5 Security limits of Gaussian and wireless channels

This chapter extends the results obtained in Chapter 3 and Chapter 4 for discrete memoryless channels and sources to Gaussian channels and wireless channels, for which numerical applications provide insight beyond that of the general formula in Theorem 3.3. Gaussian channels are of particular importance, not only because the secrecy capacity admits a simple, intuitive, and easily computable expression but also because they provide a reasonable approximation of the physical layer encountered in many practical systems. The analysis of Gaussian channels also lays the foundations for the study of wireless channels.

The application of physical-layer security paradigms to wireless channels is perhaps one of the most promising research directions in physical-layer security. While wireline systems offer some security, because the transmission medium is confined, wireless systems are intrinsically susceptible to eavesdropping since all transmissions are broadcast over the air and overheard by neighboring devices. Other users can be viewed as potential eavesdroppers if they are not the intended recipients of a message. However, as seen in earlier chapters, the randomness present at the physical layer can be harnessed to provide security, and randomness is a resource that abounds in a wireless medium. For instance, we show that fading can be exploited opportunistically to guarantee secrecy even if an eavesdropper obtains on average a higher signal-to-noise ratio than a legitimate receiver.

We start this chapter with a detailed study of Gaussian channels and sources, including multiple-input multiple-output channels (Section 5.1.2). We then move on to wireless channels, and we analyze the fundamental limits of secure communications for ergodic fading (Section 5.2.1), block fading (Section 5.2.2), and quasi-static fading (Section 5.2.3).

5.1 Gaussian channels and sources

5.1.1 Gaussian broadcast channel with confidential messages

Communication over a (real) Gaussian broadcast channel with confidential messages (Gaussian BCC for short) is illustrated in Figure 5.1. This channel model is a specific instance of a BCC in which the codewords transmitted by Alice are corrupted by additive Gaussian noise. Specifically, the relationships between the inputs and outputs

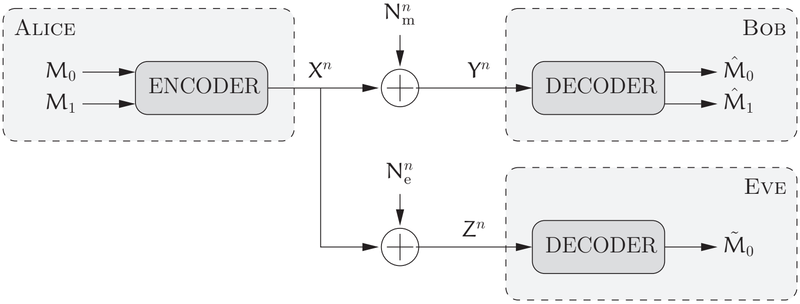

Figure 5.1 Communication over a Gaussian BCC.

of the channel are given by

$$Y_i = X_i + N_{m,i} \quad \text{and} \quad Z_i = X_i + N_{e,i},$$

where the noise processes $\{N_{m,i}\}_{i\geqslant 1}$ and $\{N_{e,i}\}_{i\geqslant 1}$ are i.i.d. and

$$N_{m,i} \sim \mathcal{N}(0, \sigma_m^2) \qquad \text{and} \qquad N_{e,i} \sim \mathcal{N}(0, \sigma_e^2).$$

The statistics of $N_{m,i}$ and $N_{e,i}$ are assumed known to the transmitter, the receiver, and the eavesdropper prior to transmission. The input of the channel is also subject to an average power constraint

$$\frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[X_i^2\right] \leqslant P.$$

Definitions 3.6 and 3.7 for codes, achievable rates, and the secrecy capacity then apply readily to the Gaussian BCC. The key property of the Gaussian BCC that makes it more amenable to study than the general BCC is that either the eavesdropper's channel is stochastically degraded with respect to the main channel or the main channel is stochastically degraded with respect to the eavesdropper's channel. In fact, if $\sigma_e^2 \geqslant \sigma_m^2$, the marginal probabilities $p_{Y|X}$ and $p_{Z|X}$ are the same as those of the channel characterized by

$$Y_i = X_i + N_{m,i} \quad \text{and} \quad Z_i = Y_i + N_i' \qquad \text{with } N_i' \sim \mathcal{N}(0, \sigma_e^2 - \sigma_m^2).$$

Similarly, if $\sigma_e^2 < \sigma_m^2$, the marginal probabilities $p_{Y|X}$ and $p_{Z|X}$ are the same as those of the channel characterized by

$$Z_i = X_i + N_{e,i} \quad \text{and} \quad Y_i = Z_i + N_i'' \qquad \text{with } N_i'' \sim \mathcal{N}(0, \sigma_m^2 - \sigma_e^2).$$

In the latter case, the secrecy capacity is zero according to Proposition 3.4.

Theorem 5.1 (Liang *et al.*). *The secrecy-capacity region of the Gaussian BCC is*

$$\mathcal{C}^{\text{GBCC}} = \bigcup_{\beta\in[0,1]} \left\{ (R_0, R_1) : \begin{array}{l} R_0 \leqslant \min\left(\frac{1}{2}\log\left(1+\frac{(1-\beta)P}{\sigma_m^2+\beta P}\right), \frac{1}{2}\log\left(1+\frac{(1-\beta)P}{\sigma_e^2+\beta P}\right)\right) \\ R_1 \leqslant \left(\frac{1}{2}\log\left(1+\frac{\beta P}{\sigma_m^2}\right) - \frac{1}{2}\log\left(1+\frac{\beta P}{\sigma_e^2}\right)\right)^{+} \end{array} \right\}.$$

Proof. If we treat the Gaussian BCC as a special case of the BCC studied in Section 3.5, then the achievability of $\mathcal{C}^{\text{GBCC}}$ follows from Theorem 3.3 with the following choice of random variables:

$$\mathsf{U} \sim \mathcal{N}(0, (1-\beta)P), \quad \mathsf{V} \triangleq \mathsf{U} + \mathsf{X}' \text{ with } \mathsf{X}' \sim \mathcal{N}(0, \beta P) \quad \text{and} \quad \mathsf{X} \triangleq \mathsf{V}.$$

To make the proof rigorous, we would need to modify the proof of Section 3.5.2 appropriately to take into account the continuous nature of the Gaussian BCC and the power constraint. This can be done by noting that strongly typical sequences can be replaced by weakly typical sequences in the random-coding argument to handle continuous distributions.[1] Then, the input power constraint can be dealt with by introducing an error event that accounts for the violation of the constraint as done in [3, Chapter 9].

For the converse part of the proof, note that all the steps in Section 3.5.3 up to (3.57) involve "basic" properties of mutual information (the chain rule and positivity) that hold irrespective of the continuous or discrete nature of the channel. Therefore, if a rate pair (R_0, R_1) is achievable for the Gaussian BCC, it must hold for any $\epsilon > 0$ that

$$R_0 \leqslant \min\left(\frac{1}{n}\sum_{i=1}^{n}\mathbb{I}\big(\mathsf{M}_0\tilde{\mathsf{Z}}^{i+1}\mathsf{Y}^{i-1};\mathsf{Y}_i\big), \frac{1}{n}\sum_{i=1}^{n}\mathbb{I}\big(\mathsf{M}_0\tilde{\mathsf{Z}}^{i+1}\mathsf{Y}^{i-1};\mathsf{Z}_i\big)\right) + \delta(\epsilon),$$

$$R_1 \leqslant \frac{1}{n}\sum_{i=1}^{n}\left(\mathbb{I}\big(\mathsf{M}_1;\mathsf{Y}_i|\mathsf{M}_0\mathsf{Y}^{i-1}\tilde{\mathsf{Z}}^{i+1}\big) - \mathbb{I}\big(\mathsf{M}_1;\mathsf{Z}_i|\mathsf{M}_0\mathsf{Y}^{i-1}\tilde{\mathsf{Z}}^{i+1}\big)\right) + \delta(\epsilon), \tag{5.1}$$

where we have used $\mathsf{Y}^{i-1} \triangleq (\mathsf{Y}_1 \dots \mathsf{Y}_{i-1})$, and $\tilde{\mathsf{Z}}^{i+1} = (\mathsf{Z}_{i+1} \dots \mathsf{Z}_n)$. Next, we introduce the random variables $\mathsf{U}_i \triangleq \mathsf{Y}^{i-1}\tilde{\mathsf{Z}}^{i+1}\mathsf{M}_0$ and $\mathsf{V}_i \triangleq \mathsf{U}_i\mathsf{M}_1$. One can verify that the joint distribution of U_i, V_i, X_i, Y_i, and Z_i satisfies

$$\forall (u, v, x, y, z) \in \mathcal{U}\times\mathcal{V}\times\mathcal{X}\times\mathcal{Y}\times\mathcal{Z}$$
$$p_{\mathsf{U}_i}(u)p_{\mathsf{V}_i|\mathsf{U}_i}(v|u)p_{\mathsf{X}_i|\mathsf{V}_i}(x|v)p_{\mathsf{YZ}|\mathsf{X}}(y, z|x),$$

where $p_{\mathsf{YZ}|\mathsf{X}}$ are the transition probabilities of the Gaussian BCC. On substituting these random variables into (5.1), we obtain

$$R_0 \leqslant \min\left(\frac{1}{n}\sum_{i=1}^{n}\mathbb{I}(\mathsf{U}_i;\mathsf{Y}_i), \frac{1}{n}\sum_{i=1}^{n}\mathbb{I}(\mathsf{U}_i;\mathsf{Z}_i)\right) + \delta(\epsilon), \tag{5.2}$$

$$R_1 \leqslant \frac{1}{n}\sum_{i=1}^{n}(\mathbb{I}(\mathsf{V}_i;\mathsf{Y}_i|\mathsf{U}_i) - \mathbb{I}(\mathsf{V}_i;\mathsf{Z}_i|\mathsf{U}_i)) + \delta(\epsilon). \tag{5.3}$$

It remains to upper bound (5.2) and (5.3) with terms that depend on the power constraint P. We first assume that $\sigma_{\text{m}}^2 \leqslant \sigma_{\text{e}}^2$ so that the eavesdropper's channel is stochastically degraded with respect to the main channel. We expand $(1/n)\sum_{i=1}^{n}\mathbb{I}(\mathsf{U}_i;\mathsf{Y}_i)$ in terms of the differential entropy as

$$\frac{1}{n}\sum_{i=1}^{n}\mathbb{I}(\mathsf{U}_i;\mathsf{Y}_i) = \frac{1}{n}\sum_{i=1}^{n}\mathbb{h}(\mathsf{Y}_i) - \frac{1}{n}\sum_{i=1}^{n}\mathbb{h}(\mathsf{Y}_i|\mathsf{U}_i), \tag{5.4}$$

[1] Note that the use of weakly typical sequences limits us to bounds on the probability of error of the form $\mathbf{P}_{\text{e}}(\mathcal{C}_n) \leqslant \delta(\epsilon)$ instead of $\mathbf{P}_{\text{e}}(\mathcal{C}_n) \leqslant \delta_\epsilon(n)$ for DMCs; however, this has no effect on the secrecy-capacity region.

and we bound each sum separately. Notice that $\mathbb{E}\left[\mathsf{Y}_i^2\right] = \mathbb{E}\left[\mathsf{X}_i^2\right] + \sigma_{\mathrm{m}}^2$ since $\mathsf{Y}_i = \mathsf{X}_i + \mathsf{N}_{\mathrm{m},i}$ and X_i is independent of $\mathsf{N}_{\mathrm{m},i}$. The differential entropy of Y_i is upper bounded by the entropy of a Gaussian random variable with the same variance; therefore,

$$\frac{1}{n}\sum_{i=1}^{n}\mathbb{h}(\mathsf{Y}_i) \leqslant \frac{1}{n}\sum_{i=1}^{n}\frac{1}{2}\log\left(2\pi e\left(\mathbb{E}\left[\mathsf{X}_i^2\right] + \sigma_{\mathrm{m}}^2\right)\right).$$

Since $x \mapsto \log(2\pi e x)$ is a concave function of x, we have, by application of Jensen's inequality,

$$\frac{1}{n}\sum_{i=1}^{n}\frac{1}{2}\log\left(2\pi e\left(\mathbb{E}\left[\mathsf{X}_i^2\right] + \sigma_{\mathrm{m}}^2\right)\right) \leqslant \frac{1}{2}\log\left(2\pi e\left(\frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\left[\mathsf{X}_i^2\right] + \sigma_{\mathrm{m}}^2\right)\right).$$

On setting $Q \triangleq (1/n)\sum_{i=1}^{n}\mathbb{E}\left[\mathsf{X}_i^2\right]$, we finally obtain

$$\frac{1}{n}\sum_{i=1}^{n}\mathbb{h}(\mathsf{Y}_i) \leqslant \frac{1}{2}\log\left(2\pi e\left(Q + \sigma_{\mathrm{m}}^2\right)\right). \tag{5.5}$$

To bound the second sum $(1/n)\sum_{i=1}^{n}\mathbb{h}(\mathsf{Y}_i|\mathsf{U}_i)$, notice that

$$\frac{1}{n}\sum_{i=1}^{n}\mathbb{h}(\mathsf{Y}_i|\mathsf{U}_i) \leqslant \frac{1}{n}\sum_{i=1}^{n}\mathbb{h}(\mathsf{Y}_i) \leqslant \frac{1}{2}\log\left(2\pi e\left(Q + \sigma_{\mathrm{m}}^2\right)\right).$$

Moreover, because $\mathsf{U}_i \rightarrow \mathsf{X}_i \rightarrow \mathsf{Y}_i\mathsf{Z}_i$ forms a Markov chain, we have

$$\frac{1}{n}\sum_{i=1}^{n}\mathbb{h}(\mathsf{Y}_i|\mathsf{U}_i) \geqslant \frac{1}{n}\sum_{i=1}^{n}\mathbb{h}(\mathsf{Y}_i|\mathsf{X}_i\mathsf{U}_i) = \frac{1}{n}\sum_{i=1}^{n}\mathbb{h}(\mathsf{Y}_i|\mathsf{X}_i) = \frac{1}{2}\log\left(2\pi\sigma_{\mathrm{m}}^2\right).$$

Since $x \mapsto \frac{1}{2}\log\left(2\pi e\left(xQ + \sigma_{\mathrm{m}}^2\right)\right)$ is a continuous function on the interval $[0, 1]$, the intermediate-value theorem ensures the existence of $\beta \in [0, 1]$ such that

$$\frac{1}{n}\sum_{i=1}^{n}\mathbb{h}(\mathsf{Y}_i|\mathsf{U}_i) = \frac{1}{2}\log\left(2\pi e\left(\beta Q + \sigma_{\mathrm{m}}^2\right)\right). \tag{5.6}$$

On substituting (5.5) and (5.6) into (5.4), we obtain

$$\begin{aligned}\frac{1}{n}\sum_{i=1}^{n}\mathbb{I}(\mathsf{U}_i;\mathsf{Y}_i) &\leqslant \frac{1}{2}\log\left(2\pi e\left(Q + \sigma_{\mathrm{m}}^2\right)\right) - \frac{1}{2}\log\left(2\pi e\left(\beta Q + \sigma_{\mathrm{m}}^2\right)\right)\\ &= \frac{1}{2}\log\left(1 + \frac{(1-\beta)Q}{\sigma_{\mathrm{m}}^2}\right). \end{aligned}\tag{5.7}$$

We now need to upper bound $(1/n)\sum_{i=1}^{n}\mathbb{I}(\mathsf{Z}_i;\mathsf{U}_i)$. If we follow the same steps as above with Z_i in place of Y_i, we obtain the upper bound

$$\frac{1}{n}\sum_{i=1}^{n}\mathbb{I}(\mathsf{U}_i;\mathsf{Z}_i) \leqslant \frac{1}{2}\log\left(1 + \frac{(1-\beta')Q}{\sigma_{\mathrm{m}}^2}\right),$$

with $\beta' \in [0, 1]$. Unfortunately, this upper bound is not really useful because β' is a priori different from β; we need an alternative technique to show that $(1/n)\sum_{i=1}^{n}\mathbb{I}(\mathsf{U}_i;\mathsf{Z}_i)$ can be upper bounded with the *same* parameters β and Q as $(1/n)\sum_{i=1}^{n}\mathbb{I}(\mathsf{U}_i;\mathsf{Y}_i)$. The key tool that allows us to do so is the entropy–power inequality introduced in Lemma 2.14.

Note that we can repeat the steps leading to (5.5) with Z_i in place of Y_i to obtain

$$\frac{1}{n}\sum_{i=1}^{n}\mathbb{h}(\mathsf{Z}_i)\leqslant\frac{1}{2}\log\left(2\pi e\left(Q+\sigma_\mathrm{e}^2\right)\right);\tag{5.8}$$

therefore, we need to develop a lower bound for $(1/n)\sum_{i=1}^{n}\mathbb{h}(\mathsf{Z}_i|\mathsf{U}_i)$ as a function of β and Q. Since we have assumed that the eavesdropper's channel is stochastically degraded with respect to the main channel, we can write $\mathsf{Z}_i=\mathsf{Y}_i+\mathsf{N}_i'$ with $\mathsf{N}_i'\sim\mathcal{N}\left(0,\sigma_\mathrm{e}^2-\sigma_\mathrm{m}^2\right)$. Applying the entropy–power inequality to the random variable Z_i conditioned on $\mathsf{U}_i=u_i$, we have

$$\begin{aligned}\mathbb{h}(\mathsf{Z}_i|\mathsf{U}_i=u_i)&=\mathbb{h}(\mathsf{Y}_i+\mathsf{N}_i'|\mathsf{U}_i=u_i)\\&\geqslant\frac{1}{2}\log\left(2^{2\mathbb{h}(\mathsf{Y}_i|\mathsf{U}_i=u_i)}+2^{2\mathbb{h}(\mathsf{N}_i'|\mathsf{U}_i=u_i)}\right)\\&=\frac{1}{2}\log\left(2^{2\mathbb{h}(\mathsf{Y}_i|\mathsf{U}_i=u_i)}+2\pi e\left(\sigma_\mathrm{e}^2-\sigma_\mathrm{m}^2\right)\right).\end{aligned}$$

Therefore,

$$\begin{aligned}\frac{1}{n}\sum_{i=1}^{n}\mathbb{h}(\mathsf{Z}_i|\mathsf{U}_i)&=\frac{1}{n}\sum_{i=1}^{n}\mathbb{E}_{\mathsf{U}_i}[\mathbb{h}(\mathsf{Z}_i|\mathsf{U}_i)]\\&\geqslant\frac{1}{2n}\sum_{i=1}^{n}\mathbb{E}_{\mathsf{U}_i}\left[\log\left(2^{2\mathbb{h}(\mathsf{Y}_i|\mathsf{U}_i)}+2\pi e\left(\sigma_\mathrm{e}^2-\sigma_\mathrm{m}^2\right)\right)\right]\\&\overset{(a)}{\geqslant}\frac{1}{2n}\sum_{i=1}^{n}\log\left(2^{2\mathbb{E}_{\mathsf{U}_i}[\mathbb{h}(\mathsf{Y}_i|\mathsf{U}_i)]}+2\pi e\left(\sigma_\mathrm{e}^2-\sigma_\mathrm{m}^2\right)\right)\\&=\frac{1}{2n}\sum_{i=1}^{n}\log\left(2^{2\mathbb{h}(\mathsf{Y}_i|\mathsf{U}_i)}+2\pi e\left(\sigma_\mathrm{e}^2-\sigma_\mathrm{m}^2\right)\right)\\&\overset{(b)}{\geqslant}\frac{1}{2}\log\left(2^{2(1/n)\sum_{i=1}^{n}\mathbb{h}(\mathsf{Y}_i|\mathsf{U}_i)}+2\pi e\left(\sigma_\mathrm{e}^2-\sigma_\mathrm{m}^2\right)\right)\\&\overset{(c)}{=}\frac{1}{2}\log\left(2\pi e\left(\beta Q+\sigma_\mathrm{m}^2\right)+2\pi e\left(\sigma_\mathrm{e}^2-\sigma_\mathrm{m}^2\right)\right)\\&=\frac{1}{2}\log\left(2\pi e\left(\beta Q+\sigma_\mathrm{e}^2\right)\right),\end{aligned}\tag{5.9}$$

where both (a) and (b) follow from the convexity of the function $x\mapsto\log(2^x+c)$ for $c\in\mathbb{R}_+$ and Jensen's inequality while (c) follows from (5.6). Hence,

$$\begin{aligned}\frac{1}{n}\sum_{i=1}^{n}\mathbb{I}(\mathsf{U}_i;\mathsf{Z}_i)&=\frac{1}{n}\sum_{i=1}^{n}(\mathbb{h}(\mathsf{Z}_i)-\mathbb{h}(\mathsf{Z}_i|\mathsf{U}_i))\\&\leqslant\frac{1}{2}\log\left(2\pi e\left(Q+\sigma_\mathrm{e}^2\right)\right)-\frac{1}{2}\log\left(2\pi e\left(\beta Q+\sigma_\mathrm{e}^2\right)\right)\\&=\frac{1}{2}\log\left(1+\frac{(1-\beta)Q}{\sigma_\mathrm{e}^2}\right),\end{aligned}\tag{5.10}$$

where the inequality follows from (5.8) and (5.9). On substituting (5.7) and (5.10) into (5.2), we obtain

$$R_0 \leqslant \min\left(\frac{1}{2}\log\left(1+\frac{(1-\beta)Q}{\sigma_{\mathrm{m}}^2}\right), \frac{1}{2}\log\left(1+\frac{(1-\beta)Q}{\sigma_{\mathrm{e}}^2}\right)\right)+\delta(\epsilon). \tag{5.11}$$

We now develop an upper bound for R_1 as a function of the same parameters Q and β starting from (5.3). First, we eliminate the auxiliary random variable V_i by introducing the random variable X_i as follows:

$$\begin{aligned}
&\frac{1}{n}\sum_{i=1}^{n}(\mathbb{I}(\mathsf{V}_i;\mathsf{Y}_i|\mathsf{U}_i)-\mathbb{I}(\mathsf{V}_i;\mathsf{Z}_i|\mathsf{U}_i))\\
&\quad=\frac{1}{n}\sum_{i=1}^{n}(\mathbb{I}(\mathsf{V}_i\mathsf{X}_i;\mathsf{Y}_i|\mathsf{U}_i)-\mathbb{I}(\mathsf{X}_i;\mathsf{Y}_i|\mathsf{U}_i\mathsf{V}_i)-\mathbb{I}(\mathsf{V}_i\mathsf{X}_i;\mathsf{Z}_i|\mathsf{U}_i)+\mathbb{I}(\mathsf{X}_i;\mathsf{Z}_i|\mathsf{U}_i\mathsf{V}_i))\\
&\quad\overset{(a)}{=}\frac{1}{n}\sum_{i=1}^{n}(\mathbb{I}(\mathsf{X}_i;\mathsf{Y}_i|\mathsf{U}_i)-\mathbb{I}(\mathsf{X}_i;\mathsf{Z}_i|\mathsf{U}_i)-\mathbb{I}(\mathsf{X}_i;\mathsf{Y}_i|\mathsf{U}_i\mathsf{V}_i)+\mathbb{I}(\mathsf{X}_i;\mathsf{Z}_i|\mathsf{U}_i\mathsf{V}_i))\\
&\quad=\frac{1}{n}\sum_{i=1}^{n}(\mathbb{I}(\mathsf{X}_i;\mathsf{Y}_i|\mathsf{U}_i)-\mathbb{I}(\mathsf{X}_i;\mathsf{Z}_i|\mathsf{U}_i)-\mathbb{I}(\mathsf{X}_i;\mathsf{Y}_i\mathsf{Z}_i|\mathsf{U}_i\mathsf{V}_i)+\mathbb{I}(\mathsf{X}_i;\mathsf{Z}_i|\mathsf{Y}_i\mathsf{U}_i\mathsf{V}_i)\\
&\qquad\qquad+\mathbb{I}(\mathsf{X}_i;\mathsf{Z}_i|\mathsf{U}_i\mathsf{V}_i))\\
&\quad\overset{(b)}{=}\frac{1}{n}\sum_{i=1}^{n}(\mathbb{I}(\mathsf{X}_i;\mathsf{Y}_i|\mathsf{U}_i)-\mathbb{I}(\mathsf{X}_i;\mathsf{Z}_i|\mathsf{U}_i)-\mathbb{I}(\mathsf{X}_i;\mathsf{Y}_i\mathsf{Z}_i|\mathsf{U}_i\mathsf{V}_i)+\mathbb{I}(\mathsf{X}_i;\mathsf{Z}_i|\mathsf{U}_i\mathsf{V}_i))\\
&\quad\overset{(c)}{\leqslant}\frac{1}{n}\sum_{i=1}^{n}(\mathbb{I}(\mathsf{X}_i;\mathsf{Y}_i|\mathsf{U}_i)-\mathbb{I}(\mathsf{X}_i;\mathsf{Z}_i|\mathsf{U}_i)),
\end{aligned}$$

where (a) follows from $\mathbb{I}(\mathsf{V}_i;\mathsf{Z}_i|\mathsf{U}_i\mathsf{X}_i)=\mathbb{I}(\mathsf{V}_i;\mathsf{Y}_i|\mathsf{U}_i\mathsf{X}_i)=0$ since $\mathsf{U}_i\rightarrow\mathsf{V}_i\rightarrow\mathsf{X}_i\rightarrow\mathsf{Y}_i\mathsf{Z}_i$ forms a Markov chain, (b) follows from $\mathbb{I}(\mathsf{X}_i;\mathsf{Z}_i|\mathsf{U}_i\mathsf{V}_i\mathsf{Y}_i)=0$ since Z_i is stochastically degraded with respect to Y_i, and (c) follows from $\mathbb{I}(\mathsf{X}_i;\mathsf{Z}_i|\mathsf{U}_i\mathsf{V}_i)\leqslant\mathbb{I}(\mathsf{X}_i;\mathsf{Z}_i\mathsf{Y}_i|\mathsf{U}_i\mathsf{V}_i)$. Next, we use (5.6) and (5.9) to introduce β and Q as follows:

$$\begin{aligned}
&\frac{1}{n}\sum_{i=1}^{n}(\mathbb{I}(\mathsf{X}_i;\mathsf{Y}_i|\mathsf{U}_i)-\mathbb{I}(\mathsf{X}_i;\mathsf{Z}_i|\mathsf{U}_i))\\
&\quad=\frac{1}{n}\sum_{i=1}^{n}(\mathbb{h}(\mathsf{Y}_i|\mathsf{U}_i)-\mathbb{h}(\mathsf{Y}_i|\mathsf{X}_i\mathsf{U}_i)-\mathbb{h}(\mathsf{Z}_i|\mathsf{U}_i)+\mathbb{h}(\mathsf{Z}_i|\mathsf{X}_i\mathsf{U}_i))\\
&\quad\leqslant\frac{1}{2}\log\left(2\pi e\left(\beta Q+\sigma_{\mathrm{m}}^2\right)\right)-\frac{1}{2}\log\left(2\pi e\sigma_{\mathrm{m}}^2\right)\\
&\qquad-\frac{1}{2}\log\left(2\pi \mathrm{e}\left(\beta Q+\sigma_{\mathrm{e}}^2\right)\right)+\frac{1}{2}\log\left(2\pi e\sigma_{\mathrm{e}}^2\right)\\
&\quad=\frac{1}{2}\log\left(1+\frac{\beta Q}{\sigma_{\mathrm{m}}^2}\right)-\frac{1}{2}\log\left(1+\frac{\beta Q}{\sigma_{\mathrm{e}}^2}\right).
\end{aligned}\tag{5.12}$$

By substituting (5.12) into (5.3), we obtain the desired upper bound for R_1:

$$R_1 \leqslant \frac{1}{2}\log\left(1+\frac{\beta Q}{\sigma_{\mathrm{m}}^2}\right) - \frac{1}{2}\log\left(1+\frac{\beta Q}{\sigma_{\mathrm{e}}^2}\right) + \delta(\epsilon). \tag{5.13}$$

If $\sigma_{\mathrm{e}}^2 \leqslant \sigma_{\mathrm{m}}^2$, then the main channel is stochastically degraded with respect to the eavesdropper's channel and $R_1 = 0$ by virtue of Proposition 3.4. By swapping the roles of Y_i and Z_i in the proof, the reader can verify that (5.11) still holds. We combine the two cases $\sigma_{\mathrm{e}}^2 \leqslant \sigma_{\mathrm{m}}^2$ and $\sigma_{\mathrm{e}}^2 \geqslant \sigma_{\mathrm{m}}^2$ by writing

$$R_0 \leqslant \min\left(\frac{1}{2}\log\left(1+\frac{(1-\beta)Q}{\sigma_{\mathrm{m}}^2}\right), \frac{1}{2}\log\left(1+\frac{(1-\beta)Q}{\sigma_{\mathrm{e}}^2}\right)\right) + \delta(\epsilon),$$

$$R_1 \leqslant \left(\frac{1}{2}\log\left(1+\frac{\beta Q}{\sigma_{\mathrm{m}}^2}\right) - \frac{1}{2}\log\left(1+\frac{\beta Q}{\sigma_{\mathrm{e}}^2}\right)\right)^+ + \delta(\epsilon).$$

To conclude the proof, notice that

$$Q \mapsto \min\left(\frac{1}{2}\log\left(1+\frac{(1-\beta)Q}{\sigma_{\mathrm{m}}^2}\right), \frac{1}{2}\log\left(1+\frac{(1-\beta)Q}{\sigma_{\mathrm{e}}^2}\right)\right)$$

and

$$Q \mapsto \left(\frac{1}{2}\log\left(1+\frac{\beta Q}{\sigma_{\mathrm{m}}^2}\right) - \frac{1}{2}\log\left(1+\frac{\beta Q}{\sigma_{\mathrm{e}}^2}\right)\right)^+$$

are increasing functions of Q and, by definition, $Q = (1/n)\sum_{i=1}^n \mathbb{E}\left[\mathsf{X}_i^2\right] \leqslant P$. Additionally, ϵ can be chosen arbitrarily small; therefore, it must hold that

$$R_0 \leqslant \min\left(\frac{1}{2}\log\left(1+\frac{(1-\beta)P}{\sigma_{\mathrm{m}}^2}\right), \frac{1}{2}\log\left(1+\frac{(1-\beta)P}{\sigma_{\mathrm{e}}^2}\right)\right),$$

$$R_1 \leqslant \left(\frac{1}{2}\log\left(1+\frac{\beta P}{\sigma_{\mathrm{m}}^2}\right) - \frac{1}{2}\log\left(1+\frac{\beta P}{\sigma_{\mathrm{e}}^2}\right)\right)^+. \qquad \square$$

In contrast to the general BCC, the capacity region of the Gaussian BCC does not require the introduction of a prefix channel. In fact, the proof of Theorem 5.1 shows that the choice $\mathsf{X} = \mathsf{V}$ is optimal. The typical shape of the region $\mathcal{C}^{\mathrm{GBCC}}$ is illustrated in Figure 5.2, together with the capacity region of the same Gaussian broadcast channel *without* confidential messages. It may seem that communicating securely inflicts a strong rate penalty and that a significant portion of the available capacity has to be sacrificed to confuse the eavesdropper; however, this is again somewhat misleading because the achievability proof shows that it is possible to transmit an additional individual message to the legitimate receiver. On specializing the results of Section 3.6.1 and assuming $\sigma_{\mathrm{m}}^2 \leqslant \sigma_{\mathrm{e}}^2$, we see that it is actually possible to transmit three messages over a Gaussian broadcast channel with confidential messages:

(1) a common message to both Bob and Eve at rate

$$R_0 = \min\left(\frac{1}{2}\log\left(1+\frac{(1-\beta)P}{\sigma_{\mathrm{m}}^2+\beta P}\right), \frac{1}{2}\log\left(1+\frac{(1-\beta)P}{\sigma_{\mathrm{e}}^2+\beta P}\right)\right);$$

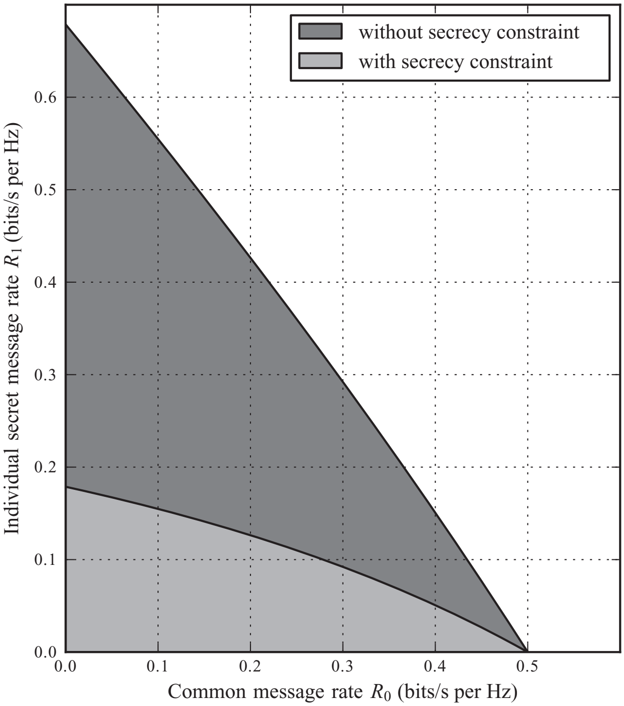

Figure 5.2 Secrecy-capacity region and capacity region of a Gaussian broadcast channel with $\sigma_\mathrm{m} = 0.8$, $\sigma_\mathrm{e} = 1$, and $P = 1$. The light gray region is the secrecy-capacity region, whereas the darker gray region is the capacity region without secrecy constraints.

(2) a confidential message to Bob at rate

$$R_1 = \frac{1}{2}\log\left(1 + \frac{\beta P}{\sigma_\mathrm{m}^2}\right) - \frac{1}{2}\log\left(1 + \frac{\beta P}{\sigma_\mathrm{e}^2}\right);$$

(3) a public message to Bob with no guaranteed secrecy at rate

$$R_\mathrm{d} = \frac{1}{2}\log\left(1 + \frac{\beta P}{\sigma_\mathrm{e}^2}\right).$$

Without any common message sent to Eve ($\beta = 1$ and $R_0 = 0$), the total rate effectively available to communicate with Bob is $R_1 + R_\mathrm{d} = \frac{1}{2}\log\left(1 + P/\sigma_\mathrm{m}^2\right)$, which is the capacity of the main channel.

The secrecy capacity of the Gaussian WTC is obtained by specializing Theorem 5.1 to $\beta = 1$ ($R_0 = 0$).

Corollary 5.1 (Leung-Yan-Cheong and Hellman). *The secrecy capacity of the Gaussian WTC is*

$$C_\mathrm{s} = \left(\frac{1}{2}\log\left(1 + \frac{P}{\sigma_\mathrm{m}^2}\right) - \frac{1}{2}\log\left(1 + \frac{P}{\sigma_\mathrm{e}^2}\right)\right)^+ \triangleq (C_\mathrm{m} - C_\mathrm{e})^+,$$

where $C_\mathrm{m} \triangleq \frac{1}{2}\log\left(1 + P/\sigma_\mathrm{m}^2\right)$ is the capacity of the main channel and $C_\mathrm{e} \triangleq 1 + P/\sigma_e^2$ is that of the eavesdropper's channel.

The expression for the secrecy capacity of the Gaussian WTC implies that secure communication is possible if and only if the legitimate receiver has a better signal-to-noise ratio (SNR) than that of the eavesdropper. In practice, this is likely to happen if the eavesdropper is located farther away from the transmitter than the legitimate receiver and receives attenuated signals. Near-field communication is a good example of such a situation, but this requires the eavesdropper to have a disadvantage at the physical layer itself. Also notice that, unlike the channel capacity, the secrecy capacity does not grow unbounded as $P \to \infty$. Taking the limit in Corollary 5.1, we obtain

$$\lim_{P\to\infty} C_{\mathrm{s}}(P) = \left(\frac{1}{2}\log\left(\frac{\sigma_{\mathrm{e}}^2}{\sigma_{\mathrm{m}}^2}\right)\right)^+ .$$

Therefore, increasing the power results in only marginal secrecy gains beyond a certain point.

Remark 5.1. *All of the results above extend to the* complex *Gaussian WTC, for which the noise sources are complex and circularly symmetric, that is* $\mathsf{N}_{\mathrm{m},i} \sim \mathcal{CN}(0, \sigma_{\mathrm{m}}^2)$ *and* $\mathsf{N}_{\mathrm{e},i} \sim \mathcal{CN}(0, \sigma_{\mathrm{e}}^2)$*, and can account for constant (and known) multiplicative coefficients* $h_{\mathrm{m}} \in \mathbb{C}$ *and* $h_{\mathrm{e}} \in \mathbb{C}$ *in the main channel and in the eavesdropper's channel, respectively. By noting that a complex Gaussian WTC is equivalent to two parallel real Gaussian WTCs with power constraint* $P/2$ *(and half the noise variance), and that a multiplicative coefficient induces a scaling of the received SNR, the secrecy capacity follows directly from the previous analysis and we have*

$$C_{\mathrm{s}} = \left(\log\left(1 + \frac{|h_{\mathrm{m}}|^2 P}{\sigma_{\mathrm{m}}^2}\right) - \log\left(1 + \frac{|h_{\mathrm{e}}|^2 P}{\sigma_{\mathrm{e}}^2}\right)\right)^+ .$$

Remark 5.2. *Suppose that the eavesdropper's noise is known to be Gaussian, but the variance is known only to satisfy* $\sigma_{\mathrm{e}}^2 \geqslant \sigma_0^2$ *for some fixed* σ_0^2*. One can check that a set of Gaussian channels with noise variance* $\sigma_{\mathrm{e}}^2 \geqslant \sigma_0^2$ *forms a class of stochastically degraded channels, as introduced in Definition 3.10. Proposition 3.3 guarantees that a wiretap code designed for an eavesdropper's noise variance* σ_0^2 *will also ensure secrecy if the actual variance is* $\sigma_{\mathrm{e}}^2 \geqslant \sigma_0^2$*.*

5.1.2 Multiple-input multiple-output Gaussian wiretap channel

Generalizing the results obtained in the previous section to a multiple-input multiple-output (MIMO) situation is not merely useful for the sake of completeness; it also allows us to study the effect of spatial dimensionality and collusion of eavesdroppers on secure communications rates. The MIMO wiretap channel[2] is illustrated in Figure 5.3. The numbers of antennas used by the transmitter, receiver, and eavesdropper are denoted n_{t}, n_{r}, and n_{e}, respectively. Notice that the model does not distinguish between a single eavesdropper with multiple antennas and a set of multiple eavesdroppers who collude

[2] This model is also called the multiple-input multiple-output multiple-eavesdropper (MIMOME) channel to emphasize that all parties have multiple antennas.

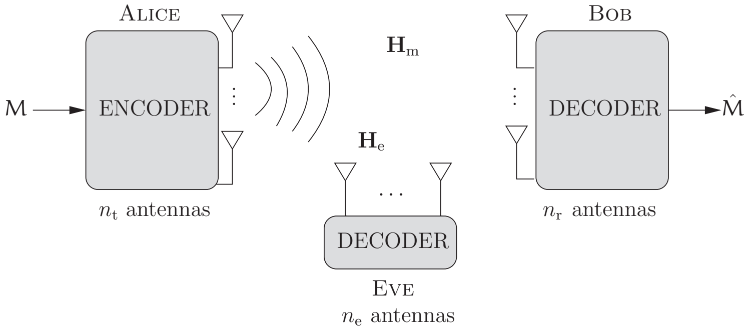
ALICE
BOB
M
ENCODER
$\mathbf{H}_{\mathrm{m}}$
$\mathbf{H}_{\mathrm{e}}$
DECODER
$\hat{\mathrm{M}}$
n_{t} antennas
n_{r} antennas
DECODER
EVE
n_{e} antennas

Figure 5.3 Communication over a MIMO Gaussian WTC.

and process their measurements jointly. In practice, there is a physical limit to the number of useful collocated antennas that one can deploy; therefore, a collusion of eavesdroppers is likely to be more powerful than a single eavesdropper with multiple antennas.

For a Gaussian MIMO wiretap channel (Gaussian MIMO WTC for short), the relationships between the inputs and outputs of the channel at each time i are

$$\mathrm{Y}_i^{n_{\mathrm{r}}} = \mathbf{H}_{\mathrm{m}}\mathrm{X}_i^{n_{\mathrm{t}}} + \mathrm{N}_{\mathrm{m},i} \quad \text{and} \quad \mathrm{Z}_i^{n_{\mathrm{e}}} = \mathbf{H}_{\mathrm{e}}\mathrm{X}_i^{n_{\mathrm{t}}} + \mathrm{N}_{\mathrm{e},i},$$

where $\mathrm{X}_i^{n_{\mathrm{t}}} \in \mathbb{C}^{n_{\mathrm{t}}\times 1}$ is the channel input vector, $\mathbf{H}_{\mathrm{m}} \in \mathbb{C}^{n_{\mathrm{r}}\times n_{\mathrm{t}}}$ and $\mathbf{H}_{\mathrm{e}} \in \mathbb{C}^{n_{\mathrm{e}}\times n_{\mathrm{t}}}$ are deterministic complex matrices, $\mathrm{Y}_i^{n_{\mathrm{r}}} \in \mathbb{C}^{n_{\mathrm{r}}\times 1}$ is the legitimate receiver's observation vector, and $\mathrm{Z}_i^{n_{\mathrm{e}}} \in \mathbb{C}^{n_{\mathrm{e}}\times 1}$ is the eavesdropper's observation vector. The channel matrices $\mathbf{H}_{\mathrm{m}}$ and $\mathbf{H}_{\mathrm{e}}$ are fixed for the entire transmission and known to all three terminals. The noise processes $\{\mathrm{N}_{\mathrm{m},i}\}_{i\geqslant 1}$ and $\{\mathrm{N}_{\mathrm{e},i}\}_{i\geqslant 1}$ are i.i.d.; at each time i the vectors $\mathrm{N}_{\mathrm{m},i} \in \mathbb{C}^{n_{\mathrm{r}}\times 1}$ and $\mathrm{N}_{\mathrm{e},i} \in \mathbb{C}^{n_{\mathrm{e}}\times 1}$ are circularly symmetric complex Gaussian random vectors with covariance matrices $\mathbf{K}_{\mathrm{m}} = \sigma_{\mathrm{m}}^2\mathbf{I}_{n_{\mathrm{r}}}$ and $\mathbf{K}_{\mathrm{e}} = \sigma_{\mathrm{e}}^2\mathbf{I}_{n_{\mathrm{e}}}$, respectively, where $\mathbf{I}_n$ is the identity matrix of dimension n. The channel input is also subject to the long-term average power constraint $(1/n)\sum_{i=1}^n \mathbb{E}\left[\left\|\mathrm{X}_i^{n_{\mathrm{t}}}\right\|^2\right] \leqslant P$.

Theorem 5.2 (Khisti and Wornell, Oggier and Hassibi, Liu and Shamai). *The secrecy capacity of the Gaussian MIMO WTC is*

$$C_{\mathrm{s}}^{\mathsf{MIMO}} = \max\left(\log\left|\mathbf{I}_{n_{\mathrm{r}}} + \frac{1}{\sigma_{\mathrm{m}}^2}\mathbf{H}_{\mathrm{m}}\mathbf{K}_{\mathrm{X}}\mathbf{H}_{\mathrm{m}}^{\dagger}\right| - \log\left|\mathbf{I}_{n_{\mathrm{e}}} + \frac{1}{\sigma_{\mathrm{e}}^2}\mathbf{H}_{\mathrm{e}}\mathbf{K}_{\mathrm{X}}\mathbf{H}_{\mathrm{e}}^{\dagger}\right|\right),$$

where the maximization is over all positive semi-definite matrices $\mathbf{K}_{\mathrm{X}}$ *such that* $\mathrm{tr}(\mathbf{K}_{\mathrm{X}}) \leqslant P$.

The expression for $C_{\mathrm{s}}^{\mathsf{MIMO}}$ is the natural generalization of the scalar case obtained in Corollary 5.1 which we could have expected; however, the proof of this result is significantly more involved. On the one hand, the achievability of rates below $C_{\mathrm{s}}^{\mathsf{MIMO}}$ follows from Corollary 3.4, which can be shown to hold for continuous vector channels with multiple inputs and outputs. Choosing an $n_{\mathrm{t}} \times n_{\mathrm{t}}$ positive semi-definite matrix $\mathbf{K}$ such that $\mathrm{tr}(\mathbf{K}) = P$ and substituting the random variables

$$\mathrm{V} \sim \mathcal{CN}(0, \mathbf{K}) \quad \text{and} \quad \mathrm{X} \triangleq \mathrm{V} \tag{5.14}$$

into Corollary 3.4 yields the desired result. On the other hand, proving that the choice of random variables in (5.14) is optimal is arduous because, in general and in contrast to the scalar Gaussian WTC, the eavesdropper's channel is not stochastically degraded with respect to the main channel. We refer the reader to the bibliographical notes at the end of this chapter for references to various proofs.

The maximization over covariance matrices subject to a trace constraint in the expression for $C_{\text{s}}^{\text{MIMO}}$ makes it difficult to develop much intuition from Theorem 5.2 directly. Nevertheless, it is possible to develop a necessary and sufficient condition for $C_{\text{s}}^{\text{MIMO}} = 0$ that admits a more intuitive interpretation.

Proposition 5.1 (Khisti and Wornell)**.** *The secrecy capacity of the Gaussian MIMO WTC is zero if and only if* $\lambda_{\max}(\mathbf{H}_{\text{w}}, \mathbf{H}_{\text{e}}) \leqslant 1$, *where*

$$\lambda_{\max}(\mathbf{H}_{\text{w}}, \mathbf{H}_{\text{e}}) \triangleq \sup_{\mathbf{v}\in\mathbb{C}^{n_{\text{t}}}} \frac{\sigma_{\text{e}}}{\sigma_{\text{m}}} \frac{\|\mathbf{H}_{\text{m}}\mathbf{v}\|}{\|\mathbf{H}_{\text{e}}\mathbf{v}\|}.$$

Sketch of proof. The kernel of a matrix $\mathbf{H}$ is $\text{Ker}(\mathbf{H}) \triangleq \{\mathbf{v} : \mathbf{H}\mathbf{v} = \mathbf{0}\}$. If $\text{Ker}(\mathbf{H}_{\text{e}}) \cap \text{Ker}(\mathbf{H}_{\text{m}})^{\perp} \neq \emptyset$, there exists a vector $\mathbf{v}$ such that $\|\mathbf{H}_{\text{m}}\mathbf{v}\| > 0$ and $\|\mathbf{H}_{\text{e}}\mathbf{v}\| = 0$. In this case, $\lambda_{\max}$ is undefined and the transmitter can communicate securely by beamforming his signal in the direction of $\mathbf{v}$, which is unheard by the eavesdropper. Notice that this strategy does not require a wiretap code and beamforming is sufficient to secure communications.

If $\text{Ker}(\mathbf{H}_{\text{e}}) \cap \text{Ker}(\mathbf{H}_{\text{m}})^{\perp} = \emptyset$, then beamforming is not sufficient to secure communications. Nevertheless, if $\lambda_{\max}(\mathbf{H}_{\text{w}}, \mathbf{H}_{\text{e}}) > 1$, then there exists $\mathbf{v}$ with $\|\mathbf{v}\| = 1$ such that $\|\mathbf{H}_{\text{m}}\mathbf{v}\|/\sigma_{\text{m}} > \|\mathbf{H}_{\text{e}}\mathbf{v}\|/\sigma_{\text{e}}$; in other words, even though the eavesdropper overhears all signals, there exists (at least) one direction in which the legitimate receiver benefits from a higher gain than the eavesdropper. Substituting the random variables

$$\mathsf{V} \sim \mathcal{CN}(0, P\mathbf{v}\mathbf{v}^{\text{T}}) \quad \text{and} \quad \mathsf{X} \triangleq \mathsf{V}$$

into Corollary 3.4 shows that

$$C_{\text{s}} \geqslant \log\left|\mathbf{I}_{n_{\text{r}}} + \frac{P}{\sigma_{\text{m}}^2}\mathbf{H}_{\text{m}}\mathbf{v}\mathbf{v}^{\dagger}\mathbf{H}_{\text{m}}^{\dagger}\right| - \log\left|\mathbf{I}_{n_{\text{r}}} + \frac{P}{\sigma_{\text{e}}^2}\mathbf{H}_{\text{e}}\mathbf{v}\mathbf{v}^{\dagger}\mathbf{H}_{\text{e}}^{\dagger}\right|. \tag{5.15}$$

Using the identity $\log|\mathbf{I} + \mathbf{AB}| = \log|\mathbf{I} + \mathbf{BA}|$, we can rewrite (5.15) as

$$C_{\text{s}} \geqslant \log\left(1 + \frac{P}{\sigma_{\text{m}}^2}\|\mathbf{H}_{\text{m}}\mathbf{v}\|^2\right) - \log\left(1 + \frac{P}{\sigma_{\text{e}}^2}\|\mathbf{H}_{\text{e}}\mathbf{v}\|^2\right),$$

and the right-hand side is strictly positive since $\|\mathbf{H}_{\text{m}}\mathbf{v}\|/\sigma_{\text{m}} > \|\mathbf{H}_{\text{e}}\mathbf{v}\|/\sigma_{\text{e}}$.

If $\lambda_{\max}(\mathbf{H}_{\text{w}}, \mathbf{H}_{\text{e}}) \leqslant 1$, it is also possible to show that $C_{\text{s}}^{\text{MIMO}} = 0$. The proof hinges on a closed-form expression for $C_{\text{s}}^{\text{MIMO}} = 0$ in the high-SNR regime obtained using a generalized singular-value decomposition of $\mathbf{H}_{\text{m}}$ and $\mathbf{H}_{\text{e}}$. We refer the reader to [83, 84] for details of the proof. □

As expected, Proposition 5.1 confirms that secure communication is possible if the transmitter can beamform his signals in such a direction that the eavesdropper does not overhear. Perhaps more interestingly, Proposition 5.1 also shows that the secrecy capacity is strictly positive as long as the transmitter can beamform his signals in a

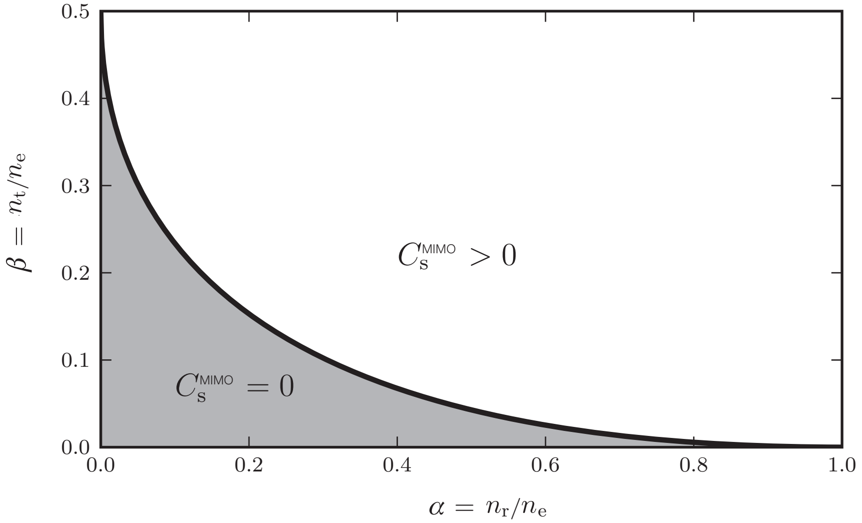

Figure 5.4 Condition for zero secrecy capacity in the limit of a large number of antennas. The elements of $\mathbf{H}_{\mathrm{m}}$ and $\mathbf{H}_{\mathrm{e}}$ are assumed to be generated i.i.d. according to the distribution $\mathcal{CN}(0, 1)$ and $\sigma_{\mathrm{m}} = \sigma_{\mathrm{e}} = 1$.

direction for which the eavesdropper obtains a lower SNR than does the legitimate receiver. In other words, the combination of coding and beamforming is more powerful than beamforming alone. Without additional assumptions about the specific structure of $\mathbf{H}_{\mathrm{m}}$ and $\mathbf{H}_{\mathrm{e}}$, little can be said regarding the existence of a secure beamforming direction. Nevertheless, if the entries of $\mathbf{H}_{\mathrm{m}}$ and $\mathbf{H}_{\mathrm{e}}$ are generated i.i.d. according to $\mathcal{CN}(0, 1)$ and if their realizations are known to Alice, Bob, and Eve, the behavior of $C_{\mathrm{s}}^{\mathrm{MIMO}}$ can be further analyzed using tools from random-matrix theory.

Proposition 5.2 (Khisti and Wornell)**.** *Suppose that $\sigma_{\mathrm{m}} = \sigma_{\mathrm{e}} = 1$ and n_{r}, n_{t}, and n_{e} go to infinity while the ratios $\alpha \triangleq n_{\mathrm{r}}/n_{\mathrm{e}}$ and $\beta \triangleq n_{\mathrm{t}}/n_{\mathrm{e}}$ are kept fixed. Then, the secrecy capacity converges almost surely to zero if and only if*

$$0 \leqslant \beta \leqslant \frac{1}{2}, \quad 0 \leqslant \alpha \leqslant 1, \quad \textit{and} \quad \alpha \leqslant \left(1 - \sqrt{2\beta}\right)^2.$$

The proof of Proposition 5.2 can be found in [83, 84]. Proposition 5.2 allows us to relate the possibility of secure communication directly to the number of antennas deployed by Alice, Bob, and Eve. As expected, and as illustrated in Figure 5.4, the secrecy capacity is positive as long as Eve does not deploy too many antennas compared with the numbers deployed by Alice and Bob. For instance, if $\alpha = 0$, which corresponds to a single receive antenna for Bob, the secrecy capacity is positive if Eve has fewer than twice as many antennas as Alice. For $\beta = 0$, which corresponds to a single transmit antenna for Alice, the secrecy capacity is positive provided that Eve has fewer antennas than Bob. This leads to the pessimistic conclusion that little can be done against an all-powerful eavesdropper who is able to deploy many antennas; however, one can perhaps draw a more optimistic conclusion and argue that Alice and Bob can mitigate the impact of colluding eavesdroppers by deploying multiple transmit and receive antennas.

We conclude this section on the MIMO Gaussian WTC with a brief discussion of a suboptimal strategy that sheds light on the choice of the input covariance matrix $\mathbf{K}_\mathsf{X}$ in Theorem 5.2. Let $r = \text{rk}(\mathbf{H}_\text{m})$ and consider the compact singular-value decomposition $\mathbf{H}_\text{m} = \mathbf{U}_\text{m}\Lambda_\text{m}\mathbf{V}_\text{m}^\dagger$, in which $\mathbf{U}_\text{m} \in \mathbb{C}^{n_\text{r}\times r}$ and $\mathbf{V}_\text{m} \in \mathbb{C}^{n_\text{t}\times r}$ have unitary columns, and $\Lambda_\text{m} \in \mathbb{C}^{r\times r}$ is a diagonal matrix with non-zero diagonal terms. We construct a unitary matrix $\mathbf{V} \in \mathbb{C}^{n_\text{t}\times n_\text{t}}$, by appending appropriate column vectors to $\mathbf{V}_\text{m}$, and we let

$$\mathbf{V} \triangleq (\mathbf{V}_\text{m}\ \mathbf{V}_\text{n}) \quad \text{with} \quad \mathbf{V}_\text{m} \triangleq (\mathbf{v}_1 \dots \mathbf{v}_r) \quad \text{and} \quad \mathbf{V}_\text{n} \triangleq \left(\mathbf{v}_{r+1} \dots \mathbf{v}_{n_\text{t}}\right).$$

This decomposition allows us to interpret the channel to the legitimate receiver as n_t parallel channels, of which only the first r can effectively be used for communication. Alice simultaneously transmits r symbols $b_1, \dots, b_r$ by sending the vector

$$\mathbf{x} = \sum_{j=1}^{r} b_j \mathbf{v}_j + \sum_{j=r+1}^{n_\text{t}} n_j \mathbf{v}_\mathbf{j},$$

where $\{n_j\}_{j=r+1}^{n_\text{t}}$ are dummy noise symbols. These dummy symbols do not affect Bob's received signal because they lie in the kernel of $\mathbf{H}_\text{m}$, but they are mixed with the useful symbols in Eve's received signal. This scheme is called an *artificial noise transmission* strategy since it consists essentially of transmitting information in the direction of the non-zero singular values of $\mathbf{H}_\text{m}$, and sending noise in all other directions to harm the eavesdropper. A simple way of ensuring that the power constraint $(1/n)\sum_{i=1}^{n} \mathbb{E}\left[\left\|\mathsf{X}_i^{n_t}\right\|^2\right] \leqslant P$ is satisfied is to allocate the same average power P/n_t to all n_t sub-channels. In this case, achievable secure communication rates are given by the following proposition.

Proposition 5.3 (Khisti *et al.*). *The artificial noise transmission strategy achieves all the secure rates R_s such that*

$$R_\text{s} < \log\left|\mathbf{I}_\text{r} + \frac{P}{\sigma_\text{m}^2 n_\text{t}}\Lambda_\text{m}\Lambda_\text{m}^\dagger\right| + \log\left|\mathbf{V}_\text{m}^\dagger\left(\mathbf{I} + \frac{P}{\sigma_\text{e}^2 n_\text{t}}\mathbf{H}_\text{e}^\dagger\mathbf{H}_\text{e}\right)^{-1}\mathbf{V}_\text{m}\right|$$

Proof. The secure communication rates are obtained by substituting the random variables

$$\mathsf{V} \triangleq \sum_{j=1}^{r} \mathsf{B}_j \mathbf{v}_j \quad \text{and} \quad \mathsf{X} = \mathsf{V} + \sum_{j=r+1}^{n_\text{t}} \mathsf{N}_j \mathbf{v}_j$$

into Corollary 3.4, where the random variables $\{\mathsf{B}_j\}_{j=1}^{r}$ and $\{\mathsf{N}_j\}_{j=r+1}^{n_\text{t}}$ are i.i.d. and drawn according to $\mathcal{CN}(0, P/n_\text{t})$. Then,

$$\begin{aligned}
\mathbb{I}(\mathsf{V};\mathsf{Y}) &= \mathbb{h}(\mathsf{Y}) - \mathbb{h}(\mathsf{Y}|\mathsf{X}) && (5.16)\\
&= \log\left|\sigma_\text{m}^2\mathbf{I} + \frac{P}{n_\text{t}}\mathbf{H}_\text{m}\mathbf{V}\mathbf{V}^\dagger\mathbf{H}_\text{m}^\dagger\right| - \log\left|\sigma_\text{m}^2\mathbf{I}\right| \\
&= \log\left|\mathbf{I} + \frac{P}{\sigma_\text{m}^2 n_\text{t}}\mathbf{U}_\text{m}\Lambda_\text{m}\mathbf{V}_\text{m}^\dagger\mathbf{V}\mathbf{V}^\dagger\mathbf{V}_\text{m}\Lambda_\text{m}^\dagger\mathbf{U}_\text{m}^\dagger\right| \\
&= \log\left|\mathbf{I} + \frac{P}{\sigma_\text{m}^2 n_\text{t}}\Lambda_\text{m}\Lambda_\text{m}^\dagger\right|, && (5.17)
\end{aligned}$$

where we have used $\mathbf{V}_{\mathrm{m}}^{\dagger}\mathbf{V}_{\mathrm{m}} = \mathbf{I}_{\mathrm{r}}$, $\mathbf{U}_{\mathrm{m}}^{\dagger}\mathbf{U}_{\mathrm{m}} = \mathbf{I}_{\mathrm{r}}$, and $\log|\mathbf{I} + \mathbf{AB}| = \log|\mathbf{I} + \mathbf{BA}|$ to obtain the last equality. Similarly,

$$
\begin{aligned}
\mathbb{I}(\mathsf{V};\mathsf{Z}) &= \mathbb{h}(\mathsf{Z}) - \mathbb{h}(\mathsf{Z}|\mathsf{V})\\
&= \log\left|\sigma_{\mathrm{e}}^2\mathbf{I} + \frac{P}{n_{\mathrm{t}}}\mathbf{H}_{\mathrm{e}}\mathbf{V}\mathbf{V}^{\dagger}\mathbf{H}_{\mathrm{e}}^{\dagger}\right| - \log\left|\sigma_{\mathrm{e}}^2\mathbf{I} + \frac{P}{n_{\mathrm{t}}}\mathbf{H}_{\mathrm{e}}\mathbf{V}_{\mathrm{n}}\mathbf{V}_{\mathrm{n}}^{\dagger}\mathbf{H}_{\mathrm{e}}^{\dagger}\right|\\
&= \log\left|\mathbf{I} + \frac{P}{\sigma_{\mathrm{e}}^2 n_{\mathrm{t}}}\mathbf{H}_{\mathrm{e}}\mathbf{H}_{\mathrm{e}}^{\dagger}\right| - \log\left|\mathbf{I} + \frac{P}{\sigma_{\mathrm{e}}^2 n_{\mathrm{t}}}\mathbf{V}_{\mathrm{n}}\mathbf{V}_{\mathrm{n}}^{\dagger}\mathbf{H}_{\mathrm{e}}^{\dagger}\mathbf{H}_{\mathrm{e}}\right|.
\end{aligned}
$$

Since $\mathbf{V}$ is unitary, $\mathbf{V}_{\mathrm{n}}\mathbf{V}_{\mathrm{n}}^{\dagger} + \mathbf{V}_{\mathrm{m}}\mathbf{V}_{\mathrm{m}}^{\dagger} = \mathbf{I}$; hence,

$$
\begin{aligned}
&\log\left|\mathbf{I} + \frac{P}{\sigma_{\mathrm{e}}^2 n_{\mathrm{t}}}\mathbf{V}_{\mathrm{n}}\mathbf{V}_{\mathrm{n}}^{\dagger}\mathbf{H}_{\mathrm{e}}^{\dagger}\mathbf{H}_{\mathrm{e}}\right|\\
&\quad= \log\left|\mathbf{I} + \frac{P}{\sigma_{\mathrm{e}}^2 n_{\mathrm{t}}}(\mathbf{I} - \mathbf{V}_{\mathrm{m}}\mathbf{V}_{\mathrm{m}}^{\dagger})\mathbf{H}_{\mathrm{e}}^{\dagger}\mathbf{H}_{\mathrm{e}}\right|\\
&\quad= \log\left|\left(\mathbf{I} + \frac{P}{\sigma_{\mathrm{e}}^2 n_{\mathrm{t}}}\mathbf{H}_{\mathrm{e}}^{\dagger}\mathbf{H}_{\mathrm{e}}\right)\left(\mathbf{I} - \frac{P}{\sigma_{\mathrm{e}}^2 n_{\mathrm{t}}}\left(\mathbf{I} + \frac{P}{\sigma_{\mathrm{e}}^2 n_{\mathrm{t}}}\mathbf{H}_{\mathrm{e}}^{\dagger}\mathbf{H}_{\mathrm{e}}\right)^{-1}\mathbf{V}_{\mathrm{m}}\mathbf{V}_{\mathrm{m}}^{\dagger}\mathbf{H}_{\mathrm{e}}^{\dagger}\mathbf{H}_{\mathrm{e}}\right)\right|.
\end{aligned}
$$

Therefore,

$$
\begin{aligned}
\mathbb{I}(\mathsf{V};\mathsf{Z}) &= -\log\left|\mathbf{I} - \frac{P}{\sigma_{\mathrm{e}}^2 n_{\mathrm{t}}}\left(\mathbf{I} + \frac{P}{\sigma_{\mathrm{e}}^2 n_{\mathrm{t}}}\mathbf{H}_{\mathrm{e}}^{\dagger}\mathbf{H}_{\mathrm{e}}\right)^{-1}\mathbf{V}_{\mathrm{m}}\mathbf{V}_{\mathrm{m}}^{\dagger}\mathbf{H}_{\mathrm{e}}^{\dagger}\mathbf{H}_{\mathrm{e}}\right|\\
&= -\log\left|\mathbf{I} - \frac{P}{\sigma_{\mathrm{e}}^2 n_{\mathrm{t}}}\mathbf{V}_{\mathrm{m}}^{\dagger}\mathbf{H}_{\mathrm{e}}^{\dagger}\mathbf{H}_{\mathrm{e}}\left(\mathbf{I} + \frac{P}{\sigma_{\mathrm{e}}^2 n_{\mathrm{t}}}\mathbf{H}_{\mathrm{e}}^{\dagger}\mathbf{H}_{\mathrm{e}}\right)^{-1}\mathbf{V}_{\mathrm{m}}\right|\\
&= -\log\left|\mathbf{V}_{\mathrm{m}}^{\dagger}\left(\mathbf{I} + \frac{P}{\sigma_{\mathrm{e}}^2 n_{\mathrm{t}}}\mathbf{H}_{\mathrm{e}}^{\dagger}\mathbf{H}_{\mathrm{e}}\right)^{-1}\mathbf{V}_{\mathrm{m}}\right|. \qquad (5.18)
\end{aligned}
$$

By Corollary 3.4, all the rates $R_{\mathrm{s}} < \mathbb{I}(\mathsf{V};\mathsf{Y}) - \mathbb{I}(\mathsf{V};\mathsf{Z})$ with $\mathbb{I}(\mathsf{V};\mathsf{Y})$ given by (5.17) and $\mathbb{I}(\mathsf{V};\mathsf{Z})$ given by (5.18) are achievable. □

The idea of introducing artificial noise into the system to hinder the eavesdropper is a powerful concept that will reappear in Chapter 8 for multi-user secure communication systems.

Remark 5.3. *Although the signaling used in the artificial noise transmission strategy relies solely on knowledge of* $\mathbf{H}_{\mathrm{m}}$ *and does not exploit knowledge of the eavesdropper's channel* $\mathbf{H}_{\mathrm{e}}$*, notice that knowledge of* $\mathbf{H}_{\mathrm{e}}$ *is* required *in order to design the wiretap code and select the secure communication rate appropriately. Hence, the artificial noise operates in only a* semi-blind *fashion.*

5.1.3 Gaussian source model

A Gaussian source model for secret-key agreement consists of a memoryless source $(\mathcal{XYZ}, p_{\mathsf{XYZ}})$ whose components are jointly Gaussian with zero mean. The distribution is entirely characterized by the second-order moments

$$\mathbb{E}\left[\mathsf{X}^2\right] = \sigma_{\mathsf{X}}^2, \quad \mathbb{E}\left[\mathsf{Y}^2\right] = \sigma_{\mathsf{Y}}^2, \quad \mathbb{E}\left[\mathsf{Z}^2\right] = \sigma_{\mathsf{Z}}^2,$$
$$\mathbb{E}[\mathsf{XY}] = \rho_1\sigma_{\mathsf{X}}\sigma_{\mathsf{Y}}, \quad \mathbb{E}[\mathsf{XZ}] = \rho_2\sigma_{\mathsf{X}}\sigma_{\mathsf{Z}}, \quad \mathbb{E}[\mathsf{YZ}] = \rho_3\sigma_{\mathsf{Y}}\sigma_{\mathsf{Z}},$$

where ρ_1, ρ_2, and ρ_3 are the correlation coefficients of the source components. The definitions of key-distillation strategies, achievable key rates, and the secret-key capacity are those used for discrete memoryless sources. A closer look at the proof of the upper bound for the secret-key capacity in Section 4.2.1 shows that the derivation does not rely on the discrete nature of the source $(\mathcal{XYZ}, p_{\mathsf{XYZ}})$; however, the achievability proof based on a conceptual WTC relies on the crypto lemma, which does not apply to Gaussian random variables. Nevertheless, we show in this section that the lower bound is still valid for a Gaussian source model.

Proposition 5.4. *For a Gaussian source model,*

$$\mathbb{I}(\mathsf{X};\mathsf{Y}) - \min(\mathbb{I}(\mathsf{X};\mathsf{Z}), \mathbb{I}(\mathsf{Y};\mathsf{Z})) \leqslant C_{\mathrm{s}}^{\mathrm{SM}} \leqslant \min(\mathbb{I}(\mathsf{X};\mathsf{Y}), \mathbb{I}(\mathsf{X},\mathsf{Y}|\mathsf{Z})).$$

Proof. The upper bound follows from the same steps as in the proof of Theorem 4.1, and we need only show that the lower bound holds. To do so, we construct a conceptual WTC as in Section 4.2.1 but we use this time the addition over real numbers. Specifically, to send a symbol $\mathsf{U} \in \mathbb{R}$ independent of the DMS to Bob, Alice observes a realization X of the DMS and transmits $\mathsf{U} + \mathsf{X}$ over the public channel, where $+$ denotes the usual addition over $\mathbb{R}$. This creates a conceptual memoryless WTC, for which Bob observes $(\mathsf{U} + \mathsf{X}, \mathsf{Y})$ and Eve observes $(\mathsf{U} + \mathsf{X}, \mathsf{Z})$. From the results of Chapter 3, we know that the secrecy capacity is at least

$$\mathbb{I}(\mathsf{U};\mathsf{Y},\mathsf{U}+\mathsf{X}) - \mathbb{I}(\mathsf{U};\mathsf{Z},\mathsf{U}+\mathsf{X}),$$

where the distribution p_{U} can be chosen arbitrarily; here, we choose $\mathsf{U} \sim \mathcal{N}(0, P)$ for some $P > 0$. Using the chain rule of mutual information repeatedly, we obtain

$$\begin{aligned}
&\mathbb{I}(\mathsf{U};\mathsf{Y},\mathsf{U}+\mathsf{X}) - \mathbb{I}(\mathsf{U};\mathsf{Z},\mathsf{U}+\mathsf{X})\\
&\quad = \mathbb{I}(\mathsf{U};\mathsf{Y}) + \mathbb{I}(\mathsf{U};\mathsf{U}+\mathsf{X}|\mathsf{Y}) - \mathbb{I}(\mathsf{U};\mathsf{Z}) - \mathbb{I}(\mathsf{U};\mathsf{U}+\mathsf{X}|\mathsf{Z})\\
&\quad = \mathbb{h}(\mathsf{U}|\mathsf{Z}) - \mathbb{h}(\mathsf{U}|\mathsf{Y}) + \mathbb{h}(\mathsf{U}+\mathsf{X}|\mathsf{Y}) - \mathbb{h}(\mathsf{U}+\mathsf{X}|\mathsf{UY}) - \mathbb{h}(\mathsf{U}+\mathsf{X}|\mathsf{Z})\\
&\qquad + \mathbb{h}(\mathsf{U}+\mathsf{X}|\mathsf{UZ})\\
&\quad \overset{(a)}{=} \mathbb{h}(\mathsf{U}|\mathsf{Z}) - \mathbb{h}(\mathsf{U}|\mathsf{Y}) + \mathbb{h}(\mathsf{U}+\mathsf{X}|\mathsf{Y}) - \mathbb{h}(\mathsf{X}|\mathsf{Y}) - \mathbb{h}(\mathsf{U}+\mathsf{X}|\mathsf{Z}) + \mathbb{h}(\mathsf{X}|\mathsf{Z}). \qquad (5.19)
\end{aligned}$$

Equality (a) follows because U is independent of (X, Y), which implies that

$$\mathbb{h}(\mathsf{U}+\mathsf{X}|\mathsf{UY}) = \mathbb{h}(\mathsf{X}|\mathsf{UY}) = \mathbb{h}(\mathsf{X}|\mathsf{Y}) \quad \text{and} \quad \mathbb{h}(\mathsf{U}+\mathsf{X}|\mathsf{UZ}) = \mathbb{h}(\mathsf{X}|\mathsf{Z}).$$

Now,

$$\begin{aligned}
\mathbb{h}(\mathsf{U}|\mathsf{Z}) - \mathbb{h}(\mathsf{U}+\mathsf{X}|\mathsf{Z}) &\leqslant \mathbb{h}(\mathsf{U}|\mathsf{Z}) - \mathbb{h}(\mathsf{U}+\mathsf{X}|\mathsf{Z},\mathsf{X})\\
&= \mathbb{h}(\mathsf{U}|\mathsf{Z}) - \mathbb{h}(\mathsf{U}|\mathsf{Z},\mathsf{X})\\
&= 0,
\end{aligned}$$

where the last equality follows again from the independence of U and (X, Z). Also,

$$\mathbb{h}(U|Z) - \mathbb{h}(U + X|Z) \geqslant \mathbb{h}(U|Z) - \mathbb{h}(U + X) \geqslant \log\left(\frac{P}{P + \sigma_x^2}\right),$$

where the last inequality follows from $\mathbb{h}(U|Z) = \mathbb{h}(U) = \log(2\pi e P)$ and the bound $\mathbb{h}(U + X) \leqslant \log(2\pi e(P + \sigma_x^2))$. Because all communication takes place over a public noiseless channel (of infinite capacity), P can be arbitrarily large,[3] and, for any $\epsilon > 0$, we can choose P such that

$$|\mathbb{h}(U|Z) - \mathbb{h}(U + X|Z)| \leqslant \frac{\epsilon}{2}. \tag{5.20}$$

Repeating the same argument with Y instead of Z shows that for P large enough we have

$$|\mathbb{h}(U|Y) - \mathbb{h}(U + X|Y)| \leqslant \frac{\epsilon}{2}. \tag{5.21}$$

On combining (5.19), (5.20), and (5.21), we obtain

$$\begin{aligned}\mathbb{I}(U; Y, U + X) - \mathbb{I}(U; Z, U + X) &\geqslant \mathbb{h}(X|Z) - \mathbb{h}(X|Y) - \epsilon \\ &= \mathbb{I}(X; Y) - \mathbb{I}(X; Z) - \epsilon.\end{aligned}$$

Since $\epsilon > 0$ can be chosen arbitrarily small, we must have

$$C_s^{\mathrm{SM}} \geqslant \mathbb{I}(X; Y) - \mathbb{I}(X; Z).$$

Similarly, by interchanging the roles of Y and Z, we can show that

$$C_s^{\mathrm{SM}} \geqslant \mathbb{I}(X; Y) - \mathbb{I}(Y; Z).$$ □

Remark 5.4. *There is no loss of generality by restricting our analysis to a centered Gaussian source model. If* X*,* Y*, and* Z *have non-zero means* μ_1*,* μ_1*, and* μ_3*, one can simply consider the centered random variables* $X' \triangleq X - \mu_1$*,* $Y' \triangleq Y - \mu_2$*, and* $Z' \triangleq Z - \mu_3$ *and note that the bounds on the secret-key capacity remain unchanged.*

The bounds given by Proposition 5.4 can be computed explicitly in terms of the parameters ρ_1, ρ_2, and ρ_3.

Corollary 5.2. *The secret-key capacity of a Gaussian source model satisfies*

$$\begin{aligned}&\max\left(\frac{1}{2}\log\left(\frac{1-\rho_2^2}{1-\rho_1^2}\right), \frac{1}{2}\log\left(\frac{1-\rho_3^2}{1-\rho_1^2}\right)\right) \\ &\qquad \leqslant C_s^{\mathrm{SM}} \leqslant \min\left(\frac{1}{2}\log\left(\frac{1}{1-\rho_1^2}\right), \frac{1}{2}\log\left(\frac{(1-\rho_2^2)(1-\rho_3^2)}{1+2\rho_1\rho_2\rho_3-\rho_1^2-\rho_2^2-\rho_3^2}\right)\right).\end{aligned}$$

[3] Note that our ability to choose P as large as desired is a mathematical convenience rather than a realistic solution. In practice, even public communication would be subject to a power constraint and thus to a rate constraint.

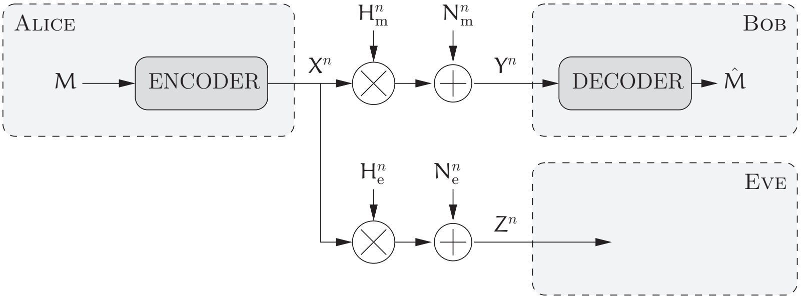

Figure 5.5 Communication over a wireless channel in the presence of an eavesdropper.

Remark 5.5. *Note that if $\rho_2 \geqslant \rho_1$ and $\rho_3 \geqslant \rho_1$ the lower bound obtained is negative and not really useful. Nevertheless, it is sometimes still possible to obtain a positive secret-key rate using an advantage-distillation protocol, as discussed in Section 4.3.1.*

Example 5.1. An interesting instance of a Gaussian source model is one in which $X \sim \mathcal{N}(0, P)$ is a Gaussian random variable transmitted over a Gaussian WTC, such that

$$Y = X + N_m \quad \text{and} \quad Z = X + N_e$$

with $N_m \sim \mathcal{N}(0, \sigma_m^2)$ and $N_e \sim \mathcal{N}(0, \sigma_e^2)$. In this case, Corollary 4.1 and Proposition 5.4 apply and $C_s^{SM} = \mathbb{I}(X; Y) - \mathbb{I}(Y; Z)$, which can be computed explicitly as

$$C_s^{SM} = \frac{1}{2} \log \left(1 + \frac{P\sigma_e^2}{(P + \sigma_e^2)\sigma_m^2} \right).$$

Note that C_s^{SM} is positive even if $\sigma_e^2 < \sigma_m^2$. In contrast, the secrecy capacity of the same Gaussian WTC given in Theorem 5.1 is

$$C_s = \left(\frac{1}{2} \log \left(1 + \frac{P}{\sigma_m^2} \right) - \frac{1}{2} \log \left(1 + \frac{P}{\sigma_e^2} \right) \right)^+,$$

which is zero if $\sigma_e^2 < \sigma_m^2$. Hence, the impossibility of secure communication over a Gaussian WTC when the eavesdropper has a higher SNR than that of the legitimate receiver is *solely* due to the restrictions placed on the communication scheme. In reality, as long as the eavesdropper obtains a different observation, the legitimate parties always have an advantage over the eavesdropper, and they can distill a secret key.

5.2 Wireless channels

The general channel model we use to investigate secure wireless communications is illustrated in Figure 5.5. For simplicity, we focus on the transmission of a single secure message and the characterization of the secrecy capacity, but all results described thereafter generalize to include a common message for the legitimate receiver and the eavesdropper. The communication channel between Alice and Bob is modeled as a *fading channel*, characterized by a random complex multiplicative coefficient H_{m} and an independent complex additive white Gaussian noise N_{m}. The coefficient H_{m} is called the *fading coefficient*, and accounts for the multipath interference occurring in a wireless transmission. The square of the magnitude of the fading coefficient, $\mathsf{G}_{\mathrm{m}} \triangleq |\mathsf{H}_{\mathrm{m}}|^2$, is called the *fading gain*. Similarly, the channel between Alice and the eavesdropper Eve is modeled as another fading channel with fading coefficient H_{e}, fading gain $\mathsf{G}_{\mathrm{e}} \triangleq |\mathsf{H}_{\mathrm{e}}|^2$, and additive white Gaussian noise N_{e}. In a continuous-time model, the time interval during which the fading coefficients remain almost constant is called a *coherence interval*; with a slight abuse of terminology, we call a realization $(h_{\mathrm{m}}, h_{\mathrm{e}})$ of the fading coefficients a coherence interval as well.

The relationships between inputs and outputs for each channel use i are given by

$$\mathsf{Y}_i = \mathsf{H}_{\mathrm{m},i}\mathsf{X}_i + \mathsf{N}_{\mathrm{m},i} \quad \text{and} \quad \mathsf{Z}_i = \mathsf{H}_{\mathrm{e},i}\mathsf{X}_i + \mathsf{N}_{\mathrm{e},i},$$

where $\mathsf{H}_{\mathrm{m},i}$, $\mathsf{N}_{\mathrm{m},i}$, $\mathsf{H}_{\mathrm{e},i}$, and $\mathsf{N}_{\mathrm{e},i}$ are mutually independent. The input of the channel is also subject to the power constraint

$$\frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\left[\mathsf{X}_i^2\right] \leqslant P.$$

The noise processes $\left\{\mathsf{N}_{\mathrm{m},i}\right\}_{i\geqslant 1}$ and $\left\{\mathsf{N}_{\mathrm{e},i}\right\}_{i\geqslant 1}$ are i.i.d. complex Gaussian with

$$\mathsf{N}_{\mathrm{m},i} \sim \mathcal{CN}(0, \sigma_{\mathrm{m}}^2) \quad \text{and} \quad \mathsf{N}_{\mathrm{e},i} \sim \mathcal{CN}(0, \sigma_{\mathrm{e}}^2).$$

Different types of fading can be modeled by choosing the statistics of the fading coefficients $\left\{\mathsf{H}_{\mathrm{m},i}\right\}_{i\geqslant 1}$ and $\left\{\mathsf{H}_{\mathrm{e},i}\right\}_{i\geqslant 1}$ appropriately. In the remainder of the section, we focus on three standard fading models.

- **Ergodic-fading model:** this model characterizes a situation in which the duration of a coherence interval is on the order of the time required to send a single symbol. The processes $\left\{\mathsf{H}_{\mathrm{m},i}\right\}_{i\geqslant 1}$ and $\left\{\mathsf{H}_{\mathrm{e},i}\right\}_{i\geqslant 1}$ are mutually independent and i.i.d.; fading coefficients change at every channel use and a codeword experiences many fading realizations.
- **Block-fading model:** in this model, a codeword experiences many fading realizations; however, the time required to send a single symbol is much smaller than the duration of a coherence interval. The processes $\left\{\mathsf{H}_{\mathrm{m},i}\right\}_{i\geqslant 1}$ and $\left\{\mathsf{H}_{\mathrm{e},i}\right\}_{i\geqslant 1}$ are again mutually independent and i.i.d., but change every N channel uses; N is assumed to be sufficiently large for asymptotic coding results to hold within each coherence interval.
- **Quasi-static fading model:** this model differs fundamentally from the previous ones in that fading coefficients are assumed to remain *constant* over the transmission of an entire codeword, but change independently and randomly from one codeword to another. The processes $\left\{\mathsf{H}_{\mathrm{m},i}\right\}_{i\geqslant 1}$ and $\left\{\mathsf{H}_{\mathrm{e},i}\right\}_{i\geqslant 1}$ are mutually independent and i.i.d., characterizing a situation in which fading variations are on the order of the time required to send an entire codeword.

Remark 5.6. *We assume that the fading processes $\{\mathsf{H}_{\mathrm{m},i}\}_{i\geqslant 1}$ and $\{\mathsf{H}_{\mathrm{e},i}\}_{i\geqslant 1}$ are mutually independent and i.i.d to simplify the analysis; however, all results described thereafter generalize to the situation in which the processes are correlated, stationary, and ergodic.*

For all three models, we illustrate the results numerically by considering the special case of i.i.d. *Rayleigh fading*, for which $\{\mathsf{H}_{\mathrm{m},i}\}_{i\geqslant 1}$ and $\{\mathsf{H}_{\mathrm{e},i}\}_{i\geqslant 1}$ are mutually independent i.i.d. complex Gaussian processes with

$$\mathsf{H}_{\mathrm{m},i} \sim \mathcal{CN}(0,\alpha_{\mathrm{m}}^2) \quad \text{and} \quad \mathsf{H}_{\mathrm{e},i} \sim \mathcal{CN}(0,\alpha_{\mathrm{e}}^2).$$

In this case, the fading gains $\mathsf{G}_{\mathrm{m},i} \triangleq |\mathsf{H}_{\mathrm{m},i}|^2$ and $\mathsf{G}_{\mathrm{e},i} = |\mathsf{H}_{\mathrm{e},i}|^2$ are exponentially distributed with respective means

$$\mu_{\mathrm{m}} \triangleq \mathbb{E}[\mathsf{G}_{\mathrm{m},i}] = \alpha_{\mathrm{m}}^2 \quad \text{and} \quad \mu_{\mathrm{e}} \triangleq \mathbb{E}[\mathsf{G}_{\mathrm{e},i}] = \alpha_{\mathrm{e}}^2.$$

The statistics of the noise $\mathsf{N}_{\mathrm{m},i}$ and $\mathsf{N}_{\mathrm{e},i}$ are assumed known to Alice, Bob, and Eve, prior to transmission. Bob has at least instantaneous access to the fading coefficient $h_{\mathrm{m},i}$ and is able to detect symbols *coherently*. In addition, Eve has instantaneous access to both of the fading coefficients $h_{\mathrm{m},i}$ and $h_{\mathrm{e},i}$ so that the information leakage is always implicitly defined as

$$\mathbf{L}(\mathcal{C}_n) \triangleq \frac{1}{n}\mathbb{I}\left(\mathsf{M};\mathsf{Z}^n|\mathsf{H}_{\mathrm{m}}^n\mathsf{H}_{\mathrm{e}}^n\mathcal{C}_n\right),$$

where $\mathsf{H}_{\mathrm{m}}^n$ and $\mathsf{H}_{\mathrm{e}}^n$ are the sequences of fading coefficients for the main and eavesdropper channel and $\mathcal{C}_n$ is the code used by Alice. Although providing the channel state information of the main channel to the eavesdropper is a pessimistic assumption, this assumption is required in the proofs. We will see that whether or not Alice has instantaneous access to the coefficients $h_{\mathrm{m},i}$ and $h_{\mathrm{e},i}$ has a significant impact on achievable communication rates, and several situations are considered in the next sections.

5.2.1 Ergodic-fading channels

For ergodic-fading channels, the processes $\{\mathsf{H}_{\mathrm{m},i}\}_{i\geqslant 1}$ and $\{\mathsf{H}_{\mathrm{e},i}\}_{i\geqslant 1}$ are mutually independent and i.i.d. We first assume that Alice, Bob, and Eve have full *channel state information* (CSI); that is, they all have access *instantaneously* to the realizations of the fading coefficients $(h_{\mathrm{m},i}, h_{\mathrm{e},i})$. In addition, a symbol sequence X^n is allowed to experience (infinitely) many fading realizations as the blocklength n goes to infinity; the average power constraint $(1/n)\sum_{i=1}^n \mathbb{E}[\mathsf{X}_i^2] \leqslant P$ is understood as a *long-term* constraint so that the power can be adjusted depending on the current fading realization.

Theorem 5.3 (Liang *et al.*). *With full CSI, the secrecy capacity of an ergodic fading wireless channel is*

$$C_{\mathrm{s}} = \max_{\gamma} \mathbb{E}_{\mathsf{G}_{\mathrm{m}}\mathsf{G}_{\mathrm{e}}}\left[\log\left(1+\frac{\gamma(\mathsf{G}_{\mathrm{m}},\mathsf{G}_{\mathrm{e}})\mathsf{G}_{\mathrm{m}}}{\sigma_{\mathrm{m}}^2}\right) - \log\left(1+\frac{\gamma(\mathsf{G}_{\mathrm{m}},\mathsf{G}_{\mathrm{e}})\mathsf{G}_{\mathrm{e}}}{\sigma_{\mathrm{e}}^2}\right)\right],$$

where $\gamma : \mathbb{R}_+^2 \to \mathbb{R}_+$ *is subject to the constraint* $\mathbb{E}[\gamma(\mathsf{G}_{\mathrm{m}},\mathsf{G}_{\mathrm{e}})] \leqslant P$.

Proof. The key idea for the achievability part of the proof is that knowledge of the CSI allows Alice, Bob, and Eve to demultiplex the ergodic-fading WTC into a set of *parallel and time-invariant* Gaussian WTCs. Specifically, this transformation can be done as follows. We partition the range of $\mathrm{G_m}$ into k intervals $[g_{\mathrm{m},i}, g_{\mathrm{m},i+1})$ with $i \in [\![1, k]\!]$. Similarly, we partition the range of fading gains $\mathrm{G_e}$ into k intervals $[g_{\mathrm{e},j}, g_{\mathrm{e},j+1})$ with $j \in [\![1, k]\!]$. For simplicity, we first assume that the fading gains are bounded (that is, $g_{\mathrm{m},k+1} < \infty$ and $g_{\mathrm{e},k+1} < \infty$) and let

$$p_i \triangleq \mathbb{P}\left[\mathrm{G_m} \in [g_{\mathrm{m},i}, g_{\mathrm{m},i+1})\right] \quad \text{and} \quad q_j \triangleq \mathbb{P}\left[\mathrm{G_e} \in [g_{\mathrm{e},j}, g_{\mathrm{e},j+1})\right].$$

For each pair of indices (i, j), Alice and Bob publicly agree on a transmit power γ_{ij} and on a wiretap code $\mathcal{C}_n^{ij}$ of length n designed to operate on a Gaussian WTC with main channel gain $g_{\mathrm{m},i}$ and eavesdropper's channel gain $g_{\mathrm{e},j+1}$. The set of transmit powers $\{\gamma_{ij}\}_{k,k}$ is also chosen such that $\sum_{i=1}^{k}\sum_{j=1}^{k} p_i q_j \gamma_{ij} \leqslant P$. If we define

$$C_{ij} \triangleq \left(\log\left(1 + \frac{g_{\mathrm{m},i}\gamma_{ij}}{\sigma_{\mathrm{m}}^2}\right) - \log\left(1 + \frac{g_{\mathrm{e},j+1}\gamma_{ij}}{\sigma_{\mathrm{e}}^2}\right)\right)^+,$$

then, for any $\epsilon > 0$, Corollary 5.1 ensures the existence of a $(2^{nR_{ij}}, n)$ code $\mathcal{C}_n^{ij}$ such that

$$R_{ij} \geqslant C_{ij} - \epsilon, \quad \frac{1}{n}\mathbf{L}(\mathcal{C}_n^{ij}) \leqslant \delta(\epsilon), \quad \text{and} \quad \mathbf{P}_{\mathrm{e}}(\mathcal{C}_n^{ij}) \leqslant \delta(\epsilon).$$

Note that a Gaussian channel with gain $g_{\mathrm{m},i}$ is stochastically degraded with respect to any Gaussian channel with gain $g \in \left[g_{\mathrm{m},i}, g_{\mathrm{m},i+1}\right)$; therefore $\mathcal{C}_n^{ij}$ also guarantees that $\mathbf{P}_{\mathrm{e}}(\mathcal{C}_n^{ij}) \leqslant \delta(\epsilon)$ for a main channel gain $g \in \left[g_{\mathrm{m},i}, g_{\mathrm{m},i+1}\right)$. Similarly, a Gaussian channel with gain $g \in \left[g_{\mathrm{e},j}, g_{\mathrm{e},j+1}\right)$ is stochastically degraded with respect to a Gaussian channel with gain $g_{\mathrm{e},j+1}$; therefore, by Proposition 3.3, $\mathcal{C}_n^{ij}$ guarantees that $\mathbf{L}(\mathcal{C}_n^{ij}) \leqslant \delta(\epsilon)$ for an eavesdropper's channel gain $g \in \left[g_{\mathrm{e},j}, g_{\mathrm{e},j+1}\right)$.

Since all fading coefficients are available to the transmitter and receivers, the ergodic-fading WTC can be demultiplexed into k^2 independent, time-invariant, Gaussian WTCs. The set of codes $\{\mathcal{C}_n^{ij}\}_{k,k}$ for the demultiplexed channels can be viewed as a single code $\mathcal{C}_n$ for the ergodic-fading channel, whose rate R_{s} is the sum of secure rates R_{ij} achieved over each channel weighted by the probability $p_i q_j$ that the code $\mathcal{C}_n^{ij}$ is used. Therefore,

$$\begin{aligned} R_{\mathrm{s}} &= \sum_{i=1}^{k}\sum_{j=1}^{k} p_i q_j R_{ij} \\ &\geqslant \sum_{i=1}^{k}\sum_{j=1}^{k} p_i q_j \left(\log\left(1 + \frac{g_{\mathrm{m},i}\gamma_{ij}}{\sigma_{\mathrm{m}}^2}\right) - \log\left(1 + \frac{g_{\mathrm{e},j+1}\gamma_{ij}}{\sigma_{\mathrm{e}}^2}\right)\right)^+ - \epsilon \end{aligned}$$

subject to the power constraint

$$\sum_{i=1}^{k}\sum_{j=1}^{k} p_i q_j \gamma_{ij} \leqslant P.$$

Additionally,

$$\frac{1}{n}\mathbf{L}(\mathcal{C}_n) = \sum_{i=1}^{k}\sum_{j=1}^{k} p_i q_j \frac{1}{n}\mathbf{L}(\mathcal{C}_n^{ij}) \leqslant \delta(\epsilon)$$

and

$$\mathbf{P}_{\mathrm{e}}(\mathcal{C}_n) = \sum_{i=1}^{k}\sum_{j=1}^{k} p_i q_j \mathbf{P}_{\mathrm{e}}(\mathcal{C}_n^{ij}) \leqslant \delta(\epsilon).$$

Note that k can be chosen arbitrarily large and ϵ can be chosen arbitrarily small. Hence, the ergodicity of the channel ensures that all rates R_{s} such that

$$R_{\mathrm{s}} < \mathbb{E}_{\mathrm{G_m G_e}}\left[\left(\log\left(1+\frac{\mathrm{G_m}\gamma(\mathrm{G_m},\mathrm{G_e})}{\sigma_{\mathrm{m}}^2}\right) - \log\left(1+\frac{\mathrm{G_e}\gamma(\mathrm{G_m},\mathrm{G_e})}{\sigma_{\mathrm{e}}^2}\right)\right)^+\right], \quad (5.22)$$

with $\gamma : \mathbb{R}^2 \rightarrow \mathbb{R}^+$ a power-allocation function such that $\mathbb{E}[\gamma(\mathrm{G_m},\mathrm{G_e})] \leqslant P$, are achievable full secrecy rates. One can further increase the upper bound in (5.22) by optimizing over the power allocations γ such that $\mathbb{E}[\gamma(\mathrm{G_m},\mathrm{G_e})] \leqslant P$. Note that the maximization over γ also allows us to drop the operator $(\cdot)^+$, which yields the expression in Theorem 5.3.

If the range of fading gain is unbounded, we define an arbitrary but finite threshold $g_{\max}$ beyond which Alice and Bob do not communicate. The multiplexing scheme developed above applies directly for fading gains below $g_{\max}$; however, there is a rate penalty because $\mathbb{P}[\mathrm{G_m} > g_{\max} \text{ or } \mathrm{G_e} > g_{\max}] > 0$ and Alice and Bob do not communicate for a fraction of fading realizations. Nevertheless, the penalty can be made as small as desired by choosing $g_{\max}$ large enough.

We omit the converse part of the proof of the theorem, which can be obtained from a converse argument for parallel Gaussian WTCs. The ideas behind the proof are similar to those used in Section 3.5.3, with the necessary modifications to account for parallel channels. We refer the interested reader to [85] for more details. □

The power allocation γ which maximizes C_{s} in Theorem 5.3 can be characterized exactly.

Proposition 5.5. *The power allocation $\gamma^* : \mathbb{R}_+^2 \rightarrow \mathbb{R}_+$ that achieves C_{s} in Theorem 5.3 is defined as follows:*

- *if $u > 0$ and $v = 0$, then*

$$\gamma^*(u,v) = \left(\frac{1}{\lambda} - \frac{1}{u}\right)^+;$$

- *if*

$$\frac{u}{\sigma_{\mathrm{m}}^2} > \frac{v}{\sigma_{\mathrm{e}}^2} > 0,$$

then

$$\gamma^*(u,v) = \frac{1}{2}\left(-\left(\frac{\sigma_\text{m}^2}{u}+\frac{\sigma_\text{e}^2}{v}\right)+\sqrt{\left(\frac{\sigma_\text{e}^2}{v}-\frac{\sigma_\text{m}^2}{u}\right)\left(\frac{4}{\lambda}+\frac{\sigma_\text{m}^2}{u}-\frac{\sigma_\text{e}^2}{v}\right)}\right)^+;$$

- $\gamma^*(u,v)=0$ *otherwise;*

with $\lambda > 0$ *such that* $\mathbb{E}[\gamma^*(\text{G}_\text{m},\text{G}_\text{e})] = P$.

Proof. For simplicity, we assume that the fading realizations take a finite number of values and we accept the fact that the proof extends to an infinite number of values. For any $(u,v)\in\mathbb{R}_+^2$, we define the function

$$f_{uv}:\gamma\mapsto\log\left(1+\frac{u\gamma}{\sigma_\text{m}^2}\right)-\log\left(1+\frac{v\gamma}{\sigma_\text{e}^2}\right).$$

If $u/\sigma_\text{m}^2 < v/\sigma_\text{e}^2$, the function f_{uv} takes negative values; hence, without loss of optimality, we can set

$$\gamma^*(u,v)=0 \quad \text{if} \quad \frac{u}{\sigma_\text{m}^2}<\frac{v}{\sigma_\text{e}^2}.$$

If $u/\sigma_\text{m}^2 \geqslant v/\sigma_\text{e}^2$, the function f_{uv} is concave in γ; consequently, the secrecy capacity, which is a weighted sum of functions f_{uv}, is concave, as well. Therefore, the optimal power allocation γ^* can be obtained by forming the Lagrangian

$$\begin{aligned}\mathcal{L} \triangleq &\sum_u\sum_v \log\left(1+\frac{\gamma(u,v)u}{\sigma_\text{m}^2}\right)p_{\text{G}_\text{m}}(u)p_{\text{G}_\text{e}}(v)\\ &-\sum_u\sum_v \log\left(1+\frac{\gamma(u,v)v}{\sigma_\text{e}^2}\right)p_{\text{G}_\text{m}}(u)p_{\text{G}_\text{e}}(v)\\ &-\lambda\sum_u\sum_v \gamma(u,v)p_{\text{G}_\text{m}}(u)p_{\text{G}_\text{e}}(v),\end{aligned}$$

and finding $\gamma(u,v)\geqslant 0$ maximizing $\mathcal{L}$ for each (u,v) such that $u/\sigma_\text{m}^2\geqslant v/\sigma_\text{e}^2$.

- If $v=0$ and $u>0$, the derivative of $\mathcal{L}$ with respect to $\gamma(u,v)$ is

  $$\frac{\partial\mathcal{L}}{\partial\gamma(u,v)}=\frac{u}{\sigma_\text{m}^2+\gamma(u,v)u}p_{\text{G}_\text{m}}(u)p_{\text{G}_\text{e}}(v)-\lambda p_{\text{G}_\text{m}}(u)p_{\text{G}_\text{e}}(v).$$

  Therefore,

  $$\frac{\partial\mathcal{L}}{\partial\gamma(u,v)}=0\Leftrightarrow\gamma(u,v)=\frac{1}{\lambda}-\frac{\sigma_\text{m}^2}{u}.$$

- If $u/\sigma_\text{m}^2 > v/\sigma_\text{e}^2 > 0$, we obtain

  $$\begin{aligned}\frac{\partial\mathcal{L}}{\partial\gamma(u,v)}=&\frac{\sigma_\text{e}^2u-\sigma_\text{m}^2v}{(\sigma_\text{m}^2+\gamma(u,v)u)(\sigma_\text{e}^2+\gamma(u,v)v)}p_{\text{G}_\text{m}}(u)\,p_{\text{G}_\text{e}}(v)\\ &-\lambda p_{\text{G}_\text{m}}(u)p_{\text{G}_\text{e}}(v).\end{aligned}$$

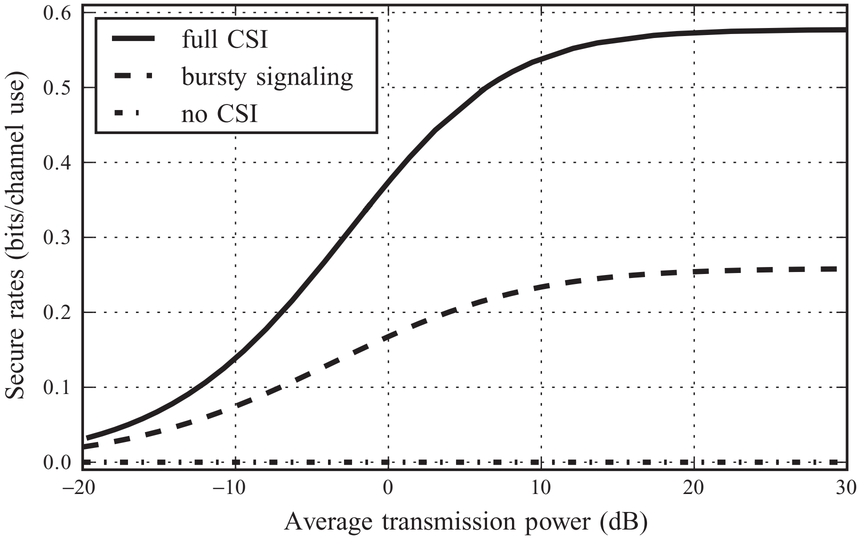

Figure 5.6 Secure communication rates over the Rayleigh fading channel for $\mu_{\mathrm{m}} = 1$, $\mu_{\mathrm{e}} = 2$, and $\sigma_{\mathrm{m}}^2 = \sigma_{\mathrm{e}}^2 = 1$, and for different knowledge of the CSI. The bursty signaling strategy is based only on knowledge of the CSI for the main channel.

Therefore,

$$\frac{\partial \mathcal{L}}{\partial \gamma(u,v)} = 0 \Leftrightarrow \frac{\sigma_{\mathrm{e}}^2 u - \sigma_{\mathrm{m}}^2 v}{(\sigma_{\mathrm{m}}^2 + \gamma(u,v)u)(\sigma_{\mathrm{e}}^2 + \gamma(u,v)v)} - \lambda = 0,$$

and, consequently,

$$\gamma(u,v) = \frac{1}{2}\left(-\left(\frac{\sigma_{\mathrm{m}}^2}{u} + \frac{\sigma_{\mathrm{e}}^2}{v}\right) + \sqrt{\left(\frac{\sigma_{\mathrm{e}}^2}{v} - \frac{\sigma_{\mathrm{m}}^2}{u}\right)\left(\frac{4}{\lambda} + \frac{\sigma_{\mathrm{e}}^2}{v} - \frac{\sigma_{\mathrm{m}}^2}{u}\right)}\right)^{+}. \qquad \square$$

Note that the optimal power-allocation strategy for the secrecy capacity with full CSI depends on the fading statistics only through the parameter λ. In addition, the fact that $\gamma^*(g_{\mathrm{m}}, g_{\mathrm{e}}) = 0$ if $g_{\mathrm{m}}/\sigma_{\mathrm{m}}^2 \leqslant g_{\mathrm{e}}/\sigma_{\mathrm{e}}^2$ is consistent with the intuition that no power should be allocated when the eavesdropper obtains a better instantaneous SNR than does the legitimate receiver.

Theorem 5.3 is illustrated in the case of Rayleigh fading in Figure 5.6. Even in this case, there is no closed-form expression for the secrecy capacity; nevertheless, since $\gamma^*(g_{\mathrm{m}}, g_{\mathrm{e}}) \to \infty$ as $P \to \infty$ for all $(g_{\mathrm{m}}, g_{\mathrm{e}})$ such that $g_{\mathrm{m}}/\sigma_{\mathrm{m}}^2 > g_{\mathrm{e}}/\sigma_{\mathrm{e}}^2$, we can approximate C_{s} in the limit of high power as follows. If $\mathbb{P}\left[\mathsf{G}_{\mathrm{m}}/\sigma_{\mathrm{m}}^2 > \mathsf{G}_{\mathrm{e}}/\sigma_{\mathrm{e}}^2\right] > 0$, then

$$\lim_{P\to\infty} C_{\mathrm{s}}(P) = \mathbb{E}_{\mathsf{G}_{\mathrm{m}}/\sigma_{\mathrm{m}}^2 > \mathsf{G}_{\mathrm{e}}/\sigma_{\mathrm{e}}^2}\left[\log\left(\frac{\sigma_{\mathrm{e}}^2}{\sigma_{\mathrm{m}}^2}\frac{\mathsf{G}_{\mathrm{m}}}{\mathsf{G}_{\mathrm{e}}}\right)\right] = \log\left(1 + \frac{\sigma_{\mathrm{e}}^2}{\sigma_{\mathrm{m}}^2}\frac{\mu_{\mathrm{m}}}{\mu_{\mathrm{e}}}\right),$$

which depends only on the ratio of the average SNR at the receiver $\mu_{\mathrm{m}} P/\sigma_{\mathrm{m}}^2$ and that at the eavesdropper $\mu_{\mathrm{e}} P/\sigma_{\mathrm{e}}^2$. Notice that, as P goes to infinity, $C_{\mathrm{s}}(P)$ is strictly positive even if, on average, the eavesdropper has a better channel than does the legitimate receiver. A

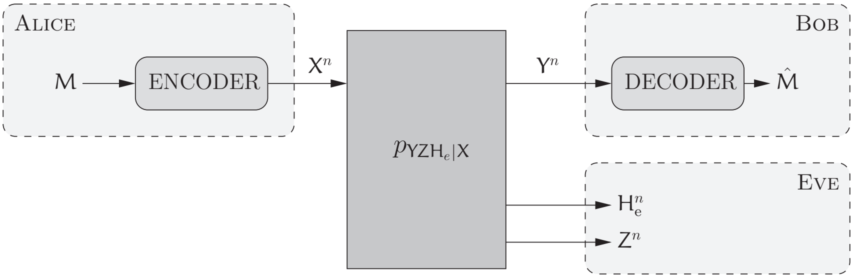

Figure 5.7 Equivalent channel model without eavesdropper's channel state information at the transmitter and legitimate receiver.

closer look at the formula for the secrecy capacity with full CSI given in Theorem 5.3 shows that the secrecy capacity is strictly positive for *any* transmit power and channel statistics, provided that $\mathbb{P}\left[\mathrm{G_m}/\sigma_{\mathrm{m}}^2 > \mathrm{G_e}/\sigma_{\mathrm{e}}^2\right] > 0$. This result contrasts sharply with the Gaussian WTC, for which secure communication is impossible if the eavesdropper has a better channel. Hence, the *fading affecting wireless channels is beneficial for security*. Nevertheless, our result relies on the demultiplexing of the ergodic-fading WTC, which requires the fading coefficients of both channels to be known at the transmitter. The optimal power allocation derived in Proposition 5.5 requires Alice to allocate *opportunistically* more power during the coherence intervals $(h_{\mathrm{m}}, h_{\mathrm{e}})$ for which Eve has a lower SNR than does Bob.

For more realistic applications, it is desirable to relax the full CSI assumption and, in particular, to evaluate secure communication rates *without* knowledge of the eavesdropper's fading coefficient h_{e} at the transmitter.

Proposition 5.6. *With CSI for the main channel but without CSI for the eavesdropper's channel, all rates R_{s} such that*

$$R_{\mathrm{s}} < \max_{\gamma} \mathbb{E}_{\mathrm{G_m G_e}}\left[\log\left(1+\frac{\gamma(\mathrm{G_m})\mathrm{G_m}}{\sigma_{\mathrm{m}}^2}\right) - \log\left(1+\frac{\gamma(\mathrm{G_m})\mathrm{G_e}}{\sigma_{\mathrm{e}}^2}\right)\right],$$

where $\gamma : \mathbb{R}_+ \to \mathbb{R}_+$ is subject to the constraint $\mathbb{E}[\gamma(\mathrm{G_m})] \leqslant P$, are achievable full secrecy rates.

Proof. The demultiplexing scheme used to prove Theorem 5.3 cannot be used directly because the transmitter and legitimate receiver do not know the eavesdropper's CSI. Nevertheless, it is still possible to demultiplex the channel based on the main channel CSI, and one can include the fading coefficients affecting the eavesdropper's channel in the channel statistics. As illustrated in Figure 5.7, the eavesdropper's knowledge of her channel coefficients can be taken into account by treating $\mathrm{H_e}$ as a second output for the eavesdropper's channel. The range of $\mathrm{G_m}$ is partitioned into k intervals $[g_{\mathrm{m},i}, g_{\mathrm{m},i+1})$ with $i \in [\![1, k]\!]$. For simplicity, we assume again that the fading gain is bounded ($g_{\mathrm{m},k+1} < \infty$) and let

$$p_i \triangleq \mathbb{P}\left[\mathrm{G_m} \in [g_{\mathrm{m},i}, g_{\mathrm{m},i+1})\right].$$

For each index $i \in [\![1, k]\!]$, Alice and Bob publicly agree on a transmit power γ_i and on a wiretap code $\mathcal{C}_n^i$ designed to operate on a WTC with transition probabilities $p^{(i)}_{\mathsf{YZH_e|X}}$, such that the marginal $p^{(i)}_{\mathsf{Y|X}}$ corresponds to a Gaussian channel with known constant channel gain $g_{\mathrm{m},i}$ while $p^{(i)}_{\mathsf{ZH_e|X}}$ corresponds to a fading eavesdropper channel with i.i.d. fading coefficient $\mathsf{H_e}$ treated as a second output for the eavesdropper. Since the fading coefficient $\mathsf{H_e}$ is independent of the input, note that

$$\forall (x, z, h_\mathrm{e}) \quad p^{(i)}_{\mathsf{ZH_e|X}}(z, h_\mathrm{e}|x) \triangleq p_{\mathsf{Z|H_eX}}(z|h_\mathrm{e}, x)\, p_{\mathsf{H_e}}(h_\mathrm{e}).$$

The set of transmit powers $\{\gamma_i\}_k$ is also chosen such that $\sum_{i=1}^k p_i\gamma_i \leqslant P$. We can apply Theorem 3.4 to this channel and, for any $\epsilon > 0$ and input distribution p_X, this shows the existence of a wiretap code $\mathcal{C}_n^i$ of length n with rate

$$R_i \geqslant \mathbb{I}(\mathsf{X};\mathsf{Y}) - \mathbb{I}(\mathsf{X};\mathsf{ZH_e}) - \epsilon,$$

such that $(1/n)\mathbf{L}(\mathcal{C}_n^i) \leqslant \delta(\epsilon)$ and $\mathbf{P}_\mathrm{e}(\mathcal{C}_n^i) \leqslant \delta(\epsilon)$. In particular, for the specific choice $\mathsf{X} \sim \mathcal{CN}(0, \gamma_i)$, we obtain

$$\mathbb{I}(\mathsf{X};\mathsf{Y}) = \log\left(1 + \frac{g_{\mathrm{m},i}\gamma_i}{\sigma_\mathrm{m}^2}\right)$$

and

$$\mathbb{I}(\mathsf{X};\mathsf{ZH_e}) = \mathbb{I}(\mathsf{X};\mathsf{H_e}) + \mathbb{I}(\mathsf{X};\mathsf{Z|H_e}) = \mathbb{E}_{\mathsf{G_e}}\left[\log\left(1 + \frac{\mathsf{G_e}\gamma_i}{\sigma_\mathrm{e}^2}\right)\right],$$

where we have used $\mathbb{I}(\mathsf{X};\mathsf{H_e}) = 0$ since $\mathsf{H_e}$ is independent of the channel input X by assumption. Therefore,

$$R_i \geqslant \log\left(1 + \frac{g_{\mathrm{m},i}\gamma_i}{\sigma_\mathrm{m}^2}\right) - \mathbb{E}_{\mathsf{G_e}}\left[\log\left(1 + \frac{\mathsf{G_e}\gamma_i}{\sigma_\mathrm{e}^2}\right)\right] - \epsilon.$$

Because the fading coefficient $\mathsf{H_m}$ is known by the transmitter and receivers, this ergodic-fading WTC can be demultiplexed into k WTCs with time-invariant Gaussian main channel and fading eavesdropper's channel as in Figure 5.7. The set of codes $\{\mathcal{C}_n^i\}_k$ for the demultiplexed channels can be viewed as a single code $\mathcal{C}_n$ for the ergodic-fading channel, whose rate is

$$\begin{aligned} R_\mathrm{s} &= \sum_{i=1}^k p_i R_i \\ &= \sum_{i=1}^k p_i \left(\log\left(1 + \frac{g_{\mathrm{m},i}\gamma_i}{\sigma_\mathrm{m}^2}\right) - \mathbb{E}_{\mathsf{G_e}}\left[\log\left(1 + \frac{\mathsf{G_e}\gamma_i}{\sigma_\mathrm{e}^2}\right)\right]\right) - \epsilon, \end{aligned}$$

and subject to the constraint

$$\sum_{i=1}^k p_i\gamma_i \leqslant P.$$

In addition,

$$\frac{1}{n}\mathbf{L}(\mathcal{C}_n) = \sum_{i=1}^{k} p_i \frac{1}{n}\mathbf{L}(\mathcal{C}_n^i) \leqslant \delta(\epsilon)$$

and

$$\mathbf{P}_{\mathrm{e}}(\mathcal{C}_n) = \sum_{i=1}^{k} p_i \mathbf{P}_{\mathrm{e}}(\mathcal{C}_n^i) \leqslant \delta(\epsilon).$$

Note that k can be chosen arbitrarily large and ϵ can be chosen arbitrarily small. Hence, the ergodicity of the channel guarantees that all rates R_{s} such that

$$R_{\mathrm{s}} < \mathbb{E}_{\mathrm{G_m G_e}}\left[\log\left(1+\frac{\mathrm{G_m}\gamma(\mathrm{G_m})}{\sigma_{\mathrm{e}}^2}\right) - \log\left(1+\frac{\mathrm{G_e}\gamma(\mathrm{G_m})}{\sigma_{\mathrm{e}}^2}\right)\right] \tag{5.23}$$

with $\mathbb{E}[\gamma(\mathrm{G_m}, \mathrm{G_e})] \leqslant P$ are achievable full secrecy rates. Finally, we can improve the upper bound in (5.23) by optimizing over all power allocations γ satisfying the constraint $\mathbb{E}_{\mathrm{G_m}}[\gamma(\mathrm{G_m})] \leqslant P$. □

Although the achievable rates in Theorem 5.3 and Proposition 5.6 differ only in the arguments of the power-allocation function γ, this similarity is misleading because the underlying codes are fundamentally different. In Theorem 5.3, all parties have access to full CSI about the channels, and the code is composed of independent wiretap codes for Gaussian WTCs that are multiplexed to adapt to the time-varying fading gains. However, in Proposition 5.6, the code is composed of independent wiretap codes that are interleaved to adapt to the main channel fading gain only and whose codewords spread over many different realizations of the eavesdropper's channel gain.

The optimal power allocation $\gamma : \mathbb{R}_+ \to \mathbb{R}_+$ for Proposition 5.6 cannot be derived exactly because the objective function

$$f_u : \gamma \mapsto \log\left(1+\frac{\gamma u}{\sigma_{\mathrm{m}}^2}\right) - \mathbb{E}\left[\log\left(1+\frac{\gamma \mathrm{G_e}}{\sigma_{\mathrm{e}}^2}\right)\right]$$

is not concave in γ. A Lagrangian maximization as in Proposition 5.5 would allow us to compute achievable full secrecy rates, but, in general, γ does not admit a closed-form expression. Instead, we consider a simple *bursty signaling*[4] strategy, in which the transmitter selects a threshold $\tau > 0$ and allocates power as

$$\gamma(u) = \begin{cases} P_\tau \triangleq P/\mathbb{P}[\mathrm{G_m} > \tau] & \text{if} \quad u > \tau, \\ 0 & \text{otherwise.} \end{cases}$$

For Rayleigh fading, we can compute the bound in Theorem 5.6 in closed form in terms of the exponential-integral function

$$\mathrm{E}_1 : x \to \int_x^\infty \frac{e^{-y}}{y}\,\mathrm{d}y.$$

[4] Bursty signaling is also called "on–off" power control.

Evaluating (5.23) explicitly for bursty signaling over a wireless channel with i.i.d. Rayleigh fading shows that all secure rates R_s such that

$$R_\text{s} < \exp\left(-\frac{\tau}{\mu_\text{m}}\right)\log\left(1+\frac{\tau P_\tau}{\sigma_\text{m}^2}\right)+\exp\left(\frac{\sigma_\text{m}^2}{\mu_\text{m}P_\tau}\right)\text{E}_1\left(\frac{\sigma_\text{m}^2}{\mu_\text{m}P_\tau}+\frac{\tau}{\mu_\text{m}}\right)\log(e)$$
$$-\exp\left(\frac{\sigma_\text{e}^2}{\mu_\text{e}P_\tau}-\frac{\tau}{\mu_\text{m}}\right)\text{E}_1\left(\frac{\sigma_\text{e}^2}{\mu_\text{e}P_\tau}\right)\log(e).$$

are achievable. As illustrated in Figure 5.6, the lack of knowledge about the eavesdropper's channel has a detrimental effect on secure communication rates.

If assumptions are further relaxed, and no CSI is available at the transmitter, then power cannot be allocated to avoid harmful situations in which the eavesdropper has a higher SNR than that of the legitimate receiver. In particular, if $\mathbb{E}[\mathsf{G}_\text{e}]/\sigma_\text{e}^2 \geqslant \mathbb{E}[\mathsf{G}_\text{m}]/\sigma_\text{m}^2$ and the eavesdropper obtains a better average SNR than does the legitimate receiver, the secrecy capacity without any CSI is zero.

5.2.2 Block-fading channels

It is important to realize that the conclusions drawn regarding the effect of CSI depend on the fading statistics considered; different fading models lead to slightly different conclusions. In this section, we consider a *block-fading* model, for which the coherence interval is sufficiently long that coding can also be performed *within* the interval. Specifically, the processes $\left\{\mathsf{H}_{\text{m},i}\right\}_{i\geqslant 1}$ and $\left\{\mathsf{H}_{\text{e},i}\right\}_{i\geqslant 1}$ are i.i.d., but for each realization $(h_{\text{m},i}, h_{\text{e},i})$ the relationships between channel inputs and outputs are

$$\begin{cases}\mathsf{Y}_{i,j} = h_{\text{m},i}\mathsf{X}_{i,j} + \mathsf{N}_{\text{m},i,j},\\ \mathsf{Z}_{i,j} = h_{\text{e},i}\mathsf{X}_{i,j} + \mathsf{N}_{\text{e},i,j},\end{cases} \quad \text{for} \quad j \in [\![1, N]\!],$$

where N is assumed to be sufficiently large for asymptotic coding results to hold. If the transmitter and receivers have CSI about all channels, then the demultiplexing and power-allocation scheme used for the ergodic-fading WTC can be used, and the secrecy capacity is given again by Theorem 5.3 with the optimal power allocation of Proposition 5.5. The situation is quite different without knowledge about the eavesdropper's fading at the transmitter. In fact, for the ergodic-fading model considered in Section 5.2.1, the transmitter is allowed a single channel use per coherence interval; consequently, the information leaked to the eavesdropper can be arbitrarily large. In contrast, for the block-fading model, the transmitter can *code* within each coherence interval and the information leaked to the eavesdropper *cannot exceed* the information communicated to the legitimate receiver. Specifically, we let X^N represent a coded sequence chosen at random in the transmitter's codebook and sent during one coherence interval, and we let Z^N denote the corresponding eavesdropper's observation. Then, it holds that

$$\mathbb{I}\left(\mathsf{X}^N;\mathsf{Z}^N\right) \leqslant \mathbb{H}\left(\mathsf{X}^N\right) < \infty,$$

because X^N takes a *finite* number of values.

Theorem 5.4 (Gopala *et al.*). *The secrecy capacity of a block-fading WTC with CSI about the main channel but no CSI about the eavesdropper's channel is*

$$C_s = \max_{\gamma} \mathbb{E}_{G_m G_e}\left[\left(\log\left(1+\frac{\gamma(G_m)G_m}{\sigma_m^2}\right) - \log\left(1+\frac{\gamma(G_m)G_e}{\sigma_e^2}\right)\right)^+\right],$$

subject to the constraint $\mathbb{E}[\gamma(G_m)] \leqslant P$.

Proof. We provide only the achievability part of the proof, and refer the reader to [86] for details regarding the converse. The key ideas behind the code construction are to code within each coherence interval in order to bound the information leaked to the eavesdropper and to spread the codewords over many realizations of the eavesdropper's fading gain. The proof is greatly simplified by noting that the block-fading channel can be treated as an ergodic-fading channel with a *vector* input X^N and *vector* outputs Y^N and Z^N such that

$$Y^N = H_m X^N + N_m^N \quad \text{and} \quad Z^N = H_e X^N + N_e^N.$$

Therefore, we can use the same approach as in the proof of Proposition 5.6.

The range of G_m is partitioned into k intervals $[g_{m,i}, g_{m,i+1})$ with $i \in [\![1,k]\!]$. We assume the fading gain to be bounded ($g_{m,k+1} < \infty$), and we let

$$p_i \triangleq \mathbb{P}\left[G_m \in [g_{m,i}, g_{m,i+1})\right].$$

For each index $i \in [\![1,k]\!]$, Alice and Bob publicly agree on a transmit power γ_i and on a wiretap code $\mathcal{C}_n^i$ of length n designed to operate on a *vector* WTC with transition probabilities $p^{(i)}_{Y^N Z^N H_e|X^N}$. Note that the marginal $p^{(i)}_{Y^N|X^N}$ is such that

$$\forall (y^N, x^N) \quad p^{(i)}_{Y^N|X^N}(y^N|x^N) = \prod_{i=1}^{N} p_{Y|X}(y_i|x_i),$$

where $p^{(i)}_{Y|X}$ corresponds to a Gaussian channel with known constant fading coefficient $h_{m,i}$. Similarly, the marginal $p^{(i)}_{Z^N H_e|X^N}$ is such that

$$\forall (z^N, h_e, x^N) \quad p^{(i)}_{Z^N H_e|X^N}(z^N, h_e|x^N) = \left(\prod_{i=1}^{N} p_{Z|H_e X}(z_i, |h_e, x_i)\right) p_{H_e}(h_e),$$

where $p_{Z|H_e X}$ corresponds to a fading eavesdropper channel with fading coefficient H_e available to the eavesdropper. The set of transmit powers is also chosen such that $\sum_{i=1}^k p_i \gamma_i \leqslant P$. By Theorem 3.4, for any $\epsilon > 0$ and input distribution p_{X^N}, there exists a wiretap code $\mathcal{C}_n^i$ of length n with rate

$$R_i \geqslant \mathbb{I}(X^N; Y^N) - \mathbb{I}(X^N; Z^N H_e) - \epsilon, \tag{5.24}$$

measured in bits per *vector* channel use and such that $(1/n)\mathbf{L}(\mathcal{C}_n^i) \leqslant \delta(\epsilon)$ and $\mathbf{P}_e(\mathcal{C}_n^i) \leqslant \delta(\epsilon)$. We are free to optimize the distribution of X^N as long as the power constraint $\sum_{j=1}^N \mathbb{E}\left[X_j^2\right] \leqslant \gamma_i$ is satisfied; in particular, we can choose X^N to represent the codewords chosen uniformly at random in a codebook such that

$$\log\left(1+\frac{g_{\mathrm{m},i}\gamma_i}{\sigma_{\mathrm{m}}^2}\right)-\epsilon \leqslant \mathbb{H}\left(\mathsf{X}^N\right) \leqslant \log\left(1+\frac{g_{\mathrm{m},i}\gamma_i}{\sigma_{\mathrm{m}}^2}\right),$$

and whose probability of error over a Gaussian channel with gain $g_{\mathrm{m},i}$ is at most $\delta(\epsilon)$. The existence of this code is ensured directly by the channel coding theorem if N is large enough. Since X^N represents a codeword in a codebook, it follows from Fano's inequality that

$$\mathbb{H}\left(\mathsf{X}^N|\mathsf{Y}^N\right) \leqslant N\delta(\epsilon).$$

Therefore,

$$\mathbb{I}\left(\mathsf{X}^N;\mathsf{Y}^N\right) = \mathbb{H}\left(\mathsf{X}^N\right) - \mathbb{H}\left(\mathsf{X}^N|\mathsf{Y}^N\right) \geqslant N\log\left(1+\frac{g_{\mathrm{m},i}\gamma_i}{\sigma_{\mathrm{m}}^2}\right) - N\delta(\epsilon). \qquad (5.25)$$

Note that $\mathbb{I}\left(\mathsf{X}^N;\mathsf{H}_\mathrm{e}\right)=0$ because the fading coefficient H_e is independent of the input and that the channel is memoryless; therefore,

$$\begin{aligned}\mathbb{I}\left(\mathsf{X}^N;\mathsf{Z}^N\mathsf{H}_\mathrm{e}\right) &= \mathbb{I}\left(\mathsf{X}^N;\mathsf{Z}^N|\mathsf{H}_\mathrm{e}\right)\\ &= \mathbb{E}_{\mathsf{H}_\mathrm{e}}\left[\mathbb{I}\left(\mathsf{X}^N;\mathsf{Z}^N|\mathsf{H}_\mathrm{e}\right)\right]\\ &\leqslant N\mathbb{E}_{\mathsf{G}_\mathrm{e}}\left[\log\left(1+\frac{\gamma_i\mathsf{G}_\mathrm{e}}{\sigma_\mathrm{e}^2}\right)\right]. \qquad (5.26)\end{aligned}$$

Finally, note that the following trivial upper bound holds:

$$\forall h_\mathrm{e}\quad \mathbb{I}\left(\mathsf{X}^N;\mathsf{Z}^N|\mathsf{H}_\mathrm{e}=h_\mathrm{e}\right) \leqslant \mathbb{H}\left(\mathsf{X}^N\right) \leqslant N\log\left(1+\frac{g_{\mathrm{m},i}\gamma_i}{\sigma_{\mathrm{m}}^2}\right). \qquad (5.27)$$

On combining (5.25), (5.26), and (5.27) in (5.24) we obtain

$$R_i \geqslant N\mathbb{E}_{\mathsf{G}_\mathrm{e}}\left[\left(\log\left(1+\frac{g_{\mathrm{m},i}\gamma_i}{\sigma_{\mathrm{m}}^2}\right)-\log\left(1+\frac{\gamma_i\mathsf{G}_\mathrm{e}}{\sigma_\mathrm{e}^2}\right)\right)^+\right]-N\delta(\epsilon).$$

Since the fading coefficient H_m is known by the transmitter and receivers, the channel can be demultiplexed into k vector input WTCs. The set of codes $\{\mathcal{C}_n^i\}_k$ for the demultiplexed vector channels can be viewed as a single code $\mathcal{C}_n$ for the block-ergodic fading channel, whose rate in bits per channel use is

$$\begin{aligned}R_\mathrm{s} &= \frac{1}{N}\sum_{i=1}^k p_i R_i\\ &\geqslant \sum_{i=1}^k p_i\mathbb{E}_{\mathsf{G}_\mathrm{e}}\left[\left(\log\left(1+\frac{g_{\mathrm{m},i}\gamma_i}{\sigma_{\mathrm{m}}^2}\right)-\log\left(1+\frac{\gamma_i\mathsf{G}_\mathrm{e}}{\sigma_\mathrm{e}^2}\right)\right)^+\right]-\delta(\epsilon),\end{aligned}$$

and subject to the constraint $\sum_{i=1}^k p_i\gamma_i \leqslant P$. In addition,

$$\frac{1}{nN}\mathbf{L}(\mathcal{C}_n) = \frac{1}{N}\sum_{i=1}^k p_i\frac{1}{n}\mathbf{L}(\mathcal{C}_n^i) \leqslant \delta(\epsilon)$$

and

$$\mathbf{P}_{\mathrm{e}}(\mathcal{C}_n) = \sum_{i=1}^{k} p_i \mathbf{P}_{\mathrm{e}}(\mathcal{C}_n^i) \leqslant \delta(\epsilon).$$

Note that k can be chosen arbitrarily large and ϵ can be chosen arbitrarily small. Hence, the ergodicity of the channel guarantees that all rates R_{s}, such that

$$R_{\mathrm{s}} < \mathbb{E}_{\mathrm{G_m G_e}}\left[\left(\log\left(1 + \frac{\mathrm{G_m}\gamma(\mathrm{G_m})}{\sigma_{\mathrm{m}}^2}\right) - \log\left(1 + \frac{\mathrm{G_e}\gamma(\mathrm{G_m})}{\sigma_{\mathrm{e}}^2}\right)\right)^+\right],$$

with $\mathbb{E}_{\mathrm{G_m}}[\gamma(\mathrm{G_m}] \leqslant P$, are achievable full secrecy rates (in bits per channel use). □

Theorem 5.4 differs from Corollary 5.6 only by the presence of the operator $(\cdot)^+$ in the expectation, which appears because the information leaked to the eavesdropper within each coherence interval is bounded. The formula for the secrecy capacity highlights again that fading is beneficial for security and, in contrast to ergodic fading, the lack of knowledge about the eavesdropper's CSI at the transmitter seems to incur a lesser penalty for block-ergodic fading. For Rayleigh fading, the upper bound in Theorem 5.4 can be computed in closed form for the bursty signaling strategy defined in Section 5.2.1. Bursty signaling over wireless channels with i.i.d. Rayleigh fading can achieve all rates R_{s} such that

$$\begin{aligned} R_{\mathrm{s}} < {} & \exp\left(-\frac{\tau}{\mu_{\mathrm{m}}}\right)\log\left(1 + \frac{\tau P_\tau}{\sigma_{\mathrm{m}}^2}\right) + \exp\left(\frac{\sigma_{\mathrm{m}}^2}{\mu_{\mathrm{m}} P_\tau}\right)\mathrm{E}_1\left(\frac{\tau}{\mu_{\mathrm{m}}} + \frac{\sigma_{\mathrm{m}}^2}{\mu_{\mathrm{m}} P_\tau}\right)\log(e) \\ & + \exp\left(\frac{\sigma_{\mathrm{e}}^2}{\mu_{\mathrm{e}} P_\tau} - \frac{\tau}{\mu_{\mathrm{m}}}\right)\left(\mathrm{E}_1\left(\frac{\sigma_{\mathrm{e}}^2 \tau}{\mu_{\mathrm{e}} \sigma_{\mathrm{m}}^2} + \frac{\sigma_{\mathrm{e}}^2}{\mu_{\mathrm{e}} P_\tau}\right) - \mathrm{E}_1\left(\frac{\sigma_{\mathrm{e}}^2}{\mu_{\mathrm{e}} P_\tau}\right)\right)\log(e) \\ & - \exp\left(\frac{\sigma_{\mathrm{e}}^2}{\mu_{\mathrm{e}} P_\tau} - \frac{\sigma_{\mathrm{m}}^2}{\mu_{\mathrm{m}} P_\tau}\right)\mathrm{E}_1\left(\left(\frac{1}{\mu_{\mathrm{m}}} + \frac{\sigma_{\mathrm{e}}^2}{\mu_{\mathrm{e}} \sigma_{\mathrm{m}}^2}\right)\left(\tau + \frac{\sigma_{\mathrm{m}}^2}{P_\tau}\right)\right)\log(e). \end{aligned} \quad (5.28)$$

Interestingly, if P goes to infinity and τ goes to zero, (5.28) becomes

$$R_{\mathrm{s}} < \log\left(1 + \frac{\sigma_{\mathrm{e}}^2}{\sigma_{\mathrm{m}}^2}\frac{\mu_{\mathrm{m}}}{\mu_{\mathrm{e}}}\right).$$

Note that the right-hand side is the secrecy capacity with full CSI as P goes to infinity. Therefore, for the block-fading model, the bursty signaling strategy approaches the secrecy capacity in the limit of large power. This is illustrated in Figure 5.8, which shows the secrecy capacity of a block-fading model with perfect knowledge of all fading coefficients and the secure rate achievable with the bursty signaling strategy for different values of the power P.

5.2.3 Quasi-static fading channels

In this last section, we consider the situation in which the fading coefficients $\{\mathrm{H}_{\mathrm{m},i}^n\}_{i\geqslant 1}$ and $\{\mathrm{H}_{\mathrm{e},i}^n\}_{i\geqslant 1}$ remain constant over the transmission of an entire codeword and

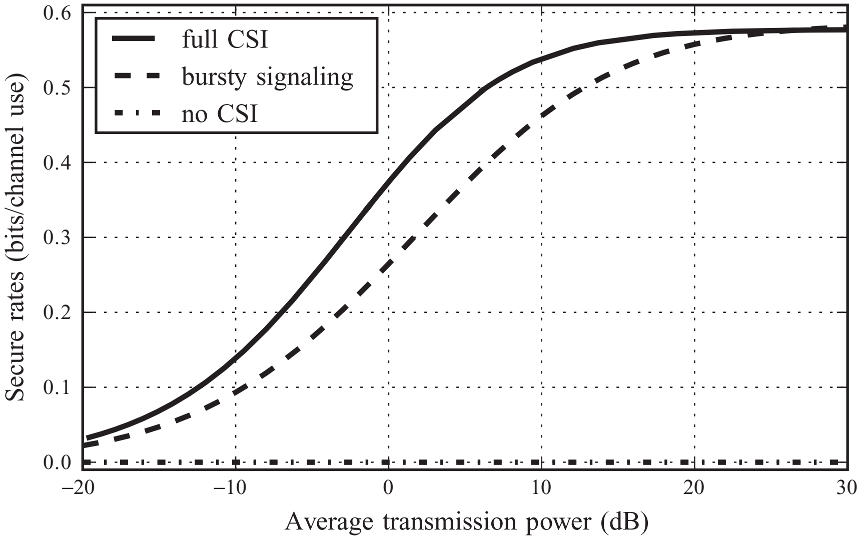

Figure 5.8 Secure communication rates over the Rayleigh block-fading channel with parameters $\mu_\mathrm{m} = 1$, $\mu_\mathrm{e} = 2$, and $\sigma_\mathrm{m}^2 = \sigma_\mathrm{e}^2 = 1$.

change independently at random from one codeword to another. This contrasts with the ergodic-fading and block-fading models, in which every transmitted codeword experiences many fading realizations during transmission. This model is often called a *quasi-static* fading model, and, for each coherence interval characterized by fading realizations $(h_\mathrm{m}, h_\mathrm{e})$, the model reduces to a Gaussian WTC defined by

$$\mathsf{Y}_i = h_\mathrm{m}\mathsf{X}_i + \mathsf{N}_{\mathrm{m},i} \quad \text{and} \quad \mathsf{Z}_i = h_\mathrm{e}\mathsf{X}_i + \mathsf{N}_{\mathrm{e},i}.$$

The input is subject to a power constraint $(1/n)\sum_{i=1}^{n} \mathbb{E}\left[\mathsf{X}_i^2\right] \leqslant P$, which is interpreted as a short-term constraint and must be satisfied within each coherence interval. Again, this contrasts with the long-term power constraint we used for the ergodic-fading and block-fading models, and the short-term constraint of the quasi-static model prevents the transmitter from allocating power opportunistically depending on the fading gain; nevertheless, the transmitter can still adapt its coding rate to the realization of the fading coefficients. While we have seen in previous sections that the possibility of secure communications with ergodic fading is determined by the *average* fading realization, we will see that secure communications over quasi-static channels are determined by the *instantaneous* one.

If the transmitter, the legitimate receiver, and the eavesdropper have perfect knowledge of the instantaneous realizations of the fading coefficients $(h_\mathrm{m}, h_\mathrm{e})$, the wiretap code used for each realization of the fading can be chosen opportunistically. The aggregate secure communications rate achievable over a long period of time is then given by the following theorem.

Theorem 5.5 (Barros and Rodrigues)**.** *With full CSI, the average secrecy capacity of a quasi-static wiretap channel is*

$$C_{\mathrm{s}}^{\mathrm{avg}} = \mathbb{E}_{\mathrm{G_m G_e}}\left[C_{\mathrm{s}}^{\mathrm{inst}}(\mathrm{G_m}, \mathrm{G_e})\right],$$

where $C_{\mathrm{s}}^{\mathrm{inst}}(g_{\mathrm{m}}, g_{\mathrm{e}})$ *is the* instantaneous secrecy capacity*, defined as*

$$C_{\mathrm{s}}^{\mathrm{inst}}(g_{\mathrm{m}}, g_{\mathrm{e}}) \triangleq \left(\log\left(1 + \frac{g_{\mathrm{m}}P}{\sigma_{\mathrm{m}}^2}\right) - \log\left(1 + \frac{g_{\mathrm{e}}P}{\sigma_{\mathrm{e}}^2}\right)\right)^{+}.$$

In the case of i.i.d. Rayleigh fading, $C_{\mathrm{s}}^{\mathrm{avg}}$ can be computed explicitly using the exponential-integral function as

$$\begin{aligned} C_{\mathrm{s}}^{\mathrm{avg}} &= \exp\left(\frac{\sigma_{\mathrm{m}}^2}{\mu_{\mathrm{m}}P}\right)\mathrm{E}_1\left(\frac{\sigma_{\mathrm{m}}^2}{\mu_{\mathrm{m}}P}\right)\log(e) \\ &\quad - \exp\left(\frac{\sigma_{\mathrm{m}}^2}{\mu_{\mathrm{m}}P} + \frac{\sigma_{\mathrm{e}}^2}{\mu_{\mathrm{e}}P}\right)\mathrm{E}_1\left(\frac{\sigma_{\mathrm{m}}^2}{\mu_{\mathrm{m}}P} + \frac{\sigma_{\mathrm{e}}^2}{\mu_{\mathrm{e}}P}\right)\log(e), \end{aligned}$$

and one can check that

$$\lim_{P\to\infty} C_{\mathrm{s}}^{\mathrm{avg}}(P) = \log\left(1 + \frac{\sigma_{\mathrm{e}}^2}{\sigma_{\mathrm{m}}^2}\frac{\mu_{\mathrm{m}}}{\mu_{\mathrm{e}}}\right).$$

If the transmitter knows the fading coefficient h_{m} of the main channel but does not know the fading coefficient h_{e} of the eavesdropper's channel, then the average secrecy capacity for a quasi-static fading model is zero, no matter what the statistics of the channels are. In fact, since a codeword experiences a single realization of the fading gain, the probability of the eavesdropper obtaining a better instantaneous SNR for an entire codeword is always strictly positive, and no coding can guarantee secrecy. Nevertheless, one can still obtain insight into the security of wireless communications by taking a probabilistic view of security.

If we assume that the transmitter knows h_{m}, then the rate of the code used within each coherence interval can be adapted to guarantee reliability; however, without knowledge of h_{e}, the transmitter can use only a wiretap code *targeted* for a predefined secure communication rate R. Whenever the realization g_{e} is such that $R < C_{\mathrm{s}}^{\mathrm{inst}}(g_{\mathrm{m}}, g_{\mathrm{e}})$, it follows from Remark 5.2 that the message is transmitted securely; however, if $R > C_{\mathrm{s}}^{\mathrm{inst}}(g_{\mathrm{m}}, g_{\mathrm{e}})$, then some information is leaked to the eavesdropper. This behavior can be characterized by using the notion of *the outage probability of the secrecy capacity*.

Definition 5.1. *If the transmitter knows the fading coefficient of the main channel, the outage probability of the secrecy capacity is defined as*

$$P_{\mathrm{out}}(R) \triangleq \mathbb{P}_{\mathrm{G_m G_e}}\left[C_{\mathrm{s}}^{\mathrm{inst}}(\mathrm{G_m}, \mathrm{G_e}) < R\right].$$

For Rayleigh fading, $P_{\mathrm{out}}(R)$ takes the closed-form expression

$$P_{\mathrm{out}}(R) = 1 - \frac{\mu_{\mathrm{m}}}{\mu_{\mathrm{m}} + 2^R\mu_{\mathrm{e}}\sigma_{\mathrm{m}}^2/\sigma_{\mathrm{e}}^2}\exp\left(-\sigma_{\mathrm{m}}^2\frac{2^R - 1}{\mu_{\mathrm{m}}P}\right).$$

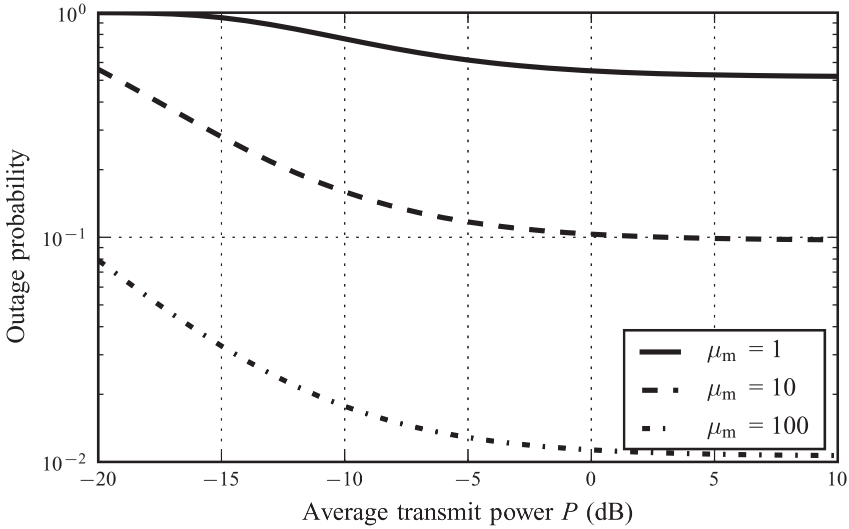

Figure 5.9 Outage probability of the secrecy capacity for various values of μ_{m} ($R = 0.1$, $\mu_{\mathrm{e}} = 1$, $\sigma_{\mathrm{m}}^2 = \sigma_{\mathrm{e}}^2 = 1$).

Figure 5.9 illustrates the behavior of $P_{\text{out}}(R)$ as a function of the transmit power P for various values of the average fading gain μ_{m}. The channel statistics must give Alice and Bob a clear advantage over Eve in order to achieve low values of the outage probability. The relevance of the outage approach is also very much application-dependent, insofar as even leaking information with a low probability might sometimes be unacceptable.

Note that $P_{\text{out}}(R)$ is a decreasing function of P and cannot be reduced by decreasing the transmission power. However, reducing the targeted secure transmission rate R reduces the outage probability, and the minimum outage probability is obtained as R goes to zero, that is

$$P_{\text{out}}(0) = \frac{\mu_{\mathrm{e}}}{\mu_{\mathrm{e}} + \mu_{\mathrm{m}}\sigma_{\mathrm{m}}^2/\sigma_{\mathrm{e}}^2},$$

which is always strictly positive. As expected, no matter what the transmitter does, information is leaked to the eavesdropper. Despite this seemingly disappointing result, it is worth noting that the outage probability is a pessimistic metric, which does not discriminate between events for which $R \gg C_{\mathrm{s}}$ and events for which R exceeds C_{s} by a small amount. In addition, if the fading realizations are independent, outage events are independent of each other as well; as a result, a security leakage at a given time instant does not necessarily hinder security at later times.

Remark 5.7. *If the transmitter does not have any CSI, both reliability and security need to be assessed in terms of outage. The definition of the outage probability can be modified to*

$$P_{\text{out}} \triangleq \mathbb{P}_{\mathrm{G_m G_e}}\left[C_{\mathrm{s}}^{\text{inst}}(\mathrm{G_m}, \mathrm{G_e}) < R, C_{\mathrm{m}}^{\text{inst}}(\mathrm{G_m}) < R\right],$$

where $C_{\mathrm{m}}^{\text{inst}}(g_{\mathrm{m}}) \triangleq \log\left(1 + g_{\mathrm{m}}P/\sigma_{\mathrm{m}}^2\right)$ *is the instantaneous main channel capacity.*

5.3 Conclusions and lessons learned

The secrecy capacity of a Gaussian WTC admits a simple characterization as the difference between the main channel capacity and the eavesdropper's channel capacity. Consequently, secure communication over a Gaussian WTC is possible if and only if the legitimate receiver obtains a higher SNR than does the eavesdropper. This result is somewhat disappointing because it seems to limit the scope of applications. However, as shown by the analysis of Gaussian source models, this limitation can be overcome by considering more powerful communication schemes exploiting feedback, such as secret-key agreement schemes.

Our analysis of the MIMO Gaussian WTC leads to a severe conclusion: little can be done against the collusion of many eavesdroppers. Nevertheless, the MIMO model may be overly pessimistic because it ignores the communication requirements of the eavesdroppers. Most often, the bandwidth of eavesdroppers will be limited, which is likely to mitigate the detrimental impact of a collusion. On a more positive note, our study shows that coding for secrecy is, in general, more powerful than beamforming alone.

Perhaps surprisingly, the fluctuations of received SNR induced by fading in wireless transmissions are beneficial for security. If the instantaneous fading realizations can be accurately estimated by the transmitter, transmit power can be allocated opportunistically to the fading realizations for which the eavesdropper obtains a lower instantaneous SNR than that of the legitimate receiver. As a result, strictly positive secure communication rates are achievable even if, on average, the eavesdropper obtains a better SNR than that of the legitimate receiver. For some fading models, this is possible even if the transmitter does not have access to the eavesdropper's instantaneous fading realization.

5.4 Bibliographical notes

The secrecy capacity of the physically degraded Gaussian wiretap channel was established by Leung-Yan-Cheong and Hellman [87], and its generalization to the Gaussian BCC is due to Liang, Poor, and Shamai [85]. For the Gaussian WTC, an elegant converse proof based on the relation between MMSE and mutual information has been proposed by Bustin, Liu, Poor, and Shamai [88]. The secrecy capacity of the MIMOME channel was characterized by Khisti and Wornell [83, 84], Oggier and Hassibi [89], and Liu and Shamai [90], using different techniques (see also an earlier result of Shafiee, Liu, and Ulukus [91]). Although the general form of the covariance matrix $\mathbf{K}_X$ maximizing C_s^MIMO is not known, the optimal signaling strategies are known in certain regimes. At high SNR, Khisti and Wornell have shown that it is sufficient to transmit in (all) the directions in which the legitimate receiver has a better SNR than that of the eavesdropper. At low SNR, Gursoy has shown that it is sufficient to transmit in the direction of the largest eigenvalue of the matrix $\mathbf{H}_\text{m}^\dagger\mathbf{H}_\text{m} - (\sigma_\text{m}^2/\sigma_\text{e}^2)\mathbf{H}_\text{e}^\dagger\mathbf{H}_\text{e}$ [92]. The benefit of transmitting artificial noise in the null space of the main channel to impair the eavesdropper's observation was first suggested by Negi and Goel [93, 94] and subsequently analyzed by Khisti, Wornell, Wiesel, and Eldar [95].

The beneficial role of fading for secure communications was highlighted by Barros and Rodrigues [96] for the quasi-static fading wireless channel. The secrecy-capacity region of ergodic-fading channels with perfect channel state information (CSI) about all channels was characterized by Liang, Poor, and Shamai [85]. Bursty signaling was shown to mitigate the absence of information about the eavesdropper's fading by Li, Yates, and Trappe [97] for i.i.d. Rayleigh fading. The secrecy capacity of block-fading channels with no information about the eavesdropper's channels was established by Gopala, Lai, and El Gamal [86], and the near optimality of bursty signaling was proved for i.i.d. Rayleigh block-fading in the high-power regime. A closed-form expression for the secrecy capacity of wireless channels with correlated fading in the limit of high power can be found in [98]. The security of frequency-selective channels has been studied by Koyluoglu, El Gamal, Lai, and Poor [99] and Kobayashi, Debbah, and Shamai [100]. Bloch and Laneman investigated the impact of imperfect CSI on achievable secure rates for general WTCs [101] and showed that little CSI is needed to enable secure communication over wireless channels. Studies of secure wireless communications in terms of the outage probability can be found in [96] for quasi-static fading channels and in [85] for ergodic-fading channels. Tang, Liu, Spasojević, and Poor also analyzed the outage probability of secure hybrid-ARQ schemes [102]. A layered broadcast coding approach, which operates both in ergodic and in non-ergodic fading, has been investigated by Tang, Poor, Liu, and Spasojević [103] as well as Liang, Lai, Poor, and Shamai [104].

Although this chapter primarily focused on the problem of secure communication over wireless channels, many results extend to secret-key agreement over wireless channels. Bloch, Barros, Rodrigues, and McLaughlin investigated key-distillation strategies for quasi-static fading channels [105], and Wong, Bloch, and Shea studied the secret-key capacity of MIMO ergodic channels [106]. Wilson, Tse, and Sholtz [107] also performed an extensive analysis of secret sharing using the reciprocity of an ultrawideband channel. All these studies highlight again the beneficial role of fading for secrecy. In addition, since the channel fading coefficients can always be included in the statistics of the source used for key distillation, key-distillation strategies are often less sensitive to the availability of CSI than wiretap codes.

Practical constructions of wiretap codes for Gaussian and wireless communications remain elusive, but Bloch, Barros, Rodrigues, and McLaughlin [105] proposed a pragmatic approach to secure wireless communications that is based on key-agreement techniques over quasi-static fading channels, which was shown to incur little loss of secure rate in certain regimes.