Chapter 7
Cooperative Secrecy in Wireless Communications*

Ersen Ekrem and Sennur Ulukus

7.1 Introduction

The broadcast nature of wireless communications leads to two concepts: cooperation and secrecy. The basis for both cooperation and the potential lack of secrecy is the over-heard information at the unintended parties, which wireless communication channel provides for free. It is well-established that users can help increase each others' rates by intelligently using their over-heard information. It is also well-accepted that the leakage of information through the over-heard signals may cause loss of confidentiality and secrecy. Cooperation and secrecy have been studied individually over the past three decades following the seminal papers of van der Meulen [1] who introduced the relay channel, which is the simplest model for cooperative communications and Wyner [2] who introduced the wire-tap channel, which is the simplest model to study secrecy in communications. It is interesting to note that, both of these are simple three-node networks, where in the former, the sole purpose of the third node (relay) is to increase the achievable rate of the single-user channel between the transmitter and the receiver by transmitting signals based on its over-heard information, while in the latter, the third node (eavesdropper) is a passive entity which uses its over-heard information to extract as much information as possible about the messages transmitted in the single-user communication channel between the transmitter and the receiver. In this chapter, we will summarize the mostly separate literatures on cooperation and secrecy.

More recently, there has been a tremendous amount of interest and some initial work on the interactions of cooperation and secrecy. The recent literature on the

S. Ulukus (✉)
Department of Electrical and Computer Engineering
University of Maryland, College Park
MD 20742, USA
e-mail: ulukus@umd.edu

*Portions of the material have appeared previously in "Secrecy in Cooperative Relay Broadcast Channels," Proceedings of the IEEE International Symposium on Information Theory, 2008. ©IEEE 2008

R. Liu, W. Trappe (eds.), *Securing Wireless Communications at the Physical Layer*,
DOI 10.1007/978-1-4419-1385-2_7,

interactions of cooperation and secrecy can be divided into two groups: the first group includes channel models where there is a group of cooperating partners (either in a basic relay network or in a multiple access channel) and a separate external eavesdropper. It is clear that the cooperation among the users can increase both the achievable rates and the secrecy of the transmitting user. As we will see, there are various ways in which users can cooperate when secrecy is one of the objectives of cooperation; for instance, users may cooperate by relaying/forwarding each others' messages or by explicitly jamming the external eavesdropper, both of which resulting in the effective end result of improving the communication quality of the main link with respect to the communication quality of the eavesdropping link. In this chapter, we will summarize the recent literature on cooperation to improve secrecy in the presence of an external eavesdropper.

Perhaps a more complex and practically more relevant set of interactions arise between cooperation and secrecy, when we consider channel models where the potential cooperating partners are also treated as potential eavesdroppers. In this model, all nodes are active participants of a network, and are motivated to improve each others' rates, however, would also like to keep their messages as confidential as possible. Practical examples could be imagined, for instance, where there is a broadcast network where it is in the network's interest to improve rates through cooperation, however, the content of the messages may be viewed only by certain authorized users (who might have paid for the service). The central question in this context is: is there a trade-off or a synergy between cooperation and secrecy, i.e., does cooperation cause additional leakage of information (in addition to what wireless communication channel already provides as a result of over-heard information), or can cooperation improve secrecy by limiting or reversing the leakage of information? Although the entire scope of interactions between cooperation and secrecy is not fully understood yet, our and other researchers' recent results suggest that, whether there is a trade-off or synergy between cooperation and secrecy depends on the form of cooperation protocol being used. Very briefly: if cooperation is accomplished via a decode-and-forward type method, i.e., if the cooperating party is allowed (or required) to decode the message it is supposed to forward, then, cooperation and secrecy may be conflicting goals, however, if we require the cooperating party to forward the message without decoding it, as in compress-and-forward and amplify-and-forward type schemes, then cooperation may improve secrecy. This is mainly because, with such cooperating strategies, a cooperating party would increase the rate of the main link to levels which are not decodable at the cooperating party itself. In this chapter, we will summarize the recent literature on the interactions of cooperation and secrecy when the legitimate users of the network are viewed as potential eavesdroppers.

7.2 Cooperation

The relay channel, which is the simplest model of a cooperative network, was introduced more than three decades ago by van der Meulen [1]. The relay channel, which is shown in Fig. 7.1, consists of three nodes: a transmitter, a relay, and a receiver.

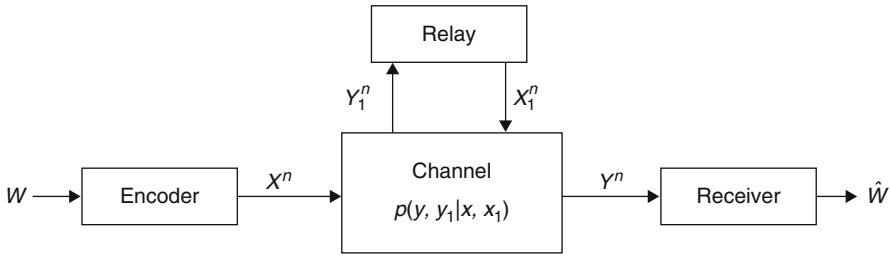

Fig. 7.1 The relay channel

The sole purpose of the relay node is to help increase the rate of communication between the transmitter and the receiver. Despite the simplicity of its model, the capacity of the general relay channel is still an open problem. The landmark paper on the relay channel is Cover and El Gamal's 1979 paper [3] which proposed the two basic cooperation strategies, which are still the best-known achievable schemes today: decode-and-forward (DAF) and compress-and-forward (CAF).

Both DAF and CAF are block coding schemes. In DAF, the relay decodes the message of the current block in its entirety and sends a cooperative signal in the next block, which helps the receiver to decode the message sent by the transmitter in the previous block. The original work of Cover and El Gamal uses irregular encoding (which refers to different codebook sizes at the transmitter and the relay), block Markov superposition encoding, random partitioning, and successive decoding. Later, Carleial [4] and Willems [5] showed that the same rates can be achieved using codebooks of identical sizes at the relay and the transmitter with sliding-window or backward decoding methods. DAF can achieve rates up to

$$\max_{p(x,x_1)} \min\{I(X; Y_1|X_1), I(X, X_1; Y)\}. \tag{7.1}$$

The first term inside the min comes from the fact that the relay needs to decode the message in its entirety. The second term can be interpreted as the rate of a multiple access channel (MAC) from the transmitter and the relay to the receiver, where the two transmitters have a common message to send. This rate is achievable since the relay decoded the message sent by the transmitter, and therefore constructed a common message. The main drawback of DAF is that it restricts the overall achievable rate by the achievable rate of the transmitter-relay link. To overcome this difficulty, [3] proposed the CAF scheme.

In CAF, the relay node does not try to decode the message, instead it sends a quantized and compressed version of its observation to the receiver. The receiver exploits the statistical dependence of the channel outputs at the relay and the receiver to decode the message intended for it. In this case, the quality of the quantization and compression at the relay node plays a crucial role. This, in turn, depends on the rate of the relay-receiver link. For example, if the relay could convey its observation to the receiver perfectly (i.e., infinite-capacity relay-receiver link), then rates up to

$$\max_{p(x)} I(X; Y, Y_1) \tag{7.2}$$

would be achievable. This is the rate that would be achievable if the receiver had two antennas. Since the relay-receiver link is noisy, the achievable rate of the CAF scheme is smaller. The rates achievable by CAF are given as

$$\max_{p(x)p(x_1)} I(X;\hat{Y}_1,Y|X_1) \tag{7.3}$$

where the random variables in Eq. (7.3) are subject to the constraint

$$I(X_1;Y) \geq I(\hat{Y}_1;Y_1|X_1,Y) \tag{7.4}$$

where $\hat{Y}_1$ denotes the compressed version of Y_1, the observation of the relay. The constraint in Eq. (7.4) relates the quality of compression to the rates achievable between the relay and the receiver. As we alluded to earlier, the main advantage of CAF is that the relay does not need to decode the message itself in order to help the receiver. This aspect of CAF will become crucial when we impose a secrecy constraint on the relay node.

In the basic relay network, we have a dedicated relay node whose sole purpose is to help increase the rate of the transmitter by utilizing its observation which is correlated with the transmitted message. This basic idea can be generalized to larger networks, where all nodes have their own messages to send, and have observations which are correlated with the transmitted messages of the other users in the network. The simplest such example is the multiple access channel with generalized feedback (MAC-GF), which is shown in Fig. 7.2, where each user has a different feedback signal which is correlated with the message of the other user. For this channel, strategies similar to DAF and CAF can be used, after appropriate modifications are done, so that the messages of the users are superimposed with the cooperative signals. This channel model was studied by King [6] and Cover and Leung [7] for the special case of common feedback, i.e., $Y_1 = Y_2 = Y^*$, and by Carleial [4] and Willems [5] for the general case of different feedback signals at the two transmitters. Achievable schemes presented in [4–7] basically rely on the DAF principle of [3], where both users decode (completely or partially) the cooperation signals. The differences in these papers lie in their encoding and decoding strategies. For example, Carleial uses regular encoding with sliding-window decoding, while Willems uses

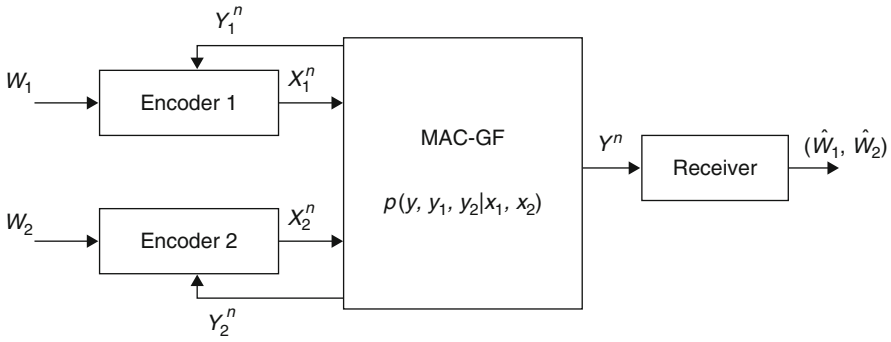

Fig. 7.2 MAC with generalized feedback

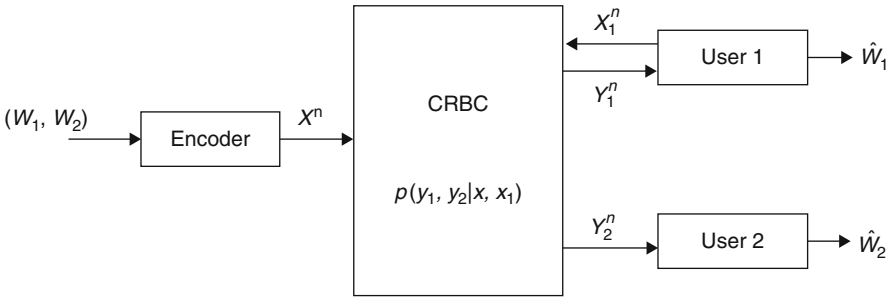

Fig. 7.3 Cooperative relay broadcast channel

regular encoding with backward decoding. In contrast to DAF, CAF has attracted less attention in the context of MAC-GF. References [8] and [9] consider CAF-type cooperation in MAC-GF. The relative performances of DAF and CAF in MAC-GF depends on many parameters. Generally speaking, if the inter-user links are relatively better than the user-receiver links, then DAF performs better, while if the user-receiver links are better than the inter-user links, then CAF performs better.

Recently, Sendonaris, Erkip, and Aazhang [10], employed DAF-based coding schemes developed for MAC-GF in fading cellular wireless communication systems to demonstrate significant gains in achievable rates, and introduced the concept of user cooperation diversity. More recently, [11] combined the concepts of user cooperation and power control to further improve rates with respect to the rates that are achievable by cooperation-only and power-control-only schemes; while user cooperation exploits spatial diversity and power control exploits time diversity in a fading wireless channel, the approach in [11] exploits both forms of diversity simultaneously.

The "dual" of MAC-GF is the broadcast channel with cooperating decoders, where the cooperation is done on the receiver side, using the links between the receivers. We will refer to this channel model as the cooperative relay broadcast channel (CRBC), see Fig. 7.3. Although Fig. 7.3 shows a one-sided cooperation link between the receivers, its extension to two-sided cooperation case is straightforward. This channel model was studied extensively in [12–14]. Similar to the basic relay channel model, since each user's observation contains some information about the message intended for the other user, the users can serve as relays for each another. Hence, the basic DAF and CAF schemes can be modified accordingly to find achievable rates in this channel model as well.

7.3 Information Theoretic Secrecy

The first information theoretic treatment of communication secrecy is due to Wyner [2] who considered a wiretap channel, see Fig. 7.4, where there is a transmitter, a receiver and a wiretapper, which wants to extract as much information as possible about the ongoing legitimate communication, using its over-heard information.

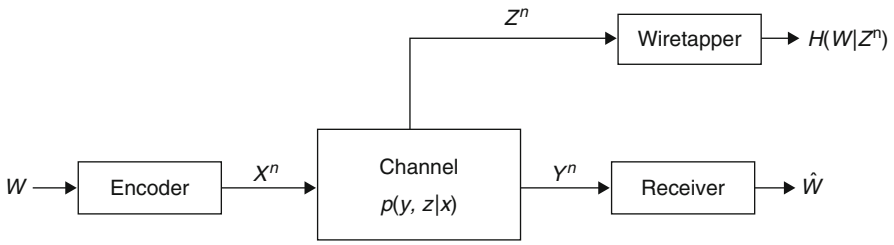

Fig. 7.4 The wiretap channel

Wyner considered a special kind of wiretap channel, called the degraded wiretap channel, where the signal that the wiretapper gets is a degraded version of the signal that the receiver observes. Wyner measured the secrecy of communication by the conditional entropy of the message given the channel output of the wiretapper. This quantity is termed as the equivocation-rate and is given by

$$\frac{1}{n}H(W_1|Z^n). \tag{7.5}$$

The equivocation-rate reflects the remaining uncertainty in the message given the wiretapper's channel observation. A rate pair (R_1, R_e) is said to be achievable if rate R_1 is achievable with vanishingly small probability of error while R_e satisfies

$$\lim_{n\to\infty} \frac{1}{n}H(W_1|Z^n) \geq R_e. \tag{7.6}$$

When the equivocation-rate of the message is equal to the message rate, i.e., $R_1 = R_e$, we say that these rates are achievable with perfect secrecy. Correspondingly, the maximum of such rates is called the secrecy capacity. Wyner's wiretap channel is a degraded wiretap channel in the sense that the involved random variables satisfy the following Markov chain

$$X \to Y \to Z. \tag{7.7}$$

For this channel, Wyner determined the rate equivocation-rate region, i.e., the set of all achievable (R_1, R_e) pairs. The secrecy capacity of this channel, i.e., the largest achievable R_1 such that $R_1 = R_e$, is

$$C^s = \max_{p(x)} I(X;Y|Z) = \max_{p(x)} [I(X;Y) - I(X;Z)] \tag{7.8}$$

where the second equality follows from the degradedness condition in Eq. (7.7). The secrecy capacity in Eq. (7.8) can be interpreted as being the largest difference between the receiver's and the wiretapper's achievable rates. Therefore, to be able to transmit all of its messages with perfect secrecy, the wiretapper needs to "sacrifice" the following amount of rate

$$I(X;Z) \tag{7.9}$$

from its otherwise achievable rate $I(X;Y)$. The rate in Eq. (7.9) that the transmitter should give up as the price for perfect secrecy corresponds to the amount of rate the wiretapper can decode.

Following Wyner's work, Csiszar and Korner [15] considered the general, not necessarily degraded, wiretap channel and found the rate equivocation-rate region. Csiszar and Korner consider a much general setup, where a transmitter not only wants to send a confidential message to one of the receivers, but also wants to send a common (public) message to both receivers. In this case, the eavesdropper may be thought of as another legitimate user in the system, in the sense that the transmitter wishes to send a message to it. Besides finding the capacity region of such a general wiretap channel, another important contribution of [15] is its converse technique, which in years since then, has been the standard method to prove converses in various secrecy problems. Yet another fundamental contribution of [15] is the introduction of an auxiliary random variable, which plays a crucial role in the secrecy of general, not necessarily degraded, wiretap channels. After showing that the following secrecy rates

$$I(X;Y) - I(X;Z) \tag{7.10}$$

are achievable with perfect secrecy for all $p(x)$, Csiszar and Korner introduce a memoryless channel with input V and outputs Y, Z. Since any encoder defined for this channel can be properly modified using the conditional distribution of X conditioned on V, this new channel can achieve the following secrecy rates

$$I(V;Y) - I(V;Z). \tag{7.11}$$

By the nature of the new channel from V to Y, Z, we need to have the following Markov chain satisfied

$$V \to X \to (Y, Z). \tag{7.12}$$

The operation of creation of V is referred to as "channel prefixing" and the processing from the message carrying signal V to the channel input X is called "pre-processing."

We note that Eq. (7.11) has the same interpretation as Eq. (7.8): it can be viewed as the maximum difference between the achievable rates of the receiver and the wiretapper, where now the maximum is taken over all channel input distributions $p(x)$ and pre-processing $p(x|v)$. This *stochastic* encoding from the message carrying signal V to the channel input X can be interpreted as introducing additional randomness to both channels, i.e., the main channel from X to Y and the eavesdropping channel from X to Z. Clearly, this additional randomness will hurt both of the achievable rates. This can be seen by observing that $I(V;Y) \leq I(X;Y)$ and $I(V;Z) \leq I(X;Z)$ from the data processing inequality [16] applied to the Markov chain in Eq. (7.12). The auxiliary random variable V will be useful in channels where the decrease in the rate due to the use of the auxiliary random variable is more in the eavesdropper link than in the main link.

We note that the selection of $V = X$ (i.e., no pre-processing) is in general potentially suboptimal. We also note that, despite this, for all the channels where secrecy capacity has been identified, e.g., the scalar Gaussian channel [17], the parallel Gaussian channel which also models the fading Gaussian wiretap channel where all the parties know the instantaneous realizations of all the fading channel gains [18, 19], and the MIMO Gaussian channel [20–22], this selection has been shown to be optimal. However, there are channels, such as the fading Gaussian wiretap channel without channel state information of the wiretapper at the transmitter [23], it was shown that choosing $V = X$ is strictly suboptimal. Finally, we note that, for some channels, the secrecy capacity is attained when both the main channel and the wiretapper channel operate at their own capacity achieving distributions, i.e., the $p(x)$ that maximizes the difference in Eq. (7.8) is the same as the $p(x)$ that maximizes $I(X;Y)$ and $I(X;Z)$ individually. The scalar Gaussian channel [17] is such an example. Note that this is not true for the MIMO Gaussian channel [20–22].

After the pioneering works in [2, 15], secrecy of multi-user systems has been studied only recently. Even though there has been a recent surge of papers on various aspects of multi-user secrecy, here, for the sake of compactness, we will only refer to the part of the literature which relates to the interactions of cooperation and secrecy. These works can be broadly classified into three groups.

The first group contains the works where cooperation is accomplished without the cooperating party using its over-heard information. This is different than the classical sense of cooperation, where the cooperating party uses its over-heard information to "strengthen" the main link. In this first group, the cooperating party improves the relative strength of the main link by weakening the eavesdropping link. We call this class of cooperation *oblivious cooperation* since the cooperating party does not use its over-heard information. We will further partition this group of works into two: in the first sub-group, cooperation is accomplished by cooperating user sending dummy codewords from a codebook, akin to Wyner's idea of associating multiple codewords with a message. We will discuss this kind of cooperation under the title of *implicit cooperation and noise forwarding*. In the second sub-group, the cooperating party sends explicit jamming signals. This is akin to Csiszar and Korner's idea of channel prefixing by introducing an auxiliary random variable. In Gaussian channels, the additional randomness that can be introduced by pre-processing from V to X can be interpreted as *jamming*. We will discuss this kind of cooperation under the title of *cooperative jamming and artificial noise*. Instances of such oblivious cooperation arise in the MAC with an external wiretapper (MAC-WT), the interference channel, and the relay-eavesdropper channel with an external eavesdropper, where the relay does not make use of its over-heard information. We will focus on these two kinds of oblivious cooperation in Sect. 7.4.

The second group contains the works where the cooperating party helps the main link in the classical sense of cooperation, i.e., it strengthens the main link by using its over-heard information. The basic channel model for this group is the relay-eavesdropper channel, where we have a standard relay channel and an external

eavesdropper. In this case, the relay node helps the transmitter-receiver pair by using DAF and CAF cooperation schemes. These schemes increase both achievable rates and the equivocation-rates. We will focus on this kind of active cooperation in Sect. 7.5.

The third group contains the works where secrecy constraints are placed on the cooperating parties themselves. The basic question here is: can an eavesdropper help increase the secrecy of a transmitter by sending cooperation signals? The basic channel models to investigate these seemingly contradicting goals of a relay node are the relay channel, MAC-GF and CRBC. We will focus on this kind of interaction between cooperation and secrecy in Sect. 7.6.

7.4 Oblivious Cooperation for Secrecy

In this section, we discuss cooperation strategies where the cooperating party (we will also refer to it as the helper) does not need to have any information regarding the transmitted message. Here, the helper either does not have a channel output (as in MAC-WT), or even if it does (as in the relay-eavesdropper channel), it ignores it. We will discuss two different cooperation strategies.

In the first one, the helper sends a portion of the dummy codewords that the transmitter needs to send to have secrecy. These dummy codewords refer to Wyner's idea of associating multiple codewords with a single message. Since the cost of these dummy codewords is a decrease in the transmitter's rate, if the helper takes the responsibility of sending these dummy codewords, then the secrecy rate of the transmitter may improve. The amount of improvement depends on the relative strengths of the helper-receiver and the helper-eavesdropper links. If the helper-receiver link is stronger, then the secrecy rate of the transmitter can be improved. However, if the helper-eavesdropper link is stronger, then, since the eavesdropper can decode these dummy codewords, the helper will not be able to improve the secrecy rate of the transmitter.

The second oblivious cooperation strategy we will discuss aims to overcome this drawback. If the helper-eavesdropper link is stronger, then the helper may more explicitly *attack* the eavesdropper. We note though that when the helper attacks the eavesdropper, by the broadcast nature of wireless communications, it attacks the main receiver as well. The hope of the helper is that even though it attacks both the eavesdropper and the main receiver, it hurts the eavesdropper more. In Gaussian channels, this attack can be in the form of injecting additional noise to the channel. In a more abstract level, the attack of the helper can be interpreted as sending independent codewords whose rate is above the decoding capability of both the eavesdropper and the receiver. In addition, this jamming attack can be interpreted as using an explicit auxiliary random variable in the achievable rates, as in the channel prefixing idea of Csiszar-Korner. As we alluded to earlier, the effect of the auxiliary random variable is to introduce additional randomness to both the eavesdropper and the main link; and in a Gaussian channel, jamming will correspond to a certain kind of auxiliary random variable selection, as we will show later.

7.4.1 Implicit Cooperation and Noise-Forwarding

In this section, we discuss the cooperation strategy where the helper sends a portion of the non-information-bearing codewords to improve the secrecy of the transmitter. This cooperation strategy can be used in MAC-WT where the helper does not have a channel output, or in the relay-eavesdropper channel where the helper (the relay) may not want to use its over-heard information. We will start with MAC-WT; see Fig. 7.5.

This channel model is first studied in [24, 25]. In this channel, in addition to equivocation-rates measuring each user's individual secrecy, we need to have a joint equivocation-rate to account for the loss of secrecy if the eavesdropper uses a joint decoding strategy

$$\frac{1}{n}H(W_1|Z^n), \quad \frac{1}{n}H(W_2|Z^n), \quad \frac{1}{n}H(W_1,W_2|Z^n) \tag{7.13}$$

where the last term will dictate that the message pair (W_1, W_2) should not be jointly decodable by the eavesdropper. Using these secrecy constraints, we can show that we have the following *perfect secrecy* achievable region

$$R_1 \leq [I(V_1;Y|V_2) - I(V_1;Z)]^+ \tag{7.14}$$

$$R_2 \leq [I(V_2;Y|V_1) - I(V_2;Z)]^+ \tag{7.15}$$

$$R_1 + R_2 \leq [I(V_1,V_2;Y) - I(V_1,V_2;Z)]^+ \tag{7.16}$$

for any distribution of the form

$$p(v_1)p(v_2)p(x_1|v_1)p(x_2|v_2)p(y,z|x_1,x_2) \tag{7.17}$$

where $(x)^+$ denotes $\max(0,x)$, and these rates are perfect secrecy rates in the sense that rates R_1 and R_2 are achievable with the equivocation-rates of $R_{e,1} = R_1$ and

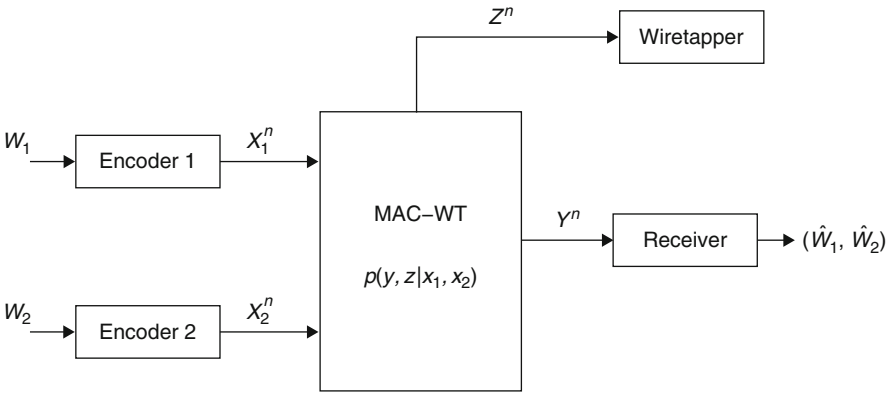

Fig. 7.5 MAC wiretap channel

$R_{e,2} = R_2$. The perfect secrecy rates in Eqs. (7.14–7.16) are the most general achievable rates for MAC-WT reported anywhere so far. Although we skip the details here, these rates can be obtained from the rates presented in [24, 25] by using channel prefixing and by introducing two independent auxiliary random variables V_1 and V_2 for users 1 and 2, respectively. The introduction of the auxiliary random variables is not trivial and it will play a crucial role in our exposition below, especially in the next section.

From a cooperation point of view, an interesting implication of the achievable region in Eqs. (7.14–7.16) is that it represents an *implicit cooperation* between users. To see this, assume that the rate pair (R_1, R_2) is on the sum-rate line. For users to operate on this line, they need to *jointly* "sacrifice" a total rate of

$$I(V_1, V_2; Z) \tag{7.18}$$

from their otherwise achievable sum-rate of $I(V_1, V_2; Y)$. However, how this total rate is shared among the users, i.e., how much rate each user has to give up is not clear at this point. To understand how this rate might be shared among the users, first note that the sum-rate line lies between the following two points:

$$\text{Point A:} \quad R_1 = I(V_1; Y|V_2) - I(V_1; Z) \tag{7.19}$$

$$R_2 = I(V_2; Y) - I(V_2; Z|V_1), \tag{7.20}$$

$$\text{Point B:} \quad R_1 = I(V_1; Y) - I(V_1; Z|V_2) \tag{7.21}$$

$$R_2 = I(V_2; Y|V_1) - I(V_2; Z). \tag{7.22}$$

If the system operates at Point A, then user 1 acts as if it is in a single-user wiretap channel and "sacrifices" a rate of

$$I(V_1; Z) \tag{7.23}$$

which also is the largest rate that the eavesdropper can decode without cancelling user 2's signal. However, user 2, besides decreasing its achievable rate from a possible $I(V_2; Y|V_1)$ to $I(V_2; Y)$, also puts more dummy codewords to the channel, namely at the rate of $I(V_2; Z|V_1)$, to ensure that the sum-rate secrecy constraint is satisfied. If user 1 starts putting more dummy codewords to the channel, then user 2's secrecy rate begins to increase, and the operating point moves away from Point A and eventually reaches Point B where the roles of the two users are reversed.

To solidify these ideas, let us introduce the Gaussian MAC-WT

$$Y = X_1 + X_2 + N_1 \tag{7.24}$$

$$Z = \sqrt{h_1} X_1 + \sqrt{h_2} X_2 + N_2 \tag{7.25}$$

where N_1, N_2 are independent zero-mean Gaussian random variables with unit-variance, h_1, h_2 denote the channel gains of the eavesdropper channel. Here, we will assume that h_1 and h_2 satisfy

$$h_1 \leq \frac{1}{1 + P_2}, \quad h_2 \leq \frac{1}{1 + P_1} \tag{7.26}$$

to ensure that both users have positive secrecy rates in their corresponding single-user channels, and that the region in Eqs. (7.14–7.16) takes the form of a non-degenerate pentagon. Moreover, we impose the usual power constraints on X_1, X_2 as $E[X_1^2] \leq P_1$ and $E[X_2^2] \leq P_2$.

The optimal selection of the random variables V_1, V_2, X_1, X_2 in Eqs. (7.14–7.16) is an open problem. If we select both $V_1 = X_1$ and $V_2 = X_2$ (i.e., no pre-processing) and X_1 and X_2 to be Gaussian with zero-mean and variances P_1, P_2, respectively, the rate region in Eqs. (7.14–7.16), becomes

$$R_1 \leq \frac{1}{2}\log\left(1+P_1\right) - \frac{1}{2}\log\left(1+\frac{h_1P_1}{h_2P_2+1}\right) \tag{7.27}$$

$$R_2 \leq \frac{1}{2}\log\left(1+P_2\right) - \frac{1}{2}\log\left(1+\frac{h_2P_2}{h_1P_1+1}\right) \tag{7.28}$$

$$R_1+R_2 \leq \frac{1}{2}\log\left(1+P_1+P_2\right) - \frac{1}{2}\log\left(1+h_1P_1+h_2P_2\right). \tag{7.29}$$

For this selection of random variables, Point A is

$$\text{Point A:} \quad R_1 = \frac{1}{2}\log\left(1+P_1\right) - \frac{1}{2}\log\left(1+\frac{h_1P_1}{h_2P_2+1}\right) \tag{7.30}$$

$$R_2 = \frac{1}{2}\log\left(1+\frac{P_2}{P_1+1}\right) - \frac{1}{2}\log\left(1+h_2P_2\right) \tag{7.31}$$

where user 2 takes the responsibility of transmitting more of

$$\frac{1}{2}\log\left(1+h_1P_1+h_2P_2\right). \tag{7.32}$$

Consequently, operating at Point A, user 1 benefits from the presence of user 2. If the second user did not exist in the system, the maximum secrecy rate user 1 could achieve would be

$$\frac{1}{2}\log\left(1+P_1\right) - \frac{1}{2}\log\left(1+h_1P_1\right) \tag{7.33}$$

which is strictly smaller than Eq. (7.30). This shows that although user 2 does not know anything about user 1's message, it can still help to improve user 1's secrecy rate by sending independent dummy codewords. The dummy codewords user 2 has, in effect, serves to "enlarge" the size of dummy codewords user 1 associates with any given message, as in the original idea of Wyner.

In the above example, we assumed that $h_1, h_2 < 1$ through Eq. (7.26) to ensure that each user had positive secrecy rates even without the help of the other user, i.e., in a corresponding single-user channel. Let us now look at another case, where one of the users does not have positive secrecy in the absence of the other user. In particular, let us assume that $h_1 > 1$. From Eq. (7.33), it is clear that user 1 cannot have a positive secrecy rate in its corresponding single-user channel. This is

essentially because, the rate user 1 has to "sacrifice" in order to have perfect secrecy, i.e., $(1/2)\log(1+h_1P_1)$ is larger than the rate its main receiver can "afford", i.e., $(1/2)\log(1+P_1)$. However, if we can get user 2 to carry the responsibility of some of the rate to be "sacrificed," then we may be able to provide positive secrecy rate for user 1.

To demonstrate that, let us assume that $h_2 < 1$, i.e., user 2 is able to have a positive secrecy rate in the absence of user 1. Since user 2's overall link is better than user 1's, user 2 can pay a portion of the rate to be "sacrificed." Furthermore, if h_1, h_2 satisfy

$$h_1 \leq 1 + h_2P_2, \quad h_2 \leq \frac{1}{1+P_1} \tag{7.34}$$

both rates in Eq. (7.30) and in Eq. (7.31) will be positive. Thus, this example demonstrates that, although user 1 cannot have a positive secrecy rate in its corresponding single-user channel, user 2 can help it to have a positive secrecy rate by taking the responsibility of "confusing" the receiver on user 1's behalf. We remark that for this type cooperation to be effective, the helper's link to the receiver should be stronger than its link to the eavesdropper. For example, if we had $h_1, h_2 > 1$, then sum-rate would vanish with this kind of scheme and no one can have positive secrecy.

In the above examples, we assumed $V_1 = X_1$, $V_2 = X_2$ and X_1, X_2 are Gaussian random variables. As a more general comment, we can say that, if for every V_2, we have

$$I(V_2;Y) \leq I(V_2;Z) \tag{7.35}$$

then the eavesdropper can decode whatever user 2 sends, and consequently, its taking part in the transmission of user 1's dummy codewords cannot provide any gain for the secrecy of user 1. Nevertheless, to summarize the discussion above, with the achievable rates in Eqs. (7.14–7.16) (which are in general sub-optimal), and with the selection of random variables as $V_1 = X_1$, $V_2 = X_2$ and X_1, X_2 as Gaussian (which are also sub-optimal), the existence of user 2 in the system may improve the single-user perfect secrecy rate of user 1 (as in the first example), and provide a positive perfect secrecy to user 1, even when the single-user perfect secrecy rate of user 1 is zero (as in the second example).

A technique called *noise forwarding* is proposed in [26], where in a relay eavesdropper channel (see Fig. 7.6), the relay disregards its channel observation, and sends dummy codewords from a codebook. The ultimate receiver performs successive decoding, where it first decodes the dummy codeword of the relay, and then decodes the message of the transmitter. It was shown in [26] that the following perfect secrecy rate is achievable

$$\begin{aligned} &I(V_1;Y|V_2) + \min\left[I(V_2;Y), I(V_2;Z|V_1)\right] \\ &\qquad - \min\left[I(V_2;Y), I(V_2;Z)\right] - I(V_1;Z|V_2) \end{aligned} \tag{7.36}$$

for any joint distribution of the form

$$p(v_1)p(v_2)p(x|v_1)p(x_1|v_2)p(y,y_1,z|x,x_1). \tag{7.37}$$

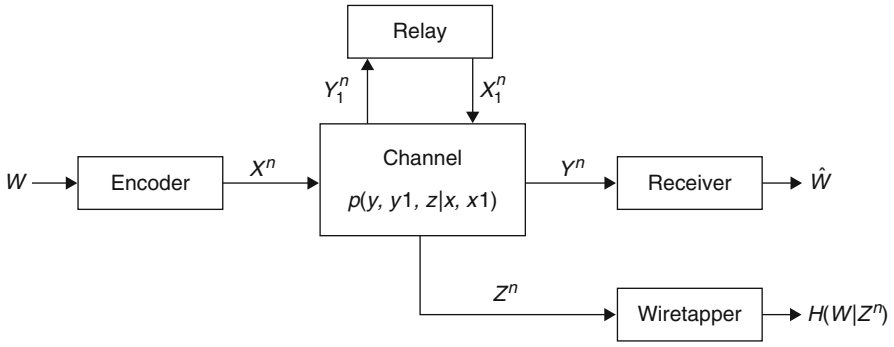

Fig. 7.6 Relay-eavesdropper channel

An alternative decoding strategy for the receiver could be a joint decoding strategy, in which case, the following perfect secrecy rate can be shown to be achievable

$$R_1 \leq I(V_1; Y|V_2) - I(V_1; Z) \tag{7.38}$$

$$R_1 \leq I(V_1, V_2; Y) - I(V_1, V_2; Z) \tag{7.39}$$

for any joint distribution of the form given in Eq. (7.37). We note that the rates in Eqs. (7.38, 7.39) can be obtained from Eqs. (7.14–7.16) by setting $R_2 = 0$. Therefore, we conclude that, the noise forwarding scheme proposed in [26] can be interpreted as an implicit cooperation scheme which is described above. References [27, 28] combine *implicit cooperation* with more explicit *jamming-type* cooperative strategies that we will discuss in the next section, to come up with achievable schemes for the interference channel (see Fig. 7.7), where one of the users does not have a message to send but acts as a pure interferer for both receivers.

Finally, we note that for the rates in Eq. (7.36) and in Eqs. (7.38, 7.39) to be larger than

$$I(V_1; Y|V_2) - I(V_1; Z|V_2) \tag{7.40}$$

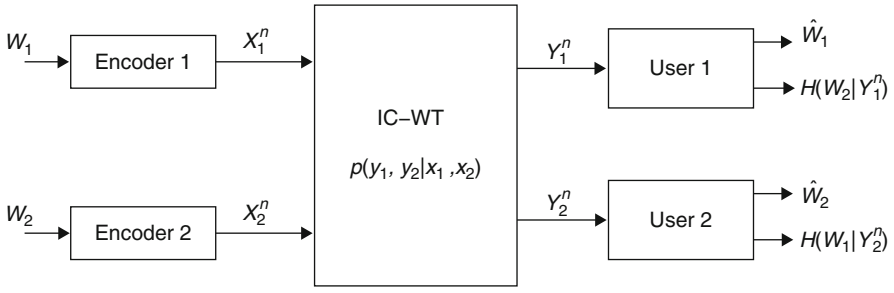

Fig. 7.7 Interference channel with confidential messages

which is the rate obtained when both the eavesdropper and the receiver are able to decode the relay's dummy codewords, we need

$$I(V_2; Z) \leq I(V_2; Y) \tag{7.41}$$

which is equivalent to saying that the helper-receiver link is stronger than the helper-eavesdropper link. Thus, if the helper-eavesdropper link is stronger than the helper-receiver link, then this kind of *implicit* cooperation strategies may not improve the secrecy rates. In such cases, we need more *explicit* cooperation strategies, which can be interpreted as *jamming*, which we will discuss in detail in the next section.

7.4.2 Cooperative Jamming and Artificial Noise

In the previous section, we assumed that at least one of the users has a relatively stronger channel to the main receiver and it was able to help the other user by sending dummy codewords, which had the end effect of enlarging the dummy codebook size of the user being helped. We now move on to an opposite situation and ask whether the user with a relatively weaker main channel can help the other user. To gain insight, we consider the Gaussian MAC-WT with $h_1 < 1 < h_2$. Here, user 2 is the weaker of the two users. We go back to the set of achievable secrecy rates in MAC-WT given in Eqs. (7.14–7.16), and pick the random variables as $X_1 = V_1$ and $X_2 = U_2$, where V_1 and U_2 are independent Gaussian random variables with zero-mean and variances P_1 and P_2, respectively, and are independent of V_2. With this selection, the achievable secrecy rate for user 1 given in Eq. (7.14) becomes

$$\frac{1}{2}\log\left(1+\frac{P_1}{P_2+1}\right)-\frac{1}{2}\log\left(1+\frac{h_1P_1}{h_2P_2+1}\right) \tag{7.42}$$

as compared to its single-user perfect secrecy rate

$$\frac{1}{2}\log\left(1+P_1\right)-\frac{1}{2}\log\left(1+h_1P_1\right). \tag{7.43}$$

We note that the rate in Eq. (7.42) is strictly larger than the rate in Eq. (7.43) for certain range of values for h_1 and h_2. Furthermore, if we select the channel gains as $1 < h_1 < h_2$, then the rate in Eq. (7.43) is negative while the rate in Eq. (7.42) can be positive.

This strategy was proposed in [25] and was named *cooperative jamming*. Reference [25] uses a Wyner-type achievable scheme with Gaussian signalling and does not employ auxiliary random variables. After observing that, in a situation where $h_2 > 1$, the second user cannot have positive secrecy, [25] proposes that, user 2 may transmit Gaussian noise to jam the eavesdropper, and in effect, help the first user, hence the name *cooperative jamming*. As noted in [25], this jamming will hurt both the eavesdropper and the main receiver due to the broadcast nature of wireless communications, and it will result in an improvement in the secrecy rate of user 1, if

it hurts the eavesdropper more. In the above discussion, we showed that cooperative jamming can be extracted via a special kind of auxiliary random variable selection from our achievable rates in Eqs. (7.14–7.16).

As a possible extension, one can consider "mixed" auxiliary random variable selection as $X_1 = V_1 + U_1$ and $X_2 = V_2 + U_2$, where V_1, U_1, V_2 and U_2 are all independent Gaussian random variables with variances αP_1, $(1-\alpha)P_1$, βP_2 and $(1-\beta)P_2$, respectively, where $0 \leq \alpha, \beta \leq 1$. Note that, with this selection, the powers of X_1 and X_2 come out to be P_1 and P_2. This selection corresponds to each transmitter dividing its signal into two: a component that carries the message (V_i) and a component that jams the channel (U_i). We note that all transmission schemes discussed so far can be viewed as special case of this general scheme where we took α and β to be either 0 or 1. We need to note that this mixed strategy of joint signal transmission and jamming does not improve the rates achievable by Eqs. (7.14–7.16), i.e., if we insert these "mixed" random variables into the achievable rates in Eqs. (7.14–7.16) and optimize the achievable rates over all α, β in $[0, 1]$, we observe that we should choose α and β to be either 0 or 1. This means that each user should either send a useful message without pre-processing, or it should send complete jamming signal without any signal component [25].

Similar ideas have been developed in the context of the interference channel with secrecy constraints. Consider the interference channel shown in Fig. 7.7 where there are two transmitters and two receivers, and each transmitter wishes to communicate with one of the receivers treating the other receiver as an eavesdropper. Reference [29] showed that the following set of rates are achievable with perfect secrecy

$$R_1 \leq I(V_1; Y_1) - I(V_1; Y_2|V_2) \tag{7.44}$$

$$R_2 \leq I(V_2; Y_2) - I(V_2; Y_1|V_1) \tag{7.45}$$

for any joint distribution of the form

$$p(v_1)p(v_2)p(x_1|v_1)p(x_2|v_2)p(y_1, y_2|x_1, x_2). \tag{7.46}$$

To understand how previous cooperation strategy can be effective in this channel, let us introduce the Gaussian interference channel

$$Y_1 = X_1 + \sqrt{\alpha_1} X_2 + N_1 \tag{7.47}$$

$$Y_2 = \sqrt{\alpha_2} X_1 + X_2 + N_2 \tag{7.48}$$

where N_1, N_2 are zero-mean, unit-variance Gaussian random variables. Moreover, we again have power constraints on X_1, X_2 as $E[X_1^2] \leq P_1$ and $E[X_2^2] \leq P_2$.

To see how a jamming strategy can improve the rates in this case, let us first assume that both users send only their useful messages using Gaussian codebooks, i.e., let us pick $V_1 = X_1$ and $V_2 = X_2$ and X_1 and X_2 to be Gaussian with zero-mean and variances of P_1 and P_2, respectively. This selection leads to the following rate

region

$$R_1 = \frac{1}{2}\log\left(1 + \frac{P_1}{\alpha_1 P_2 + 1}\right) - \frac{1}{2}\log\left(1 + \alpha_2 P_1\right) \tag{7.49}$$

$$R_2 = \frac{1}{2}\log\left(1 + \frac{P_2}{\alpha_2 P_1 + 1}\right) - \frac{1}{2}\log\left(1 + \alpha_1 P_2\right). \tag{7.50}$$

Now, let us assume that user 2's signal has a partial jamming component, which can be achieved by choosing $X_1 = V_1$ and $X_2 = V_2 + U_2$ where V_1, V_2, and U_2 are independent zero-mean Gaussian random variables with variances P_1, βP_2, $(1-\beta)P_2$, respectively, and $0 \leq \beta \leq 1$. Then, the achievable rate region becomes

$$R_1 = \frac{1}{2}\log\left(1 + \frac{P_1}{\alpha_1 P_2 + 1}\right) - \frac{1}{2}\log\left(1 + \frac{\alpha_2 P_1}{(1-\beta)P_2}\right) \tag{7.51}$$

$$R_2 = \frac{1}{2}\log\left(1 + \frac{\beta P_2}{(1-\beta)P_2 + \alpha_2 P_1 + 1}\right) - \frac{1}{2}\log\left(1 + \frac{\alpha_1 P_2}{(1-\beta)P_2 + 1}\right). \tag{7.52}$$

We observe that with this selection of random variables user 2 has increased the secrecy rate of user 1. We also note that user 2 accomplished this by jamming its own receiver. In [29], authors call this strategy *artificial noise.*

Both *cooperative jamming* and *artificial noise* can be generalized to arbitrary (not necessarily Gaussian) channels [27, 28]. In fact, injecting additional Gaussian noise into Gaussian channels can be thought of as sending dummy codewords whose rate is above the decoding capability of both the eavesdropper and the receiver. Since neither receiver can decode and remove the dummy codeword from the received signal, the end result of this strategy becomes making both channels noisier than they actually are.

In conclusion, in this section, we reviewed two *oblivious* cooperation techniques where a cooperating partner helps increase the secrecy rate of another user without knowing anything about the signal transmitted by that user. In the first one, the helper sends dummy codewords from a codebook. The rate of these dummy codewords is chosen such that the receiver is able to decode them. Consequently, this strategy improves the secrecy of the user when the helper-receiver link is stronger than the helper-eavesdropper link. In the second one, the helper sends explicit jamming signals. This strategy is equivalent for the helper to send dummy codewords whose rate is larger than the decoding capability of both the eavesdropper and the receiver. Therefore, this strategy is effective when the helper-eavesdropper link is stronger than the helper-receiver link.

7.5 Active Cooperation for Secrecy

In the previous section we reviewed cooperation schemes where the cooperating parties help the main receiver by weakening the eavesdropping link without using any knowledge of the message being transmitted. In this section we will review

cooperation schemes where the cooperating parties will help the main receiver by strengthening the main link by relaying the message. Therefore, the cooperation in this section will be *active* and it will use the over-heard information of the cooperating party.

To this end, we consider the relay-eavesdropper channel (see Fig. 7.6) which was considered in [26] and [30]. In the relay-eavesdropper channel, the relay node will use DAF and CAF methods to strengthen the main link. If the relay uses DAF, then the following secrecy rates are achievable

$$\min\left[I(V_1,V_2;Y),I(V_1;Y_1|V_2)\right]-I(V_1,V_2;Z) \tag{7.53}$$

for any joint distribution of the form

$$p(v_1,v_2)p(x,x_1|v_1,v_2)p(y,y_1,z|x,x_1). \tag{7.54}$$

The first term in Eq. (7.53) is simply the achievable rate of the relay channel when the relay uses DAF, and the second term is the rate that the eavesdropper can extract simultaneously from the relay and the transmitter.

Similar to the relay channel without an eavesdropper, the effectiveness of DAF depends on the quality of the transmitter-relay link as the overall rate is limited by the rate of this link. Besides that, in the relay-eavesdropper channel, the relative strengths of the relay-receiver and the relay-eavesdropper links become critical. For example, if the relay-eavesdropper link is stronger than the relay-receiver link, then all of the cooperative information sent by the relay will be decodable by the eavesdropper. In this case, the relay may not improve the secrecy of the transmitter. Consequently, for DAF to be effective in the relay-eavesdropper channel, not only that the relay-transmitter link should be stronger than the transmitter-receiver link, but also the relay-receiver link should be stronger than the relay-eavesdropper link.

To solidify ideas, let us assume that for every V_2 satisfying the Markov chain

$$V_2 \rightarrow (X,X_1) \rightarrow (Y,Y_1,Z) \tag{7.55}$$

we have

$$I(V_2;Y) \leq I(V_2;Z) \tag{7.56}$$

which is similar to the definition of *less noisy* channel [15]. This condition implies that the relay-eavesdropper link is stronger than the relay-receiver link. For such channels, achievable secrecy rate given in Eq. (7.53) can be upper bounded as

$$\min\left[I(V_1,V_2;Y),I(V_1;Y_1|V_2)\right]-I(V_1,V_2;Z) \leq I(V_1,V_2;Y)-I(V_1,V_2;Z) \tag{7.57}$$

$$\leq I(V_1;Y|V_2)-I(V_1;Z|V_2). \tag{7.58}$$

The upper bound in Eq. (7.58) corresponds to the case when both the eavesdropper and the receiver are able to decode the signal of the relay. Hence, in a channel where

the relay-eavesdropper link is strong, e.g., as in Eq. (7.56), DAF will not be able to improve the secrecy of the transmitter. This shows that the effectiveness of DAF for secrecy purposes depends on the position of the relay node in the corresponding network topology.

CAF can also be used for the relay-eavesdropper channel as it is done in [26] to improve the quality of the main link. It is well-known that CAF performs better than DAF in the relay channel when the transmitter-relay link is worse than the transmitter-receiver link. To judge the effectiveness of CAF in the relay-eavesdropper channel, we again need to consider the relative strengths of the relay-receiver and the relay-eavesdropper links. If the relay-eavesdropper link is stronger, then CAF may not lead to an increase in the secrecy, similar to the DAF case. Moreover, in this case, noise forwarding will not improve secrecy either. In this case, the most effective method the relay can employ may be cooperative jamming, as in this case the relay may harm the eavesdropper more than it harms the receiver.

As an example, let us introduce the Gaussian relay-eavesdropper channel:

$$Y = X + X_1 + N_1 \tag{7.59}$$

$$Y_1 = \sqrt{h_1}X + X_1 + N_2 \tag{7.60}$$

$$Z = \sqrt{h_2}X + \sqrt{h_3}X_1 + N_z \tag{7.61}$$

where h_1, h_2, h_3 are the channel gains and N_1, N_2, N_3 are independent Gaussian random variables with zero-mean and unit-variance. Let us also assume that $h_1 \leq 1 \leq h_2 \leq h_3$, i.e., the transmitter-relay link is worse than the transmitter-receiver-link, and the eavesdropper is close to the transmitter and the relay.

First, we note that if the relay does not transmit anything, then the corresponding secrecy rate of the transmitter is 0, because $1 < h_2$. Now, let us investigate how relay might help. If we compute the secrecy rate achievable by DAF with the selection of $V_1 = X$, $V_2 = X_1$ and X and X_1 to be Gaussian with zero-mean, variances of P_1 and P_2, respectively, and having a correlation coefficient of ρ, we get

$$\frac{1}{2}\log\left(1 + h_1(1-\rho^2)P_1\right) - \frac{1}{2}\log\left(1 + h_2P_1 + h_3P_2 + 2\rho\sqrt{h_2h_3}\sqrt{P_1P_2}\right). \tag{7.62}$$

We note that the expression in Eq. (7.62) is less than 0, and therefore, DAF cannot provide a positive secrecy rate for the transmitter with this selection of random variables. In addition, if we use noise forwarding, and pick the random variables in Eq. (7.36) as $V_1 = X$, $V_2 = X_1$ and X and X_1 to be independent Gaussian with zero-mean, variances of P_1 and P_2, we cannot have any positive secrecy either.

On the other hand, if we select $V_1 = X$ and $X_1 = U$ where X and U are independent (and independent of V_2) Gaussian with zero-mean and variances of P_1 and P_2, respectively, for either DAF or noise forwarding, we get

$$\frac{1}{2}\log\left(1 + \frac{P_1}{1+P_2}\right) - \frac{1}{2}\log\left(1 + \frac{h_2P_1}{1+h_3P_2}\right) \tag{7.63}$$

which is positive if the power of the relay satisfies

$$P_2 \geq \frac{h_2 - 1}{h_3 - h_2}. \tag{7.64}$$

Thus, this selection of auxiliary random variables, which in fact implements *cooperative jamming* in a relay-eavesdropper channel, can yield positive secrecy rates.

So far, in this section, we discussed the ways in which a relay node can help increase the secrecy of a transmitter by strengthening the main link by using DAF and CAF. As suggested by [31], the relay may be captured by an adversary and may be forced to help the eavesdropper. In that case as well, one can come up with cooperation strategies by which the relay helps the eavesdropper, as discussed in [31]. Moreover, the relay-eavesdropper channel can be generalized to a two-sided cooperation channel as is done in [32]. In [32], there is an external eavesdropper in a MAC-GF. Reference [32] uses the cooperation method of [5] for MAC-GF which is a generalization of DAF.

7.6 Untrusted Helpers

In previous sections, we discussed the effectiveness of cooperation among a set of nodes against an external eavesdropper. In this section, we will discuss the interactions that arise between cooperation and secrecy, when the eavesdropper is not an external entity. In this section, the eavesdropper will be a member of the network, and we will ask if utilizing the eavesdropper as a cooperating partner will reduce the secrecy of the main link further or if it will improve it.

The basic models to study these interactions are the simple three-node relay channel, MAC-GF and CRBC. In the relay channel case, we treat the relay also as an eavesdropper, and ask the question: can the relay node improve the equivocation-rate of the transmitter measured at the relay by putting cooperation signals into the channel? Note that, in this channel model, we are able to observe the effects of the relay's actions on the secrecy of the transmitter. In MAC-GF and CRBC channel models, we have the added opportunity of studying the effects of a relaying node's actions on the equivocation-rates of not only the transmitting node, but also the relaying node itself. In particular, in MAC-GF, both users treat each other as cooperating partners as well as eavesdroppers. There, we observe the effects of user 1's actions on the secrecy of user 2 as well as on the secrecy of user 1 itself. In CRBC, the setting is reversed, in the sense that the cooperation (and also eavesdropping) take place at the receiver end. Here also, we observe the actions of receiver 1 (which also relays signals to receiver 2) on the secrecy of the messages sent to receiver 1 and the secrecy of the messages sent to receiver 2.

7.6.1 Relay Channel with Secrecy Constraints

Here we consider a basic three-node relay network, as shown in Fig. 7.1. The transmitter wishes to communicate with the receiver at the highest possible reliable rate, R_1. The goal of the relay node is to assist this communication. At the same time, the relay node acts as an eavesdropper. Therefore, we measure the secrecy of the communication by the equivocation-rate of the message measured at the relay node

$$\frac{1}{n} H\left(W|Y_1^n, X_1^n\right). \tag{7.65}$$

The overarching goal is to characterize all achievable (R_1, R_e) pairs which will be spanned by tracing all possible actions of the relay node. This is a very difficult problem, and we will provide only a partial characterization.

This problem was first addressed in [33]. In the model of [33], the transmitter sends a common message to both the relay and the receiver, and also a confidential message to the receiver. Achievable schemes presented [33] rely on the DAF technique. In particular, the relay uses a partial DAF strategy where the common message and a part of the confidential message is decoded and forwarded to the receiver. The secrecy rate achieved by this scheme is

$$I(V;Y|X_1) - I(V;Y_1|X_1) \tag{7.66}$$

where V is a random variable that satisfies the Markov chains

$$V \to (X, X_1) \to (Y, Y_1) \qquad \text{and} \qquad X_1 \to V \to X. \tag{7.67}$$

We note that the rate in Eq. (7.66) is exactly the secrecy rate achievable in the underlying wiretap channel. This can be seen by noting the conditioning to X_1 of both mutual information terms has the effect of removing the signal of the relay node from the received signals Y_1 and Y. This removes the channel input of the relay channel from the system, and the channel model becomes exactly that of the wiretap channel. Therefore, we conclude that as long as the relay node uses a DAF-type cooperation, even though it can increase the achievable rate of the transmitter, it does not increase the secrecy rate of the transmitter. This conclusion is quite intuitive, because although the relay node can increase the rate of the transmitter, it cannot increase it beyond the amount that it itself can decode. Consequently, the secrecy rate, which is, roughly speaking, the difference between the rates of the receiver and the eavesdropper (relay in this case), cannot be increased if the relay node uses a DAF-type cooperation strategy.

To gain more insight let us consider the Gaussian relay channel:

$$Y = X + X_1 + Z_1 \tag{7.68}$$

$$Y_1 = X + Z_2 \tag{7.69}$$

where Z_1, Z_2 are independent Gaussian random variables with zero-mean and variances of N_1 and N_2, respectively. In addition, we have the usual power constraints: $E[X^2] \leq P_1$ and $E[X_1^2] \leq P_2$. The achievable rate in Eq. (7.66) yields [33]

$$\frac{1}{2}\log\left(1+\frac{P_1}{N_1}\right)-\frac{1}{2}\log\left(1+\frac{P_1}{N_2}\right). \tag{7.70}$$

This is also exactly equal to the secrecy rate achievable in the underlying wiretap channel, i.e., the achievable secrecy rate when the relay is not transmitting. Consequently, when $N_1 > N_2$, i.e., when the relay (eavesdropper) has a better channel than the receiver, this rate vanishes. Consequently, DAF-based relaying does not help as far as secrecy is concerned.

Reference [33] also provided outer bounds for the secrecy capacity. The upper bound [33] gave for the secrecy rate evaluates to

$$\frac{1}{2}\log\left(1+\frac{P_1}{N_1}+\frac{P_1}{N_2}\right)-\frac{1}{2}\log\left(1+\frac{P_1}{N_2}\right) \tag{7.71}$$

for the Gaussian relay channel under consideration. We note that this upper bound does not vanish when $N_1 > N_2$. Although this outer bound does not lead us to the ultimate achievable secrecy rate, at least, it does not preclude the transmitter node to have secret communication when the relay (eavesdropper) has a better channel. Therefore, it leaves it a possibility that secret communication may be attained by using cooperation schemes other than DAF.

The interaction of cooperation and secrecy has been further studied in [34] focusing on two special classes of the relay channel. In the first special class, there is an orthogonal link between the transmitter and the relay and there is a MAC from the transmitter and the relay to the receiver. The capacity of this relay channel was found in [35]. In [34], the secrecy capacity of this channel is determined. Since the orthogonal link between the transmitter and the relay does not interfere with the rest of the channel, [34] finds that all of the confidential information should be sent without using this orthogonal link. Hence, for this channel, the relay is found to be useless from the secrecy point of view.

In the second special class considered in [34], there is an orthogonal link between the relay and the receiver, and the transmitter has a broadcast channel to the relay and the receiver. Reference [34] proposed to use CAF for this channel and analyzed its performance. The CAF-based cooperation scheme is not specific to this channel model, and can be used in any relay channel. The secrecy rate achievable by CAF is found as

$$I(X;Y,\hat{Y}_1|X_1)-I(X;Y_1|X_1) \tag{7.72}$$

where the random variables in Eq. (7.72) are subject to the constraint

$$I(X_1;Y)\geq I(\hat{Y}_1;Y_1|Y,X_1) \tag{7.73}$$

and X and X_1 are independent. The secrecy rate in Eq. (7.72) can be decomposed as

$$[I(X;Y|X_1) - I(X;Y_1|X_1)] + I(X;\hat{Y}_1|X_1,Y) \tag{7.74}$$

where the first term may be viewed as the secrecy rate of the underlying wiretap channel, and the second term may be interpreted as the additional secrecy rate CAF-based cooperation provides. Consequently, if this second term is non-negative, then the relay, by employing CAF, not only improves the rate of the transmitter, but also improves the secrecy rate of the transmitter.

To examine this possibility in more depth, let us focus on the special class of Gaussian relay channel considered in [34]. In this channel, the receiver observes $Y = (Y_t, Y_r)$, where

$$Y_t = X + Z_t \tag{7.75}$$

$$Y_r = bX_1 + Z_r \tag{7.76}$$

$$Y_1 = aX + Z_1 \tag{7.77}$$

where Z_t, Z_r, Z_1 are independent Gaussian random variables with zero-mean and unit-variance. We also assume $E[X^2] \leq P$ and $E[X_1^2] \leq P$. For this channel, CAF yields the following the secrecy rate

$$\frac{1}{2}\log\left(1 + P + \frac{a^2P}{1+N_c}\right) - \frac{1}{2}\log\left(1 + a^2P\right) \tag{7.78}$$

where N_c is given by

$$N_c = \frac{\left(a^2+1\right)P + 1}{b^2P(P+1)}. \tag{7.79}$$

The rate in Eq. (7.78) is obtained from Eqs. (7.72) and (7.73) and using independent Gaussian channel inputs. The compressed signal is selected as $\hat{Y}_1 = Y_1 + Z_c$, where Z_c is the compression noise that is Gaussian with zero-mean and variance of N_c, which is chosen to meet the constraint in Eq. (7.73). We can now compare the rate given in Eq. (7.78) with the corresponding wiretap channel, where the relay node does not transmit a signal. We first note that, in the corresponding wiretap channel, secrecy rate is zero whenever $a > 1$. However, the rate in Eq. (7.78) can be positive even when $a > 1$ if b is sufficiently large, i.e., if the relay-receiver link is strong enough. Although we considered a special class of relay channels in this example, the same conclusion holds for the general Gaussian relay channel in Eqs. (7.68, 7.69). Specifically, the examples provided for the Gaussian MAC-GF and CRBC in the next two sections highlight this fact since these channels subsume the Gaussian relay channel.

In conclusion, we observed that CAF can increase the secrecy rate with respect to the underlying wiretap channel. The basic reason for this is that, using CAF, the relay node can increase the overall achievable rate of the network to levels which are not decodable at the relay node. This, in effect, increases the difference of the rates in the transmitter-relay and transmitter-receiver links, which, roughly speaking, corresponds to the secrecy rate.

7.6.2 MAC-GF with Confidential Messages

In this section, we consider MAC-GF, shown in Fig. 7.2, where both users have their own messages to send, and they both receive feedback signals that are correlated with the message of the other user. These signals can be used to cooperate and increase the rates; however, these signals are also the basis for loss of secrecy. In this section, each user will consider the other user both as a cooperating partner and also as an eavesdropper. This channel model can be considered as a two-sided version of the relay channel, where the relaying nodes have their own messages as well. There are two rates, R_1 and R_2, and two equivocation-rates $R_{e,1}$ and $R_{e,2}$. Our main motivation to study this channel model is to understand the implications of the actions (i.e., cooperation) of one user on the rate and secrecy of the other user, as well as on the rate and secrecy of itself. This could not be studied in the classical relay channel, as the relay node does not have its own messages, and therefore, its own rate and equivocation-rate.

MAC-GF was studied from a secrecy point of view in [36, 37], and [38]. References [36] and [37] did not use the feedback signals in their encoding functions, i.e., the users were not allowed to cooperate. Consequently, the only effect of the feedback signals in [36, 37] was the loss of secrecy. Reference [38], on the other hand, allows the encoding functions to depend on the feedback signals, i.e., it allows users to cooperate, and it investigates the effects of cooperation on the secrecy of the users. We know that both DAF and CAF can be used as methods of cooperation, and they would both increase the achievable rates. However, as observed in the relay channel as well, DAF is not likely to improve the secrecy rates. CAF, on the other hand, is likely to improve the secrecy rates of the users. We show in [38] that the following secrecy rates are achievable if both users employ CAF-based cooperation

$$R_1 \leq R_1' - I(X_1; Y_2, \hat{Y}_1 | U_1, U_2, X_2) \tag{7.80}$$

$$R_2 \leq R_2' - I(X_2; Y_1, \hat{Y}_2 | U_1, U_2, X_1) \tag{7.81}$$

where the pairs $\left(R_1', R_2'\right)$ belong to

$$\mathcal{C}_2\left(R_1, R_2\right) = \left\{ \begin{array}{r} R_1' \leq I(X_1; Y, \hat{Y}_1, \hat{Y}_2 | U_1, U_2, X_2) \\ R_2' \leq I(X_2; Y, \hat{Y}_1, \hat{Y}_2 | U_1, U_2, X_1) \\ R_1' + R_2' \leq I(X_1, X_2; Y, \hat{Y}_1, \hat{Y}_2 | U_1, U_2) \end{array} \right\} \tag{7.82}$$

for any distribution of the form

$$\begin{aligned} &p(u_1)p(x_1|u_1)p(\hat{y}_1|u_1, x_1, y_1)p(u_2)p(x_2|u_2) \\ &p(\hat{y}_2|u_2, x_2, y_2)p(y, y_1, y_2|x_1, x_2) \end{aligned} \tag{7.83}$$

subject to the constraints

$$I(\hat{Y}_1; Y_1|U_1, X_1) \leq I(U_1, \hat{Y}_1; Y|U_2) \tag{7.84}$$

$$I(\hat{Y}_2; Y_2|U_2, X_2) \leq I(U_2, \hat{Y}_2; Y|U_1) \tag{7.85}$$

$$I(\hat{Y}_1; Y_1|U_1, X_1) + I(\hat{Y}_2; Y_2|U_2, X_2) \leq I(U_1, U_2; Y) + I(\hat{Y}_1; Y|U_1, U_2) + I(\hat{Y}_2; Y|U_1, U_2). \tag{7.86}$$

To examine whether this achievable scheme enlarges the secrecy region of MAC-GF with respect to the case where feedback signals are not used, i.e., users are not allowed to cooperate, we will evaluate the region given by Eqs. (7.80–7.86) for the Gaussian MAC-GF:

$$Y_1 = X_1 + X_2 + Z_1 \tag{7.87}$$

$$Y_2 = X_1 + X_2 + Z_2 \tag{7.88}$$

$$Y = X_1 + X_2 + Z \tag{7.89}$$

where Z_1, Z_2, Z are independent Gaussian random variables with zero-mean and variances of N_1, N_2, and N, respectively. We also impose power constraints of P_1 and P_2 on X_1 and X_2.

For this Gaussian channel, if $N_2 < N$ (resp. $N_1 < N$), then user 1 (resp. user 2) cannot have positive secrecy if users *do not* cooperate. To see this point, let us consider the MAC channel from the users to the receiver and the channel from user 1 to user 2. This channel can be viewed as a Gaussian wiretap channel where user 2 is the wiretapper. Consequently, if the wiretapper's channel (the channel from user 1 to user 2), is less noisy than the main channel (the channel from the users to the receiver), i.e., if $N_2 < N$, then all the messages sent to the receiver by user 1 can be decoded by user 2, as well. Thus, the secrecy rate of user 1 is zero. Let us consider the specific example: $N_1 = N_2 = 0.75, N = 1$. We plot the secrecy rates given by the achievable region of Eqs. (7.80–7.86) in Fig. 7.8. We observe that, thanks to

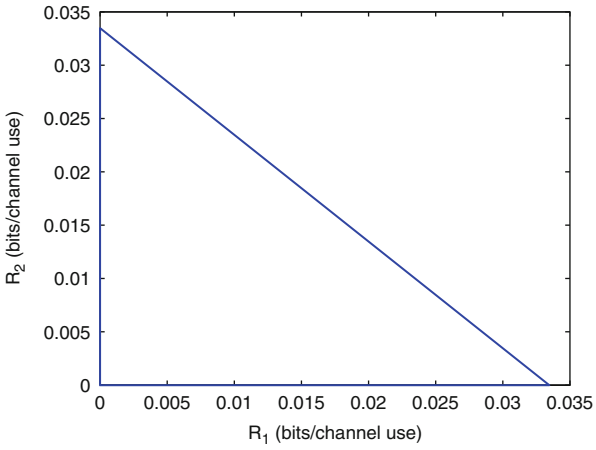

Fig. 7.8 Effect of CAF on the secrecy of MAC-GF

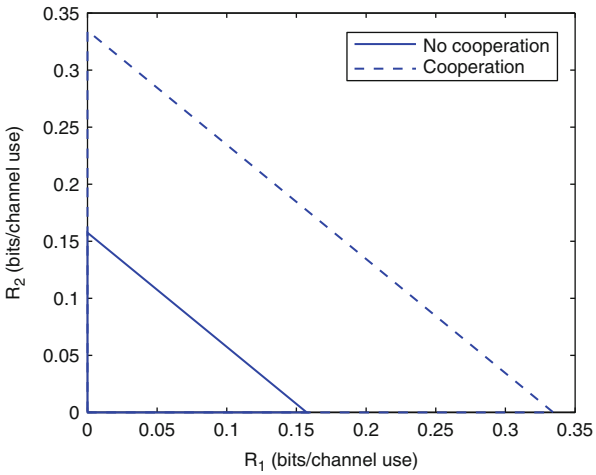

Fig. 7.9 Comparison of cooperation and no-cooperation in MAC-GF

CAF-based cooperation, both users are able to achieve positive secrecy rates. We observe that each user achieves the largest secrecy rate when the other user does not send any confidential messages but act as a pure relay. We consider another channel with parameters $N_1 = N_2 = 1.25, N = 1$. In this MAC-GF, both users achieve positive secrecy rates even without cooperation. Figure 7.9 shows that CAF-based cooperation enlarges this secrecy region.

7.6.3 CRBC with Confidential Messages

In this section, we consider CRBC, shown in Fig. 7.3, where the transmitter has messages to send to both receivers, and there is a one-sided cooperation link from user 1 to user 2. In this section, user 2 will consider user 1 as a cooperating partner and also an eavesdropper, and user 1 will consider user 2 as an eavesdropper. As in the previous section on MAC-GF, in this channel model, we have two rates and two equivocation-rates. Our goal is to understand the effects of the actions (e.g., cooperation, jamming, etc.) of user 1 on the rates and secrecy of both users.

We showed in [39] that the following secrecy rates are achievable by using a CAF-based cooperation scheme at user 1,

$$R_1 \leq I(V_1; Y_1|X_1) - I(V_1; Y_2, \hat{Y}_1|V_2, X_1) - I(V_1; V_2) \tag{7.90}$$

$$R_2 \leq I(V_2; Y_2, \hat{Y}_1|X_1) - I(V_2; Y_1|V_1, X_1) - I(V_1; V_2) \tag{7.91}$$

where the random variables involved are subject to the constraint

$$I(\hat{Y}_1; Y_1|X_1, V_1) \leq I(\hat{Y}_1, X_1; Y_2) \tag{7.92}$$

for any joint distribution of the form

$$p(v_1, v_2)p(x_1)p(x|v_1, v_2)p(\hat{y}_1|x_1, y_1, v_1)p(y_1, y_2|x, x_1). \tag{7.93}$$

In this achievable scheme, the transmitter uses Marton's scheme [40] for broadcast channels and user 1 employs CAF for relay channels. To examine the potentail improvement in the secrecy rates with this scheme, we consider a Gaussian CRBC:

$$Y_1 = X + Z_1 \tag{7.94}$$

$$Y_2 = X + X_1 + Z_2 \tag{7.95}$$

where Z_1, Z_2 are independent Gaussian random variables with zero-mean and variances of N_1 and N_2, respectively. We impose power constraints of P and aP on X and X_1.

If user 1 does not transmit any signals, i.e., $X_1 = \phi$, then the channel becomes a Gaussian broadcast channel, and it will be degraded in one of the directions. Consequently, in this broadcast channel, both users cannot have positive secrecy rates simultaneously. However, if we compute the achievable region in Eqs. (7.90–7.93) for $N_1 = 1, N_2 = 2, P = 8$ for various values of a, we obtain the achievable secrecy region shown in Fig. 7.10. We observe that although user 2 cannot have positive secrecy rate in the underlying broadcast channel since $N_1 < N_2$, the cooperation of user 1 enables user 2 to have positive secrecy rates.

The previous achievable scheme and the Gaussian channel example provide us with a limited picture of what can be achieved. In particular, the above proposed achievability scheme implicitly assumes that the cooperating user (user 1) is the stronger of the two users. Thus, a natural question is, what happens if the cooperating user is the weaker of the two users? If user 1 does not transmit any signals, then it cannot have a positive secrecy rate. However, the question here is: can user 1 *help itself* to have positive secrecy? The answer is positive if user 1 utilizes the cooperative link to jam user 2. An even more interesting question is whether both users can have positive secrecy rates simultaneously, when user 1 (cooperating user) is the weaker of the two users. To make this possible, we proposed an achievable scheme that

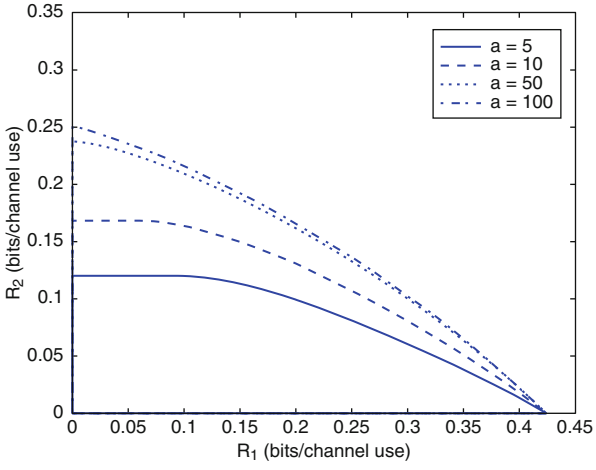

Fig. 7.10 CRBC channel: secrecy region (©IEEE 2008)

combines jamming and relaying in [39]. This scheme yields the rates

$$R_1 \leq I(V_1; Y_1|X_2, U) - I(V_1; \hat{Y}_1, Y_2|U, V_2) - I(V_1; V_2) \tag{7.96}$$

$$R_2 \leq I(V_2; Y_2, \hat{Y}_1|U) - I(V_2; Y_1|U, V_1, X_2) - I(V_1; V_2) \tag{7.97}$$

subject to the constraint

$$I(\hat{Y}_1; Y_1|U, V_1) \leq I(U, \hat{Y}_1; Y_2) \tag{7.98}$$

for any joint distribution of the form

$$p(v_1, v_2)p(x|v_1, v_2)p(u)p(\hat{y}_1|u, v_1, y_1)p(x_1|u) \tag{7.99}$$

First, we note that this achievable scheme can be obtained from the one in Eqs. (7.90–7.93) via prefixing user 1's input, X_1, with another channel whose input is U. In this achievable scheme, U denotes the actual help signal that should be decoded by user 2 in order to get the compressed version of user 1's observation, $\hat{Y}_1$, whereas X_1, that is correlated with U, contains the jamming attack. Therefore, since user 2's channel is attacked, the information user 2 can gather from its observation about V_1 decreases, making it possible for user 1 to have positive secrecy when it is the weaker one of the two users.

Next, we provide a Gaussian example with $N_1 > N_2$, i.e., user 1 is the weaker of the two users. In this Gaussian channel, the overall strategy works as follows. First, user 1 makes user 2's observation more noisy to provide secrecy for itself via injecting the channel with additional Gaussian noise. Assuming that user 1 has large enough power, this ultimately changes the strengths of two the channels, i.e., now user 1 becomes the stronger of the two users. Now, we are back to the previous case, and user 1 relays its observation to user 2 to provide provide positive secrecy for user 2 in its attacked channel. The numerical example for this case is given in Fig. 7.11 for $N_1 = 2, N_2 = 1$ showing that both users enjoy positive secrecy rates thanks to a combination of cooperation and jamming.

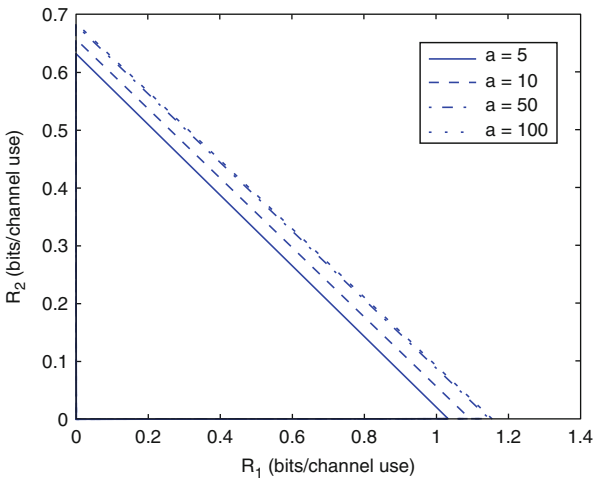

Fig. 7.11 CRBC channel: joint jamming and relaying (©IEEE 2008)

7.7 Conclusions

In this chapter, we reviewed the current literature on cooperation, secrecy and the interactions of the two. Our emphasis has mainly been on how cooperation can improve secrecy. We investigated channel models where users cooperate to defeat an external eavesdropper, as well as channels where cooperating parties are treated as potential eavesdroppers. We have demonstrated that there are various ways users can cooperate to improve secrecy: users can cooperate even when they do not know the messages of each other (as in *oblivious* cooperation), they can cooperate in the traditional sense by forwarding information about each others' message (as in *active* cooperation), and finally, users can improve secrecy of the transmitters even when they themselves are treated as eavesdroppers (as in the case of *untrusted helpers*).

References

[1] E. C. van der Meulen. Three-terminal communication channels. *Adv. Appl. Probab.*, 3:120–154, 1971.
[2] A. Wyner. The wire-tap channel. *Bell Syst. Tech. J.*, 54(8):1355–1387, Jan. 1975.
[3] T. M. Cover and A. El Gamal. Capacity theorems for the relay channel. *IEEE Trans. Inf. Theory*, IT-25(5):572–584, Sep. 1979.
[4] A. Carleial. Multiple access channels with different generalized feedback signals. *IEEE Trans. Inf. Theory*, 28(6):841–850, Nov. 1982.
[5] F. Willems, E. van der Meulen, and J. Schalkwijk. Achievable rate region for the multiple access channel with generalized feedback. In *41st Asilomar Conf. Signals, Syst. Comp.*, Nov. 1983.
[6] R. C. King. *Multiple access channels with generalized feedback*. PhD thesis, Stanford Univ., Stanford, CA, Mar. 1978.
[7] T. Cover and C. Leung. An achievable rate region for the multiple access channel with feedback. *IEEE Trans. Inf. Theory*, 27(5):292–298, May 1981.
[8] M. A. Khojastepour, A. Sabharwal, and B. Aazhang. Improved achievable rates for user cooperation and relay channels. In *IEEE Int. Symp. Inf. Theory*, Jun. 2004.
[9] L. Ong and M. Motani. Coding strategies for multiple-access channels with feedback and correlated sources. *IEEE Trans. Inf. Theory*, 53(10):3476–3497, Oct. 2007.
[10] A. Sendonaris, E. Erkip, and B. Aazhang. User cooperation diversity-part I: System description. *IEEE Trans. Commun.*, 51(11):1927–1938, Nov. 2003.
[11] O. Kaya and S. Ulukus. Power control for fading cooperative multiple access channels. *IEEE Trans. Wireless Commun.*, 6(8):2915–2923, Aug. 2007.
[12] R. Dabora and S. Servetto. Broadcast channels with cooperating decoders. *IEEE Trans. Inf. Theory*, 52(12):5438–5454, Dec. 2006.
[13] Y. Liang and G. Kramer. Rate regions for relay broadcast channel. *IEEE Trans. Inf. Theory*, 53(10):3517–3535, Oct. 2007.
[14] Y. Liang and V. V. Veeravalli. Cooperative relay broadcast channels. *IEEE Trans. Inf. Theory*, 53(3):900–928, Mar. 2007.
[15] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, IT-24(3):339–348, May 1978.
[16] T. Cover and J. Thomas. *Elements of Information Theory*. Wiley & Sons, 2006. 2nd edition.
[17] S. K. Leung-Yan-Cheong and M. E. Hellman. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory*, 24(4):451–456, Jul. 1978.

[18] Z. Li, R. Yates, and W. Trappe. Secrecy capacity of independent parallel channels. In *44th Annu. Allerton Conf. Commun. Control Comput.*, Sep. 2006.

[19] Y. Liang, H. V. Poor, and S. Shamai. Secure communication over fading channels. 54(6):2470–2492, Jun. 2008.

[20] A. Khisti and G. Wornell. Secure transmission with multiple antennas: The MISOME wiretap channel. Submitted to *IEEE Trans. Inf. Theory*, Aug. 2007.

[21] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wiretap channel. Submitted to *IEEE Trans. Inf. Theory*, Oct. 2007.

[22] S. Shafiee, N. Liu, and S. Ulukus. Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel. *IEEE Trans. Inf. Theory*, 55(9):4033–4039, Sep. 2009.

[23] Z. Li, R. Yates, and W. Trappe. Secure communication with a fading eavesdropper channel. In *IEEE ISIT*, Jun. 2007.

[24] E. Tekin and A. Yener. The Gaussian multiple access wire-tap channel. *IEEE Trans. Inf. Theory*, 54(12):5747–5755, Dec. 2008.

[25] E. Tekin and A. Yener. The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming. *IEEE Trans. Inf. Theory*, 54(6):2735–2751, Jun. 2008.

[26] L. Lai and H. El Gamal. The relay-eavesdropper channel: Cooperation for secrecy. *IEEE Trans. Inf. Theory*, 54(9):4005–4019, Sep. 2008.

[27] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. Interference-assited secrect communication. In *IEEE Inf. Theory Workshop*, May 2008.

[28] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. The Gaussian wiretap channel with a helping interferer. In *IEEE Int. Symp. Inf. Theory*, Jul. 2008.

[29] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy capacity regions. *IEEE Trans. Inf. Theory*, 54(6):2493–2507, Jun. 2008.

[30] M. Yuksel and E. Erkip. The relay channel with a wire-tapper. In *41st Annu. Conf. Inf. Sci. Syst.*, Mar. 2007.

[31] M. Yuksel and E. Erkip. Secure communication with a relay helping the wiretapper. In *IEEE Inf. Theory Workshop*, Sep. 2007.

[32] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. Multiple access channels with generalized feedback and confidential messages. In *IEEE Inf. Theory Workshop Front. Coding Theory*, Sep. 2007.

[33] Y. Oohama. Relay channels with confidential messages. Submitted to *IEEE Trans. Inf. Theory,* Mar. 2007.

[34] X. He and A. Yener. On the equivocation region of relay channels with orthogonal components. In *41st Asilomar Conf. Signals Syst. Comp.*, Nov. 2007.

[35] A. El Gamal and S. Zahedi. Capacity of a class of relay channels with orthogonal components. *IEEE Trans. Inf. Theory*, 51(5):1815–1817, May 2005.

[36] Y. Liang and H. V. Poor. Multiple access channels with confidential messages. *IEEE Trans. Inf. Theory*, 54(3):976–1002, Mar. 2008.

[37] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic. The discrete memoryless multiple access channel with confidential messages. In *IEEE Int. Symp. Inf. Theory*, Jul. 2006.

[38] E. Ekrem and S. Ulukus. Effects of cooperation on the secrecy of multiple access channels with generalized feedback. In *CISS*, Mar. 2008.

[39] E. Ekrem and S. Ulukus. Secrecy in cooperative relay broadcast channels. In *IEEE Int. Symp. Inf. Theory*, Jul. 2008.

[40] K. Marton. A coding theorem for the discrete memoryless channels. *IEEE Trans. Inf. Theory*, 25(1):306–311, May 1979.