On the Secrecy Rate of Multi-Antenna Wiretap Channel under Finite-Alphabet Input

Shafi Bashar, *Student Member, IEEE*, Zhi Ding, *Fellow, IEEE*, and Chengshan Xiao, *Fellow, IEEE*

***Abstract*—This work investigates the effect of limiting source signals to finite-alphabet on the secrecy rate of a multi-antenna wiretap system. Existing works have characterized maximum achievable secrecy rate or secrecy capacity for single- and multi-antenna systems based on Gaussian source signals and secrecy code. Despite the impracticality of Gaussian source, its compact closed-form expression of mutual information motivated broad use of Gaussian input assumption. For practical consideration, we study the effect of finite discrete-constellation on instantaneous and ergodic secrecy rate of multiple-antenna wire-tap channels. Our results demonstrate substantial difference between systems involving finite-alphabet inputs and systems with Gaussian inputs. Results from Gaussian inputs serve as upper-bound of secrecy rate for practical systems with finite alphabet inputs.**

***Index Terms*—Wiretap channel, eavesdropping, information-theoretic security, ergodic secrecy rate, finite-alphabet input.**

I. Introduction

Wireless communications, despite broad popularity, are vulnerable to potential security threats such as passive eavesdropping and active jamming. Traditionally, security of a system has been dealt with in the higher layers of the communication protocol stack by relying on authentication and cryptography. However, in recent years, there has been a growing research interest in the security of wireless systems from a physical layer perspective. In a wiretap channel environment introduced by Wyner [1], a sender "Alice" wishes to transmit a secret message to the intended receiver "Bob" in the presence of a passive eavesdropper "Eve". Wyner [1] showed that when the Alice-to-Eve channel is a degraded version of the Alice-to-Bob channel, Alice can encode and send secure messages to the destination at a nonzero secrecy rate. In [2], a generalization for the non-degraded broadcast channel is proposed. In [3], secrecy capacity of a Gaussian wiretap channel is shown achievable using random Gaussian codebook. In [4], the secrecy capacity of a multi-antenna Gaussian channel is achieved using proper beamforming and by encoding the message using a Gaussian random codebook.

Even though for both single- and multi-antenna Gaussian wiretap channels, the codebook that achieves secrecy capacity turns out to be Gaussian, however, such codebooks are not realizable in practice. In contrast to the Gaussian codebook, practical wiretap codes are constrained by finite alphabet symbols. Due to this constraint, the achievable secrecy rate for a finite-alphabet input scenario would differ from the secrecy rate achievable using a Gaussian codebook.

In this work, we investigate the effect of finite-alphabet input on ergodic secrecy rate of a multi-antenna system. We observe that ergodic secrecy rate in fact decreases with increasing signal-to-noise ratio (SNR) without power control at Alice. To maximize the achievable ergodic secrecy rate, we propose a power control algorithm for arbitrary input distribution by exploiting the relationship between the mutual information and the received mmse proposed in [5], [6]. Our observations suggest that proper transmission power should decrease with increasing SNR in case of finite-alphabet input. The excess unused transmission power can be utilized to further increase the secrecy by transmitting a jamming signal.

II. Preliminaries and System Description

We consider simple wiretap system model in which the transmitter (Alice) has M_t antennas whereas both the intended receiver Bob and the passive eavesdropper Eve have a single receive antenna. Denote the received signals at Bob and Eve as y_b and y_e, respectively. Their received signals are

$$\begin{aligned} y_b &= \sqrt{\gamma p}\,\mathbf{h}_b^H\mathbf{x} + v_b \\ y_e &= \sqrt{\gamma p}\,\mathbf{h}_e^H\mathbf{x} + v_e \end{aligned}$$

where $\mathbf{h}_b \in \mathbb{C}^{M_t}$ and $\mathbf{h}_e \in \mathbb{C}^{M_t}$ are, respectively, the multi-input-single-output (MISO) channels from Alice-to-Bob and from Alice-to-Eve. The noise v_b and v_e are zero-mean unit-variance complex Gaussian random variables independent of each other. The data signal is s which is transmitted by Alice in the form of $\mathbf{x} = \mathbf{w}s$, where $\mathbf{w}$ is a unit norm beamforming vector. We denote s as a zero-mean, unit-norm random data. For ease of calculation we express the transmit power as $\gamma \cdot p$, where $0 \leq p \leq 1$ indicates the fraction of the available transmission power γ used for transmission. We define SNR (signal-to-noise ratio) of the system as the ratio between the total available transmission power to noise power, independent of the actual value of p used for transmission, i.e., SNR $= \gamma$.

In ergodic case, it is assumed that Alice knows the channel information of Bob but is unaware of Eve's channel information. For analysis, Alice relies on the channel statistics information of Eve. In a generic setting, Eve's channel is assumed to be a vector of independent Gaussian complex random elements, i.e. $\mathbf{h}_e \in \mathcal{CN}(\mathbf{0}, \mathbf{I})$. For Gaussian input, the optimal covariance matrix to maximize the achievable ergodic secrecy rate is shown to be a rank one matrix [7], i.e., a beamforming vector, and the achievable ergodic secrecy rate can be found by solving the following optimization problem

$$\max_{\mathbf{w},p} \log\left(1+\gamma p\left|\mathbf{w}^H\mathbf{h}_b\right|^2\right) - \mathbb{E}\left[\log\left(1+\gamma p\left|\mathbf{w}^H\mathbf{h}_e\right|^2\right)\right]. \quad (1)$$

It has been shown in [8] that the optimal strategy is to apply beamforming in the direction of Bob's channel. Henceforth,

S. Bashar and Z. Ding are with the Department of Electrical and Computer Engineering, Univ. of California, Davis, CA, 95616, USA (e-mail: mabashar@ucdavis.edu).

C. Xiao is with the Department of Electrical and Computer Engineering, Missouri University of Science and Technology, Rolla, MO, 65409, USA.

This material is based upon work supported by the National Science Foundation under Grants No. 0520126.

Digital Object Identifier 10.1109/LCOMM.2011.032811.102539

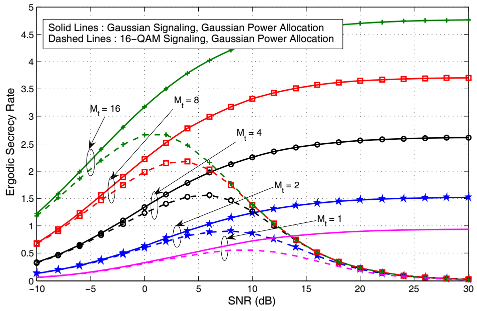

Fig. 1. Ergodic secrecy rate for naive beamforming.

we refer to such beamforming along Bob in a security setting as “naive beamforming”. For an arbitrary input distribution, the following rate is achievable under “naive beamforming”:

$$R_{\text{sec}}\left(\gamma, p\right) = \mathcal{I}\left(\gamma p \left\|\mathbf{h}_b\right\|^2\right) - \mathbb{E}\left[\mathcal{I}\left(\gamma p\, t\right)\right]. \tag{2}$$

Here, we define $\mathcal{I}\left(\rho\right) = I\left(s; \sqrt{\rho}s + v\right)$; also $t = \left|\mathbf{h}_e^H \mathbf{w}\right|^2$ is an exponential random variable for a known value of Bob's channel $\mathbf{h}_b$, when using naive beamforming $\mathbf{w} = \mathbf{h}_b \big/ \left\|\mathbf{h}_b\right\|$.

III. Optimization of Power Usage

Observe, from the achievable secrecy rate formula (2), that the optimal strategy of “naive beamforming” does not necessarily require transmission of information at full power. This is because sending signal at full power can also boost the probability of its full detection by Eve. Hence, there is an optimum value of power usage for $0 \leq p \leq 1$ rather than $p = 1$. Specifically, we should optimize the power usage at Alice to maximize the achievable secrecy rate under the optimal “naive beamforming” strategy.

A. Optimum Power Usage for Gaussian Input

When the channel input is Gaussian, from (1), we can easily determine the maximum achievable ergodic secrecy rate by solving the following optimization problem

$$R_{\text{sec}} = \max_{0 \leq p \leq 1} \log\left(1 + \gamma p \left\|\mathbf{h}_b\right\|^2\right) - \exp\left(\frac{1}{p\gamma}\right) \cdot \mathrm{E}_1\left(\frac{1}{p\gamma}\right) \tag{3}$$

where $\mathrm{E}_1\left(x\right) = \int_x^\infty \exp\left(-u\right) u^{-1} du$. Note, however, that the optimization for the practical finite alphabet input can be cumbersome. For this reason, we may be tempted to apply the optimum power factor p^*_{gauss} found for Gaussian input signal to the case involving finite-alphabet input. Such a blind-faith application could in fact be treacherous. To illustrate the possible effect of such a *laissez faire* approach, we will numerically evaluate the resulting ergodic secrecy rate achieved from applying the “optimum power factor” p^*_{gauss} optimized for Gaussian input signals to the transmission of both Gaussian and finite-alphabet inputs.

Fig. 1 illustrates ergodic secrecy rate at various SNR levels for both Gaussian input and 16-QAM input signals. In both cases, “naive beamforming” is accompanied by the power factor p^*_{gauss} chosen from solving optimization problem of Eq. (3). Different numbers of transmit antenna M_t =1, 2, 4, 8, 16 are also tested. The results clearly show that the ergodic secrecy rate for Gaussian input increases as SNR grows because of the optimum power factor p^*_{gauss} for every cases.

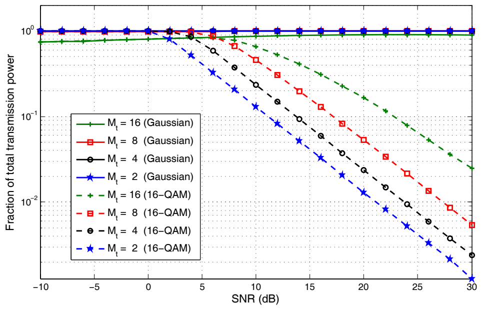

Fig. 2. Comparison between p^*_{gauss} and p^*_{finite}.

However, the ergodic secrecy rate achieved by transmitting finite-alphabet input using the same power factor p^*_{gauss} may in fact decrease as SNR increases (because Eve can decode the message with better accuracy). Indeed, the same power factor when applied to a finite-alphabet input at high SNR drives the mutual information for both Bob and Eve to the point of the saturation of $\log_2 16 = 4$ b/s/Hz under 16-QAM, thereby rendering secrecy rate in Eq. (2) to approaching zero. Therefore, we should optimize the power usage factor specifically for the finite-alphabet input instead of relying on the Gaussian Assumption.

B. Power Optimization Algorithm for Finite Alphabet Input

In this sub-section, we develop a numerical algorithm for optimization of transmission power by maximizing the ergodic secrecy rate under finite-alphabet input signals. Recall that, under naive beamforming, the power optimization for maximum ergodic secrecy requires the solution to the following optimization problem

$$R_{\text{sec}}\left(\gamma\right) = \max_{0 \leq p \leq 1} \mathcal{I}\left(\gamma p \left\|\mathbf{h}_b\right\|^2\right) - \int_0^\infty \mathcal{I}\left(\gamma p t\right) \exp\left(-t\right) dt. \tag{4}$$

In general, it is difficult to find the expression for mutual information $I(X;Y)$ for arbitrary input distributions. However, a numerical optimization method can be applied. In order to solve the above optimization problem, we will use the following results from [5], [6]

$$\frac{d\mathcal{I}\left(\rho\right)}{d\rho} = \mathrm{mmse}\left(\rho\right). \tag{5}$$

Here, mmse(.) is the minimum mean square error (MMSE) at the receiver. Applying the chain rule, we find the derivative of the objective function (4) with respect to p as

$$\nabla_p = \gamma \left\|\mathbf{h}_b\right\|^2 \mathrm{mmse}\left(\gamma p \left\|\mathbf{h}_b\right\|^2\right) - \gamma \int_0^\infty t\ \mathrm{mmse}\left(\gamma p t\right) \exp\left(-t\right) dt.$$

Note that the MMSE function for different discrete constellations (e.g., M-PSK, M-QAM) has been given in [9]. We therefore propose solving the optimization problem (4) using the gradient search steps in Algorithm 1.

Algorithm 1 Power Control for Arbitrary Input Distribution

```
1) Initialize $p_0$ such that $0 \leq p_0 \leq 1$. Set step-size $\mu$.
2) Calculate $\nabla_{p_k}$.
3) Update $p_{k+1}$ with $\nabla_{p_k}$ as : $p_{k+1} \leftarrow p_k + \mu \nabla_{p_k}$.
4) If $p_{k+1} > 1$, set $p_{k+1} \leftarrow 1$. If $p_{k+1} < 0$, set $p_{k+1} \leftarrow 0$.
5) Set $k \leftarrow k + 1$.
6) Go to Step 2 until stopping criterion is reached.
```

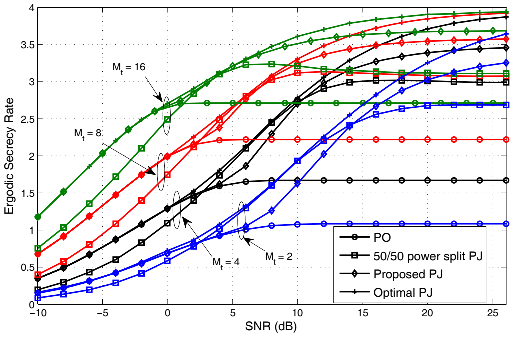

Fig. 3. Comparison between PO and PJ methods.

Figure 2 compares the transmission powers needed to maximize the ergodic secrecy rate for Gaussian input [Eq. (3)] and for 16-QAM input (Algorithm 1). In contrast to the Gaussian input power allocation p^*_{gauss} which employs almost all available transmission power, the finite input power allocation p^*_{finite} from Algorithm 1 in fact decreases with an increase in SNR. This observation, i.e., full transmit power may in fact not needed, was also made in [8], albeit for the Gaussian input case.

IV. Security Enhancement via Signal and Jamming Power Allocation

An interesting work [10] proposed a secrecy enhancement technique for multiple-antenna transmission by employing a part of the transmission power to simultaneously transmit jamming signal and the message signal. Consider the signal transmission by Alice. Simultaneous active jamming against Eve means that transmitted signal $\mathbf{x}$ consists of two parts, i.e., $\mathbf{x} = \sqrt{\gamma}\left(\sqrt{p}\mathbf{w}s + \mathbf{u}\right)$, which is formed by the message signal s, the beamforming vector $\mathbf{w}$, and the jamming signal vector $\mathbf{u}$. Define $\mathbf{Z}_b$ as an orthonormal basis spanning the null-space of $\mathbf{h}_b$. Because Alice does not have knowledge of the Alice-to-Eve channel $\mathbf{h}_e$, it sends jamming signals to blanket all directions orthogonal to the desired channel $\mathbf{h}_b$ [10]. Therefore, the jamming vector should be of the form $\mathbf{u} = \mathbf{Z}_b\mathbf{v}$ where $\mathbf{v}$ is a vector of $M_t - 1$ i.i.d. complex Gaussian random elements, i.e., $\mathbf{v} \sim \mathcal{CN}\left(\mathbf{0}, \sigma_v^2\mathbf{I}\right)$. [10] find the optimum power division between useful signal and jamming that maximizes the ergodic secrecy rate. Unfortunately, the non-convexity of the above optimization problem may require exhaustive search. More specifically, for an arbitrary input distribution, the optimization problem without a compact closed-form expression leads to higher complexity.

Our observation in Fig. 2 indicates a more natural computationally efficient way of power division for finite-alphabet case. For finite-alphabet input, the power control algorithm 1 uses only a fraction of the total available power for signal transmission at high SNR. In contrast, for Gaussian input, almost all available power is required. Therefore, unlike [10], we do not need to perform an exhaustive search to optimize the power division. Instead, we can use the large amount of excess power to transmit jamming signal for finite-alphabet input. The steps are as follows:

1) Find the optimum power allocation p^*_{finite} using Algorithm 1. Set $p = p^*_{\text{finite}}$.
2) Set $\sigma_v^2 = (1-p)\big/(M_t - 1)$.

In Fig. 3, we present the effect of jamming signal transmission on the ergodic secrecy rate for a 16-QAM input. We refer to the method that only uses proper power control based on Algorithm 1 for useful signal transmission as power only (PO) method. In contrast, the method where jamming signal is transmitted in addition to the power control algorithm is referred to as power control and jamming (PJ) method. In Fig. 3, we compare PO, optimal PJ as in [10], proposed PJ and a 50/50 power split PJ [11]. At low SNR, almost all power is needed for transmission of the useful signal, and hence no power is left for transmission of the jamming signal. Therefore, at low SNR regime, proposed PJ has the same performance as the optimal PJ. Even though for Gaussian signaling, 50/50 power split PJ achieves the performance of the optimal PJ [11], we observe that for finite-alphabet input, the 50/50 power split PJ achieves such performance only for moderate to high SNR regime. At high SNR regime, the propose PJ has the closest performance to the optimal PJ. We also observe that, at very high SNR, the ergodic secrecy rate for the optimal PJ gets closer to 4 b/s/Hz, which is the maximum achievable rate for a 16-QAM input constellation. Without transmitting jamming signal, such rate would have not been possible.

V. Conclusion

In this letter, we characterized the effect of finite-alphabet input on the secrecy performance of a MISOSE system. We presented a power optimization algorithm to maximize the achievable ergodic secrecy rate for arbitrary input distributions. Since the optimum transmission power for finite-alphabet input decreases with increasing SNR, we can achieve better secrecy rate by utilizing the unused transmission power for sending jamming signal along the null space of the intended receiver in an MISOSE system. We note that, by employing the unused power for jamming signal transmission, we can achieve secrecy rate close to $\log_2 M$ b/s/Hz.

References

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

[2] I. Csiszár and J. Korner, “Broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 24, pp. 339–348, 1978.

[3] S. Leung-Yan-Cheong and M. Hellman, “The Gaussian wire-tap channel,” *IEEE Trans. Inf. Theory*, vol. 24, pp. 451–456, 1978.

[4] A. Khisti and G. Wornell, “Secure transmission with multiple antennas I: the MISOME wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 56, pp. 3088–3104, 2010.

[5] D. Guo, S. Shamai, and S. Verdú, “Mutual information and minimum mean-square error in Gaussian channels,” *IEEE Trans. Inf. Theory,*, vol. 51, pp. 1261–1282, 2005.

[6] D. Palomar and S. Verdú, “Gradient of mutual information in linear vector Gaussian channels,” *IEEE Trans. Inf. Theory*, vol. 52, pp. 141–154, 2006.

[7] J. Li and A. Petropulu, “On ergodic secrecy rate for Gaussian MISO wiretap channels,” *IEEE Trans. Wireless Commun.*, pp. 1–12, 2011 (available via early access).

[8] S. Shafiee and S. Ulukus, “Achievable rates in Gaussian MISO channels with secrecy constraints,” in *Proc. IEEE International Symp. Inform. Theory*, 2007, pp. 2466–2470.

[9] A. Lozano, A. Tulino, and S. Verdú, “Optimum power allocation for parallel Gaussian channels with arbitrary input distributions,” *IEEE Trans. Inf. Theory*, vol. 52, pp. 3033–3051, 2006.

[10] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180–2189, 2008.

[11] X. Zhou and R. McKay, “Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation,” *IEEE Trans. Veh. Technol.*, vol. 59, pp. 3831–3842, 2010.