

Chapter 2

Obtaining Secrecy Through Intentional Uncertainty*

Satashu Goel and Rohit Negi

2.1 Introduction

The tremendous popularity of wireless medium for communications is mainly because of the broadcast nature, which allows access to multimedia and information without restriction on the user's location. However, guaranteeing secure communication in a wireless medium is made difficult by the same broadcast nature, which makes it easy to eavesdrop on an ongoing communication, while making it nearly impossible to detect eavesdropping. The time-varying and unreliable nature of the wireless channels poses further difficulties. However, the same physical properties, which have a detrimental effect on reliability in communication, provide an opportunity to enhance the secrecy of communication, if used carefully.

The foundation for the theory of secrecy systems was laid by Claude Shannon in [1]. He showed that perfect secrecy can be obtained only if the size of the secret key is at least as large as the size of the message. Perfect secrecy means that the intended receiver can decode the secret message without any error, while the eavesdrop cannot decode the secret message. The underlying assumptions in this analysis were,

- the eavesdropper can utilize infinite computational power and time,
- both the receiver and the eavesdropper receive precisely the same signal.

The first assumption results in the worst case scenario in terms of the resources assumed at the eavesdropper, and therefore, leads to *provable* secrecy. The second assumption may only be valid in certain special cases, e.g., if the channels to both the receiver and the eavesdropper are noiseless. This would be a reasonable model if only the higher layers of networking are of interest, and an idealized (error-free bit

S. Goel (✉)
Carnegie Mellon University, 5000 Forbes Avenue
Pittsburgh, PA
e-mail: satashu@cmu.edu

*Portions of the material have appeared in "Guaranteeing Secrecy using Artificial Noise," IEEE Transactions on Wireless Communications, vol. 7, no. 6, June 2008, ©IEEE 2008.

pipe) model for the physical layer can be used. However, this restrictive assumption results in the pessimistic result mentioned above.

In cryptography, the effect of the physical layer is usually ignored, and secrecy is ensured through encoding and decoding at a higher layer. In particular, it is assumed that both the receiver and the eavesdropper receive exactly the same message, and the encoding and decoding process is known to both of them. The secret key is assumed known only to the receiver and the transmitter. The eavesdropper must determine the secret key (and hence, the secret message) from the received signal. However, the key must be at least as large as the secret message itself, based on Shannon's result mentioned above. The key assumption that allows the cryptographic algorithms to provide secrecy using a key much smaller than the message is that the eavesdropper has limited computing resources and time. The difficulty in decrypting the received signal is often based on a known difficult problem, e.g., prime factorization [2].

In many practical systems, the eavesdropper may have a worse channel than the receiver, e.g., if the eavesdropper *wire-taps* the receiver's channel, thus experiencing noise from both the receiver's channel and its own channel. This wire-tap channel model was analyzed in [3], which showed that in fact perfect secrecy can be guaranteed for a non-zero information rate, if the eavesdropper has a degraded channel compared to the receiver. Perfect secrecy is possible for the wire-tap channel, because of the relaxed assumption on the signal received by the eavesdropper. The system was characterized by *secrecy capacity*, which is the maximum possible rate for which perfect secrecy can be achieved. In this analysis, the eavesdropper was assumed to have unlimited computing resources and time, unlike the assumption in cryptography, and therefore, the secrecy is provable. The secrecy results were obtained using information theoretic tools, and hence, this form of secrecy is called information theoretic secrecy. The secrecy guarantees, in this case, are closely related to the physical layer model, which is ignored in the cryptographic approach.

In a broadcast medium, the eavesdropper and the receiver will, in general, have different channels, and hence, the degraded (wire-tap) channel model may not hold. Communication of secret messages over broadcast channels was considered in [4], which showed that perfect secrecy can be guaranteed for a non-zero information rate, if the eavesdropper's channel is worse than the receiver's channel. In a wireless environment, there is no guarantee that the eavesdropper's channel will be worse than the receiver's channel. For example, the eavesdropper may have a larger channel gain if it is closer to the transmitter, compared to the receiver. Further, the effective channel gain may be increased using directional antennas [5]. If the eavesdropper channel turns out to be better than the receiver's channel, secrecy capacity is zero. It may appear that provable secrecy cannot be guaranteed in such a scenario. How can we design a communication system, which can overcome the eavesdropper's advantage of a better channel? In this chapter, we will show that it is in fact possible to utilize communication theoretic ideas to ensure secrecy of communication, even when the eavesdropper may have a better channel. In particular, we will show how multiple transmit antennas may be used to obtain non-zero secrecy capacity. The key idea in this chapter is that the transmitter can use the degrees of freedom, provided by multiple transmit antennas, to enhance the rate of secret communication, instead of

using them to increase the information rate. The method essentially involves creating intentional uncertainty or “artificial noise”.

The remainder of the chapter is organized as follows. Section 2.2 provides an overview of the key results on perfect secrecy that will be used in this chapter. Section 2.3 formally describes the system under consideration and the assumptions involved. Section 2.4 presents the scheme for introducing intentional uncertainty in the transmitted signal to obtain secrecy. The scheme is first described in a simple scenario in Sect. 2.4.1. The scheme is then generalized to the multiple input multiple output (MIMO) scenario in Sect. 2.4.3. Section 2.5 describes the related work on achieving perfect secrecy over wireless channels. Finally, Sect. 2.6 concludes this chapter.

2.2 Overview of Secrecy Capacity

In this section, we will provide a brief overview of relevant results on information theoretic secrecy. The notion of secrecy capacity was introduced in [3]. The paper considered a wire-tap model, where the eavesdropper’s channel is a degraded version of the receiver’s channel. Secrecy capacity for the *Gaussian* wire-tap channel was obtained in [6]. As a generalization of the wire-tap model, secrecy capacity for broadcast channels was obtained in [4]. We now present the assumptions and results used in the wiretap model, and the broadcast model. We denote the sequence $h^k \triangleq (h_1, h_2, \dots, h_k)$.

2.2.1 Assumptions

We first present the assumptions common to the various models considered in information theoretic secrecy. Additional assumptions, specific to a given model, will be presented along with the description of the model. In contrast to the cryptographic approach, it is assumed that the transmitter and the intended receiver do not share a secret key. Thus, the information theoretic secrecy schemes discussed in this chapter enable secret communication without requiring a prior exchange of a secret key, although the guaranteed information rates may be smaller. The advantages of both these approaches can be utilized by using the provable information theoretic secrecy schemes to establish a shared secret key, and then use the traditional symmetric key encryption to achieve a higher information rate. Authentication, however, is assumed, meaning that the transmitter and the receiver can verify each others identity. Alternatively, a passive eavesdropper is assumed which only listens but does not transmit.

It is assumed that both, the receiver and the eavesdropper can estimate their own channels perfectly. The transmitter is assumed to know the receiver’s channel through (authenticated) feedback. However, it does not know the eavesdropper’s channel, since the eavesdropper is passive. Further, the transmitter may not know the location, or the presence, of the eavesdropper(s). Thus, this chapter considers secrecy of communication under the assumption that the eavesdropper’s channel gain is not known to the transmitter.

2.2.2 Wire-Tap Model

The wire-tap model was introduced in [3]. In contrast to Shannon's assumption of both the receiver and the eavesdropper receiving the same signal [1], the paper assumed that the eavesdropper puts a wire-tap on the receiver's channel, and hence, receives a degraded version of the signal at the receiver. The key property that enabled secret communication in this case, even in the absence of a shared secret key, was that the eavesdropper's channel is noisier than the receiver's channel. The wire-tap model is appropriate for wireline systems.

The transmitter encodes a block of K symbols of the secret message into a block of N coded symbols. That is, secret message m^K is encoded into symbols x^N , which is the input to the receiver's channel. The output of the receiver's channel is $z^N = f(x^N)$, where $f(\cdot)$ is a random mapping. The receiver estimates the secret message based on z^N . z^N is the input to the wire-tap channel, whose output $y^N = g(z^N)$ is observed by the eavesdropper, where $g(\cdot)$ is another random mapping. The eavesdropper tries to decode the secret message based on y^N . The rate of secret information is given by $R = H(m^K)/N$, which is the per symbol entropy of the secret message. The eavesdropper's uncertainty about the secret message, after it has observed y^N , is measured by *equivocation* per source letter $R_e \doteq H(m^K|y^N)/K$. For simplification in notation, we can normalize equivocation by the source entropy per source letter, resulting in *fractional equivocation* $\Delta \doteq H(m^K|y^N)/H(m^K)$ [6]. The achievable rate region in terms of (R, Δ) was obtained in [3]. The specific case where $\Delta = 1$ has special significance, since $\Delta = 1$ ensures that the eavesdropper is as ignorant of the secret message after observing y^N , as it was before observing y^N . That is, observing the output of the wire-tap channel does not increase eavesdropper's knowledge about the secret message. Thus, *perfect secrecy* is said to be achieved if $\Delta = 1$. Rate R is achievable with perfect secrecy if for every $\epsilon > 0$, there exists a (k, n) code such that $k/n > R - \epsilon$, $\Delta > 1 - \epsilon$, and $Pr\{\text{decoding error}\} < \epsilon$ at the receiver. Essentially, perfect secrecy means that the receiver can decode the secret message with negligible decoding error probability, while the eavesdropper cannot decode the secret message. Further, *secrecy capacity* C_s was defined as the maximum achievable rate R such that perfect secrecy is maintained (i.e., $\Delta = 1$). Wyner [3] showed that for most channels, a non-zero secrecy capacity is achievable, i.e., $C_s > 0$, assuming that the eavesdropper's channel is a degraded version of the receiver's channel.

Note that the secrecy condition $\Delta = 1$ restricts the rate at which the eavesdropper can obtain the secret information. A stricter secrecy condition can be used for discrete memoryless channels, which restricts the total amount of secret information obtained by the eavesdropper without any reduction in the secrecy capacity, as shown by [7]. However, it is not known if a similar result holds for the Gaussian case considered in this chapter. Therefore, we will use the secrecy condition presented above.

The secrecy capacity for the Gaussian wire-tap channel was obtained in an explicit form in [6]. Both the receiver's and eavesdropper's channels were assumed to be additive white Gaussian noise (AWGN) channels, with the channel outputs given by,

$$z_k = x_k + n_k, \quad (2.1)$$

$$y_k = z_k + e_k, \quad (2.2)$$

where n_k and e_k are i.i.d. additive white Gaussian noise (AWGN) samples with variances σ_n^2 and σ_e^2 , respectively, and they are independent of each other. Thus, the equivalent transmitter-eavesdropper channel is an AWGN channel with noise variance $\sigma_n^2 + \sigma_e^2$. An average power constraint (over a codeword of length N) of P_0 was assumed, so that

$$\frac{1}{N} \sum_{i=1}^N \mathbf{E}[X_i^2] \leq P_0. \quad (2.3)$$

It was shown that the secrecy capacity for the Gaussian wire-tap model is given by,

$$C_s = \frac{1}{2} \log(1 + P_0/\sigma_n^2) - \frac{1}{2} \log(1 + P_0/(\sigma_n^2 + \sigma_e^2)). \quad (2.4)$$

The secrecy capacity, in this case, is given by the difference in the capacity of the receiver's channel and that of the eavesdropper's channel. Further, note that the secrecy capacity is positive for any power P_0 as long as $\sigma_e > 0$, i.e., as long as the eavesdropper's channel is degraded. An important question was whether the existence of non-zero secrecy capacity is only possible for the wire-tap model (which is a good model for wireline systems, but not for wireless systems).

2.2.3 Broadcast Model

In [4], the more general broadcast channel model was considered, where the eavesdropper's channel need not be a degraded version of the receiver's channel. In this model, the receiver and the eavesdropper have separate channels, and x^N is the input to both the channels. The outputs of these channels z^N and y^N are observed by the receiver and the eavesdropper, respectively. This is a more appropriate model for communication over the wireless broadcast channel. Again, perfect secrecy was defined in terms of equivocation, and secrecy capacity C_s was defined as the maximum rate at which secret information can be sent to the receiver, under perfect secrecy. It was shown that the secrecy capacity is given by [4],

$$C_s = \max[I(U; Z) - I(U; Y)], \quad (2.5)$$

where the maximization is over the joint distributions of random variables U, X which satisfy the Markov chain $U \rightarrow X \rightarrow YZ$. Instead of attempting to find the optimal transmission strategy, we will consider a particular strategy for generating the codeword x^N . Therefore, we obtain an achievable lower bound to Eq. (2.5). Notice that the term to be maximized in Eq. (2.5) is the difference in the mutual information between the transmitter and the receiver versus the eavesdropper. This

is similar to the difference in channel capacities in Eq. (2.4) but this result holds for more general channels.

We will use the result in Eq. (2.5), since the focus of this chapter is on secure communication over wireless channels. However, the eavesdropper can use the physical properties of the wireless medium to ensure that its channel is not worse than the receiver's channel, forcing the secrecy capacity to zero. For example, the eavesdropper may move closer to the transmitter than the receiver, or it can use directional antennas to increase its overall channel gain. We take a concrete example to show how such a scheme may affect secrecy capacity.

2.2.4 A Motivating Example

Let us consider a simple example where all the nodes—transmitter, receiver, and eavesdropper, have a single antenna each. We assume a simple flat-fading channel model [8] for both the transmitter-receiver and transmitter-eavesdropper channels. x_k is the transmitted symbol at time k , whereas z_k and y_k are the output samples of the receiver and eavesdropper channels, respectively, at time k . The output samples z_k and y_k are related to the transmitted symbol as,

$$z_k = h_k x_k + n_k, \quad (2.6)$$

$$y_k = g_k x_k + e_k, \quad (2.7)$$

where h_k and g_k are the time-varying channel gains in the receiver and eavesdropper channel, respectively. n_k and e_k are i.i.d. additive white Gaussian noise samples with variance σ_n^2 and σ_e^2 , respectively. A block fading model is assumed for h_k and g_k , meaning that they remain constant for a block of large number of symbols, and are independent across blocks. The assumption of constant h_k and g_k over a large number of symbols allows us to apply information theoretic results Eq. (2.5) in each block. The variation of h_k and g_k from block to block allows us to model the time-varying nature of a wireless channel (assuming the variation is slow). Across blocks, h_k and g_k are assumed to be complex numbers, i.i.d. Gaussian distributed (assuming Rayleigh fading), and independent of each other. A power constraint of P_0 is assumed, similar to Eq. (2.3). The average SNR at the receiver is given by $SNR_r = \mathbf{E}[|h_k|^2] P_0 / \sigma_n^2$. Similarly, the average SNR at the eavesdropper is given by $SNR_e = \mathbf{E}[|g_k|^2] P_0 / \sigma_e^2$.

The capacity of the transmitter-receiver channel is given by,

$$C = \log(1 + |h_k|^2 P_0 / \sigma_n^2). \quad (2.8)$$

The secrecy capacity is given by [4],

$$C_s = \left(\log(1 + |h_k|^2 P_0 / \sigma_n^2) - \log(1 + |g_k|^2 P_0 / \sigma_e^2) \right)^+, \quad (2.9)$$

where $(x)^+ \doteq \max(0, x)$. Note that both capacity C and secrecy capacity C_s are random variables, since they depend on h_k and g_k , which are random. We will

evaluate the performance in terms of outage probability. An outage occurs if the capacity (or the secrecy capacity) is smaller than a certain fixed value, called *outage capacity*, i.e., probability that a certain outage capacity cannot be supported. The secrecy requirements may be specified in terms of a certain outage probability, say 10^{-3} , at a desired outage capacity. For capacity, the outage probability for a certain outage capacity C_{outage} is defined as $Pr\{C < C_{outage}\}$. Outage probability for secrecy capacity is defined similarly. Another metric of interest may be expected capacity, which can be readily computed from the outage capacity versus outage probability curve.

Let us consider a specific scenario, to study the behavior of secrecy capacity. Assume that $SNR_e = SNR_r = 20$ dB (this can happen if they are at the same distance from the transmitter). The secrecy capacity will be zero whenever $|h_k| \leq |g_k|$ (assuming $\sigma_n^2 = \sigma_e^2$). It is easily seen using the symmetry of the problem, that the probability of this event is $1/2$. Thus, $C_s = 0$ with probability $1/2$. Clearly, the performance will be much worse when SNR_e is larger.

The outage probabilities for capacity C and secrecy capacity C_s , for various SNR_e , are shown in Fig. 2.1. The capacities are measured in nats/symbol (instead of bits/symbol), which means that we use $\log_e(\cdot)$ for calculating entropy. SNR_r is fixed at 20 dB, while SNR_e is varied from 10 to 30 dB. A higher SNR_e implies that the eavesdropper is closer to the transmitter, which results in a higher outage probability. For capacity, an outage probability of 10^{-2} can be achieved for $C_{outage} \sim 0.7$ nats/symbol. For secrecy capacity, however, even an outage probability of 10^{-1} can be barely achieved for an outage capacity of 0.1 nats/symbol, even when the eavesdropper's channel is 10 dB worse than the receiver's channel. In this chapter, the focus is on the worst case performance when the eavesdropper's SNR is much better than the receiver's SNR. However, the performance degrades rapidly as SNR_e increases. Clearly, the performance will not be good enough at large SNR_e , as evidenced from the plot for $SNR_e = 30$ dB. Note the rapid decay in performance with increasing SNR_e . Ideally, we would like to guarantee a low outage probability for secrecy capacity at a non-negligible outage capacity. The results in Fig. 2.1, however, suggest that providing such guarantees may be extremely difficult.

We will now present a secrecy scheme which uses the degrees of freedom provided by multiple transmit antennas, to add artificially generated noise to the secret message such that the eavesdropper is unable to decode the message. The receiver, on the other hand, can still decode the message, since the *artificial noise* is generated such that the receiver's channel is not affected. We will introduce the system model and notation in the next section.

2.3 System Description

In this section, we formally present the system model and notation. We begin by describing the scenario, and then discuss the assumptions of our model. We denote vectors and matrices with bold font, and the Hermitian operator by \dagger .

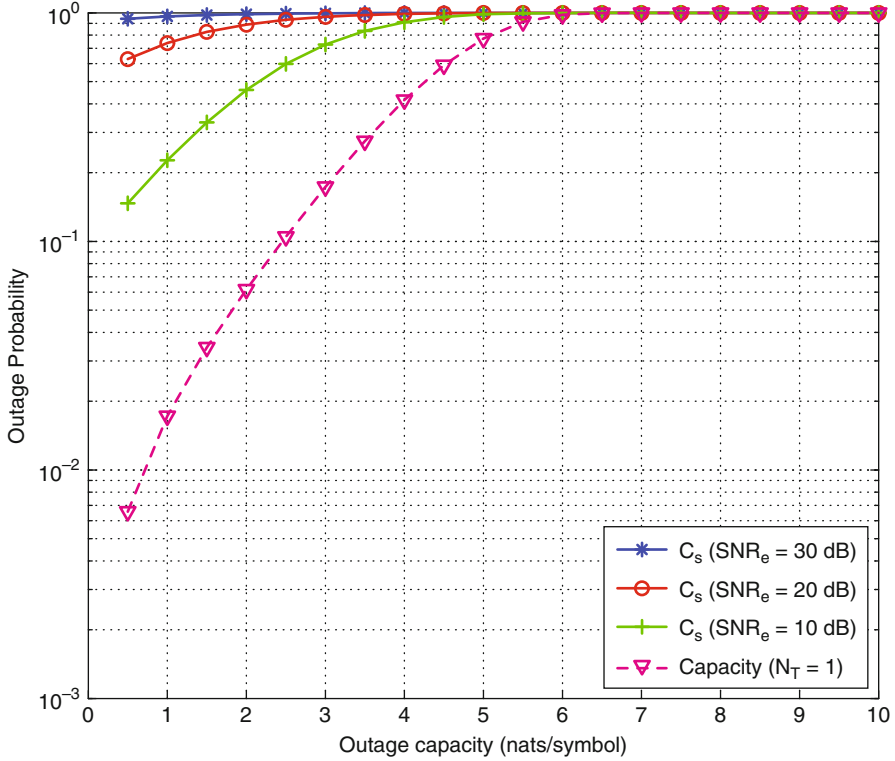


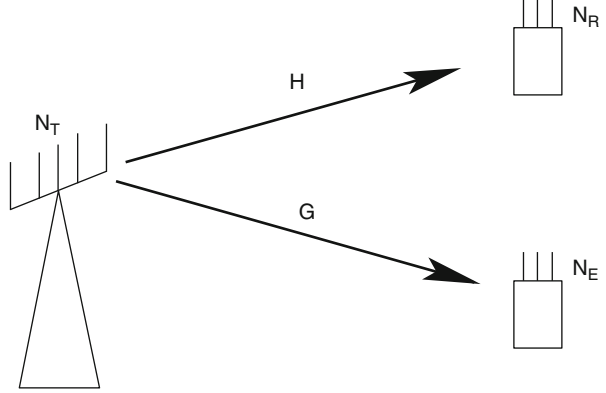
Fig. 2.1 Outage probability

2.3.1 Scenario

We consider the scenario where a transmitter wants to send information to the intended receiver secretly, over a wireless link, so that a passive eavesdropper cannot decode the secret information. This scenario is shown in Fig. 2.2. The transmitted signal propagates through the wireless medium and is received by both the receiver and the eavesdropper. The received signal suffers from both path loss and additive noise. The transmitter, receiver, and eavesdropper are assumed to have N_T , N_R , and N_E antennas respectively. The transmitter-receiver channel at time k is denoted by the $N_R \times N_T$ matrix \mathbf{H}_k . The j^{th} row of \mathbf{H}_k relates the received signal at the j^{th} receive antenna to the transmitted signal. In particular, the element of \mathbf{H}_k denoted by $h_{i,j}$, is the channel gains from transmit antenna i to receive antenna j . If \mathbf{x}_k is the transmitted signal, and \mathbf{z}_k is the received signal, both at time k , then the received signal is given by,

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{x}_k + \mathbf{n}_k, \quad (2.10)$$

Fig. 2.2 Framework for secrecy capacity



where the components of \mathbf{n}_k are i.i.d. Additive White Gaussian Noise (AWGN) samples with variance σ_n^2 . Similarly, the transmitter-eavesdropper channel is denoted by the $N_E \times N_T$ matrix \mathbf{G}_k , and signal received by the eavesdropper (\mathbf{y}_k) is given by,

$$\mathbf{y}_k = \mathbf{G}_k \mathbf{x}_k + \mathbf{e}_k, \quad (2.11)$$

where the components of \mathbf{e}_k are i.i.d. Additive White Gaussian Noise (AWGN) samples with variance σ_e^2 .

The multiple antennas at the eavesdropper can also be used as a model for multiple eavesdroppers, each with a single antenna, colluding to decode the secret information. A single eavesdropper with multiple antennas (equal to the number of eavesdroppers each with a single antenna) will model the case where the received signal from all the eavesdroppers can be processed by a central node, and thus, represents the worst case scenario in terms of maintaining secrecy.

The secrecy condition is defined in terms of fractional equivocation, defined as $\Delta \doteq H(m^K | \mathbf{y}^N) / H(m^K)$. Perfect secrecy is achieved if $\Delta = 1$. Secrecy capacity C_s is defined as the maximum rate at which secret information may be sent to the receiver, under perfect secrecy.

2.3.2 Assumptions

We assume that both, the receiver and the eavesdropper can estimate their own channels perfectly. The transmitter is assumed to know the receiver's channel \mathbf{H}_k through (authenticated) feedback over the wireless channel. However, it does not know the eavesdropper's channel \mathbf{G}_k , since the eavesdropper is passive. The eavesdropper, on the other hand, is assumed to know both the receiver's channel (since the receiver broadcasts its channel \mathbf{H}_k) as well as its own channel. This represents the best possible scenario for the eavesdropper.

Both the receiver's and the eavesdropper's channels are assumed to be slowly varying. A block fading model is assumed, meaning that the channel gain matrices \mathbf{H}_k and \mathbf{G}_k remain constant over a *block* of large number of symbols, and the gains are independent across blocks. The block fading model allows the application of information theoretic results in each block separately, where the channel gains are fixed. In each block, one codeword is transmitted, spanning the length of the block. The codeword is generated using an encoder chosen for the particular block based on the channel gains in the current block.

The transmitter is assumed to have a power constraint of P_0 , i.e., $\mathbf{E}[\mathbf{x}_k^\dagger \mathbf{x}_k] \leq P_0$.

2.4 Intentional Uncertainty Using Multiple Antennas

In Sect. 2.2.4, we saw that the secrecy capacity is close to zero with a high probability when the eavesdropper has a better channel than the intended receiver. This situation may easily occur in the broadcast wireless medium if, either the eavesdropper is closer to the transmitter, or the eavesdropper uses a directional antenna for reception (resulting in higher overall gain). Thus, at the first glance, it seems that guaranteeing information theoretic secrecy in a wireless environment may not be possible. Ideally, we would like to design a secrecy scheme which can guarantee non-zero secrecy capacity, even when the eavesdropper has a better channel than the receiver. However, this must be achieved without assuming the secrecy of channel gain information, and without the knowledge of the eavesdropper's location or its channel gain information. This section will present a secrecy scheme which shows that it is indeed possible to achieve non-zero secrecy capacity under the above stated conditions.

As shown in the previous section, the lower bound on secrecy capacity is the difference of two terms. The first term is the mutual information between the transmitter and the receiver $I(X; Z)$. An upper bound on this term is the capacity of the transmitter-receiver link. From the first term, we must subtract the mutual information between the transmitter and the eavesdropper $I(X; Y)$. For fixed channels \mathbf{H}_k , \mathbf{G}_k and given the statistics for \mathbf{x}_k , mutual information $I(X; Y)$ is fixed. Ideally, we would like to minimize the mutual information term $I(X; Y)$, while at the same time, maximize $I(X; Z)$. How can this be done, if the eavesdropper's channel \mathbf{G}_k is not known (since $I(X; Z)$ depends on \mathbf{G}_k)? One way to achieve this would be to somehow degrade the eavesdropper's channel, perhaps by introducing some intentional uncertainty in the transmitted signal. However, the uncertainty must be introduced such that the receiver's channel is unaffected. Further, the uncertainty must degrade the eavesdropper's channel substantially, regardless of the position of the eavesdropper. It may seem unlikely that designing such a scheme is at all possible. We now present a method for obtaining secrecy by introducing intentional uncertainty in the form of *artificial noise*. For simplicity in presentation, we will first present the case where the receiver and the eavesdropper each have a single antenna only, while the transmitter has multiple antennas.

2.4.1 Artificial Noise Generation Using Multiple Transmit Antennas

We now describe an approach that can selectively degrade the eavesdropper's channel. This is achieved by transmitting artificially generated noise along with the information signal. Formally, the transmitter chooses the transmitted signal \mathbf{x}_k as the *sum* of the information bearing signal \mathbf{s}_k and the *artificial noise* signal \mathbf{w}_k ,

$$\mathbf{x}_k = \mathbf{s}_k + \mathbf{w}_k. \quad (2.12)$$

The artificial noise is transmitted so that the intended receiver does not receive additional noise. This is achieved by generating the artificial noise such that it lies in the null space of the receiver's channel \mathbf{H}_k , i.e., $\mathbf{H}_k \mathbf{w}_k = \mathbf{0}$. Then, the received signal at the receiver is,

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{s}_k + \mathbf{n}_k. \quad (2.13)$$

Note how the artificial noise is nulled by the receiver's channel. Thus, the receiver only receives the information bearing signal, corrupted by AWGN. The transmit power dedicated to the information bearing signal, given by $P_{info} = \mathbf{E}[\mathbf{s}_k^\dagger \mathbf{s}_k]$, is smaller than the total transmit power P_0 , since some of the transmit power is used for artificial noise. This limits the information rate for secret information. The eavesdropper's channel \mathbf{G}_k is, in general, different from the receiver's channel \mathbf{H}_k . Hence, the artificial noise will not be nulled out in the eavesdropper's case. Indeed, the received signal for the eavesdropper is given by,

$$\mathbf{y}_k = \mathbf{G}_k \mathbf{s}_k + \mathbf{G}_k \mathbf{w}_k + \mathbf{e}_k. \quad (2.14)$$

Note that the artificial noise is present in Eq. (2.14), as opposed to Eq. (2.13). The artificial noise \mathbf{w}_k is generated as complex Gaussian random vector in the null space of \mathbf{H}_k . In particular, if \mathbf{Z}_k is an orthonormal basis for the null space, meaning that $\mathbf{Z}_k^\dagger \mathbf{Z}_k = \mathbf{I}$, then $\mathbf{w}_k = \mathbf{Z}_k \mathbf{v}_k$, where the elements of \mathbf{v}_k are i.i.d. complex Gaussian random variables, independent of each other, each with mean zero and variance σ_v^2 . The components of \mathbf{w}_k are Gaussian distributed as well but are not independent of each other. For the eavesdropper, both \mathbf{e}_k and $\mathbf{G}_k \mathbf{w}_k$ act as noise. Therefore, the eavesdropper's channel has an effective noise power of $\mathbf{E}|\mathbf{G}_k \mathbf{w}_k|^2 + \sigma_e^2$. Using Eq. (2.5), the secrecy capacity lower bound, in this case, is given by,

$$C_s \geq C_{sec} = \left(I(Z; U) - I(Y; U) \right)^+ \quad (2.15)$$

$$= \left(\log \left(1 + \frac{|\mathbf{H}_k \mathbf{p}_k|^2 \sigma_u^2}{\sigma_n^2} \right) - \log \left(1 + \frac{|\mathbf{G}_k \mathbf{p}_k|^2 \sigma_u^2}{\mathbf{E}|\mathbf{G}_k \mathbf{w}_k|^2 + \sigma_e^2} \right) \right)^+. \quad (2.16)$$

We have obtained a lower bound here, since we are using a specific scheme for introducing artificial noise, which may not be optimal.

Since the eavesdropper is passive, the transmitter is unaware of the eavesdropper's channel \mathbf{G}_k , and hence, it chooses the transmitted signal vector \mathbf{s}_k to maximize the

first term in Eq. (2.15). This is achieved by matching the signal vector \mathbf{s}_k to its channel \mathbf{H}_k , so that $\mathbf{s}_k = \mathbf{p}_k u_k$, where $\mathbf{p}_k = \mathbf{H}_k^\dagger / \|\mathbf{H}_k\|$, and u_k is the information signal. Thus, the secret message is transmitted in the range space of \mathbf{H}_k , while the artificial noise is transmitted in its null space. Hence, the two kind of signals are transmitted in orthogonal sub-spaces.

Intuitively, the outage probability of secrecy capacity should improve substantially as the number of transmit antennas increase. The secret message is always transmitted in the range space of \mathbf{H}_k , which is one dimensional here. The artificial noise, on the other hand, is transmitted in all the remaining dimensions ($N_T - 1$). As N_T increases, the probability that \mathbf{G}_k has a large component along \mathbf{H}_k reduces rapidly, since \mathbf{H}_k spans only 1 out of N_T dimensions. On the other hand, the probability of \mathbf{G}_k having a large component in the null space of \mathbf{H}_k increases rapidly, since the null space spans $N_T - 1$ out of N_T dimensions. Thus, with a high probability, $\mathbf{G}_k \mathbf{p}_k$ is small, while $\mathbf{G}_k \mathbf{w}_k$ is large, leading to a small $I(Y; U)$ based on Eq. (2.16).

Note the differences between Eq. (2.16) and Eq. (2.9). In Eq. (2.16), the first term involves σ_u^2 instead of P_0 , since only part of the available transmit power is used to transmit the information bearing signal. The rest of the power is transmitted as artificial noise, which only affects the eavesdropper's channel, as shown by the second term in Eq. (2.16).

The secrecy capacity lower bound C_{sec} obtained in Eq. (2.16) is a random variable because it depends on random channel gains \mathbf{H}_k and \mathbf{G}_k . In this scenario, the metrics of interest are the average of secrecy capacity and its outage probability. Even though \mathbf{G}_k is unknown at the transmitter, its statistics may be known. The average is taken over the random channel gains \mathbf{H}_k and \mathbf{G}_k to yield,

$$\overline{C_{sec}} \doteq \max_{f_1(\sigma_u^2, \sigma_v^2) \leq P_0} \mathbf{E}_{\mathbf{H}_k, \mathbf{G}_k} [C_{sec}]. \quad (2.17)$$

The outage probability for a given outage capacity C_{outage} is the probability that the secrecy capacity lower bound is smaller than the outage capacity, i.e., $\Pr\{C_{sec} < C_{outage}\}$.

We will now show how the artificial noise is different from AWGN, even though both of them affect the eavesdropper in the same manner. Equation (2.16) holds for specific values of noise powers σ_n^2 and σ_e^2 . In practice, the thermal noise power depends on temperature and bandwidth, while the channel gains are dependent on the transmitter-receiver distance. For convenience, let us normalize Eq. (2.16) by a factor of $\|\mathbf{G}_k\|$, so that the distance between the transmitter and the eavesdropper is modeled not by the channel gains $\|\mathbf{G}_k\|$, but by the noise power σ_e^2 . Thus, we can study the effect of eavesdropper's position on the secrecy capacity lower bound.

The key problem that we noticed in Sect. 2.2.4 was that the eavesdropper may have a better channel than the receiver, if it is closer to the transmitter, or if it uses a directed antenna for reception. This would imply a smaller σ_e^2 . In terms of maintaining secrecy, the worst case scenario would occur if $\sigma_e^2 \rightarrow 0$, i.e., if the eavesdropper's channel is noiseless. This is the *minimum* secrecy capacity that can be guaranteed regardless of the eavesdropper's position. Hence, it is called minimum

guaranteed secrecy capacity and is given by [9],

$$C_{sec,mg} = \left(\log \left(1 + \frac{\|\mathbf{H}_k\|^2 \sigma_u^2}{\sigma_n^2} \right) - \log \left(1 + \frac{|\mathbf{G}_k \mathbf{p}_k|^2 \sigma_u^2}{(\mathbf{G}_k \mathbf{Z}_k \mathbf{Z}_k^\dagger \mathbf{G}_k^\dagger) \sigma_v^2} \right) \right)^+. \quad (2.18)$$

Notice that in the absence of artificial noise ($\sigma_v^2 = 0$), the second term in Eq. (2.18) will be infinite, leading to minimum guaranteed secrecy capacity lower bound being identically zero, i.e., $C_{sec,mg} \doteq 0$. The presence of artificial noise limits the second term in Eq. (2.18) (mutual information between the transmitter and the eavesdropper), allowing for non-zero minimum guaranteed secrecy capacity. Further, the choice of σ_v^2 lies with the transmitter, and it can be increased up to the total available power P_0 to ensure secrecy in communication, unlike thermal noise power which is fixed.

Again, $C_{sec,mg}$ in Eq. (2.18) is a random variable, since it depends on the random channel gains \mathbf{H}_k and \mathbf{G}_k . Appropriate values for σ_u^2 and σ_v^2 are chosen based on the statistics of \mathbf{H}_k and \mathbf{G}_k . The average minimum guaranteed secrecy capacity is defined by taking expectation of $C_{sec,mg}$ over \mathbf{H}_k and \mathbf{G}_k , and by choosing the optimum σ_u^2 and σ_v^2 . Formally,

$$\overline{C_{sec,mg}} \doteq \max_{f_1(\sigma_u^2, \sigma_v^2) \leq P_0} \mathbf{E}_{\mathbf{H}_k, \mathbf{G}_k} [C_{sec,mg}]. \quad (2.19)$$

The outage probability for a given outage capacity C_{outage} is given by $Pr\{C_{sec,mg} < C_{outage}\}$.

2.4.2 Example

We now present an example to show the efficacy of the artificial noise technique, in providing secrecy. We compare the outage probability obtained, when using the artificial noise technique, with that obtained without the artificial noise. The artificial noise is generated using five transmit antennas. The receiver and the eavesdropper are assumed to have one antenna each. 70% power was used for the information signal (i.e., $\sigma_u^2/P_0 = 0.7$), while rest of the power was used for generating artificial noise.

In Fig. 2.3, we have superimposed the results obtained using artificial noise ($N_T = 5$), with the results in Fig. 2.1. The figure shows that the outage curve for capacity has improved. Instead of ~ 0.7 nats/symbol, now ~ 5 nats/symbol can be guaranteed at an outage probability of 10^{-2} . However, the improvement in the outage curve for secrecy capacity is far more dramatic. In contrast to not being able to provide any rate guarantees at outage probability of even 10^{-1} (assuming $SNR_e \geq 20$ dB), we can now guarantee a secrecy rate of ~ 3 nats/symbol at outage probability of 10^{-2} for the worst case scenario ($SNR_e \rightarrow \infty$). Note that the outage capacities for secrecy capacity and capacity are of the same order.

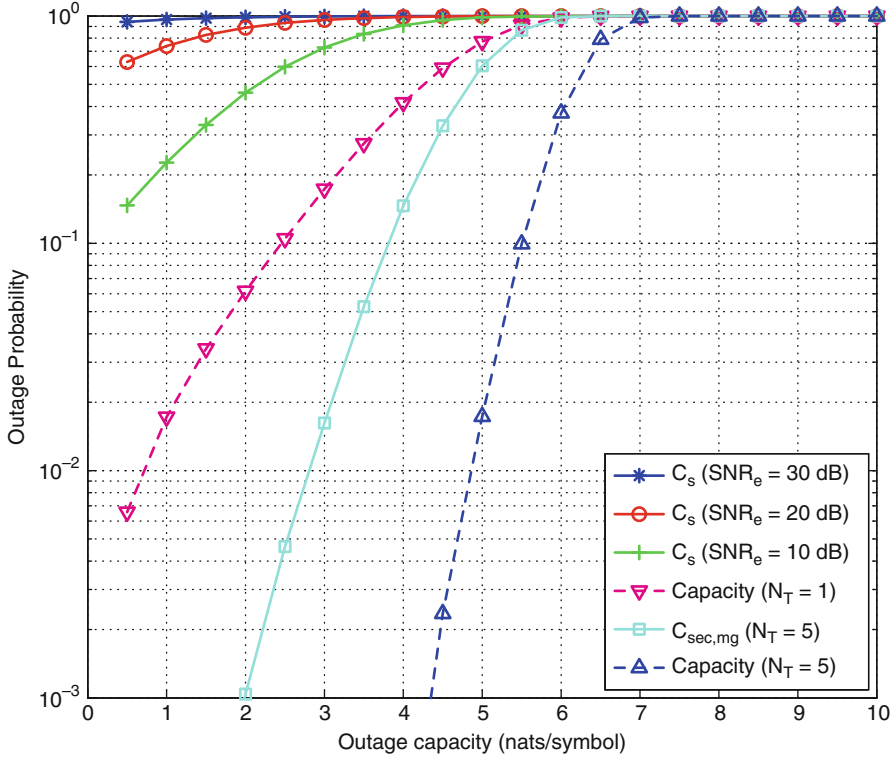


Fig. 2.3 Outage probability using artificial noise

2.4.3 Artificial Noise Generation in MIMO Scenario

Section 2.4.1 showed how artificial noise can be used to attain low outage probability for secrecy capacity, when both the receiver and the eavesdropper have a single antenna each. The scheme presented there can be extended to a more general scenario, where all the nodes—transmitter, receiver and eavesdropper may have multiple antennas. However, the artificial noise must be generated more carefully in this case. In particular, it is important to determine the number of dimensions to use for the artificial noise versus the information bearing signal, to ensure that minimum guaranteed secrecy capacity is non-zero.

Since we now have a matrix channel in Eq. (2.13), we will need to use results on multiple input multiple output (MIMO) capacity. For the receiver's channel given by Eq. (2.13), the capacity is given by $\log |\mathbf{I} + \mathbf{H}_k \mathbf{Q}_s \mathbf{H}_k^\dagger / \sigma_n^2|$ (see [10] for details), where $\mathbf{Q}_s = \mathbf{E}[s_k s_k^\dagger]$ is the covariance matrix for the information signal s_k , which is Gaussian distributed. Notice that this capacity expression reduces to $\log(1 + |\mathbf{H}_k|^2 \sigma_u^2 / \sigma_n^2)$ (in Eq. (2.16)), when $N_R = 1$.

The eavesdropper has a matrix channel as well, and the noise $\mathbf{G}_k \mathbf{w}_k + \mathbf{e}_k$ is characterized by the covariance matrix given by ([9]),

$$\mathbf{K} = (\mathbf{G}_k \mathbf{Z}_k \mathbf{Z}_k^\dagger \mathbf{G}_k^\dagger) \sigma_v^2 + \mathbf{I} \sigma_e^2. \quad (2.20)$$

As discussed in Sect. 2.4.1, the worst-case situation occurs when the eavesdropper has a noiseless channel, i.e., $\sigma_e^2 \rightarrow 0$. Then, the only noise received by the eavesdropper is the artificial noise, and hence, the noise covariance matrix is given by,

$$\mathbf{K}' = (\mathbf{G}_k \mathbf{Z}_k \mathbf{Z}_k^\dagger \mathbf{G}_k^\dagger) \sigma_v^2. \quad (2.21)$$

The capacity of the eavesdropper's channel is $\log(|\mathbf{K}' + \mathbf{G}_k \mathbf{Q}_s \mathbf{G}_k^\dagger|/|\mathbf{K}'|)$ [10].

Therefore, the minimum guaranteed secrecy capacity in this case is given by [9],

$$C_{sec,mg} = \log|\mathbf{I} \sigma_n^2 + \mathbf{H}_k \mathbf{Q}_s \mathbf{H}_k^\dagger| - \log(|\mathbf{K}' + \mathbf{G}_k \mathbf{Q}_s \mathbf{G}_k^\dagger|/|\mathbf{K}'|), \quad (2.22)$$

where $\mathbf{Q}_s = \mathbf{E}[\mathbf{s}_k \mathbf{s}_k^\dagger]$ and \mathbf{s}_k is complex Gaussian distributed. Further, $\mathbf{K}' = (\mathbf{G}_k \mathbf{Z}_k \mathbf{Z}_k^\dagger \mathbf{G}_k^\dagger) \sigma_v^2$. We immediately note that in order to avoid the case $|\mathbf{K}'| = 0$, the rank of \mathbf{Z}_k (which lies in the null-space of \mathbf{H}_k), must be at least N_E . Therefore, the transmitter must use at least N_E dimensions to transmit artificial noise, say N_{ND} dimensions. The remaining dimensions ($N_T - N_{ND}$) can be used to transmit the information bearing signal. On the other hand, at most N_R dimensions can be used to transmit the information bearing signal, since the receiver has only N_R antennas. Since both these conditions must be satisfied, the information bearing signal is transmitted in $N_S = \min(N_T - N_{ND}, N_R)$ dimensions. Further details on artificial noise generation may be found in [9]. A key observation in [9] was that the minimum guaranteed MIMO secrecy capacity does not behave like the usual MIMO capacity. In particular, it was shown that the minimum guaranteed MIMO secrecy capacity does not increase monotonically with the minimum of transmitter and receive antennas. This was confirmed both by analytical results in the case of large number of antennas, and simulation results for small number of antennas.

Goel and Negi [9] showed that analytical results can be obtained for secrecy capacity, in the regime of large number of antennas. The paper obtained a lower bound on the average minimum guaranteed secrecy capacity $\bar{C}_{sec,mg}(LB)$ using results from the theory of random matrices [12]. In particular, $\bar{C}_{sec,mg}(LB)$ was obtained in terms of eigenvalues of a Wishart matrix $\tilde{\mathbf{G}}_2 \tilde{\mathbf{G}}_2^\dagger$, where $\tilde{\mathbf{G}}_2$ represents the equivalent channel from the artificial noise signal \mathbf{v}_k to the eavesdropper [9]. The elements of $\tilde{\mathbf{G}}_2$ are i.i.d. complex Gaussian random variables. The eigenvalues are given by [11, 12],

$$p(\lambda) = \begin{cases} \frac{1}{\pi} \sqrt{\frac{\beta}{\lambda} - \frac{1}{4} \left(1 + \frac{\beta-1}{\lambda}\right)^2}, & \text{if } (\sqrt{\beta} - 1)^2 \leq \lambda \leq (\sqrt{\beta} + 1)^2 \\ 0, & \text{otherwise,} \end{cases} \quad (2.23)$$

where β depends on the dimensions of $\tilde{\mathbf{G}}_2$ as $\beta = N_{ND}/N_E$. Then, the lower bound $\overline{C_{sec,mg}}(LB)$ can be obtained as [9],

$$\begin{aligned} \overline{C_{sec,mg}} &\geq \overline{C_{sec,mg}}(LB) = \max_{tr(\mathbf{H}_k \mathbf{Q}_s \mathbf{H}_k^\dagger) + N_{ND} \sigma_v^2 \leq P_0} \\ \mathbb{E}[\log |\mathbf{I} \sigma_n^2 + \mathbf{H}_k \mathbf{Q}_s \mathbf{H}_k^\dagger| - \sum_i \log \left(\frac{P_{info} + \lambda_i \sigma_v^2}{\lambda_i \sigma_v^2} \right)] & \end{aligned} \quad (2.24)$$

where $P_{info} = tr(\mathbf{H}_k \mathbf{Q}_s \mathbf{H}_k^\dagger)$ is the transmit power of the information signal. $\overline{C_{sec,mg}}(LB)$ was computed numerically in [9] for various values of N_T , N_R , and N_E , and the results were compared with average capacity. The results showed that fairly large average secrecy capacity can be achieved using the artificial noise technique.

2.5 Related Work

In the last decade, several researchers have studied the problem of secret communication over the wireless medium, in presence of a passive eavesdropper.

Koorapaty, Hassan and Chennakeshu [13] presented a scheme for achieving secrecy by using the channel state information (CSI) as the secret key. In particular, the phase of the channel gain was used as the secret key, and was assumed known only to the transmitter and the receiver. The secret information was encoded into the phase of the transmitted signal. The transmitter compensated for the phase of the receiver's channel, so that the receiver could decode the secret message. The phase of the eavesdropper's channel, being different from that of the receiver's channel, in general, prevented the eavesdropper from decoding the message. However, the paper did not analyze the secrecy capacity achieved by this scheme. Hero [14] presented a more general scheme for the MIMO scenario, where perfect secrecy could be achieved under the assumption that the eavesdropper is unaware of its own channel. Essentially, the training sequence was used as the secret key in this case; assumed known only to the transmitter and the receiver. It was shown that the eavesdropper could be kept ignorant of the secret message, by choosing the space-time modulation such that the *spatial inner product* of the transmitted matrix remains constant. Note that while [13, 14] obtained secrecy by using CSI or training sequence as the secret key, the secrecy results presented in this chapter do not assume a shared secret key between the transmitter and the receiver. Li, Chen and Ratazzi [15] considered a MIMO scenario with $N_R = 1$, and an arbitrary number of antennas at the eavesdropper. The paper presented a scheme for introducing intentional ambiguity using multiple transmit antennas. A random beamforming direction was chosen such that the component along the receiver's channel is constant. The key assumption that ensured secrecy was that the eavesdropper is unaware of the receiver's channel, and hence, could not extract the signal component from the ambiguous received signal. The paper did not analyze the secrecy capacity of this scheme. Secrecy capacity for slow fading wireless channels was analyzed in [16], using the results in [4]. The

paper did not use a scheme to degrade the eavesdropper's channel by introducing ambiguity in the transmitted signal. Therefore, a non-zero secrecy capacity is possible only if the eavesdropper has a worse channel than the receiver. A fast fading channel model was considered in [17], under the assumption that the transmitter knows the channels gains of the eavesdropper's channel.

Recently, several researchers have studied the problem of secret communication over MIMO broadcast channels. Computing MIMO secrecy capacity when the eavesdropper's channel is not known at the transmitter is still an open problem. The secrecy problem in the MIMO scenario is made tractable by considering specific achievable schemes, which are not optimal. The problem is simplified by either assuming that no intentional ambiguity is introduced, or by assuming a specific encoding scheme for introducing ambiguity. Note that in the absence of intentional ambiguity (e.g., artificial noise), the secrecy capacity is zero when the eavesdropper's channel is noiseless, as opposed to the results in [9] which uses a stochastic encoder [4] to add artificial noise to the transmitted signal. References [18–21] have considered the MIMO scenario under the assumption that the eavesdropper's channel is known to the transmitter. [18] obtained the secrecy capacity for the MIMO scenario with $N_R = N_E = 1$, analytically. Shafiee, Liu and Ulukus [20] considered the MIMO case with $N_T = N_R = 2$ and $N_E = 1$, and showed that beamforming is the optimal transmission strategy in this case. The MIMO secrecy capacity for any N_T, N_R, N_E was computed in [19, 21]. Shafiee and Ulukus [22] considered the MIMO scenario under the assumption that only the eavesdropper knows its own channel. The paper considered the MIMO case with $N_R = N_E = 1$. It showed that the average secrecy capacity is maximized by beamforming in the direction of the receiver's channel.

Khisti and Wornell [23] considered the MIMO scenario with $N_R = 1$, where the eavesdropper's channel is not known at the transmitter. Instead of trying to find the optimal transmission strategy, the paper analyzed the artificial noise technique presented in [9, 25]. The paper obtained both an upper and a lower bound on the secrecy capacity in the regime of large number of antennas. Further, the paper presents upper and lower bounds on secrecy capacity for the fast fading scenario. The bounds were shown to be tight in the regime of large SNR. However, the paper used a (fixed) sub-optimal power allocation for information bearing signal and the artificial noise signal. In [24], the MIMO scenario with $N_R = N_E = 1$ was analyzed, where the transmitter sends independent confidential messages to two users with perfect secrecy. The paper presented an inner and outer bound for the capacity region.

2.6 Conclusions

The ease of passive eavesdropping in wireless networks poses a difficult challenge in providing secrecy guarantees. In this chapter, we reviewed results on information theoretic secrecy, and demonstrated using an example, that the traditional approaches are not sufficient in providing secrecy guarantees. We then presented a method of introducing intentional ambiguity (artificial noise) in the transmitted signal such that the

eavesdropper's channel is selectively degraded, thus enabling provably secure communication, based on the previous results. This chapter presented a specific scheme for introducing ambiguity in the transmitted signal, which may be sub-optimal. However, with this scheme, non-zero secrecy capacity can be guaranteed even when the eavesdropper has a noiseless channel, since the artificial noise power can be made proportional to the signal power. This is the key attribute of the artificial noise scheme presented in this chapter. Simulation results for a fading channel showed that fairly low outage probabilities can be achieved at non-negligible secrecy rates. We finally note that the problem of determining the optimal transmission strategy for perfect secrecy in a MIMO scenario is still an open problem.

References

- [1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 1949.
- [2] R. L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.
- [3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [4] I. Csiszar, J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, pp. 339–348, May 1978.
- [5] D. Welch, S. Lathrop, "Wireless security threat taxonomy," *Proc. IEEE Inf. Assurance Workshop 2003* pp. 76–83, Nov. 2006.
- [6] S. Leung-Yan-Cheong, M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
- [7] U. Maurer, S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," *LNCs*, Springer-Verlag, vol. 1807, pp. 352–368, 2000.
- [8] J. Proakis, "Digital Communications," McGraw-Hill, 1989.
- [9] S. Goel, R. Negi, "Guaranteeing secrecy using artificial noise," to appear in *IEEE Trans. Wireless Commun.*, Jun. 2008.
- [10] E. Telatar, "Capacity of multi-antenna Gaussian channels," *Eur. Trans. Telecomm. ETT*, vol. 10, no. 6, pp. 585–596, Nov. 1999.
- [11] B. M. Hochwald, T. L. Marzetta, V. Tarokh, "Multiple-antenna channel hardening and its implications for rate feedback and scheduling," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 1893–1909, Sep. 2004.
- [12] J. W. Silverstein, Z. D. Bai, "On the empirical distribution of eigenvalues of a class of large dimensional random matrices," *J. Mult. Anal.*, vol. 54, pp. 175–192, 1995.
- [13] H. Koorapaty, A. A. Hassan, S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Trans. Wireless Commun.*, pp. 52–55, Jul. 2003.
- [14] A. E. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, pp. 3235–3249, Dec. 2003.
- [15] X. Li, M. Chen, E. P. Ratazzi, "Space-time transmissions for wireless secret-key agreement with information-theoretic secrecy," *Proc. IEEE SPAWC 2005*, pp. 811–815, June 2005.
- [16] J. Barros, M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT) 2006*, Jul. 2006.
- [17] Y. Liang, H. V. Poor, S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.
- [18] Z. Li, W. Trappe, R. Yates, "Secret communication via multi-antenna transmission," *Proc. CISS '07*, Baltimore, MD, pp. 905–910, Mar. 2007.

- [19] F. Oggier, B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *Preprint*, available at http://arxiv.org/PS_cache/arxiv/pdf/0710/0710.1920v1.pdf
- [20] S. Shafiee, N. Liu, S. Ulukus, "Towards the Secrecy Capacity of the Gaussian MIMO Wire-tap Channel: The 2-2-1 Channel," *Preprint*, available at http://arxiv.org/PS_cache/arxiv/pdf/0709/0709.3541v1.pdf
- [21] A. Khisti, G. W. Wornell, "The MIMOME Channel," *Preprint*, available at http://arxiv.org/PS_cache/arxiv/pdf/0710/0710.1325v1.pdf
- [22] S. Shafiee, S. Ulukus, "Achievable rates in Gaussian MISO channels with Secrecy constraints," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT) 2007*, Jun. 2007.
- [23] A. Khisti, G. W. Wornell, "Secure Transmission with Multiple Antennas: The MIS-OME Wiretap Channel," *Preprint*, available at http://arxiv.org/PS_cache/arxiv/pdf/0708/0708.4219v1.pdf.
- [24] R. Liu, V. Poor, "Multiple Antenna Secure Broadcast over Wireless Networks," *Preprint*, available at http://arxiv.org/PS_cache/arxiv/pdf/0705/0705.1183v1.pdf.
- [25] S. Goel, R. Negi, "Secret communication in presence of colluding eavesdroppers," *Proc. MILCOM*, vol. 3, pp. 1501–1506, Nov. 2005.
- [26] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
- [27] R. Negi, S. Goel, "Secret communication using artificial noise," *Proc. VTC Fall 2005*, vol. 3, pp. 1906–1910, Sep. 2005.
- [28] G. J. Foschini, M. J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas," *Wireless Pers. Commun.* Kluwer Academic Press, no. 6, pp. 311–335, 1998.
- [29] U. M. Maurer, S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 499–514, Mar. 1999.
- [30] D. Chizhik, J. Ling, P. W. Wolniansky, R. A. Valenzuela, N. E. Costa, K. Huber, "Multiple-input-multiple-output measurements and modeling in Manhattan," *IEEE J. Select. Areas Commun.*, vol. 21, no. 3, pp. 321–331, Apr. 2003.
- [31] G. J. Foschini, D. Chizhik, M. J. Gans, C. Papadias, R. A. Valenzuela, "Analysis and performance of some basic spacetime architectures," *IEEE J. Select. Areas Commun., Special Issue on MIMO Systems*, pt. I, vol. 21, pp. 303–320, Apr. 2003.
- [32] J. N. Laneman, D. N. C. Tse, G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

Securing Wireless Communications at the Physical
Layer

Liu, R.; Trappe, W. (Eds.)

2010, XVI, 396 p., Hardcover

ISBN: 978-1-4419-1384-5