Achieving Secret Communication for Fast Rayleigh Fading Channels

Zang Li, Roy Yates, *Member, IEEE*, and Wade Trappe, *Member, IEEE*

***Abstract*—We consider a secret communication scenario where Alice wants to transmit secretly to Bob in presence of a passive eavesdropper Eve. The Alice-Bob channel is a fixed-SNR AWGN channel, while the Alice-Eve channel is a fast Rayleigh fading channel, with the channel states only known to Eve. Alice knows the statistics of Alice-Eve channel, but not the exact realizations. We investigate the achievable secrecy rates for this channel model with Gaussian signaling and discrete signaling. For Gaussian signaling, several transmission strategies according to the main channel's relative channel gain are proposed and evaluated. For discrete signaling, achievable secrecy rates with Quadrature Amplitude Modulation (QAM) are evaluated. When Bob's channel is much better than Eve's channel, simple Gaussian signaling can perform close to the upper bound, and is better than the rate achieved with M-QAM. When Bob's channel gain is on average worse than the eavesdropper's average channel gain, positive secrecy rate can still be achieved for Gaussian signaling with artificial noise injection and a burst signaling strategy. Moreover, M-QAM can outperform Gaussian signaling. The key factor that enables secret communication in this case is that both M-QAM and artificial noise limit the leakage of information when Eve's channel is unusually good.**

***Index Terms*—Security, wireless communications, secrecy rate.**

I. Introduction

ENSURING the confidentiality of communications is fundamental to securing the operation of any network. This requirement is particularly important for wireless systems, where eavesdropping is facilitated by the broadcast nature of the wireless medium. Although the nature of the wireless channel presents a challenge to providing secret communications, it might also provide the means to overcome the challenges of a broadcast medium. In particular, the time-varying wireless channel can provide a means to achieve secrecy in spite of the presence of eavesdroppers because the multipath and changing environment ensures that different users will get different instantiations of the noisy received signal. This can be utilized to achieve confidential transmission of information (such as keys that may be used to support other security services) among users.

In an information-theoretic secret communication system, a sender (Alice) wishes to reliably communicate a secret S to an intended receiver (Bob) in the presence of an eavesdropper (Eve). To do so, Alice maps S to an encoded signal $X^n = X_1, \ldots, X_n$ transmitted in n channel uses; Bob receives the channel output $Y^n = Y_1, \ldots, Y_n$ and decodes $\hat{S}$; Eve overhears a potentially different output $Z^n = Z_1, \ldots, Z_n$. The coding is designed such that Bob's decoding error can be made arbitrarily small while Eve obtains almost no information regarding the secret message, i.e., Z^n does not reduce Eve's uncertainty about the secret message. Mathematically, Eve's uncertainty regarding the secret message S is measured by the conditional entropy $H(S|Z^n)$. A secrecy rate R is said to be achievable if for any $\epsilon > 0$ there exists a rate R encoder and decoder with large enough block length n, such that

$$P(S \neq \hat{S}) \leq \epsilon, \tag{1a}$$

$$\frac{1}{n} I(S; Z^n) = \frac{H(S) - H(S|Z^n)}{n} \leq \epsilon. \tag{1b}$$

In this paper, we examine the achievable ergodic secrecy rate for the channel model where Bob has a constant gain AWGN channel, while Eve has a fast Rayleigh fading channel with additive white Gaussian noise. We assume that Eve's channel realizations are unknown to Alice and Bob, but its statistics (i.e. average channel gain) is known. We also assume that the main channel gain is known to all parties. Hence, in our work, the eavesdropper is actually quite powerful as she has the most complete channel state information. The ergodic assumption implies that the codeword is long enough to experience an ergodic realization of the channel states. We investigate the achievable secrecy rate for this channel model with Gaussian signaling and discrete signaling. For Gaussian signaling, several transmission strategies according to the main channel's relative channel gain are proposed and evaluated. For discrete signaling, achievable secrecy rates with Quadrature Amplitude Modulation (QAM) are evaluated. When Bob's channel is much better than Eve's channel, we show that simple Gaussian signaling can perform close to the upper bound, and is better than QAM in terms of achievable secrecy rate. In addition, when Bob's channel gain is on average worse than the eavesdropper's average channel gain, positive secrecy rate can still be achieved for Gaussian signaling when used with artificial noise injection and a burst signaling strategy. However, in this case, M-QAM can perform better than Gaussian signaling. The key to achieve secret communication in this case is to limit the information leakage when Eve's channel is really good.

Manuscript received July 6, 2009; revised December 30, 2009; accepted June 24, 2010. The associate editor coordinating the review of this paper and approving it for publication was R. Cheng.

Part of this work was presented in ISIT 2007.

Z. Li was with the Wireless Information Network Laboratory, Department of Electrical and Computer Engineering, Rutgers University, North Brunswick, NJ 08902 when the work was done (e-mail: zang.li@gmail.com).

R. Yates and W. Trappe are with the Wireless Information Network Laboratory, Department of Electrical and Computer Engineering, Rutgers University (e-mail: {ryates, trappe}@winlab.rutgers.edu).

The authors would like to acknowledge the support of NSF grants CNS-0721826, CNS-0626439, and CNS-0716400, and Army contract ARO W911NF-09-1-0089.

Digital Object Identifier 10.1109/TWC.2010.080210.090948

Note that, although in this model the main channel has a constant gain, not the more general fading gain random process, it is clear that the latter is a temporal concatenation of our simple model with various main channel gains. Thus, power allocation over time can be used to obtain secrecy rates of the more general model with fading on both the main channel and the eavesdropper's channel, and the main channel state known by Bob. On the other hand, although our channel model is simple, we will show that it already exhibits some intriguing behavior. It is exactly this interesting behavior that consists of the main focus of the paper. On the other hand, due to the irregular achievable rate of the constant main channel model, and that an optimal solution for this channel remains elusive, it is hard to get any analytical expression for the more general fading channel.

As for the organization of this paper, we will first briefly review the background on information theoretic secret communication in Section II, and formulate our problem in Section III. The achievable secrecy rate with Gaussian signaling is discussed in Section IV, followed by the achievable secrecy rate with discrete signaling in Section V. Finally, we conclude the paper in Section VI.

II. Background

The model of information-theoretic secret communication started with Wyner's analysis of the discrete memoryless wiretap channel [1]. In Wyner's system, Eve hears a degraded version of Bob's received signal in that the channels are defined by a Markov chain $X \rightarrow Y \rightarrow Z$. This was generalized by Csiszár and Körner [2] to a discrete memoryless broadcast system. They showed that for such a broadcast channel, the secrecy capacity, i.e. the largest achievable secrecy rate, is given by

$$\mathcal{C}_s = \max_{V \rightarrow X \rightarrow YZ} I(V;Y) - I(V;Z), \tag{2}$$

where V is an arbitrary auxiliary random variable satisfying the Markov chain $V \rightarrow X \rightarrow YZ$. Given the discrete memoryless channel (DMC) $P_{YZ|X}$, secrecy capacity is achieved by maximizing over all valid joint distributions $P_{V,X}(v,x)$.

In theory, (2) is a complete characterization of the secrecy capacity $\mathcal{C}_s$; however, many questions remain unanswered. For example, the auxiliary V is often essential but there are no systematic methods to optimize over P_V and the $P_{X|V}$ channel. However, for fixed channels, some results are known when Bob's and Eve's channels satisfy certain conditions. In [2], it was shown that if Bob's channel is *more capable* than Eve's channel in that $I(X;Y) - I(X;Z) \geq 0$ for all inputs X, then the secrecy rate $\mathcal{C}_s$ is achieved when $V = X$. Leung-Yan-Cheong and Hellman [3] showed that when both Bob's and Eve's channels are AWGN, a Gaussian input X maximizes $\mathcal{C}_s$. Thus, for a real AWGN channel model

$$Y = \sqrt{b}X + W_1, \;\; Z = \sqrt{g}X + W_2, \tag{3}$$

where both W_1 and W_2 are Gaussian white noise with unit variance, an average power P for the input X yields a secrecy capacity of

$$\mathcal{C}_s^{\text{AWGN}}(b,g,P) = \frac{1}{2}\big(\log(1+bP) - \log(1+gP)\big)^+, \tag{4}$$

where $(x)^+ = \max(x,0)$. In this case, if Eve's channel has a better SNR than Bob's channel, it is not possible to achieve secret transmission with positive rate.

On the other hand, the time-varying wireless channel provides an opportunity for secret communication. For a wiretap channel with additive white Gaussian interference known noncausally to the transmitter, a perfect-secrecy-achieving coding strategy which is optimal in some situations was proposed in [4]. A rate equivocation achievable region for the discrete memoryless wiretap channel with side information was given in [5]. When the broadcast channels are fading, Bob's channel can be better than Eve's at one time but worse at another. Outage calculations for Rayleigh fading channels were performed in [6]. When the fading channel states are known to all parties, the secrecy capacity was derived in [7]–[10] and is achievable with Gaussian random codes with optimal power adaptation. When the eavesdropper's channel is unknown but the main channel gain is known, the secrecy capacity of the slow block fading channel was derived in [10]. However, an important assumption there is that both the main channel and eavesdropper's channel vary sufficiently slowly to be modeled as constant over each fading block, but also vary sufficiently fast so that a codeword can experience an ergodic realization of fading blocks. In this paper, we consider the situation when the slow block fading assumption does not hold. In particular, Eve's channel randomly changes over each symbol time, and we assume that the codeword is long enough to see an ergodic realization of Eve's channels. We also assume that the main channel gain is known at the transmitter. When main channel state information is not completely available at the transmitter, optimal coding strategy was investigated in [11], where the secret communication problem in presence of an eavesdropper was formulated as a zero-sum game with signal-to-interference ratio being the objective function. It was shown that the optimal strategy for the legitimate user depends on the channel state information at transmitter, and the best strategies under several channel state information assumptions were discussed. A more extensive review on information theoretic secret communication can be found at [12], [13].

III. Problem Formulation

In this paper, we consider the situation when Bob's channel is an AWGN channel with a fixed SNR, while Eve has a Rayleigh fading channel with the channel statistics (not the realizations) known to the other parties. Mathematically,

$$Y_i = \sqrt{\tilde{b}}\tilde{X}_i + W_{1,i}, \tag{5a}$$

$$Z_i = \sqrt{\tilde{G}_i}\tilde{X}_i + W_{2,i}, \tag{5b}$$

where i is the time index, $W_{1,i}, W_{2,i}$ are independent white Gaussian noise with normalized variance 1, and $\tilde{b}$ is the constant channel gain for Bob. Eve's time varying channel gain $\tilde{G}_i$ is an exponential random variable due to the Rayleigh fading model, and is perfectly observable by Eve. Alice knows Eve's average channel gain $\bar{G}$, but not the exact realization. We further assume that Alice-Bob channel gain is known to all parties. By making these assumptions, we have considered a quite powerful adversarial model as Eve has more complete information of the system.

We can further normalize the channel gain of Bob by the average channel gain of Eve through the transformation

$$Y_i = \sqrt{\tilde{b}/\bar{G}}\sqrt{\bar{G}}\tilde{X}_i + W_{1,i}, \tag{6a}$$

$$Z_i = \sqrt{\tilde{G}_i/\bar{G}}\sqrt{\bar{G}}\tilde{X}_i + W_{2,i}. \tag{6b}$$

Defining $b = \tilde{b}/\bar{G}$, $G_i = \tilde{G}_i/\bar{G}$ and $X_i = \sqrt{\bar{G}}\tilde{X}_i$, we obtain the simplified channel model

$$Y_i = \sqrt{b}X_i + W_{1,i}, \tag{7a}$$

$$Z_i = \sqrt{G_i}X_i + W_{2,i}. \tag{7b}$$

Now, the normalized channel gain G_i follows exponential distribution with mean 1 and b is the relative gain of Bob against Eve, and $P = E\left[X_i^2\right] = \bar{G}E\left[\tilde{X}_i^2\right]$ is Eve's average received SNR. From now on, we will use this model, and refer to b as Bob's channel gain, and P as the average power of X. Note that the parameter b indicates whether Bob's average SNR is higher ($b > 1$) or lower ($b < 1$) than Eve's average received SNR.

If we consider the random channel observation G_i at Eve as an output, Eve's channel is equivalent to a channel with output (G, Z) and the channel transition probability is $\Pr(GZ|X) = \Pr(G)\Pr(Z|XG)$. Following Csiszár and Körner's arguments [2], the secrecy capacity of the channel model (7) is

$$\mathcal{C}_s = \max_{V\to X\to YGZ} I(V;Y) - I(V;GZ) \tag{8}$$

$$= \max_{V\to X\to YGZ} I(V;Y) - I(V;Z|G), \tag{9}$$

where (9) follows from the independence of V and G since Alice does not know G and must choose V independent of G. This channel does not satisfy the more capable condition, and it appears to be hard to obtain the optimal V and $P(X|V)$. Instead, in this work, we study the achievable secrecy rates that are possible with random Gaussian codes and with discrete signaling.

IV. Achievable Secrecy Rates with Gaussian Random Codes

The achievable secrecy rates with Gaussian random codes were studied in [14]. This work showed that when Bob's channel gain is larger than Eve's average channel gain, Gaussian random codes can achieve secrecy rate close to the secrecy capacity derived in [10] for slow block fading channels. This secrecy capacity is derived under the assumption that Eve's channel variation is sufficiently slow that long code blocks are transmitted through a fixed channel to Eve. Since any rate achievable when Eve has a fast fading channel is also achievable through sufficient interleaving when Eve has a slow block fading channel, the secrecy capacity in [10] provides an upper bound to the secrecy capacity when Eve has a fast fading channel. When Bob's channel gain is smaller than Eve's average channel gain, Gaussian random codes with artificial noise and bursting can still achieve positive secrecy rate. We briefly review the results of [14] in this section.

Define

$$\Delta(P,b) = \log_2(1+bP) - E\left[\log_2(1+GP)\right], \tag{10}$$

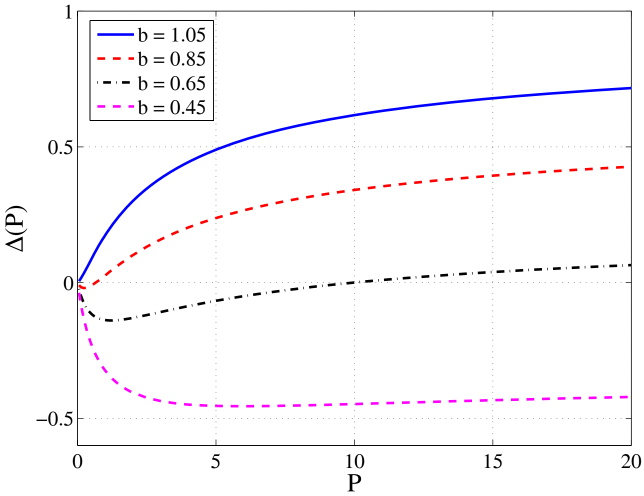


Fig. 1. The function $\Delta(P)$, given by (11), at different levels of b.

where E denotes expectation over the Rayleigh random variable G. Since $E[G] = 1$, the function, as shown in [14] can be further written as

$$\Delta(P,b) = \log_2(1+bP) - \frac{1}{\log_2 e}e^{1/P}E_1(1/P), \tag{11}$$

where $E_1(x)$, the En-function for $n = 1$, is given by

$$E_1(x) = \int_x^\infty \frac{e^{-t}}{t}dt = \int_1^\infty \frac{e^{-xt}}{t}dt$$

$$= -\gamma - \ln(x) - \sum_{n=1}^\infty \frac{(-1)^n x^n}{n!n}, \tag{12}$$

and $\gamma = 0.57721566\cdots$ is the Euler-Mascheroni constant. More detail on the En-function and Euler-Mascheroni constant can be found in [15]. The function $\Delta(P, b)$ is the difference of the main channel mutual information and the eavesdropper's information with a simple Gaussian signaling, and is a function of the signal power P and the main channel gain b. Since we will view b as a parameter of the model, we remove b from the parameter list of this function from now on to simplify the notation. Note that in [14], the log function has the base e, while here the log function has base 2, so the units will be bits per channel use. We also adopt different notations from that used in [14] for better presentation. $\Delta(P)$ is plotted in Fig. 1 at several values of b. The curves are not necessarily convex, and are not always positive. It was shown in [14] that the function is negative regardless of P if

$$b \leq \lim_{P\to\infty} \frac{1}{P}\left(e^{E\left[\ln(1+GP)\right]} - 1\right) = e^{-\gamma} \approx 0.56146. \tag{13}$$

When $b \geq 1$, the function $\Delta(P)$ is always positive for positive power P. While for $0.56146 < b < 1$, the curve is negative for small power P, but then becomes positive and remains positive when P is greater than a threshold.

A. Gaussian random codes with constant power

For this scheme, no auxiliary random variable is used and $V = X$. Moreover, the codewords are drawn from i.i.d.

Gaussian with constant power P. The achievable rate for this choice of input is given by

$$\mathcal{R}_x(P) = (I(X;Y) - I(X;Z|G))^+ \tag{14}$$
$$= \left(\log_2(1+bP) - E\big[\log_2(1+GP)\big]\right)^+ \tag{15}$$
$$= (\Delta(P))^+, \tag{16}$$

where $(x)^+ = \max(x,0)$. This rate is close to the slow fading upper bound derived in [10] when $b > 1$. But when (13) holds, the achievable rate for this scheme is zero regardless of available power.

B. Gaussian random codes with artificial noise

The previous scheme is simple, but cannot obtain a positive secrecy rate when $b < e^{-\gamma}$. An alternative strategy is to utilize the auxiliary random variable V and the virtual $V \to X$ channel to confuse Eve. A simple virtual channel is the AWGN channel $X = V + W$, where W is an artificial additive noise. The idea of adding artificial noise for secrecy is not completely new, and was explored in [16], in the context of a multiple antenna system in which the noise is chosen to be orthogonal to the information bearing signal. In our case, however, the artificial noise will affect both Bob and Eve. It follows from (7) that AWGN $V \to X$ channel yields the $V \to YZ$ broadcast channel

$$Y_i = \sqrt{b}V_i + \sqrt{b}W_i + W_{1,i}, \tag{17a}$$
$$Z_i = \sqrt{G_i}V_i + \sqrt{G_i}W_i + W_{2,i}. \tag{17b}$$

We assume V and W are independent Gaussian random variables with mean 0 and variance P_v and P_w respectively. The transmit power constraint becomes $P_x = P_v + P_w \le P$.

The secrecy rate achieved by this modified channel is

$$\mathcal{R}_v(P) = (I(V;Y) - I(V;Z|G))^+ \tag{18}$$
$$= \left(\log\left(1+\frac{bP_v}{bP_w+1}\right) - E\left[\log\left(1+\frac{GP_v}{GP_w+1}\right)\right]\right)^+ \tag{19}$$
$$= (\Delta(P_v+P_w) - \Delta(P_w))^+ \tag{20}$$
$$= (\Delta(P_x) - \Delta(P_w))^+\,. \tag{21}$$

Note that if P_w is chosen such that $\Delta(P_w) < 0$, the achievable rate with the preprocessing channel will be larger than that without the preprocessing channel for Gaussian random codes. Moreover, even when $\Delta(P_x) < 0$, which leads to zero secrecy rate for simple Gaussian codes, positive secrecy rate is still possible with the preprocessing channel as long as the difference (21) is positive.

When $b < 1$, the minimum value of $\Delta(P)$ will be negative. The optimal noise power, denoted as P_w^*, is the power that gives the minimum $\Delta(P)$. Therefore, P_w^* satisfies the condition

$$\Delta'(P)|_{P=P_w^*} = 0. \tag{22}$$

Calculating the derivative of the function $\Delta(P)$, we can see that (22) is equivalent to

$$b = \frac{E\big[G/(1+GP_w^*)\big]}{E\big[1/(1+GP_w^*)\big]} = \frac{1}{e^{1/P_w^*}E_1(1/P_w^*)} - \frac{1}{P_w^*}. \tag{23}$$

Because the value of the right side function varies from 1 to 0 as the power varies from 0 to ∞, there always exists a finite P_w^* satisfying the condition for $b \in (0,1)$. Moreover, $\Delta(P)$ is monotonically decreasing for $P < P_w^*$, and increasing for $P > P_w^*$. Therefore, if the power budget $P \le P_w^*$, since $P_w < P_x \le P$, no positive rate is achievable. If the power budget $P > P_w^*$, $P_x = P$ and $P_w = P_w^*$ maximize the achievable rate $\mathcal{R}_v(P)$.

In summary, with the strategy of injecting artificial additive independent Gaussian noise, the achievable secrecy rate is

$$\mathcal{R}_v(P) = \begin{cases} \Delta(P) - \Delta(P_w^*), & P > P_w^*, \\ 0, & P \le P_w^*. \end{cases} \tag{24}$$

Note that P_w^* increases as Bob's channel gain b decreases. When $b \ge 1$, $P_w^* = 0$ because no noise power can make $\Delta(P_w^*)$ negative. When $b < 1$, although there is no analytical solution for P_w^*, we can shown that $P > e^{\gamma+1/b}$ implies that $\mathcal{R}_x'(P) > 0$, which guarantees that $P > P_w^*$ and $\mathcal{R}_v(P) > 0$. Therefore, power $e^{\gamma+1/b}$ can serve as a rule of thumb estimate of the power needed to achieve a positive secrecy rate using noise injection.

C. Gaussian random codes with artificial noise and bursting

The previous schemes show that, when $b \ge 1$, simple Gaussian codes can achieve a positive secrecy rate regardless of the power budget; when $0 < b < 1$, the Gaussian codes with artificial noise method can achieve positive secrecy rate with sufficiently large P no matter how small b is. However, for small b, a realistic given power budget may not be sufficient. To obtain positive secrecy rate with any average power budget $\bar{P}$, a burst transmission method is proposed. In other words, the transmitter Alice chooses not to transmit for $1-\delta$ fraction of time, so that she can use a higher power in the remaining δ fraction of time when he transmits. A simple bursting strategy that uses power $\bar{P}/\delta$ for δ fraction of time and zero power otherwise achieves the average secrecy rate

$$\bar{\mathcal{R}}_s(\bar{P},\delta) = \delta\mathcal{R}_v(\bar{P}/\delta). \tag{25}$$

The optimal δ can be found by searching the $\delta^* \in (0,1)$ that makes the derivative of (25) with respective to δ be zero. If we define $\tilde{P}$ be the positive power that satisfies

$$\mathcal{R}_v(\tilde{P}) = \tilde{P}\mathcal{R}_v'(\tilde{P}), \tag{26}$$

then [14] shows that the optimal δ^* is given by

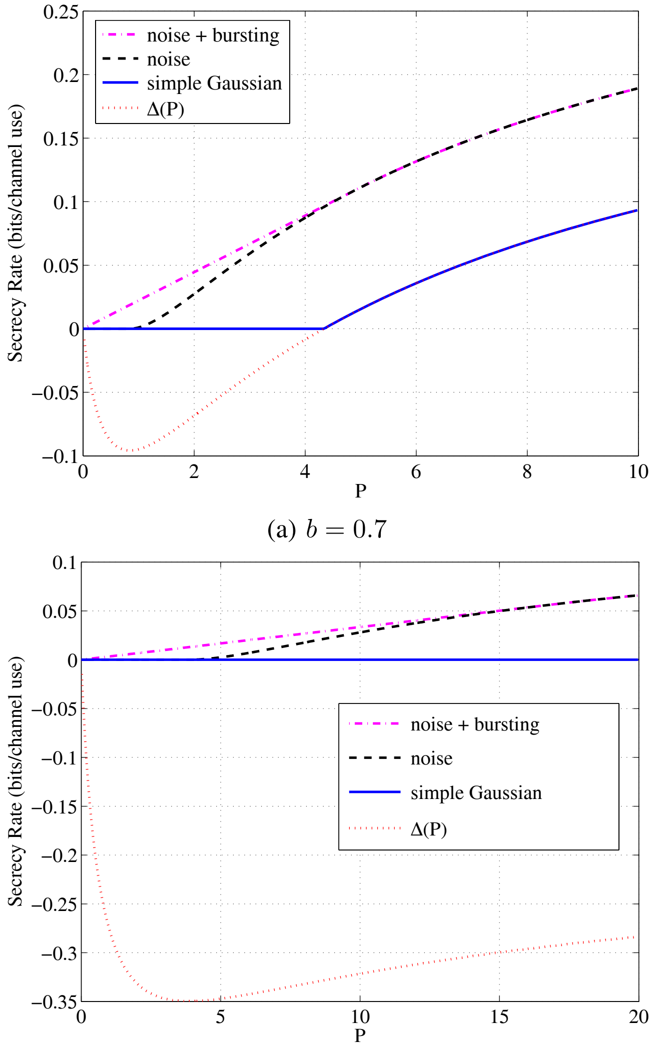
$$\delta^*(\bar{P}) = \min\{\bar{P}/\tilde{P}, 1\}. \tag{27}$$

$\delta^* = 1$ means no bursting is needed. Note that $\tilde{P}$ is actually a function of b, Bob's relative channel gain. Moreover, the condition (26) implies the line tangent to the curve $\mathcal{R}_v(P)$ at $\tilde{P}$ passes through the origin with positive slope.

Substituting the optimal δ^* given by (27) into (25), we can get the achievable rate of the burst strategy with artificial noise as

$$\bar{\mathcal{R}}_s(\bar{P}) = \begin{cases} \frac{\bar{P}}{\tilde{P}}\mathcal{R}_v(\tilde{P}) = \bar{P}\mathcal{R}_v'(\tilde{P}) & \bar{P} < \tilde{P}, \\ \mathcal{R}_v(\bar{P}) & \bar{P} \ge \tilde{P}. \end{cases} \tag{28}$$

Note that the achievable rate of the bursting strategy when $\bar{P} < \tilde{P}$ is exactly the line tangent to the curve $\mathcal{R}_v(P)$ at $\tilde{P}$.



(a) $b = 0.7$

(b) $b = 0.5$

Fig. 2. Secrecy rate with Gaussian signaling. The curve for "noise + bursting" is the secrecy rate $\bar{\mathcal{R}}_s(P)$ given by (28) with both artificial noise and bursting; the curve for "noise" is the secrecy rate $\mathcal{R}_v(P)$ given by (24) with artificial noise only; the curve for "simple Gaussian" is the secrecy rate $\mathcal{R}_x(P)$ given by (16) with simple Gaussian codes; $\Delta(P)$ is plotted as the dotted line for reference.

The achievable secrecy rate of the three strategies for $b = 0.7$ and $b = 0.5$ are plotted in Fig. 2. Artificial noise and bursting strategy allows positive secrecy rate to be achievable for all power even when Bob's channel is on average worse than Eve's channel. Note that we did not consider the limit on Alice peak transmit power here. In practice, the peak transmit power is often upper-limited and cannot be arbitrarily large. So, the actual achievable secrecy rate of the bursting scheme depends on the peak power constraint. When bursting is needed but the peak power constraint is smaller than the optimal bursting power $\tilde{P}$, the secrecy rate that Alice-Bob can achieve is reduced but still better than that without bursting when the peak power constraint is greater than the optimal artificial noise power P_w^*; if the peak power constraint is even smaller than P_w^*, no positive secrecy rate is achievable with this scheme.

V. Secrecy Rate with Discrete Signaling

We now consider secret communication using practical, discrete signaling constellations. We shall consider quadrature amplitude modulation (QAM) as an example of discrete signaling, because of its simplicity and popularity. The observations we make here for QAM will apply to other discrete constellation as well. Note that for QAM modulation, the transmitted signal is complex since it has both the in-phase and the quadrature components. Although the channel attenuation is complex, both the intended receiver and the eavesdropper are assumed to know their own channel states, so they can compensate for the channel phase rotation and reduce the channel to two real sub-channels with identical channel gain (but independent noise), one for each input dimension. Hence, we will use the real fading channel model (7) to facilitate comparison with the secrecy rates using Gaussian signaling derived in Section IV, while keeping in mind that they only represent one component of the actual channel.

Quadrature Amplitude Modulation: The signal space representation of QAM signaling is

$$\mathbf{x}_i = \begin{bmatrix} a_i \\ b_i \end{bmatrix}, \qquad i = 1, \cdots, M, \tag{29}$$

where a_i and b_i are the amplitudes of the quadratic carriers of the information bearing signal. The constellation points are equally spaced and are equally probable. In this work, we consider the case for $M = 4, 16, 64$, so a_i and b_i each takes the value from $\{(-\sqrt{M} + 2i - 1)d\}$ for $i = 1, \cdots, \sqrt{M}$ with equal probability. The parameter d is chosen such that the average power per signal dimension is P. With some algebra, we can calculate d to be

$$d = \sqrt{\frac{\sqrt{M}P}{\sum_{i=1}^{\sqrt{M}}(-\sqrt{M} + 2i - 1)^2}}. \tag{30}$$

When the input X is distributed over the discrete set $\{\mathbf{x}_i\}$, the probability density function of X can be written as

$$f_X(\mathbf{x}) = \sum_{i=1}^{M} p_i \delta(\mathbf{x} - \mathbf{x}_i), \tag{31}$$

where p_i is the probability of $\mathbf{x} = \mathbf{x}_i$, M is the total number of possible $\mathbf{x}$ values and $\delta(x)$ is the Dirac delta function. For QAM, all constellation points are equally likely, so $p_i = 1/M$.

Let $\mathcal{N}(\mathbf{t}, \mu)$ be the unit Gaussian distribution

$$\mathcal{N}(\mathbf{t}, \mu) = \frac{1}{(2\pi)^{N/2}} \exp\left(-\frac{||\mathbf{t} - \mu||^2}{2}\right), \tag{32}$$

where N is the dimensionality of the input, which is 1 for BPSK, and 2 for M-QAM and M-PSK with $M > 2$. For a discrete input with probability distribution given by (31), the distribution of the output Y, denoted by $f_Y(\mathbf{y})$, is given by

$$f_Y(\mathbf{y}) = \sum_{i=1}^{M} p_i \mathcal{N}(\mathbf{y}, \sqrt{b}\mathbf{x}_i). \tag{33}$$

The distribution of the output Z conditioned on the eavesdropper's channel realization G is given by

$$f_{Z|G}(\mathbf{z}) = \sum_{i=1}^{M} p_i \mathcal{N}(\mathbf{z}, \sqrt{g}\mathbf{x}_i). \tag{34}$$

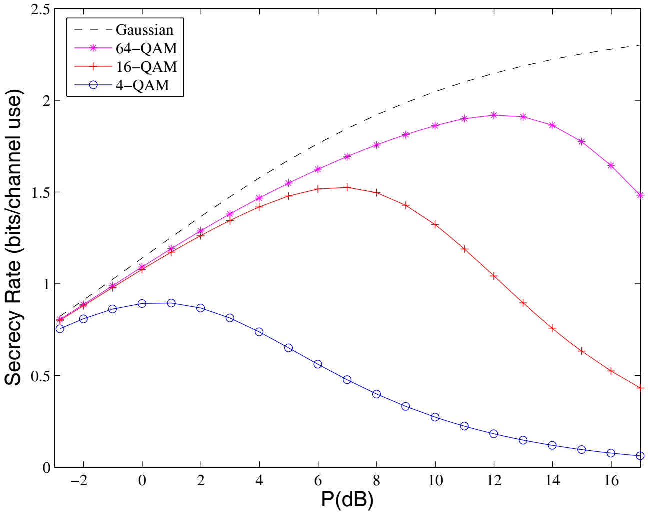


Fig. 3. Achievable secrecy rate of the fading channel (7) with Gaussian signaling, and M-QAM signaling obtained by evaluating (37). $b = 3$.

The achievable secrecy rate with $V = X$ is given by

$$\begin{aligned}\mathcal{R}_x^D &= (I(X;Y) - I(X;Z|G))^+ \qquad (35)\\ &= (H(Y) - H(Z|G))^+ \qquad (36)\\ &= \Bigg(-\int_{-\infty}^{\infty} f_Y(\mathbf{y}) \log_2(f_Y(\mathbf{y}))\, d\mathbf{y}\\ &\quad + \int_0^{\infty}\int_{-\infty}^{\infty} f_{Z|G}(\mathbf{z}) \log_2(f_{Z|G}(\mathbf{z}))\, d\mathbf{z}\, e^{-g} dg\Bigg)^+. \qquad (37)\end{aligned}$$

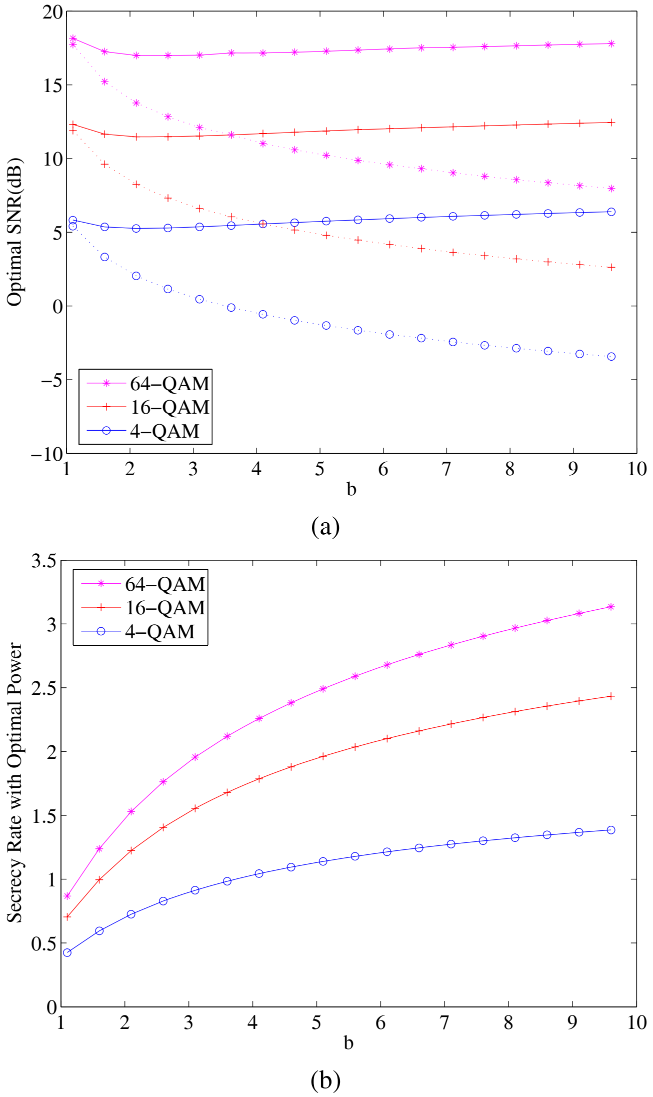
Because the analytical expression of the achievable rate is hard to obtain, we resort to numerical evaluation to gain insight on how the system behaves with M-QAM. Numerically evaluating (37) with M-QAM for $b = 3$, we obtain Fig. 3, in which the achievable secrecy rate (16) for Gaussian input is plot as well for comparison. Note that for M-QAM, there exists an optimal power P^* that maximizes the secrecy rate. Using a power greater than P^* will hurt the secrecy. This is because

$$\lim_{P\to 0} \mathcal{R}_x^D(P) = 0, \qquad (38)$$

$$\lim_{P\to\infty} \mathcal{R}_x^D(P) = \log_2 M - \log_2 M = 0. \qquad (39)$$

So if there exists a power P^* that produces maximum positive secrecy rate, it must satisfy $P^* < \infty$. That is, with increasing transmit power P, both Bob and Eve approach perfect error-free detection, which precludes secret communication to Bob. This is very different from the Gaussian input case, where larger power is always better. For the example shown in Fig. 3, Gaussian input performs better than M-QAM.

We plot the optimal channel SNR as a function of the main channel's normalized channel gain b at several constellation sizes in Fig. 4(a). The solid lines are the main channel SNR and the dashed line are the eavesdropper's channel SNR. The optimal power decreases with b to lower the eavesdropper's SNR, while maintaining the main channel SNR to an almost stable level. As the size of the constellation increases, the optimal power also increases. The secrecy rates corresponding to the optimal power are shown in Fig. 4(b).

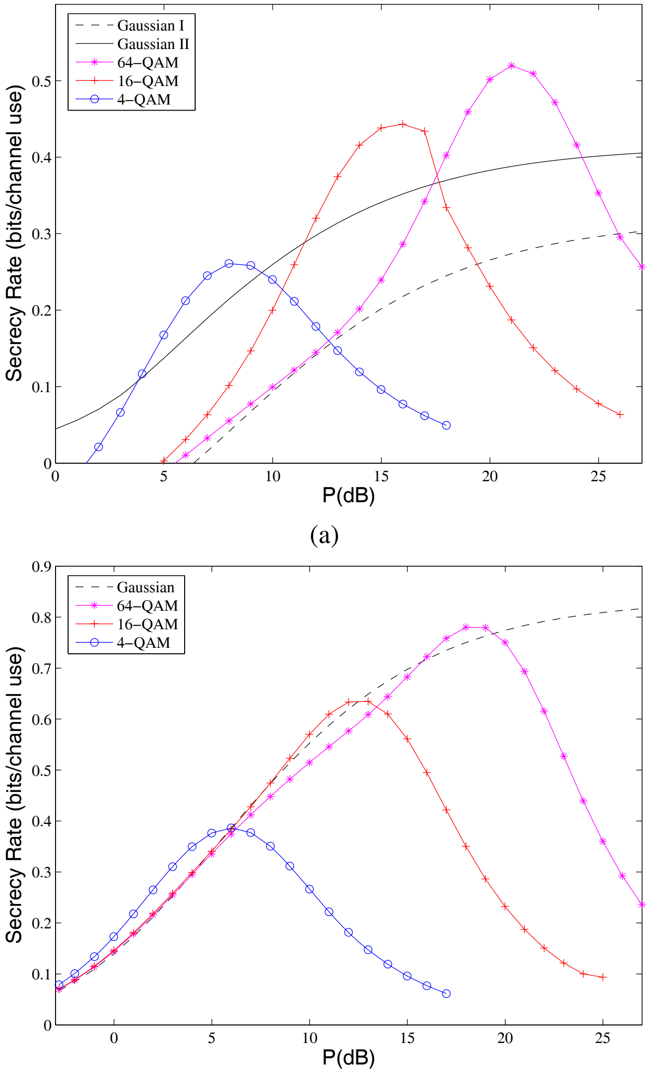


(a)

(b)

Fig. 4. (a) The channel SNR with the optimal power for fading channel model (7) with M-QAM signaling. The solid curve are the main channel optimal SNR and the dashed curves are the eavesdropper's channel average SNR. (b) The secrecy rate corresponding to the optimal power.

Gaussian input, however, is not always optimal for the fading scenario. When we evaluate the secrecy rate for $b = 0.7$ and $b = 1$ with both Gaussian inputs and QAM inputs, we get a different result, as shown in Fig. 5. Gaussian I corresponds to the strategy of using a simple Gaussian input with power P, while Gaussian II corresponds to the strategy of using a Gaussian input combined with artificial noise and bursting, as discussed in Section IV. When $b < 1$, the latter strategy can improve the achievable secrecy rate. Nevertheless, QAM signaling will outperform Gaussian signaling with optimized artificial noise and bursting. Moreover, a larger constellation is not always better than a smaller constellation. With a small power, smaller constellations work better. As the power increases, larger constellations start to perform better. Hence the optimal constellation depends on the power constraint. The figure also implies that by time sharing among the constellations, the upper envelope of the curves for M-QAM signaling can be achieved.



(a)

(b)

Fig. 5. Achievable secrecy rate of fading channel (7) with Gaussian signaling, and M-QAM signaling obtained by evaluating (37). (a) $b = 0.7$ (b) $b = 1$.

The reason that M-QAM can work better than Gaussian signaling when $b < 1$ is because discrete inputs effectively limit the information that can be obtained by the eavesdropper when her channel realizations are better than the main channel. With M-QAM signaling, Eve can never learn more than $\log M$ bits per received QAM symbol, no matter how high her received SNR is. However, with Gaussian signaling, a single received symbol can be, in principle, sufficient to reveal to Eve the entire transmitted codeword. Therefore, M-QAM provides some advantage in terms of limiting the information leakage when the eavesdropper's channel is better on average, and this advantage is more significant as the main channel channel gain gets worse. The gain diminishes when the main channel becomes comparable or even better than the eavesdropper's average channel gain.

VI. Conclusion

In this paper, we studied the achievable secrecy rate for the situation where the main channel is a constant AWGN channel, and Eve's channel is fast Rayleigh fading with unknown channel realizations to all other parties. The achievable secrecy rate for both the Gaussian signaling and M-QAM are evaluated. For Gaussian signaling, positive secrecy rate is achievable with artificial noise and bursting strategy even when Bob's channel is much worse than Eve's average channel gain. This secrecy rate is achieved without knowing when Eve's channel is bad or when Eve's channel changes. For M-QAM, we observe that the power should be carefully chosen as larger power than optimal will benefit Eve more and hurt the secrecy. When Bob's channel is better than Eve's channel, Gaussian signaling performs better than M-QAM. But when Bob's channel is worse, M-QAM can do better than Gaussian signaling. The key to achieve secret communication when Bob's channel is worse is that both M-QAM and artificial noise limit the information leakage when Eve's channel is unusually good.

References

[1] A. Wyner, "The wire-tap channel," *Bell. Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidental messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] S. K. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[4] C. Mitrpant, A. J. H. Vinck, and Y. Luo, "An achievable region for the Gaussian wiretap channel with side information," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2181–2190, May 2006.

[5] Y. Chen and A. J. H. Vinck, "Wiretap channel with side information," in *IEEE Int. Symp. Inf. Theory*, July 2006.

[6] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *IEEE Int. Symp. Inf. Theory*, July 2006.

[7] Z. Li, R. D. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *44th Annual Allerton Conference on Communications, Control and Computing*, Sep. 2006.

[8] Y. Liang and H. V. Poor, "Secure communication over fading channels. In *Forty-Fourth Annual Allerton Conference on Communications, Control and Computing*, Sep. 2006.

[9] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

[10] P. K. Gopala, L. Lai, and H. El-Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[11] A. Garnaev and W. Trappe, "An eavesdropping game with SINR as an objective function," in *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Security and Privacy in Communication Networks, Proc. 5th International ICST Conference SecureComm*, Sep. 2009.

[12] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*. Springer, 2009.

[13] Y. Liang, H. V. Poor, and S. Shamai, "Information theoretic security," in *Foundation Trends in Communication Information Theory*, vol. 5, 2008.

[14] Z. Li, R. D. Yates, and W. Trappe, "Secure communication with a fading eavesdropper channel," in *IEEE Int. Symp. Inf. Theory*, June 2007.

[15] J. Spanier and K. Oldham, "The Exponential Integral Ei() and Related Functions," ch. 37 in *An Atlas of Functions*. Washington, DC: Hemisphere, 1987.

[16] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE Vehicular Tech. Conf.*, Fall 2005.

Zang Li received her M.S. and Ph.D degree in Electrical Engineering from the Wireless Information Network Laboratory, Rutgers University in 2005 and 2009. She received her B.S. degree in Physics from Jilin University, China in 1997. Her research interests include wireless security, wireless sensor network, information theory and coding, and multimedia security.

Roy Yates received the B.S.E. degree in 1983 from Princeton and the S.M. and Ph.D. degrees in 1986 and 1990 from MIT, all in Electrical Engineering. Since 1990, he has been with the Wireless Information Networks Laboratory (WINLAB) and the ECE department at Rutgers University. Presently, he is an Associate Director of WINLAB and a Professor in the ECE Dept. He is a co-author (with David Goodman) of the textbook *Probability and Stochastic Processes: A Friendly Introduction for Electrical and Computer Engineers* published by John Wiley and Sons. He is a co-recipient (with Christopher Rose and Sennur Ulukus) of the 2003 IEEE Marconi Prize Paper Award in Wireless Communications. His research interests include information theory, power control, interference suppression and spectrum regulation for wireless systems.

Wade Trappe received his B.A. degree in Mathematics from The University of Texas at Austin in 1994, and the Ph.D. in Applied Mathematics and Scientific Computing from the University of Maryland in 2002. He is currently Associate Director at the Wireless Information Network Laboratory (WINLAB) and an associate professor in the Electrical and Computer Engineering Department at Rutgers University. His research interests include wireless security, wireless networking, multimedia security, and network security. He has led projects involving security and privacy for sensor networks, physical layer security for wireless systems, a security framework for cognitive radios, the development of wireless testbed resources, and new RFID technologies. Recently, his research group has developed several cross-layer security mechanisms for wireless networks, has developed jamming detection and jamming defense mechanisms for wireless networks, and has investigated privacy-enhancing routing methods for wireless networks. He has published over 100 papers, including two best papers in media security, a best paper on the localization of cognitive radios, and several wireless security papers in premier conferences. He has co-authored a popular textbook in the field, *Introduction to Cryptography with Coding Theory*, as well as four other books on wireless systems and multimedia security. He is a member of the IEEE Signal Processing and Communications societies, a member of the ACM, and has served on the editorial board for two IEEE journals.