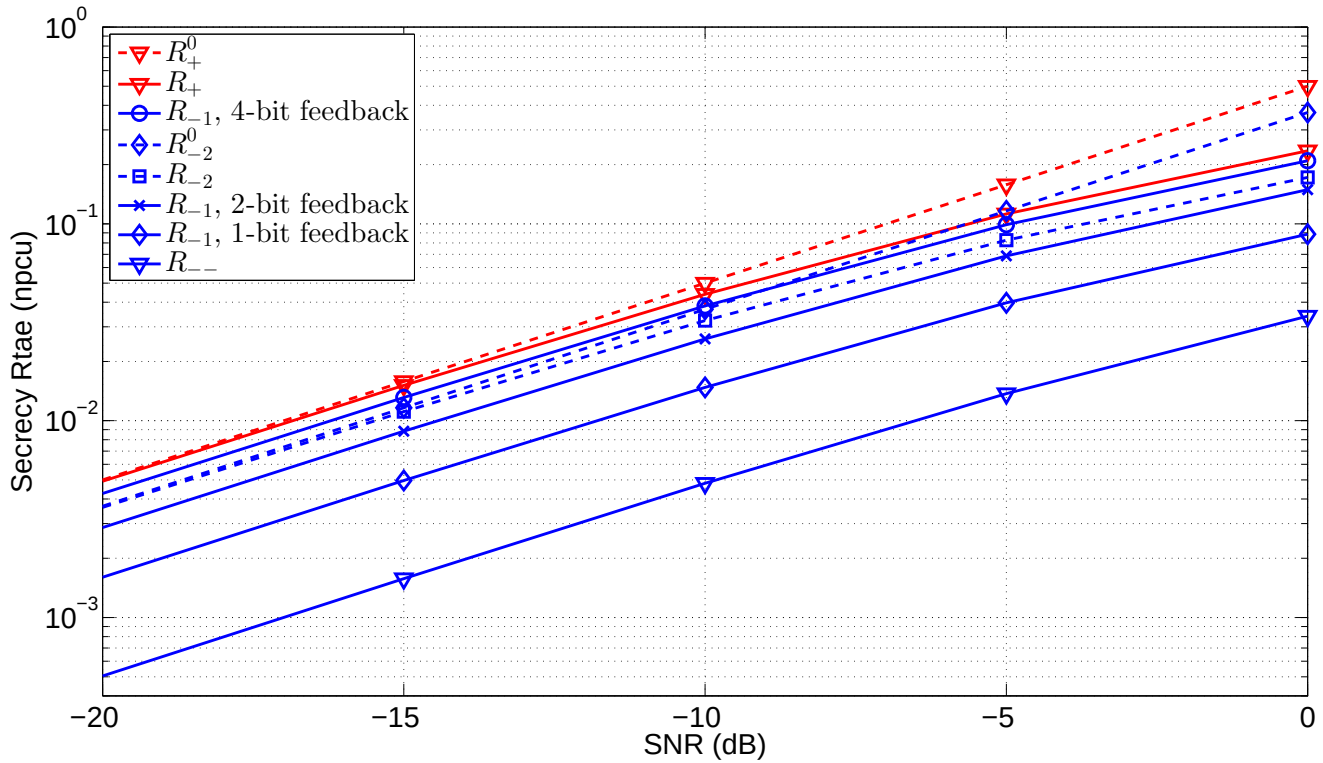


Figure 3: Achievable rates and the upper bound under STPC, for Rayleigh fading channels, with various q-bit feedback, $q = 1, 2, 4$, at low-SNR.

Numerical Results

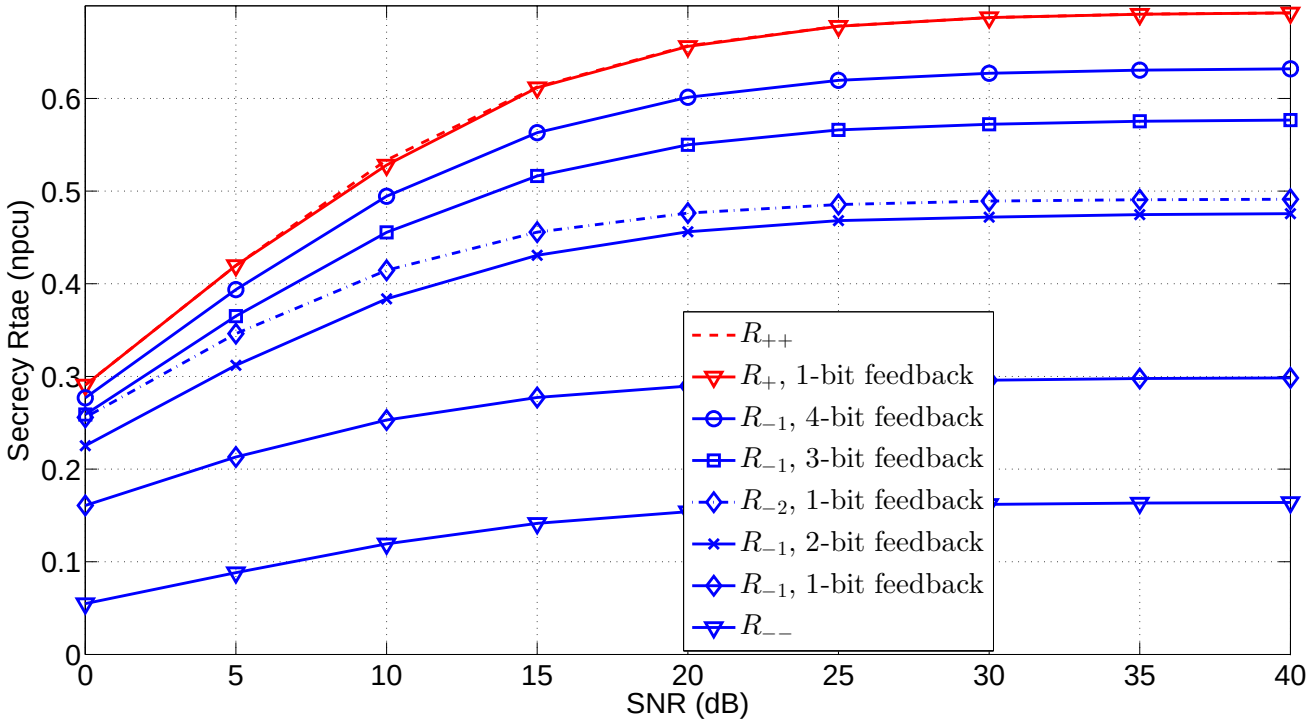


Figure 4: Achievable rates and the upper bound under LTPC, for Rayleigh fading channels, with various q-bit feedback, $q = 1, 2, 3, 4$.

Numerical Results

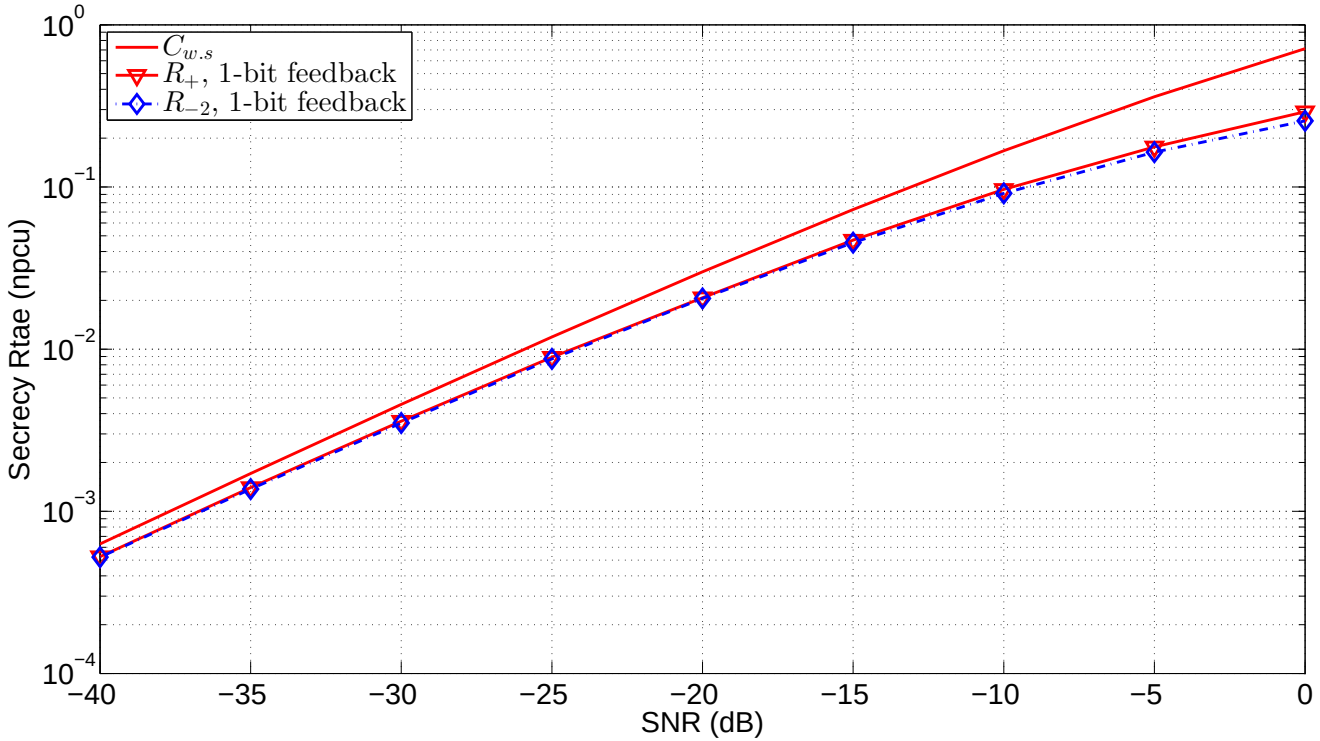


Figure 5: Achievable rate R_{-2} and the upper bound under LTPC, for Rayleigh fading channels, with 1-bit feedback, at low-SNR.

Conclusion

- ✔ A positive secrecy capacity is feasible with limited-rate feedback.
- ✔ Lower and upper bounds have been derived when an arbitrary number of feedback bits are provided to the sender by the legitimate receiver.
- ✔ When the number of feedback bits is large enough, the lower and the upper bounds coincide, thus fully characterizing the capacity in this case.
- ✔ At low-SNR, the secrecy capacity over a wide class of fading channels is (asymptotically) equal to the capacity as if there is no secrecy constraint.
- ✔ A simple on-off scheme with 1-bit feedback is capacity-achieving.

Future Research Directions

- ✔ Broadcasting common and independent messages confidentially in a block fading with feedback.
- ✔ Extend the work to active eavesdropping: Eve can either listen or jam or both.
- ✔ Exploit the low SNR results in low-rate applications:
  - ✘ Secure Task-Oriented Wireless Sensor Networks
  - ✘ Biomedical Implants: Safe remote-monitoring of wireless-enabled pacemakers, for instance.
  - ✘ Internet-of-Things (IoT): everything is connected, sometimes securely.