8 Secrecy and jamming in multi-user channels

In all of the previous chapters, we discussed the possibility of secure transmissions at the physical layer for communication models involving only two legitimate parties and a single eavesdropper. These results generalize in part to situations with more complex communication schemes, additional legitimate parties, or additional eavesdroppers. Because of the increased complexity of these "multi-user" channel models, the results one can hope to obtain are, in general, not as precise as the ones obtained in earlier chapters. In particular, it becomes seldom possible to obtain a single-letter characterization of the secrecy capacity and one must often resort to the calculation of upper and lower bounds. Nevertheless, the analysis of multi-user communication channels still provides useful insight into the design of secure communication schemes; in particular it highlights several characteristics of secure communications, most notably the importance of *cooperation*, *feedback*, and *interference*. Although these aspects have been studied extensively in the context of reliable communications and are now reasonably well understood, they do not necessarily affect secure communications in the same way as they affect reliable communications. For instance, while it is well known that cooperation among transmitters is beneficial and improves reliability, the fact that interference is also helpful for secrecy is perhaps counter-intuitive.

There are numerous variations of multi-user channel models with secrecy constraints; rather than enumerating them all, we study the problem of secure communication over a two-way Gaussian wiretap channel. This model exemplifies the specific features of most multi-user secure communication systems and its analysis directly leverages the techniques and results presented in previous chapters. We refer the interested reader to the appendix at the end of this chapter and to the monograph of Liang *et al.* [147] for an extensive list of references on multi-user secure communications.

We start this chapter by introducing the two-way Gaussian wiretap channel (Section 8.1). We then discuss in detail three secure communication strategies: cooperative jamming (Section 8.2), coded cooperative jamming (Section 8.3), and key exchange (Section 8.4).

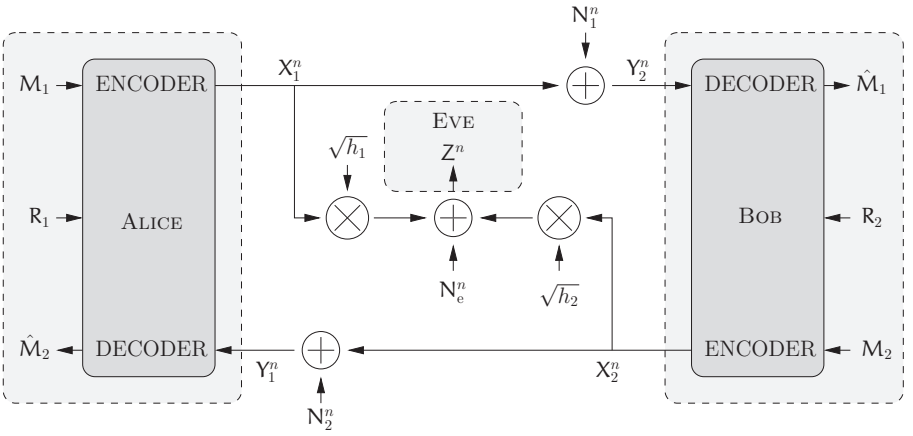

Figure 8.1 Two-way Gaussian wiretap channel with interference at the eavesdropper. M_1 and M_2 represent the messages transmitted by Alice and Bob. R_1 and R_2 represent local randomness used in the encoders.

8.1 Two-way Gaussian wiretap channel

As shown in Corollary 5.1, the secrecy capacity of a Gaussian wiretap channel is given by

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

and the secrecy capacity is zero if $\sigma_{\mathrm{m}}^2 \geqslant \sigma_{\mathrm{e}}^2$, independently of the transmit power P. To improve secure communication rates, one should either increase the signal-to-noise ratio (SNR) of the legitimate receiver or decrease the SNR of the eavesdropper. A natural approach by which to achieve the latter is to introduce interferers into the system. In particular, if the eavesdropper happens to be located closer to the interferers than the legitimate receiver, interferences may have a more detrimental effect on her than on the legitimate receiver, which can result in increased secure communication rates. Notice that this approach implicitly requires knowledge of the locations of all of the transmitters and receivers or some knowledge of all of the instantaneous channel characteristics, so that inteferers do not harm the legitimate receiver unnecessarily. In practice, this knowledge would be obtained via some cooperation mechanism between nodes; therefore, this approach was called *cooperative jamming* by Tekin and Yener to highlight the importance of interfering intelligently.

The concept of cooperative jamming can be applied in many different settings, and we refer the reader to the bibliographical notes for examples. In this chapter, we restrict our attention to the situation in which Alice or Bob plays the role of the interferer. Specifically, we consider the channel model illustrated in Figure 8.1, in which Alice and Bob communicate in full duplex over orthogonal Gaussian channels while their signals interfere at Eve's terminal. We call this model a *two-way Gaussian wiretap channel* (TWWTC for short). At every time instant i, Alice transmits symbol $X_{1,i}$

while receiving $Y_{1,i}$, Bob transmits $X_{2,i}$ while receiving $Y_{2,i}$, and Eve observes Z_i. The relationships among these symbols are given by

$$\begin{aligned} Y_{2,i} &= X_{1,i} + N_{1,i}, \\ Y_{1,i} &= X_{2,i} + N_{2,i}, \\ Z_i &= \sqrt{h_1} X_{1,i} + \sqrt{h_2} X_{2,i} + N_{e,i}. \end{aligned} \tag{8.1}$$

The processes $\{N_{1,i}\}_{i\geqslant 1}$, $\{N_{2,i}\}_{i\geqslant 1}$, and $\{N_{e,i}\}_{i\geqslant 1}$ are i.i.d. and distributed according to $\mathcal{N}(0,1)$; the real channel gains $h_1 > 0$ and $h_2 > 0$ account for the position of the eavesdropper with respect to Alice and Bob and are assumed known to all parties, including the eavesdropper. The inputs X_1^n and X_2^n to the channel are subject to the average power constraints

$$\frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[X_{1,i}^2\right] \leqslant P_1 \quad \text{and} \quad \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[X_{2,i}^2\right] \leqslant P_2.$$

Remark 8.1. *For the sake of generality, we could introduce gains g_1 and g_2 on the forward and backward channels between Alice and Bob and introduce different noise variances:*

$$\begin{aligned} Y_{2,i} &= \sqrt{g_1} X_{1,i} + N_{1,i}, \\ Y_{1,i} &= \sqrt{g_2} X_{2,i} + N_{2,i}, \\ Z_i &= \sqrt{h_1} X_{1,i} + \sqrt{h_2} X_{2,i} + N_{e,i}, \end{aligned}$$

where $\{N_{1,i}\}_{i\geqslant 1}$, $\{N_{2,i}\}_{i\geqslant 1}$, and $\{N_{e,i}\}_{i\geqslant 1}$ are i.i.d. zero-mean Gaussian noises with variances σ_1^2, σ_2^2, and σ_e^2, respectively. Nevertheless, by scaling the signals as $\tilde{Y}_{1,i} = (1/\sigma_1)Y_{1,i}$, $\tilde{X}_{1,i} = \sqrt{g_1/\sigma_1^2}X_{1,i}$, $\tilde{Y}_{2,i} = (1/\sigma_2)Y_{2,i}$, $\tilde{X}_{2,i} = \sqrt{g_2/\sigma_2^2}X_{2,i}$, and $\tilde{Z}_i = (1/\sigma_e)Z_i$, introducing channel gains $\tilde{h}_1 = h_1\sigma_1^2/(g_1\sigma_e^2)$ and $\tilde{h}_2 = h_2\sigma_2^2/(g_2\sigma_e^2)$, and redefining the power constraints as $\tilde{P}_1 = (g_1/\sigma_1^2)P_1$ and $\tilde{P}_2 = (g_2/\sigma_2^2)P_2$, one can check that we can always revert back to the more tractable model given in (8.1)*.*

The orthogonality of the channels between Alice and Bob implicitly relies on the assumption that any self-interference can be perfectly canceled out, and the form of the interference at the eavesdropper's location is valid provided that all signals are synchronized. Realistically, interfering signals are unlikely to be perfectly synchronized when they reach the eavesdropper; nevertheless, the effect of mis-synchronization can be partly included in the magnitudes of the coefficients h_1 and h_2.

The ability to achieve secure communications over the TWWTC relies once more on the use of stochastic encoders. As was done in Chapter 3 and Chapter 4, it is convenient to explicitly introduce the randomness in the encoder and to assume that Alice has access to the realizations of a DMS $(\mathcal{R}_1, p_{R_1})$ while Bob has access to the realization of a DMS $(\mathcal{R}_2, p_{R_2})$; the DMSs are independent of each other and of the noise in the channel. For clarity in the definitions, we also denote the alphabets in which the symbols X_1, X_2, Y_1, and Y_2 take their values by the letters $\mathcal{X}_1$, $\mathcal{X}_2$, $\mathcal{Y}_1$, and $\mathcal{Y}_2$, respectively. A generic code for the two-way wiretap channel is then defined as follows.

Definition 8.1. *A* $\left(2^{nR_1}, 2^{nR_2}, n,\right)$ *code* $\mathcal{C}_n$ *for the TWWTC consists of*

- *two message sets,* $\mathcal{M}_1 = [\![1, 2^{nR_1}]\!]$ *and* $\mathcal{M}_2 = [\![1, 2^{nR_2}]\!]$*;*
- *two sources of local randomness,* $(\mathcal{R}_1, p_{\mathrm{R}_1})$ *and* $(\mathcal{R}_2, p_{\mathrm{R}_2})$*;*
- *two sequences of encoding functions,* $f_{1,i} : \mathcal{M}_1 \times \mathcal{R}_1 \times \mathcal{Y}_1^{i-1} \to \mathcal{X}_1$ *and* $f_{2,i} : \mathcal{M}_2 \times \mathcal{R}_2 \times \mathcal{Y}_2^{i-1} \to \mathcal{X}_2$ *for* $i \in [\![1, n]\!]$*, which generate symbols based on the message to transmit, local randomness, and previous observations;*
- *two decoding functions,* $g_1 : \mathcal{Y}_1^n \times \mathcal{R}_1 \times \mathcal{M}_1 \to \mathcal{M}_2 \cup \{?\}$ *and* $g_2 : \mathcal{Y}_2^n \times \mathcal{R}_2 \times \mathcal{M}_2 \to \mathcal{M}_1 \cup \{?\}$.

Note that the DMSs $(\mathcal{R}_1, p_{\mathrm{R}_1})$ and $(\mathcal{R}_2, p_{\mathrm{R}_2})$ can be optimized as part of the code design. The $\left(2^{nR_1}, 2^{nR_2}, n,\right)$ code $\mathcal{C}_n$ is assumed known by Alice, Bob, and Eve. We also assume that the messages $\mathrm{M}_1 \in \mathcal{M}_1$ and $\mathrm{M}_2 \in \mathcal{M}_2$ are independent and uniformly distributed in their respective sets. The reliability performance of a $\mathcal{C}_n$ is then measured in terms of the probability of error

$$\mathbf{P}_{\mathrm{e}}(\mathcal{C}_n) \triangleq \mathbb{P}\left[\hat{\mathrm{M}}_2 \neq \mathrm{M}_2 \text{ or } \hat{\mathrm{M}}_1 \neq \mathrm{M}_1 | \mathcal{C}_n\right],$$

while its secrecy performance is measured in terms of the leakage

$$\mathbf{L}(\mathcal{C}_n) \triangleq \mathbb{I}(\mathrm{M}_1\mathrm{M}_2; \mathrm{Z}^n | \mathcal{C}_n h_1 h_2).$$

The conditioning on h_1 and h_2 reflects the fact that the channel gains are known to the eavesdropper; however, we write $\mathbb{I}(\mathrm{M}_1\mathrm{M}_2; \mathrm{Z}^n | \mathcal{C}_n)$ to simplify the notation.

Definition 8.2. *A rate pair* (R_1, R_2) *is achievable for the TWWTC if there exists a sequence of* $\left(2^{nR_1}, 2^{nR_2}, n,\right)$ *codes* $\{\mathcal{C}_n\}_{n \geqslant 1}$ *such that*

$$\lim_{n\to\infty} \mathbf{P}_{\mathrm{e}}(\mathcal{C}_n) = 0 \qquad \textit{(reliability condition)}, \tag{8.2}$$

$$\lim_{n\to\infty} \frac{1}{n}\mathbf{L}(\mathcal{C}_n) = 0 \qquad \textit{(weak secrecy condition)}. \tag{8.3}$$

Note that the secrecy condition requires a vanishing information rate leaked to the eavesdropper for messages M_1 and M_2 *jointly*, which is a stronger requirement than a vanishing information rate for messages M_1 and M_2 individually. In fact, the chain rule of mutual information and the independence of messages M_1 and M_2 guarantee that

$$\begin{aligned}\mathbb{I}(\mathrm{M}_1\mathrm{M}_2; \mathrm{Z}^n | \mathcal{C}_n) &= \mathbb{I}(\mathrm{M}_1; \mathrm{Z}^n | \mathcal{C}_n) + \mathbb{I}(\mathrm{M}_1; \mathrm{Z}^n | \mathrm{M}_2\mathcal{C}_n) \\ &\geqslant \mathbb{I}(\mathrm{M}_1; \mathrm{Z}^n | \mathcal{C}_n) + \mathbb{I}(\mathrm{M}_2; \mathrm{Z}^n | \mathcal{C}_n).\end{aligned}$$

Therefore, messages are protected individually if they are protected jointly, but the converse need not be true.

We are interested in characterizing the entire region of achievable rate pairs (R_1, R_2). Unfortunately, it is rather difficult to obtain an exact characterization because, in principle, the coding schemes in Definition 8.1 can exploit both the interference of transmitted signals at the eavesdropper's terminal and feedback. To obtain some insight, we study instead several simpler strategies that partially *decouple* these two effects;

although these strategies are likely to be suboptimal, their analysis is more amenable and will yield achievable rate regions as a function of the channel parameters h_1 and h_2 and the power constraints P_1 and P_2. Specifically, we investigate the following coding schemes.

- **Cooperative jamming:** one of the legitimate parties sacrifices his entire rate to jam the eavesdropper; this strategy has little effect on the eavesdropper's SNR if the channel gains h_1 and h_2 are small, but jamming with noise can be implemented no matter what the values of h_1 and h_2 are, and does not require synchronization between the legitimate parties.
- **Coded cooperative jamming:** both Alice and Bob transmit coded information over the channel; if $h_1 \approx h_2$, codewords interfere with roughly the same strength at Eve's terminal, which allows Alice and Bob to increase their secure communication while communicating messages; however, if h_1 or h_2 is too large, this strategy is likely to be ineffective because the eavesdropper can probably decode the interfering signals.
- **Key-exchange:** one of the legitimate parties sacrifices part of its secure communication rate to exchange a secret key, which is later used by the other party to encrypt messages with a one-time pad; this is perhaps the simplest strategy that exploits feedback, but the key-distillation strategies described in Chapter 4 could also be adapted for the TWWTC.

As a benchmark for achievable secure communication rates, we consider the region achieved with a coding scheme in which Alice and Bob ignore the interference created at the eavesdropper's terminal and do not exploit the feedback allowed by the two-way nature of the channel. This is a special instance of the generic code in Definition 8.1, for which

- Alice has a single encoding function $f_1 : \mathcal{M}_1 \times \mathcal{R}_1 \to \mathcal{X}_1^n$ and a single decoding function $g_1 : \mathcal{Y}_1^n \to \mathcal{M}_2 \cup \{?\}$;
- Bob has a single encoding function $f_2 : \mathcal{M}_2 \times \mathcal{R}_2 \to \mathcal{X}_2^n$ and a single decoding function $g_2 : \mathcal{Y}_2^n \to \mathcal{M}_1 \cup \{?\}$.

To present all subsequent results concisely, we introduce the function

$$C : \mathbb{R}^+ \to \mathbb{R}^+ : x \mapsto \frac{1}{2}\log(1+x),$$

such that $C(x)$ represents the capacity of a Gaussian channel with received SNR x.

Proposition 8.1. *The rate region $\mathcal{R}_0$ defined by*

$$\mathcal{R}_0 \triangleq \left\{(R_1, R_2): \begin{array}{l} 0 \leqslant R_1 < (C(P_1) - C(h_1 P_1))^+ \\ 0 \leqslant R_2 < (C(P_2) - C(h_2 P_2))^+ \end{array}\right\}$$

is achievable with independently designed wiretap codes that ignore feedback and the presence of interference at the eavesdropper's terminal.

Proof. Fix $\epsilon > 0$. We introduce the random variable $\mathsf{Z}_{1,i} \triangleq \sqrt{h_1}\mathsf{X}_{1,i} + \mathsf{N}_{\mathrm{e},i}$, which represents the observation of an eavesdropper who cancels out Bob's interference $\mathsf{X}_{2,i}$ perfectly, and we choose a rate R_1 that satisfies

$$0 \leqslant R_1 < (C(P_1) - C(h_1 P_1))^+. \tag{8.4}$$

By Corollary 5.1, there exists a $(2^{nR_1}, n)$ code $\mathcal{C}_1$ for communication between Alice and Bob such that

$$\mathbb{P}\left[\hat{\mathsf{M}}_1 \neq \mathsf{M}_1 \middle| \mathcal{C}_1\right] \leqslant \epsilon \quad \text{and} \quad \frac{1}{n}\mathbb{I}\big(\mathsf{M}_1; \mathsf{Z}_1^n | \mathcal{C}_1\big) \leqslant \epsilon. \tag{8.5}$$

Similarly, we introduce $\mathsf{Z}_{2,i} \triangleq \sqrt{h_2}\mathsf{X}_{2,i} + \mathsf{N}_{\mathrm{e},i}$, which represents the observation of an eavesdropper who cancels out Alice's interference $\mathsf{X}_{1,i}$ perfectly, and we choose a rate R_2 that satisfies

$$0 \leqslant R_2 < (C(P_2) - C(h_2 P_2))^+ . \tag{8.6}$$

Again, Corollary 5.1 ensures the existence of a $(2^{nR_2}, n)$ code $\mathcal{C}_2$ for communication between Bob and Alice such that

$$\mathbb{P}\left[\hat{\mathsf{M}}_2 \neq \mathsf{M}_2 \middle| \mathcal{C}_2\right] \leqslant \epsilon \quad \text{and} \quad \frac{1}{n}\mathbb{I}\big(\mathsf{M}_2; \mathsf{Z}_2^n | \mathcal{C}_2\big) \leqslant \epsilon. \tag{8.7}$$

The pair of codes $(\mathcal{C}_1, \mathcal{C}_2)$ defines a special instance of a $(2^{nR_1}, 2^{nR_2}, n)$ code $\mathcal{C}_n$ for the TWWTC, which we show achieves the rate pair (R_1, R_2) in the sense of Definition 8.2. By the union bound, (8.5), and (8.7), we obtain

$$\begin{aligned}\mathbb{P}\left[\hat{\mathsf{M}}_1 \neq \mathsf{M}_1 \text{ or } \hat{\mathsf{M}}_2 \neq \mathsf{M}_2 \middle| \mathcal{C}_1\mathcal{C}_2\right] &\leqslant \mathbb{P}\left[\hat{\mathsf{M}}_1 \neq \mathsf{M}_1 \middle| \mathcal{C}_1\right] + \mathbb{P}\left[\hat{\mathsf{M}}_2 \neq \mathsf{M}_2 \middle| \mathcal{C}_2\right] \\ &\leqslant \delta(\epsilon).\end{aligned}$$

In addition, the information rate leaked to the eavesdropper about messages M_1 and M_2 can be bounded as

$$\begin{aligned}\frac{1}{n}\mathbb{I}(\mathsf{M}_1\mathsf{M}_2; \mathsf{Z}^n | \mathcal{C}_1\mathcal{C}_2) &= \frac{1}{n}\mathbb{I}(\mathsf{M}_1; \mathsf{Z}^n | \mathcal{C}_1\mathcal{C}_2) + \frac{1}{n}\mathbb{I}(\mathsf{M}_2; \mathsf{Z}^n | \mathsf{M}_1\mathcal{C}_1\mathcal{C}_2) \\ &\leqslant \frac{1}{n}\mathbb{I}\big(\mathsf{M}_1; \mathsf{Z}^n\mathsf{X}_2^n | \mathcal{C}_1\mathcal{C}_2\big) + \frac{1}{n}\mathbb{I}\big(\mathsf{M}_2; \mathsf{Z}^n\mathsf{X}_1^n | \mathsf{M}_1\mathcal{C}_1\mathcal{C}_2\big) \\ &= \frac{1}{n}\mathbb{I}\big(\mathsf{M}_1; \mathsf{Z}_1^n\mathsf{X}_2^n | \mathcal{C}_1\mathcal{C}_2\big) + \frac{1}{n}\mathbb{I}\big(\mathsf{M}_2; \mathsf{Z}_2^n\mathsf{X}_1^n | \mathsf{M}_1\mathcal{C}_1\mathcal{C}_2\big),\end{aligned}$$

where the last equality follows because of the one-to-one mapping between $(\mathsf{Z}_1^n, \mathsf{X}_2^n)$ and $(\mathsf{Z}^n, \mathsf{X}_2^n)$ and the one-to-one mapping between $(\mathsf{Z}_2^n, \mathsf{X}_1^n)$ and $(\mathsf{Z}^n, \mathsf{X}_1^n)$. Since X_2^n is independent of M_1 and Z_1^n by construction, notice that

$$\frac{1}{n}\mathbb{I}\big(\mathsf{M}_1; \mathsf{Z}_1^n\mathsf{X}_2^n | \mathcal{C}_1\mathcal{C}_2\big) = \frac{1}{n}\mathbb{I}\big(\mathsf{M}_1; \mathsf{Z}_1^n | \mathcal{C}_1\big).$$

Similarly, since M_1 and X_1^n are independent of M_2 and Z_2^n by construction,

$$\frac{1}{n}\mathbb{I}\big(\mathsf{M}_2; \mathsf{Z}_2^n\mathsf{X}_1^n | \mathsf{M}_1\mathcal{C}_1\mathcal{C}_2\big) = \frac{1}{n}\mathbb{I}\big(\mathsf{M}_2; \mathsf{Z}_2^n | \mathcal{C}_2\big).$$

Therefore, by (8.5) and (8.7),

$$\frac{1}{n}\mathbb{I}(\mathsf{M}_1\mathsf{M}_2; Z^n|\mathcal{C}_1\mathcal{C}_2) \leqslant \frac{1}{n}\mathbb{I}\big(\mathsf{M}_1; Z_1^n|\mathcal{C}_1\big) + \frac{1}{n}\mathbb{I}\big(\mathsf{M}_2; Z_2^n|\mathcal{C}_2\big) \leqslant \delta(\epsilon).$$

Since $\epsilon > 0$ is arbitrary, all the rate pairs (R_1, R_2) satisfying (8.4) and (8.6) are achievable over the TWWTC. □

Note that $\mathcal{R}_0$ has a square shape, but the region collapses to a segment as soon as $h_1 \geqslant 1$ or $h_2 \geqslant 1$; that is, as soon as the eavesdropper obtains a better SNR than either that of Alice or that of Bob.

8.2 Cooperative jamming

As a first attempt to increase secure communication rates, we analyze a communication strategy in which Alice and Bob take turns jamming Eve to reduce her SNR. Formally, we call *cooperative jamming code* (cooperative jamming for short) an instance of the generic code in Definition 8.1 such that

- there is only one party (say Alice) that transmits a message without relying on feedback; in other words, we consider a *single* encoding function $f_1 : \mathcal{M}_1 \times \mathcal{R}_1 \to \mathcal{X}_1^n$ and a *single* decoding function $g_2 : \mathcal{R}_2 \times \mathcal{Y}_2^n \to \mathcal{M}_1 \cup \{?\}$;
- the other party (Bob) transmits a jamming signal, which could depend on past channel observations; in other words, we consider a sequence of jamming functions $f_{2,i} : \mathcal{R}_2 \times \mathcal{Y}_2^{i-1} \to \mathcal{X}_2$ for $i \in [\![1, n]\!]$.

The probability of error of such a code reduces to $\mathbb{P}\left[\hat{\mathsf{M}}_1 \neq \mathsf{M}_1|\mathcal{C}_n\right]$. Notice that restricting codes to cooperative jamming is tantamount to considering the simplified channel model illustrated in Figure 8.2, which we refer to as the *cooperative jamming channel model*. Although a cooperative code does not exploit feedback, we emphasize that it is not a trivial code because the jamming signals are allowed to depend on past observation and can be quite sophisticated. Finally, note that the roles of Alice and Bob can be reversed, with Bob transmitting messages while Alice is jamming.

Proposition 8.2 (Tekin and Yener)**.** *The region* $\mathcal{R}_{\mathrm{cj}}$ *defined as*

$$\mathcal{R}_{\mathrm{cj}} \triangleq \bigcup_{\alpha\in[0,1]} \left\{ (R_1, R_2): \begin{array}{l} 0 \leqslant R_1 < \alpha\left(C(P_1) - C\left(\dfrac{h_1 P_1}{1 + h_2 P_2}\right)\right)^+ \\ 0 \leqslant R_2 < (1-\alpha)\left(C(P_2) - C\left(\dfrac{h_2 P_2}{1 + h_1 P_1}\right)\right)^+ \end{array} \right\}$$

is achievable with cooperative jamming codes.

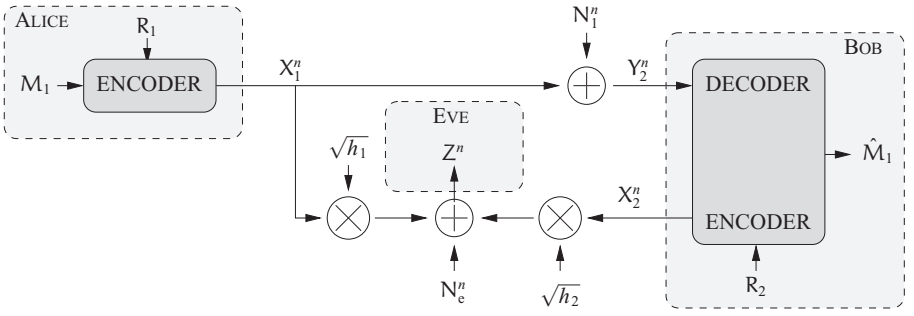

Figure 8.2 Cooperative jamming channel model. Bob helps Alice by jamming the eavesdropper and reducing its SNR.

Proof. Assume that Bob uses his entire power to jam Eve with i.i.d. Gaussian noise with variance[1] P_2. Effectively, this strategy transforms the two-way Gaussian wiretap channel into a one-way Gaussian wiretap channel from Alice to Bob characterized by the input–output relationships

$$\mathsf{Y}_{2,i} = \mathsf{X}_{1,i} + \mathsf{N}_{1,i},$$
$$\mathsf{Z}_i = \mathsf{X}_{1,i} + \mathsf{N}'_{\mathrm{e},i},$$

where $\mathsf{N}'_{\mathrm{e},i}$ is a zero-mean Gaussian random variable with variance $1 + h_2 P_2$. By Corollary 5.1, the secrecy capacity of this wiretap channel is

$$C_1 = \left(C(P_1) - C\left(\frac{h_1 P_1}{1 + h_2 P_2} \right) \right)^+.$$

Therefore, all rate pairs (R_1, R_2) with $R_2 = 0$ and $R_1 < C_1$ are achievable.

Similarly, if Alice uses her power to jam Eve with i.i.d. Gaussian noise with variance P_1, Bob effectively communicates with Alice over a Gaussian wiretap channel with secrecy capacity

$$C_2 = \left(C(P_2) - C\left(\frac{h_2 P_2}{1 + h_1 P_1} \right) \right)^+.$$

Therefore, all rate pairs (R_1, R_2) with $R_1 = 0$ and $R_2 < C_2$ are achievable.

The full region is obtained by time-sharing between these two modes of operation: during a fraction α of the time, Alice transmits with power P_1 while Bob jams with power P_2 and, during the remaining fraction $(1 - \alpha)$ of the time, Alice jams with power P_1 while Bob communicates with power P_2. □

Alice's and Bob's maximum secure communication rates in Proposition 8.2 are always higher than those obtained with the benchmark strategy; however, the jamming terminal ignores the symbols it receives and one can wonder whether adapting the jamming to

[1] Strictly speaking, transmitting i.i.d. Gaussian noise with power P_2 may violate the power constraint; nevertheless, if the variance is set to $P_2 - \epsilon$ for some arbitrary $\epsilon > 0$, then the probability of violating the constraints can be made arbitrarily small for n large enough and the results remain virtually unchanged.

past observations could yield higher secure communication rates. In an idealized case, if Bob had access to the signal X_1^n sent by Alice, he could tremendously reduce the eavesdropper's SNR by performing correlated jamming and partially canceling out X_1^n. In our setting, Bob only has causal and imperfect knowledge of X_1^n, but he might still be able to exploit the structure of the codewords. Perhaps surprisingly, it turns out that jamming Gaussian noise seems close to optimal. We establish this result precisely by deriving an upper bound on the secure communication rates achievable by Alice when Bob performs cooperative jamming.

Proposition 8.3 (Bloch)**.** *The secure rates achieved by Alice with Bob performing cooperative jamming must satisfy*

$$R_1 \leqslant \max \min(\mathbb{I}(\mathsf{X}_1;\mathsf{Y}_2), \mathbb{I}(\mathsf{X}_1;\mathsf{Y}_2|\mathsf{Z}\mathsf{X}_2) + \mathbb{I}(\mathsf{X}_2;\mathsf{Z}|\mathsf{X}_1)),$$

where the maximization is over random variables $\mathsf{X}_1, \mathsf{X}_2, \mathsf{Y}_2$, *and* Z *with joint distribution* $p_{\mathsf{X}_1\mathsf{X}_2\mathsf{Y}_2\mathsf{Z}}$ *such that*

$$\forall (x_1, x_2, y_2, z) \in \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{Y}_2 \times \mathcal{Z}$$
$$p_{\mathsf{X}_1\mathsf{X}_2\mathsf{Y}_2\mathsf{Z}}(x_1, x_2, y_2, z) = p_{\mathsf{Y}_2\mathsf{Z}|\mathsf{X}_1\mathsf{X}_2}(y_2, z|x_1, x_2) p_{\mathsf{X}_1\mathsf{X}_2}(x_1, x_2)$$

and such that $\mathbb{E}\left[\mathsf{X}_1^2\right] \leqslant P_1$, $\mathbb{E}\left[\mathsf{X}_2^2\right] \leqslant P_2$.

Proof. Let R_1 be an achievable rate with cooperative jamming, and let $\epsilon > 0$. For n sufficiently large, there exists a $(2^{nR_1}, n)$ code $\mathcal{C}_n$ such that $\mathbf{P}_{\mathrm{e}}(\mathcal{C}_n) \leqslant \delta(\epsilon)$. In the following, we omit the condition on $\mathcal{C}_n$ to simplify the notation. Fano's inequality also ensures that $(1/n)\mathbb{H}\left(\mathsf{M}_1|\mathsf{Y}_2^n\right) \leqslant \delta(\epsilon)$; therefore,

$$\begin{aligned} R_1 &\leqslant \frac{1}{n}\mathbb{H}(\mathsf{M}_1) \\ &\leqslant \frac{1}{n}\mathbb{H}(\mathsf{M}_1) - \frac{1}{n}\mathbb{H}\left(\mathsf{M}_1|\mathsf{Y}_2^n\right) + \delta(\epsilon) \\ &= \frac{1}{n}\mathbb{I}\left(\mathsf{M}_1;\mathsf{Y}_2^n\right) + \delta(\epsilon) \\ &\leqslant \frac{1}{n}\mathbb{I}\left(\mathsf{X}_1^n;\mathsf{Y}_2^n\right) + \delta(\epsilon) \\ &\leqslant \frac{1}{n}\sum_{j=1}^{n}\mathbb{I}\left(\mathsf{X}_{1,j};\mathsf{Y}_{2,j}\right) + \delta(\epsilon). \end{aligned} \tag{8.8}$$

We now develop a second upper bound that depends on the jamming input X_2 and the eavesdropper's observation Z. We do so by computing an upper bound for the secret-key capacity of the cooperative jamming channel model in Figure 8.2. This approach is motivated by two observations. First, any upper bound for the secret-key capacity is also an upper bound for the secrecy capacity because introducing public discussion cannot reduce achievable secrecy rates. Second, we already know how to obtain a single-letter upper bound for the secret-key capacity of a channel model from Theorem 4.8. The

cooperative jamming channel model is slightly different from the channel model of Chapter 4 because not only Alice but also Bob has an input to the channel. Nevertheless, the proof of Theorem 4.8 can be adapted to account for this additional channel input.

A key-distillation strategy for the cooperative jamming channel model is formally defined as follows.

Definition 8.3. *A $(2^{nR}, n)$ key-distillation strategy $\mathcal{S}_n$ for a cooperative jamming channel model consists of*

- *a key alphabet $\mathcal{K} = [\![1, 2^{nR}]\!]$;*
- *an alphabet $\mathcal{A}$ used by Alice to communicate over the public channel;*
- *an alphabet $\mathcal{B}$ used by Bob to communicate over the public channel;*
- *a source of local randomness for Alice $\left(\mathcal{R}_1, p_{\mathrm{R}_1}\right)$;*
- *a source of local randomness for Bob $\left(\mathcal{R}_2, p_{\mathrm{R}_2}\right)$;*
- *an integer $r \in \mathbb{N}^*$ that represents the number of rounds of communication;*
- *a set of n distinct integers $\{i_j\} \subseteq [\![1, r]\!]$ that represents the rounds in which Alice and Bob transmit symbols over the channel;*
- *$r - n$ encoding functions $f_i : \mathcal{B}^{i-1} \times \mathcal{R}_1 \to \mathcal{A}$ for $i \in [\![1, r]\!] \setminus \{i_j\}_n$;*
- *$r - n$ encoding functions g_i for $i \in [\![1, r]\!] \setminus \{i_j\}_n$ of the form $g_i : \mathcal{Y}_2^j \times \mathcal{A}^{i-1} \times \mathcal{R}_2 \to \mathcal{B}$ if $i \in [\![i_j + 1, i_{j+1} - 1]\!]$;*
- *n functions $h_j : \mathcal{B}^{i_j - 1} \times \mathcal{R}_1 \to \mathcal{X}_1$ for $j \in [\![1, n]\!]$ to generate channel inputs;*
- *n functions $h'_j : \mathcal{A}^{i_j - 1} \times \mathcal{R}_2 \times \mathcal{Y}_2^{j-1} \to \mathcal{X}_2$ for $j \in [\![1, n]\!]$ to generate channel inputs;*
- *a key-distillation function $\kappa_{\mathrm{a}} : \mathcal{X}_1^n \times \mathcal{B}^r \times \mathcal{R}_1 \to \mathcal{K}$;*
- *a key-distillation function $\kappa_{\mathrm{b}} : \mathcal{Y}_2^n \times \mathcal{A}^r \times \mathcal{R}_2 \to \mathcal{K}$;*

and operates as follows:

- *Alice generates a realization r_x of her source of local randomness while Bob generates r_y from his;*
- *in round $i \in [\![1, i_1 - 1]\!]$, Alice transmits message $a_i = f_i\left(b^{i-1}, r_1\right)$ and Bob transmits message $b_i = g_i\left(a^{i-1}, r_2\right)$;*
- *in round i_j with $j \in [\![1, n]\!]$, Alice transmits symbol $x_{1,j} = h_j\left(b^{i_j - 1}, r_1\right)$ and Bob transmits symbol $x_{2,j} = h'_j\left(a^{i_j - 1}, r_2, y_2^{j-1}\right)$ over the channel; Bob and Eve observe the symbols $y_{2,j}$ and z_j, respectively.*
- *in round $i \in [\![i_j + 1, i_{j+1} - 1]\!]$, Alice transmits message $a_i = f_i\left(b^{i-1}, r_1\right)$ and Bob transmits message $b_i = g_i\left(y_2^j, a^{i-1}, r_2\right)$.*
- *after the last round, Alice computes a key $\mathsf{K} = \kappa_{\mathrm{a}}(x^n, b^r, r_1)$ and Bob computes a key $\hat{\mathsf{K}} = \kappa_{\mathrm{b}}(y^n, a^r, r_2)$.*

In addition, the vectors of channel inputs X_1^n and X_2^n should satisfy the power constraints $(1/n)\sum_{i=1}^n \mathbb{E}\left[\mathsf{X}_{1,i}^2\right] \leqslant P_1$ and $(1/n)\sum_{i=1}^n \mathbb{E}\left[\mathsf{X}_{2,i}^2\right] \leqslant P_2$.

By convention, we set $i_{n+1} \triangleq r + 1$, $i_0 = 0$, $\mathcal{A}^0 = 0$, and $\mathcal{B}^0 \triangleq 0$. As in Chapter 4, the indices $\{i_j\}_n$ and the sources of local randomness $\left(\mathcal{R}_1, p_{\mathrm{R}_1}\right)$ and $\left(\mathcal{R}_2, p_{\mathrm{R}_2}\right)$ can be optimized as part of the strategy. A rate R is an achievable key rate for the cooperative channel model if the conditions in Definition 4.3 are satisfied. If R is an achievable

secret-key rate, we can follow the same steps as those leading to (4.20) and show that

$$\begin{aligned} R &\leqslant \mathbb{H}(\mathrm{K}) \\ &\leqslant \frac{1}{n}\mathbb{I}\big(\mathrm{R}_1 X_1^n; \mathrm{R}_2 Y_2^n | A^r \mathrm{B}^r Z^n\big) + \delta(\epsilon) \\ &= \frac{1}{n}\mathbb{I}\big(\mathrm{R}_1; \mathrm{R}_2 Y_2^n | A^r \mathrm{B}^r Z^n\big) + \delta(\epsilon), \end{aligned}$$

where the last equality follows because $\mathrm{X}_j = h_j(\mathrm{B}^{i_j-1}, \mathcal{R}_1)$. As in the proof of Theorem 4.8, we introduce the random variable Λ_j which represents the messages exchanged over the public channel between two successive uses of the channel:

$$\begin{aligned} \Lambda_0 &\triangleq \big(A_1, \ldots, A_{i_1-1}, \mathrm{B}_1, \ldots, \mathrm{B}_{i_1-1}\big), \\ \Lambda_j &\triangleq \big(A_{i_j+1} \ldots A_{i_{j+1}-1}, \mathrm{B}_{i_j+1} \ldots \mathrm{B}_{i_{j+1}-1}\big) \quad \text{for } j \in [\![1, n]\!]. \end{aligned}$$

We then expand $\mathbb{I}\big(\mathrm{R}_1; \mathrm{R}_2 Y_2^n | A^r \mathrm{B}^r Z^n\big)$ as

$$\begin{aligned} &\mathbb{I}\big(\mathrm{R}_1; \mathrm{R}_2 Y_2^n | A^r \mathrm{B}^r Z^n\big) \\ &\quad = \mathbb{I}(\mathrm{R}_1; \mathrm{R}_2 | \Lambda_0) + \sum_{j=1}^{n} \Big[\mathbb{I}\Big(\mathrm{R}_1; \Lambda_j | Z^j Y_2^j \mathrm{R}_2 \Lambda_0 \Lambda^{j-1}\Big) - \mathbb{I}\big(\mathrm{R}_1; \Lambda_j | Z^j \Lambda_0 \Lambda^{j-1}\big)\Big] \\ &\qquad + \sum_{j=1}^{n} \Big[\mathbb{I}\Big(\mathrm{R}_1; \mathrm{Y}_{2,j} \mathrm{Z}_j | Z^{j-1} Y_2^{j-1} \mathrm{R}_2 \Lambda_0 \Lambda^{j-1}\Big) - \mathbb{I}\big(\mathrm{R}_1; \mathrm{Z}_j | Z^{j-1} \Lambda_0 \Lambda^{j-1}\big)\Big]. \end{aligned} \tag{8.9}$$

As in (4.65), the first term in (8.9) satisfies $\mathbb{I}(\mathrm{R}_1; \mathrm{R}_2 | \Lambda_0) = 0$ by Lemma 4.2. In addition, the terms in the first sum of (8.9) satisfy

$$\mathbb{I}\Big(\mathrm{R}_1; \Lambda_j | Z^j Y_2^j \mathrm{R}_2 \Lambda_0 \Lambda^{j-1}\Big) - \mathbb{I}\big(\mathrm{R}_1; \Lambda_j | Z^j \Lambda_0 \Lambda^{j-1}\big) \leqslant 0,$$

as has already been proved for Theorem 4.8. The terms in the second sum of (8.9) can be rewritten as

$$\begin{aligned} &\mathbb{I}\Big(\mathrm{R}_1; \mathrm{Y}_{2,j} \mathrm{Z}_j | Z^{j-1} Y_2^{j-1} \mathrm{R}_2 \Lambda_0 \Lambda^{j-1}\Big) - \mathbb{I}\big(\mathrm{R}_1; \mathrm{Z}_j | Z^{j-1} \Lambda_0 \Lambda^{j-1}\big) \\ &\quad = \mathbb{H}\Big(\mathrm{Y}_{2,j} \mathrm{Z}_j | Z^{j-1} Y_2^{j-1} \mathrm{R}_2 \Lambda_0 \Lambda^{j-1}\Big) - \mathbb{H}\Big(\mathrm{Y}_{2,j} \mathrm{Z}_j | Z^{j-1} Y_2^{j-1} \mathrm{R}_2 \mathrm{R}_1 \Lambda_0 \Lambda^{j-1}\Big) \\ &\qquad - \mathbb{H}\big(\mathrm{Z}_j | Z^{j-1} \Lambda_0 \Lambda^{j-1}\big) + \mathbb{H}\big(\mathrm{Z}_j | Z^{j-1} \Lambda_0 \Lambda^{j-1} \mathrm{R}_1\big). \end{aligned}$$

We can further simplify this expression by recalling that $\mathrm{X}_{1,j} = h_j(\mathrm{B}^{i_j-1}, \mathrm{R}_1)$, $\mathrm{X}_{2,j} = h'_j(A^{i_j-1}, \mathrm{R}_2, Y_2^{j-1})$, and

$$\mathrm{R}_1 \mathrm{R}_2 Y_2^{j-1} Z^{j-1} \Lambda_0 \Lambda^{j-1} \to \mathrm{X}_{1,j} \mathrm{X}_{2,j} \to \mathrm{Y}_{2,j} \mathrm{Z}_j$$

forms a Markov chain. Using these properties, we obtain

$$\mathbb{H}\Big(\mathrm{Y}_{2,j} \mathrm{Z}_j | Z^{j-1} Y_2^{j-1} \mathrm{R}_2 \mathrm{R}_1 \Lambda_0 \Lambda^{j-1}\Big) = \mathbb{H}\big(\mathrm{Y}_{2,j} \mathrm{Z}_j | \mathrm{X}_{1,j} \mathrm{X}_{2,j}\big)$$

and

$$\mathbb{H}\big(\mathrm{Z}_j | Z^{j-1} \Lambda_0 \Lambda^{j-1} \mathrm{R}_1\big) = \mathbb{H}\big(\mathrm{Z}_j | \mathrm{X}_{1,j} Z^{j-1} \Lambda_0 \Lambda^{j-1} \mathrm{R}_1\big) \leqslant \mathbb{H}\big(\mathrm{Z}_j | \mathrm{X}_{1,j}\big).$$

Therefore, we can bound the terms in the second sum of (8.9) by

$$\begin{aligned}
&\mathbb{H}\Big(\mathsf{Y}_{2,j}\mathsf{Z}_j|\mathsf{Z}^{j-1}\mathsf{Y}_2^{j-1}\mathsf{R}_2\Lambda_0\Lambda^{j-1}\Big) - \mathbb{H}\big(\mathsf{Y}_{2,j}\mathsf{Z}_j|\mathsf{X}_{1,j}\mathsf{X}_{2,j}\big) - \mathbb{H}\big(\mathsf{Z}_j|\mathsf{Z}^{j-1}\Lambda_0\Lambda^{j-1}\big) \\
&\quad + \mathbb{H}\big(\mathsf{Z}_j|\mathsf{X}_{1,j}\big) \\
&\quad = \mathbb{H}\Big(\mathsf{Y}_{2,j}|\mathsf{Z}^{j}\mathsf{Y}_2^{j-1}\mathsf{R}_2\Lambda_0\Lambda^{j-1}\Big) + \mathbb{H}\Big(\mathsf{Z}_j|\mathsf{Z}^{j-1}\mathsf{Y}_2^{j-1}\mathsf{R}_2\Lambda_0\Lambda^{j-1}\Big) \\
&\qquad - \mathbb{H}\big(\mathsf{Y}_{2,j}|\mathsf{Z}_j\mathsf{X}_{1,j}\mathsf{X}_{2,j}\big) - \mathbb{H}\big(\mathsf{Z}_j|\mathsf{X}_{1,j}\mathsf{X}_{2,j}\big) - \mathbb{H}\big(\mathsf{Z}_j|\mathsf{Z}^{j-1}\Lambda_0\Lambda^{j-1}\big) + \mathbb{H}\big(\mathsf{Z}_j|\mathsf{X}_{1,j}\big) \\
&\quad \leqslant \mathbb{H}\big(\mathsf{Y}_{2,j}|\mathsf{Z}_j\mathsf{X}_{2,j}\big) - \mathbb{H}\big(\mathsf{Y}_{2,j}|\mathsf{Z}_j\mathsf{X}_{1,j}\mathsf{X}_{2,j}\big) - \mathbb{H}\big(\mathsf{Z}_j|\mathsf{X}_{1,j}\mathsf{X}_{2,j}\big) + \mathbb{H}\big(\mathsf{Z}_j|\mathsf{X}_{1,j}\big) \\
&\quad = \mathbb{I}\big(\mathsf{X}_{1,j};\mathsf{Y}_{2,j}|\mathsf{Z}_j\mathsf{X}_{2,j}\big) + \mathbb{I}\big(\mathsf{Z}_j;\mathsf{X}_{2,j}|\mathsf{X}_{1,j}\big).
\end{aligned}$$

All in all, we obtain our second bound:

$$R \leqslant \frac{1}{n}\sum_{j=1}^{n}\Big(\mathbb{I}\big(\mathsf{X}_{1,j};\mathsf{Y}_{2,j}|\mathsf{Z}_j\mathsf{X}_{2,j}\big) + \mathbb{I}\big(\mathsf{Z}_j;\mathsf{X}_{2,j}|\mathsf{X}_{1,j}\big)\Big) + \delta(\epsilon). \tag{8.10}$$

Finally, we introduce a random variable Q that is uniformly distributed on $[\![1, n]\!]$ and independent of all other random variables, and we define

$$\mathsf{X}_1 \triangleq \mathsf{X}_{1,\mathsf{Q}}, \qquad \mathsf{X}_2 \triangleq \mathsf{X}_{2,\mathsf{Q}}, \qquad \mathsf{Y}_2 \triangleq \mathsf{Y}_{2,\mathsf{Q}}, \qquad \text{and} \qquad \mathsf{Z} \triangleq \mathsf{Z}_{\mathsf{Q}}.$$

The transition probabilities from $\mathsf{X}_1\mathsf{X}_2$ to $\mathsf{Y}_2\mathsf{Z}$ are the original transition probabilities of the channel $p_{\mathsf{Y}_2\mathsf{Z}|\mathsf{X}_1\mathsf{X}_2}$ and, in addition, X_1 and X_2 should satisfy the power constraints $\mathbb{E}\big[\mathsf{X}_1^2\big] \leqslant P_1$ and $\mathbb{E}\big[\mathsf{X}_2^2\big] \leqslant P_2$. By substituting these random variables into (8.8) and (8.10), and using the fact that $\mathsf{Q} \to \mathsf{X}_1\mathsf{X}_1 \to \mathsf{Z}\mathsf{Y}_2$ forms a Markov chain, we obtain

$$R \leqslant \min(\mathbb{I}(\mathsf{X}_1;\mathsf{Y}_2), \mathbb{I}(\mathsf{X}_1;\mathsf{Y}_2|\mathsf{Z}\mathsf{X}_2) + \mathbb{I}(\mathsf{X}_2;\mathsf{Z}|\mathsf{X}_1)) + \delta(\epsilon).$$

Since ϵ can be chosen arbitrarily small and since we can optimize the distribution of inputs $\mathsf{X}_1\mathsf{X}_2$, we obtain the desired result. □

The optimization of the upper bound has to be performed over the random variables $(\mathsf{X}_1, \mathsf{X}_2)$ *jointly*; therefore the terms $\mathbb{I}(\mathsf{X}_1;\mathsf{Y}_2|\mathsf{Z}\mathsf{X}_2)$ and $\mathbb{I}(\mathsf{X}_2;\mathsf{Z}|\mathsf{X}_1)$ are not independent. Nevertheless, the result can still be understood intuitively as follows. The term $\mathbb{I}(\mathsf{X}_1;\mathsf{Y}_2|\mathsf{Z}\mathsf{X}_2)$ represents the secrecy rate achieved in the presence of an eavesdropper who would be able to cancel out the jamming signal X_2 perfectly, whereas the second term, $\mathbb{I}(\mathsf{X}_2;\mathsf{Z}|\mathsf{X}_1)$, represents the information that the eavesdropper has to obtain in order to "identify" the jamming signal and cancel it out. By specializing Proposition 8.3 further, we obtain the following result.

Proposition 8.4 (He and Yener)**.** *The region of rates achievable with cooperative jamming is included in the region* $\mathcal{R}_{\mathrm{cj}}^{\mathrm{out}}$ *defined as*

$$\mathcal{R}_{\mathrm{cj}}^{\mathrm{out}} = \left\{ (R_1, R_2): \begin{array}{r} 0 \leqslant R_1 \leqslant \min\left(C\left(\dfrac{P_1}{1 + h_1P_1}\right) + C(h_2P_2), C(P_1)\right) \\ 0 \leqslant R_2 \leqslant \min\left(C\left(\dfrac{P_2}{1 + h_2P_2}\right) + C(h_1P_1), C(P_2)\right) \end{array} \right\}.$$

Proof. We can further bound the result of Proposition 8.3 as

$$R_1 \leqslant \min(\max \mathbb{I}(\mathsf{X}_1;\mathsf{Y}_2), \max(\mathbb{I}(\mathsf{X}_1;\mathsf{Y}_2|\mathsf{Z}\mathsf{X}_2) + \mathbb{I}(\mathsf{X}_2;\mathsf{Z}|\mathsf{X}_1))),$$

where the maximum is taken over all joint distributions $p_{\mathsf{X}_1\mathsf{X}_2}$ such that $\mathbb{E}\left[\mathsf{X}_1^2\right] \leqslant P_1$ and $\mathbb{E}\left[\mathsf{X}_2^2\right] \leqslant P_2$. The first term, $\mathbb{I}(\mathsf{X}_1;\mathsf{Y}_2)$, cannot exceed the capacity of the channel from Alice to Bob; therefore,

$$\max \mathbb{I}(\mathsf{X}_1;\mathsf{Y}_2) \leqslant C(P_1).$$

To bound the term $\max(\mathbb{I}(\mathsf{X}_1;\mathsf{Y}_2|\mathsf{Z}\mathsf{X}_2) + \mathbb{I}(\mathsf{X}_2;\mathsf{Z}|\mathsf{X}_1))$, we introduce the random variables

$$\mathsf{Z}_1 \triangleq \sqrt{h_1}\mathsf{X}_1 + \mathsf{N}_\mathrm{e} \qquad \text{and} \qquad \mathsf{Z}_2 \triangleq \sqrt{h_2}\mathsf{X}_2 + \mathsf{N}_\mathrm{e},$$

which represent the observations of an eavesdropper who would be able to cancel out either one of the signals X_1 and X_2. Then,

$$\begin{aligned}\mathbb{I}(\mathsf{X}_1;\mathsf{Y}_2|\mathsf{Z}\mathsf{X}_2) &= \mathbb{h}(\mathsf{Y}_2|\mathsf{Z}\mathsf{X}_2) - \mathbb{h}(\mathsf{Y}_2|\mathsf{Z}\mathsf{X}_1\mathsf{X}_2)\\ &= \mathbb{h}(\mathsf{Y}_2|\mathsf{Z}_1\mathsf{X}_2) - \mathbb{h}(\mathsf{N}_1)\\ &\leqslant \mathbb{h}(\mathsf{Y}_2|\mathsf{Z}_1) - \mathbb{h}(\mathsf{N}_1)\\ &= \mathbb{h}(\mathsf{Y}_2\mathsf{Z}_1) - \mathbb{h}(\mathsf{Z}_1) - \mathbb{h}(\mathsf{N}_1). \end{aligned} \tag{8.11}$$

Similarly,

$$\begin{aligned}\mathbb{I}(\mathsf{X}_2;\mathsf{Z}|\mathsf{X}_1) &= \mathbb{h}(\mathsf{Z}|\mathsf{X}_1) - \mathbb{h}(\mathsf{Z}|\mathsf{X}_1\mathsf{X}_2)\\ &= \mathbb{h}(\mathsf{Z}_2|\mathsf{X}_1) - \mathbb{h}(\mathsf{N}_\mathrm{e})\\ &\leqslant \mathbb{h}(\mathsf{Z}_2) - \mathbb{h}(\mathsf{N}_\mathrm{e}). \end{aligned} \tag{8.12}$$

We now show that the upper bounds (8.11) and (8.12) are maximized by choosing independent Gaussian random variables for X_1 and X_2. Since (8.11) depends only on X_1 and (8.12) depends only on X_2, the bounds are maximized with independent random variables. In addition, the term $\mathbb{h}(\mathsf{Z}_2)$ is maximized if Z_2 is Gaussian, which is achieved if X_2 is Gaussian as well. To show that $\mathbb{h}(\mathsf{Y}_2|\mathsf{Z}_1)$ is also maximized with X_1 Gaussian, let $\mathrm{LLSE}(\mathsf{Z}_1)$ denote the linear least-square estimate of Y_2 based on Z_1 and let λ_{LLSE} denote the corresponding estimation error. Then,

$$\mathbb{h}(\mathsf{Y}_2|\mathsf{Z}_1) = \mathbb{h}(\mathsf{Y}_2 - \mathrm{LLSE}(\mathsf{Z}_1)|\mathsf{Z}_1) \leqslant \mathbb{h}(\mathsf{Y}_2 - \mathrm{LLSE}(\mathsf{Z}_1)) \leqslant \frac{1}{2}\log(2\pi e\lambda_{\mathrm{LLSE}}).$$

The inequalities are equalities if Y_2 and Z_1 are Gaussian, which is achieved if X_1 is Gaussian; hence, we can evaluate (8.11) and (8.12) with two independent random variables $\mathsf{X}_1 \sim \mathcal{N}(0, P_1)$ and $\mathsf{X}_2 \sim \mathcal{N}(0, P_2)$.

On substituting $\mathsf{X}_2 \sim \mathcal{N}(0, P_2)$ into (8.12), we obtain directly

$$\mathbb{I}(\mathsf{X}_2;\mathsf{Z}|\mathsf{X}_1) \leqslant C(h_2 P_2). \tag{8.13}$$

A little more work is needed to bound (8.11). If $\mathsf{X}_1 \sim \mathcal{N}(0,\, P_1)$, then the vector $(\mathsf{Y}_2,\ \mathsf{Z}_1)^\intercal$ defined as

$$\begin{pmatrix} \mathsf{Y}_2 \\ \mathsf{Z}_1 \end{pmatrix} \triangleq \begin{pmatrix} 1 \\ \sqrt{h_1} \end{pmatrix} \mathsf{X}_1 + \begin{pmatrix} 1 \\ 0 \end{pmatrix} \mathsf{N}_1 + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \mathsf{N}_\mathrm{e}$$

is also Gaussian with zero mean. Since X_1, N_1, and N_e are independent, its covariance matrix is

$$\mathbf{K}_{\mathsf{Y}_1\mathsf{Z}_2} = \begin{pmatrix} 1 + P_1 & \sqrt{h_1} P_1 \\ \sqrt{h_1} P_1 & 1 + h_1 P_1 \end{pmatrix};$$

therefore,

$$\begin{aligned} \mathbb{I}(\mathsf{X}_1; \mathsf{Y}_2 | \mathsf{Z}\mathsf{X}_2) &\leqslant \mathbb{h}(\mathsf{Y}_2\mathsf{Z}_1) - \mathbb{h}(\mathsf{Z}_1) - \mathbb{h}(\mathsf{N}_1) \\ &= \log\left(2\pi e \left|\mathbf{K}_{\mathsf{Y}_1\mathsf{Z}_2}\right|\right) - \frac{1}{2}\log(2\pi e(1 + h_1 P_1)) - \frac{1}{2}\log(2\pi e) \\ &= C(P_1 + h_1 P_1) - C(h_1 P_1) \\ &= C\left(\frac{P_1}{1 + h_1 P_1}\right). \end{aligned} \tag{8.14}$$

On combining (8.13) and (8.14), we obtain the second part of the upper bound for R_1:

$$\max(\mathbb{I}(\mathsf{X}_1; \mathsf{Y}_2 | \mathsf{Z}\mathsf{X}_2) + \mathbb{I}(\mathsf{X}_2; \mathsf{Z} | \mathsf{X}_1)) \leqslant C\left(\frac{P_1}{1 + h_1 P_1}\right) + C(h_2 P_2).$$

The bound for R_2 is obtained with identical steps by swapping the roles of Alice and Bob. □

The regions $\mathcal{R}_{\mathsf{cj}}^{\mathsf{out}}$ and $\mathcal{R}_{\mathsf{cj}}$ cannot coincide because $\mathcal{R}_{\mathsf{cj}}^{\mathsf{out}}$ has a square shape whereas $\mathcal{R}_{\mathsf{cj}}$ has a triangle shape (obtained with time-sharing). Nevertheless, Proposition 8.4 still provides a reasonably tight bound for the maximum secure rate achieved by either Alice or Bob with cooperative jamming over a wide range of channel parameters. Figure 8.3 illustrates typical regions $\mathcal{R}_{\mathsf{cj}}^{\mathsf{out}}$, $\mathcal{R}_{\mathsf{cj}}$, and $\mathcal{R}_0$, for which the extremal points of $\mathcal{R}_{\mathsf{cj}}$ are within a few tenths of a bit of the outer bound $\mathcal{R}_{\mathsf{cj}}^{\mathsf{out}}$.

Remark 8.2. *It might be somewhat surprising that an outer bound obtained by analyzing the secret-key capacity of a channel model turns out to be useful. Nevertheless, the reasonable tightness of the bound can be understood intuitively by remarking that the addition of a public channel of unlimited capacity is not a trivial enhancement. In fact, the public channel does not modify the randomness of the channel, which is the fundamental source of secrecy. As a matter of fact, we already know from Corollary 3.1 and Theorem 4.8 that the secrecy capacity and secret-key capacity of a degraded wiretap channel are equal. In the case of cooperative jamming, the channel also exhibits some degradedness, which partly explains why the approach of Proposition 8.3 is useful.*

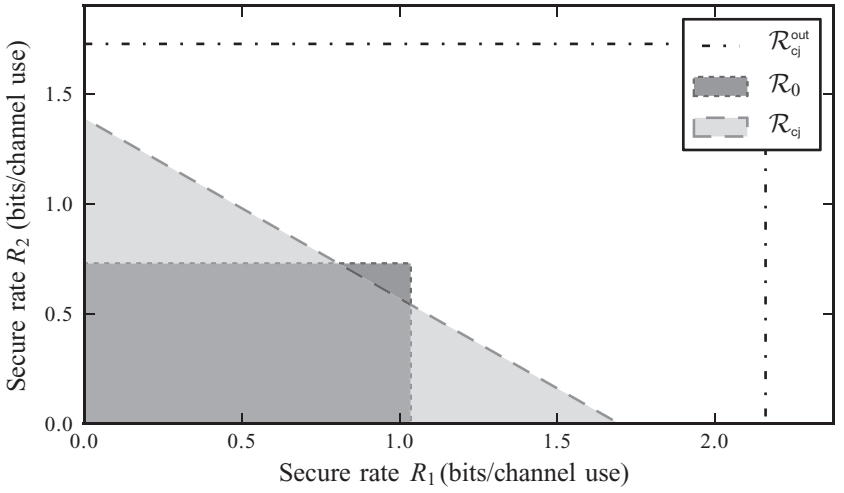

Figure 8.3 Regions $\mathcal{R}_0$, $\mathcal{R}_{\text{cj}}$, and $\mathcal{R}_{\text{cj}}^{\text{out}}$ for $h_1 = 0.2$, $h_2 = 0.3$, $P_1 = 20$, and $P_2 = 10$.

8.3 Coded cooperative jamming

Since cooperative jamming always improves the maximum secure communication rate of either Alice or Bob, cooperative jamming achieves rate pairs that are not achievable with the benchmark strategy and $\mathcal{R}_{\text{cj}} \nsubseteq \mathcal{R}_0$. Unfortunately, cooperative jamming forces either Alice or Bob to stop transmitting information. As a result, if the magnitude of the channel gains h_1 and h_2 is small ($h_1 \ll 1$ and $h_2 \ll 1$), the eavesdropper does not suffer from much interference and Alice and Bob might as well treat their channels as orthogonal wiretap channels; therefore, in general, $\mathcal{R}_0 \nsubseteq \mathcal{R}_{\text{cj}}$ either, and one cannot conclude that cooperative jamming performs strictly better than the benchmark strategy. The numerical example in Figure 8.3 is a specific case of such a situation.

To overcome this limitation, one can wonder whether Alice and Bob could achieve the effect of cooperative jamming while still communicating codewords. The interference of codewords might still have a detrimental effect on the eavesdropper, but without sacrificing the entire rate of either Alice or Bob. To emphasize that the underlying principle is similar to cooperative jamming but that the eavesdropper observes codeword interference, we call such schemes *coded cooperative jamming codes* (coded cooperative jamming for short). Formally, coded cooperative jamming is a specific instance of a code for the two-way wiretap channel such that

- there are two independent encoding functions, $f_1 : \mathcal{M}_1 \times \mathcal{R}_1 \to \mathcal{X}_1^n$ and $f_2 : \mathcal{M}_2 \times \mathcal{R}_2 \to \mathcal{X}_2^n$;
- there are two decoding functions, $g_1 : \mathcal{Y}_1^n \to \mathcal{M}_2 \cup \{?\}$ and $g_2 : \mathcal{Y}_2^n \to \mathcal{M}_1 \cup \{?\}$.

Note that coded cooperative jamming does not exploit feedback, but the codebooks used by Alice and Bob can be optimized jointly prior to transmission to maximize the effectiveness of codeword interference.

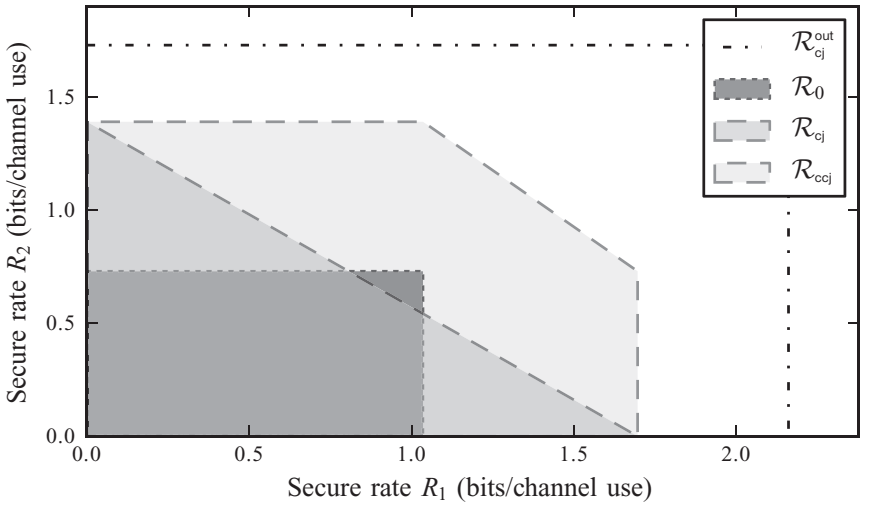

Figure 8.4 Regions $\mathcal{R}_0$, $\mathcal{R}_{cj}$, $\mathcal{R}_{ccj}$, and $\mathcal{R}_{cj}^{out}$ for $h_1 = 0.2$, $h_2 = 0.3$, $P_1 = 20$, and $P_2 = 10$.

Proposition 8.5 (Tekin and Yener)**.** *The rate region $\mathcal{R}_{ccj}$ defined as*

$$\mathcal{R}_{ccj} \triangleq \left\{ (R_1, R_2): \begin{array}{l} 0 \leqslant R_1 < \left(C(P_1) - C\left(\dfrac{h_1 P_1}{1 + h_2 P_2} \right) \right)^+ \\ 0 \leqslant R_2 < \left(C(P_2) - C\left(\dfrac{h_2 P_2}{1 + h_1 P_1} \right) \right)^+ \\ 0 \leqslant R_1 + R_2 < (C(P_1) + C(P_2) - C(h_1 P_1 + h_2 P_2))^+ \end{array} \right\}$$

is achievable with coded cooperative jamming.

Remark 8.3. *The region $\mathcal{R}_{cj}^{out}$ in Proposition 8.3 is also an outer bound for $\mathcal{R}_{ccj}$. In fact, $\mathcal{R}_{cj}^{out}$ has been derived for the case of arbitrary jamming signals, which includes codewords as a special case, and, in addition, $\mathcal{R}_{cj}^{out}$ has been obtained without requiring the jamming signals to be decoded by the non-jamming terminal. Removing this constraint cannot reduce the secure rates of the non-jamming terminal; therefore, $\mathcal{R}_{cj}^{out}$ is an outer bound for $\mathcal{R}_{cj}$.*

Before we prove Proposition 8.5, it is useful to analyze its implications. As illustrated in Figure 8.4, the shape of $\mathcal{R}_{ccj}$ is reminiscent of the capacity region of a multiple-access channel. This similarity is not fortuitous because the channel linking Alice and Bob to Eve is indeed a multiple-access channel, and we explicitly use it in the proof. By comparing Proposition 8.1 and Proposition 8.5, we see that the individual rate constraints on R_1 and R_2 are more stringent in $\mathcal{R}_0$ than they are in $\mathcal{R}_{ccj}$. In fact, if $(R_1, R_2) \in \mathcal{R}_0$ then the sum-rate satisfies

$$R_1 + R_2 < C(P_1) - C(h_1 P_1) + C(P_2) - C(h_2 P_2),$$

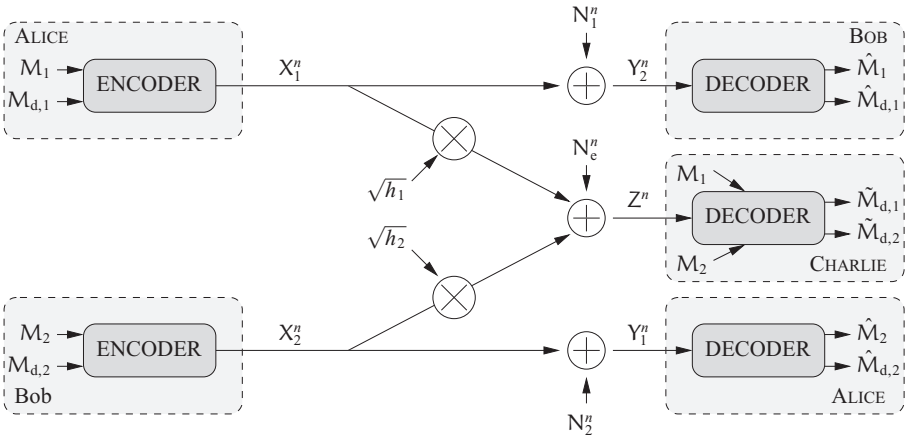

Figure 8.5 Enhanced channel for coded cooperative jamming.

which is more stringent than the sum-rate constraint in $\mathcal{R}_{\mathsf{ccj}}$ because

$$C(P_1) + C(P_2) - C(h_1P_1 + h_2P_2) = C(P_1) + C(P_2) - C(h_1P_1) - C\left(\frac{h_2P_2}{1 + h_1P_1}\right)$$
$$\geqslant C(P_1) - C(h_1P_1) + C(P_2) - C(h_2P_2).$$

Hence, in contrast with $\mathcal{R}_{\mathsf{cj}}$, we can conclude that $\mathcal{R}_0 \subseteq \mathcal{R}_{\mathsf{ccj}}$ for all channel parameters.

We now prove Proposition 8.5. The proof is based on a random-coding argument that combines the wiretap coding technique introduced in Section 3.4.1 with the multiple-access coding technique described in Section 2.3.2. As in Chapter 3, we start by constructing codes for an enhanced channel, which is illustrated in Figure 8.5. This channel enhances the original channel by

- introducing a virtual receiver, hereafter named Charlie, who observes the same output Z^n as Eve and has also access to the messages M_1 and M_2 through an error-free side channel;
- using a message $\mathrm{M}_{\mathrm{d},1}$ with uniform distribution over $[\![1, 2^{nR_{\mathrm{d},1}}]\!]$ in place of the source of local randomness $(\mathcal{R}_1, p_{\mathrm{R}_1})$ and another message $\mathrm{M}_{\mathrm{d},2}$ with uniform distribution over $[\![1, 2^{nR_{\mathrm{d},2}}]\!]$ in place of $(\mathcal{R}_2, p_{\mathrm{R}_2})$.

Formally, a code for the enhanced channel is defined as follows.

Definition 8.4. *A $(2^{nR_1}, 2^{nR_{\mathrm{d},1}}, 2^{nR_2}, 2^{nR_{\mathrm{d},2}}, n)$ code $\mathcal{C}_n$ for the enhanced channel consists of*

- *four message sets, $\mathcal{M}_1 = [\![1, 2^{nR_1}]\!]$, $\mathcal{M}_{\mathrm{d},1} = [\![1, 2^{nR_{\mathrm{d},1}}]\!]$, $\mathcal{M}_2 = [\![1, 2^{nR_2}]\!]$, and $\mathcal{M}_{\mathrm{d},2} = [\![1, 2^{nR_{\mathrm{d},2}}]\!]$;*
- *two encoding functions, $f_1 : \mathcal{M}_1 \times \mathcal{M}_{\mathrm{d},1} \to \mathcal{X}_1^n$ and $f_2 : \mathcal{M}_2 \times \mathcal{M}_{\mathrm{d},2} \to \mathcal{X}_2^n$;*
- *a decoding function $g_1 : \mathcal{Y}_1^n \to (\mathcal{M}_2 \times \mathcal{M}_{2,\mathrm{d}}) \cup \{\mathbf{?}\}$, which maps each channel observation y_1^n to a message pair $(\hat{m}_2, \hat{m}_{\mathrm{d},2}) \in \mathcal{M}_2 \times \mathcal{M}_{\mathrm{d},2}$ or an error message $\mathbf{?}$;*

- *a decoding function* $g_2 : \mathcal{Y}_2^n \to (\mathcal{M}_1 \times \mathcal{M}_{\mathrm{d},1}) \cup \{?\}$*, which maps each channel observation* y_2^n *to a message pair* $(\hat{m}_1, \hat{m}_{\mathrm{d},1}) \in \mathcal{M}_1 \times \mathcal{M}_{\mathrm{d},1}$ *or an error message* **?***;*
- *a decoding function* $h : \mathcal{Z}^n \times \mathcal{M}_1 \times \mathcal{M}_2 \to (\mathcal{M}_{\mathrm{d},1} \times \mathcal{M}_{\mathrm{d},2}) \cup \{?\}$*, which maps each channel observation* z^n *and the corresponding messages* m_1 *and* m_2 *to a message pair* $(\tilde{m}_1, \tilde{m}_2) \in \mathcal{M}_{\mathrm{d},1} \times \mathcal{M}_{\mathrm{d},2}$ *or an error message* **?**.

We assume that all messages are uniformly distributed in their respective sets. The reliability performance of a $(2^{nR_1}, 2^{nR_{\mathrm{d},1}}, 2^{nR_2}, 2^{nR_{\mathrm{d},2}}, n)$ code $\mathcal{C}_n$ is measured in terms of the average probability of error

$$\mathbf{P}_{\mathrm{e}}(\mathcal{C}_n) \triangleq \mathbb{P}\Big[(\hat{\mathsf{M}}_1, \hat{\mathsf{M}}_{\mathrm{d},1}) \neq (\mathsf{M}_1, \mathsf{M}_{\mathrm{d},1}) \text{ or } (\hat{\mathsf{M}}_2, \hat{\mathsf{M}}_{\mathrm{d},2}) \neq (\mathsf{M}_2, \mathsf{M}_{\mathrm{d},2}) \text{ or } (\tilde{\mathsf{M}}_{\mathrm{d},1}, \tilde{\mathsf{M}}_{\mathrm{d},2}) \neq (\mathsf{M}_{\mathrm{d},1}, \mathsf{M}_{\mathrm{d},2}) | \mathcal{C}_n\Big].$$

Since $\mathsf{M}_{\mathrm{d},1}$ and $\mathsf{M}_{\mathrm{d},2}$ are dummy messages that correspond to a specific choice for sources of local randomness $(\mathcal{R}_1, p_{\mathsf{R}_1})$ and $(\mathcal{R}_2, p_{\mathsf{R}_2})$, a $(2^{nR_1}, 2^{nR_{\mathrm{d},1}}, 2^{nR_2}, 2^{nR_{\mathrm{d},2}}, n)$ code $\mathcal{C}_n$ for the enhanced channel is also a $(2^{nR_1}, 2^{nR_2}, n)$ coded cooperative jamming code $\mathcal{C}_n$ for the original channel; the probability of error over the original channel does not exceed the probability of error over the enhanced channel since

$$\mathbb{P}\Big[(\mathsf{M}_1, \mathsf{M}_2) \neq (\hat{\mathsf{M}}_1, \hat{\mathsf{M}}_2) | \mathcal{C}_n\Big] \leqslant \mathbf{P}_{\mathrm{e}}(\mathcal{C}_n).$$

In addition, by virtue of Fano's inequality,

$$\frac{1}{n}\mathbb{H}(\mathsf{M}_{\mathrm{d},1}, \mathsf{M}_{\mathrm{d},2} | \mathsf{Z}^n \mathsf{M}_1 \mathsf{M}_2 \mathcal{C}_n) \leqslant \delta(\mathbf{P}_{\mathrm{e}}(\mathcal{C}_n)). \tag{8.15}$$

The above inequality is useful to evaluate the leakage to the eavesdropper guaranteed by $\mathcal{C}_n$ later on.

We begin by choosing two independent probability distributions p_{X_1} on $\mathcal{X}_1$ and p_{X_2} on $\mathcal{X}_2$. Let $0 < \epsilon < \mu_{\mathsf{X}_1\mathsf{X}_2\mathsf{YZ}}$, where

$$\mu_{\mathsf{X}_1\mathsf{X}_2\mathsf{YZ}} \triangleq \min_{(x_1,x_2,y,z)\in\mathcal{X}_1\times\mathcal{X}_2\times\mathcal{Y}\times\mathcal{Z}} p_{\mathsf{X}_1}(x_1) p_{\mathsf{X}_2}(x_2) p_{\mathsf{YZ}|\mathsf{X}_1\mathsf{X}_2}(y, z|x_1, x_2),$$

and let $n \in \mathbb{N}^*$. Let $R_1 > 0$, $R_{\mathrm{d},1} > 0$, $R_2 > 0$, and $R_{\mathrm{d},2} > 0$ be rates to be specified later. We construct a $(2^{nR_1}, 2^{nR_{\mathrm{d},1}}, 2^{nR_2}, 2^{nR_{\mathrm{d},2}}, n)$ code for the enhanced channel as follows.

- *Codebook construction.* Construct a codebook $\mathcal{C}_1$ with $\lceil 2^{nR_1} \rceil \lceil 2^{nR_{\mathrm{d},1}} \rceil$ codewords labeled $x_1^n(m_1, m_{\mathrm{d},1})$ for $m_1 \in [\![1, 2^{nR_1}]\!]$ and $m_{\mathrm{d},1} \in [\![1, 2^{nR_{\mathrm{d},1}}]\!]$, by generating the symbols $x_{1,i}(m_1, m_{\mathrm{d},1})$ for $i \in [\![1, n]\!]$, $m_1 \in [\![1, 2^{nR_1}]\!]$, and $m_{\mathrm{d},1} \in [\![1, 2^{nR_{\mathrm{d},1}}]\!]$ independently according to p_{X_1}; similarly, construct a codebook $\mathcal{C}_2$ with $\lceil 2^{nR_2} \rceil \lceil 2^{nR_{\mathrm{d},2}} \rceil$ codewords labeled $x_2^n(m_2, m_{\mathrm{d},2})$ for $m_2 \in [\![2, 2^{nR_2}]\!]$ and $m_{\mathrm{d},2} \in [\![2, 2^{nR_{\mathrm{d},2}}]\!]$, by generating the symbols $x_{2,i}(m_2, m_{\mathrm{d},2})$ for $i \in [\![2, n]\!]$, $m_2 \in [\![2, 2^{nR_2}]\!]$, and $m_{\mathrm{d},2} \in [\![2, 2^{nR_{\mathrm{d},2}}]\!]$ independently according to p_{X_2}.
- *Alice's encoder* f_1. Given $(m_1, m_{\mathrm{d},1})$, transmit $x_1^n(m_1, m_{\mathrm{d},1})$.
- *Bob's encoder* f_2. Given $(m_2, m_{\mathrm{d},2})$, transmit $x_2^n(m_2, m_{\mathrm{d},2})$.
- *Alice's decoder* f_1. Given y_1^n, output $(\hat{m}_2, \hat{m}_{\mathrm{d},2})$ if it is the unique message pair such that $\big(x_2^n(\hat{m}_2, \hat{m}_{\mathrm{d},2}), y_1^n\big) \in \mathcal{T}_\epsilon^n(\mathsf{X}_2\mathsf{Y}_1)$; otherwise, output an error **?**.

- *Bob's decoder* f_2. Given y_2^n, output $(\hat{m}_1, \hat{m}_{\mathrm{d},1})$ if it is the unique message pair such that $\left(x_1^n(\hat{m}_1, \hat{m}_{\mathrm{d},1}), y_2^n\right) \in \mathcal{T}_\epsilon^n(\mathsf{X}_1\mathsf{Y}_2)$; otherwise, output an error **?**.
- *Charlie's decoder* f_2. Given z^n, m_1, and m_2, output $(\tilde{m}_{\mathrm{d},1}, \tilde{m}_{\mathrm{d},2})$ if it is the unique message pair such that $\left(x_1^n(m_1, \tilde{m}_{\mathrm{d},1}), x_2^n(m_2, \tilde{m}_{\mathrm{d},2}), z^n\right) \in \mathcal{T}_\epsilon^n(\mathsf{X}_1\mathsf{X}_2\mathsf{Z})$; otherwise, output an error **?**.

The random variable that represents the randomly generated code $\mathcal{C}_n = (\mathcal{C}_1, \mathcal{C}_2)$ is denoted by C_n. By combining the arguments used in Section 2.3.2 for the MAC and in Section 3.4.1 for the WTC, we can show that, if

$$\begin{aligned} R_1 + R_{\mathrm{d},1} &< \mathbb{I}(\mathsf{X}_1; \mathsf{Y}_2) - \delta(\epsilon), \\ R_2 + R_{\mathrm{d},2} &< \mathbb{I}(\mathsf{X}_2; \mathsf{Y}_1) - \delta(\epsilon), \\ R_{\mathrm{d},1} &< \mathbb{I}(\mathsf{X}_1; \mathsf{Z}|\mathsf{X}_2) - \delta(\epsilon), \\ R_{\mathrm{d},2} &< \mathbb{I}(\mathsf{X}_2; \mathsf{Z}|\mathsf{X}_1) - \delta(\epsilon), \\ R_{\mathrm{d},1} + R_{\mathrm{d},2} &< \mathbb{I}(\mathsf{X}_1\mathsf{X}_2; \mathsf{Z}) - \delta(\epsilon), \end{aligned}$$

then $\mathbb{E}[\mathbf{P}_{\mathrm{e}}(\mathsf{C}_n)] \leqslant \delta(\epsilon)$ for n large enough. In particular, for the choice[2] $\mathsf{X}_1 \sim \mathcal{N}(0, P_1)$ and $\mathsf{X}_2 \sim \mathcal{N}(0, P_2)$, the constraints become

$$\begin{aligned} R_1 + R_{\mathrm{d},1} &< C(P_1) - \delta(\epsilon), \\ R_2 + R_{\mathrm{d},2} &< C(P_2) - \delta(\epsilon), \\ R_{\mathrm{d},1} &< C(h_1 P_1) - \delta(\epsilon), \\ R_{\mathrm{d},2} &< C(h_2 P_2) - \delta(\epsilon), \\ R_{\mathrm{d},1} + R_{\mathrm{d},2} &< C(h_1 P_1 + h_2 P_2) - \delta(\epsilon). \end{aligned} \tag{8.16}$$

We now compute an upper bound for $\mathbb{E}[(1/n)\mathbf{L}(\mathcal{C}_n)]$ by following steps similar to those in Section 3.4.1:

$$\begin{aligned} \mathbb{E}\left[\frac{1}{n}\mathbf{L}(\mathcal{C}_n)\right] &= \frac{1}{n}\mathbb{I}(\mathsf{M}_1\mathsf{M}_2; \mathsf{Z}^n|\mathsf{C}_n) \\ &= \frac{1}{n}\mathbb{I}(\mathsf{M}_1\mathsf{M}_2\mathsf{M}_{\mathrm{d},1}\mathsf{M}_{\mathrm{d},2}; \mathsf{Z}^n|\mathsf{C}_n) - \frac{1}{n}\mathbb{I}(\mathsf{M}_{\mathrm{d},1}\mathsf{M}_{\mathrm{d},2}; \mathsf{Z}^n|\mathsf{M}_1\mathsf{M}_2\mathsf{C}_n) \\ &= \frac{1}{n}\mathbb{I}\left(\mathsf{X}_1^n\mathsf{X}_2^n; \mathsf{Z}^n|\mathsf{C}_n\right) - \frac{1}{n}\mathbb{H}(\mathsf{M}_{\mathrm{d},1}\mathsf{M}_{\mathrm{d},2}|\mathsf{M}_1\mathsf{M}_2\mathsf{C}_n) \\ &\quad + \frac{1}{n}\mathbb{H}(\mathsf{M}_{\mathrm{d},1}\mathsf{M}_{\mathrm{d},2}|\mathsf{Z}^n\mathsf{M}_1\mathsf{M}_2\mathsf{C}_n) \\ &= \frac{1}{n}\mathbb{I}\left(\mathsf{X}_1^n\mathsf{X}_2^n; \mathsf{Z}^n|\mathsf{C}_n\right) - \frac{1}{n}\mathbb{H}(\mathsf{M}_{\mathrm{d},1}\mathsf{M}_{\mathrm{d},2}|\mathsf{C}_n) \\ &\quad + \frac{1}{n}\mathbb{H}(\mathsf{M}_{\mathrm{d},1}\mathsf{M}_{\mathrm{d},2}|\mathsf{Z}^n\mathsf{M}_1\mathsf{M}_2\mathsf{C}_n). \end{aligned} \tag{8.17}$$

[2] See the proof of Theorem 5.1 for a discussion about the transition to continuous channels.

By construction,

$$\frac{1}{n}\mathbb{H}(\mathsf{M}_{\mathrm{d},1}\mathsf{M}_{\mathrm{d},2}|\mathsf{C}_n) \geqslant R_{\mathrm{d},1} + R_{\mathrm{d},2}. \tag{8.18}$$

Next, using (8.15) and $\mathbb{E}[\mathbf{P}_{\mathrm{e}}(\mathsf{C}_n)] \leqslant \delta(\epsilon)$, we obtain

$$\begin{aligned}\frac{1}{n}\mathbb{H}(\mathsf{M}_{\mathrm{d},1}\mathsf{M}_{\mathrm{d},2}|\mathsf{Z}^n\mathsf{M}_1\mathsf{M}_2\mathsf{C}_n) &= \sum_{\mathcal{C}_n} p_{\mathsf{C}_n}(\mathcal{C}_n)\,\frac{1}{n}\mathbb{H}(\mathsf{M}_{\mathrm{d},1}\mathsf{M}_{\mathrm{d},2}|\mathsf{Z}^n\mathsf{M}_1\mathsf{M}_2\mathcal{C}_n)\\ &\leqslant \delta(n) + \mathbb{E}[\mathbf{P}_{\mathrm{e}}(\mathsf{C}_n)](R_{\mathrm{d},1} + R_{\mathrm{d},2} + \delta(n))\\ &\leqslant \delta(\epsilon).\end{aligned} \tag{8.19}$$

Finally, note that $\mathsf{C}_n \to \mathsf{X}_1^n\mathsf{X}_2^n \to \mathsf{Z}^n$ forms a Markov chain; therefore,

$$\frac{1}{n}\mathbb{I}\big(\mathsf{X}_1^n\mathsf{X}_2^n;\mathsf{Z}^n|\mathsf{C}_n\big) \leqslant \frac{1}{n}\mathbb{I}\big(\mathsf{X}_1^n\mathsf{X}_2^n;\mathsf{Z}^n\big) = \mathbb{I}(\mathsf{X}_1\mathsf{X}_2;\mathsf{Z}). \tag{8.20}$$

On substituting (8.18), (8.19), and (8.20) into (8.17), we obtain

$$\begin{aligned}\mathbb{E}\left[\frac{1}{n}\mathbf{L}(\mathcal{C}_n)\right] &\leqslant \mathbb{I}(\mathsf{X}_1\mathsf{X}_2;\mathsf{Z}) - R_{\mathrm{d},1} - R_{\mathrm{d},2} + \delta(\epsilon)\\ &= C(h_1P_1 + h_2P_2) - R_{\mathrm{d},1} - R_{\mathrm{d},2} + \delta(\epsilon).\end{aligned}$$

Note that, for any rate pair (R_1, R_2) such that

$$\begin{aligned}R_1 &< \left(C(P_1) - C\left(\frac{h_1P_1}{1 + h_2P_2}\right)\right)^+,\\ R_2 &< \left(C(P_2) - C\left(\frac{h_2P_2}{1 + h_1P_1}\right)\right)^+,\\ R_1 + R_2 &< (C(P_1) + C(P_2) - C(h_1P_1 + h_2P_2))^+,\end{aligned} \tag{8.21}$$

we can choose a rate pair $(R_{\mathrm{d},1}, R_{\mathrm{d},2})$ that satisfies

$$\begin{aligned}R_1 + R_{\mathrm{d},1} &< C(P_1) - \delta(\epsilon),\\ R_2 + R_{\mathrm{d},2} &< C(P_2) - \delta(\epsilon),\\ R_{\mathrm{d},1} + R_{\mathrm{d},2} &= C(h_1P_1 + h_2P_2) - \delta(\epsilon),\end{aligned}$$

so that R_1, $R_{\mathrm{d},1}$, R_2, and $R_{\mathrm{d},2}$ satisfy the constraints in (8.16). This choice then guarantees that

$$\mathbb{E}\left[\frac{1}{n}\mathbf{L}(\mathcal{C}_n)\right] \leqslant \delta(\epsilon).$$

By applying the selection lemma to the random variable C_n and the functions $\mathbf{P}_{\mathrm{e}}$ and $\mathbf{L}$, we conclude that there exists a specific code $\mathcal{C}_n = (\mathcal{C}_1, \mathcal{C}_2)$ such that $\mathbf{P}_{\mathrm{e}}(\mathcal{C}_n) \leqslant \delta(\epsilon)$ and $\mathbf{L}(\mathcal{C}_n) \leqslant \delta(\epsilon)$; hence, the rate pairs (R_1, R_2) satisfying (8.21) are achievable.

Remark 8.4. *Although the codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are generated according to independent distributions, note that the selection lemma selects the two codes* jointly*; therefore,*

the codes are used independently by Alice and Bob but optimized jointly to guarantee secrecy.

8.4 Key-exchange

The last scheme we analyze for the TWWTC combines some of the ideas of cooperative jamming with a simple feedback mechanism that allows one user to *transfer* part of its secret rate to the other user. The motivation for this scheme is the situation in which one of the channel gains is high, say $h_1 \gg 1$. On the one hand, Eve observes Alice's signals with a high SNR, which limits Alice's secure rates even if Bob jams. On the other hand, Eve greatly suffers from Alice's jamming, which increases Bob's secure rates. The increase in Bob's secure communication rates can be so great that it becomes advantageous for Alice to jam and help Bob send her a secret key, which she later uses to encrypt her messages with a one-time pad. The strategy we just described leads to the region of achievable rates specified in the following proposition.

Proposition 8.6 (He and Yener)**.** *The rate region $\mathcal{R}_{\text{fb}}$ defined by*

$$\mathcal{R}_{\text{fb}} \triangleq \bigcup_{\alpha\in[0,1]} \left\{ (R_1, R_2)\colon \begin{array}{l} 0 \leqslant R_1 < \alpha R_1^* \\ 0 \leqslant R_2 < (1-\alpha) R_2^* \end{array} \right\}$$

with

$$R_1^* = \max_{\beta\in[0,1]} \min \left(\beta C(P_1), \beta \left(C(P_1) - C\left(\frac{h_1 P_1}{1+h_2 P_2} \right) \right)^+ + (1-\beta) \left(C(P_2) - C\left(\frac{h_2 P_2}{1+h_1 P_1} \right) \right)^+ \right)$$

and

$$R_2^* = \max_{\beta\in[0,1]} \min \left(\beta C(P_2), \beta \left(C(P_2) - C\left(\frac{h_2 P_2}{1+h_1 P_1} \right) \right)^+ + (1-\beta) \left(C(P_1) - C\left(\frac{h_1 P_1}{1+h_2 P_2} \right) \right)^+ \right)$$

is achievable with cooperative jamming and key exchange.

Proof. We formalize the idea sketched earlier and we analyze a scheme that operates in two phases of $(1-\beta)n$ and βn channel uses, respectively, for some $\beta \in [0, 1]$. During the first $(1-\beta)n$ channel uses, Alice jams with Gaussian noise while Bob uses a wiretap code to transmit a secret key. Proposition 8.2 guarantees that Bob's key-transmission rate per n channel uses can be arbitrarily close to

$$R_{\text{f}} = (1-\beta) \left(C(P_2) - C\left(\frac{h_2 P_2}{1+h_1 P_1} \right) \right)^+ . \tag{8.22}$$

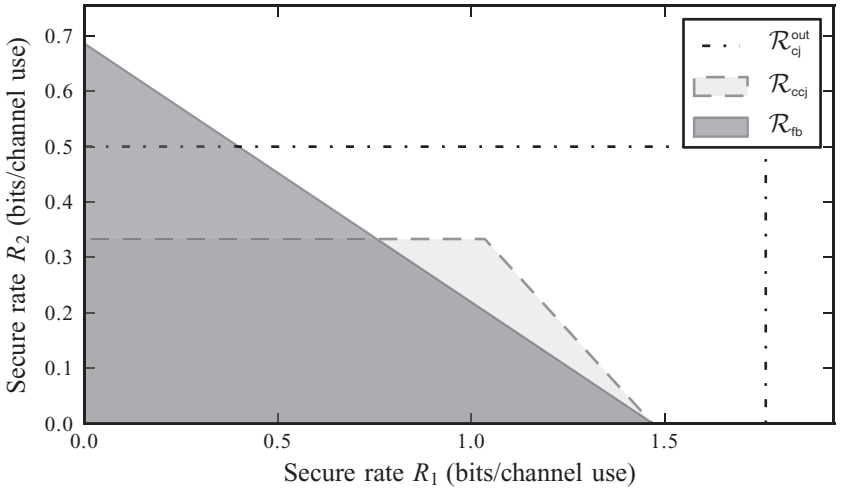

Figure 8.6 Regions $\mathcal{R}_{\text{ccj}}$, $\mathcal{R}_{\text{cj}}^{\text{out}}$, and $\mathcal{R}_{\text{fb}}$ for $h_1 = 0.2$, $h_2 = 1.3$, $P_1 = 20$, and $P_2 = 1$.

During the remaining βn channel uses, Bob jams with Gaussian noise while Alice transmits a secret message by combining a wiretap code and a one-time pad with the secret key sent by Alice as in Section 3.6.2. By Proposition 8.2 and Proposition 3.9, the secure transmission rate can be arbitrarily close to

$$\min\left(\beta C(P_1), \beta\left(C(P_1) - C\left(\frac{h_1 P_1}{1 + h_2 P_2}\right)\right)^+ + R_{\text{f}}\right). \tag{8.23}$$

On substituting (8.22) into (8.23) and optimizing over β we obtain the desired rate R_1^*. The rate R_2^* is obtained by swapping the roles of Alice and Bob, and the full region is obtained by time-sharing between these two modes of operation. □

The choice $\beta = 1$ in Proposition 8.6 eliminates the key-exchange phase of the scheme, which then reduces to the cooperative jamming in Section 8.2. Hence, we can conclude that $\mathcal{R}_{\text{cj}} \subseteq \mathcal{R}_{\text{fb}}$ for all channel parameters. The feedback scheme suffers from the same drawbacks as cooperative jamming, in that it forces either Alice or Bob to stop transmitting. Nevertheless, as illustrated in Figure 8.6, it is possible to find channel parameters for which the feedback scheme achieves rate pairs outside $\mathcal{R}_{\text{cj}}^{\text{out}}$; this result confirms that feedback and interference are fundamentally different mechanisms, thereby calling for coding schemes that combine the two techniques.

Remark 8.5. *The scheme described above is by no means the only possible scheme combining cooperative jamming and feedback. In fact, one can combine the key-exchange mechanism with coded cooperative jamming or adapt some of the key-distillation schemes described in Chapter 4. Unfortunately, it becomes rather difficult to obtain closed-form expressions for achievable rates.*

8.5 Bibliographical notes

Multi-user information-theoretic models with secrecy constraints have been the subject of intensive research. We provide a non-exhaustive but, we hope, representative list of references. Additional information can be found in the monograph of Liang *et al.* [147] and the book edited by Liu and Trappe [148].

The concept of coded cooperative jamming and cooperative jamming was introduced by Tekin and Yener for the two-way Gaussian wiretap channel and the K-user Gaussian multiple-access channel with multiple eavesdroppers [149]. The near-optimality of Gaussian noise for cooperative jamming over the two-way Gaussian wiretap channel was established by He and Yener [150] and by Bloch [151] using two different techniques. The proof developed in this chapter follows the approach of Bloch, and the property that $\mathbb{h}(Y|Z)$ is maximized for X Gaussian is due to Médard [152], an extension of which to MIMO channels was provided by Khisti and Wornell [83]. For the multiple-access channel, cooperative jamming with Gaussian noise and coded cooperative jamming with Gaussian codebooks is suboptimal, as was observed by Tang, Liu, Spasojević, and Poor [153, 154]. This suboptimality was confirmed by He and Yener, who recently showed that structured codebooks based on lattices outperform Gaussian codebooks, in general [155, 156]. The idea of cooperative jamming can be applied in many other settings, such as broadcast channels with cooperative receivers, as studied by Ekrem and Ulukus [157] and Bloch and Thangaraj [158], or from a secrecy-outage perspective in a wireless fading environment, as done by Vilela, Bloch, Barros, and McLaughlin [159]. Comprehensive discussions of cooperative jamming by He and Yener and by Ekrem and Ulukus can be found in [148, Chapter 4 and Chapter 7].

The role of interference in multi-user systems has been analyzed in various settings. For instance, Simeone and Yener [160] and Liang, Somekh-Baruch, Poor, Shamai, and Verdú [161] investigated cognitive channels with secrecy constraints, in which non-causal knowledge of other users' messages allows the legitimate user to interfere intelligently and to gain an advantage over the eavesdropper. In a slightly different setting, Mitrpant, Vinck, and Luo [162] investigated the combination of dirty-paper coding and wiretap coding and showed how knowledge of a non-causal interfering signal can be exploited for secrecy.

The importance of feedback for secure communications was originally highlighted in the context of secret-key agreement, which we discussed extensively in Chapter 4. Nevertheless, the study of secret-key capacity relies on the existence of a public channel with unlimited capacity, and recent works have analyzed the role of feedback without this assumption. For instance, Amariucai and Wei [163], Lai, El Gamal, and Poor [164], and Gündüz, Brown, and Poor [165] analyzed models in which the feedback takes place over a noisy channel but also interferes with the eavesdropper's observations. Ardestanizadeh, Franceschetti, Javidi, and Kim also analyzed a wiretap channel with rate-limited confidential feedback [34]. Note that most of these works can be viewed as special cases of the two-way wiretap channel. The key-exchange strategy for the two-way wiretap channel described in this chapter was proposed by He and Yener [150], and was combined with coded cooperative jamming by El Gamal, Koyluoglu, Youssef, and El Gamal [166]. All

these works show that, in general, strategies relying on feedback perform strictly better than do strategies without feedback. The secrecy capacity or secrecy-capacity region of channels with feedback remains elusive, although some headway has been made by He and Yener [167] for the two-way wiretap channel.

The study of feedback is one facet of the more general problem of cooperation for secrecy. For instance, the trade-off between cooperation and security has been studied in the context of relay channels with confidential messages by Oohama [168], Lai and El Gamal [169], Yuksel and Erkip [170], and He and Yener [171, 172, 173]. Among the conclusions that can be drawn from these studies is the fact that relaying improves the end-to-end communication rate between a source and a destination even if the relay is to be kept ignorant of the messages. An overview of "cooperative secrecy" by Ekrem and Ulukus can be found in [148, Chapter 7]

The generalization of the broadcast channel with confidential messages to multiple receivers and multiple eavesdroppers was studied by Khisti, Tchamkerten, and Wornell [174] as well as by Liang, Poor, and Shamai [85]. These results can be treated as special cases of the compound wiretap channels investigated by Liang, Kramer, Poor, and Shamai [175] and Bloch and Laneman [26]. Note that compound channels are relevant in practice because they offer a way of modeling the uncertainty that one might have about the actual channel to the eavesdropper. The generalization of the source models and channel models for secret-key agreement to multiple terminals has been investigated by Csiszár and Narayan [176, 177, 178] as well as by Nitinawarat, Barg, Narayan, Ye, and Reznik [179, 180].

In a slightly different spirit, the impact of security constraints in a network has been investigated by Haenggi [181] and Pinto, Barros, and Win [182] using tools from stochastic geometry. Secure communication in deterministic arbitrary networks has also been investigated by Perron, Diggavi, and Telatar [183].