# Covert Communications with Extremely Low Power under Finite Block Length over Slow Fading

Haoyue Tang*, Jintao Wang*, Yahong Rosa Zheng†
*Department of Electronic Engineering, Tsinghua University
*Tsinghua National Laboratory for Information Science and Technology (TNList), Beijing 100084, P. R. China
†Department of Electrical and Computer Engineering, Missouri University of Science and Technology, Rolla, MO, USA
Email: tanghaoyue13@tsinghua.org.cn,wangjintao@mail.tsinghua.edu.cn,zhengyr@mst.edu

***Abstract*—This paper investigates the achievable message transmission rate of covert communication over slow fading channels where the channel coefficient remains unchanged over a finite transmission block. Such communication is often implemented with an extremely low transmission power aiming to achieve low probability of detection by the eavesdropper and under tolerable probability of decoding error for the legitimate receiver. The exact expression of achievability and asymptotic covert bounds are derived, which are shown in accordance with the square root law in AWGN (Additive White Gaussian Noise) channels with large transmission blocks. The case that the eavesdropper has unknown channel state information is also studied in the paper.**

***Index Terms*—Low Power Communications; Covert Communications; Security**

## I. Introduction

Secure communication or secrecy system was first introduced by Shannon [1] in 1949 as three types of communication systems: concealment system, privacy system, and encryption system. While the encryption system has been widely studied in the past few decades and has been well utilized in practical systems, the concealment system attracts some research attentions only in recent years because of its technical difficulties. A typical concealment system, or covert communication, refers to the scenario where the transmitter Alice sends a message to the legitimate receiver Bob while hiding the message from the eavesdropper Eve, therefore the existence of the message is concealed from Eve. The methods of hiding include: 1) embedding a message in useless signals, or 2) hiding a message in noise [2]. The performance of a covert communication system is usually measured by the probability of detection and the secrecy capacity.

Previous research in covert communication focuses on the probability of false alarm or mis-detection [3]. Recently, Han *et al.* introduced the concept of *effective secrecy* that combines the probability of false alarm and mis-detection together [4]. Later, Hou and Kramer [5] showed that the capacity with effective secrecy is the same as the capacity of secure transmission in wiretap channels in which Alice conceals the message by hiding it in useless signals. With the proposed novel metric, fundamental limits on covert communication capacity are derived. The well known *square root law* describes the scale amount of information that can be covertly transmitted [2]. For binary erasure channels, it is proved that $o(\sqrt{n})$ bits can be safely transfered over $n$ channel uses [7]. For communications over AWGN channels, Bash [2] showed that the square root law holds regardless of average or peak power constraints, Wang *et al.* gave the scaling constant with the help of Fisher information and proved its achievability with source random coding [6].

It is noted that, these analysis are based on transmitting with infinite block length. In reality, the limited storage source and timely update nature of communications require that the length of transmission package is finite. Tight bounds on transmit under tolerable probability of decoding error with finite block length is derived in [8]. In [9], W. Yang and Y. Polyanskiy investigated the asymptotic behavior of wiretap channel (WTC) with tolerable information leakage rate and decoding error probability. In [10], the $\epsilon$-capacity achieving region is established to study convert communication over MIMO channels.

This paper investigates the achievable message transmission rate of covert communication over slow fading channels where the channel coefficient remains unchanged over a finite transmission block. Such communication is often implemented with an extremely low transmission power aiming to achieve low probability of detection by the eavesdropper and under tolerable decoding error probability of the legitimate receiver. The exact expression of achievability and asymptotic covert bounds are derived, which are shown in accordance with the square root law in AWGN channels with large transmission blocks.

*Notations:* Random variables are denoted with upper case letters and their realizations are denoted in lower case letters, its expectation is denoted as $E(\cdot)$. The probability of a certain event is denoted as $\Pr(\cdot)$. Matrices and vectors are written in boldface letters. The distribution of a random sequence $\mathbf{x} = [X(1), \cdots, X(n)]$ is denoted as $p(\mathbf{x})$. Matrices determinant and trace are denoted as $|\cdot|$ and $\mathrm{Tr}(\cdot)$, respectively. The entropy of a distribution $\mathbb{P}$ is denoted as $H(\mathbb{P})$. Calligraphic letters denote sets. The real part and the imaginery part of a complex number are denoted with $\Re(\cdot)$ and $\Im(\cdot)$, respectively.

## II. Preliminaries

### A. System Model

We consider covert communication over a slow fading channel (WTC) $(\mathcal{X}, P_{YZ|X}, \mathcal{Y} \times \mathcal{Z})$, as depicted in Fig. 1, where a transmitter Alice communicates with a legitimate receiver Bob in the presence of an eavesdropper Eve. Alice's encoder maps the message $M$ into a sequence of complex transmit symbols $\mathbf{x} = [X(1), \cdots, X(n)]$ at a rate $R$ and by a transmit strategy $T$, where $n$ denotes the length of the transmission block. If Alice transmits a message in the $n$ time slots, then $T = 1$, otherwise, $T = 0$.

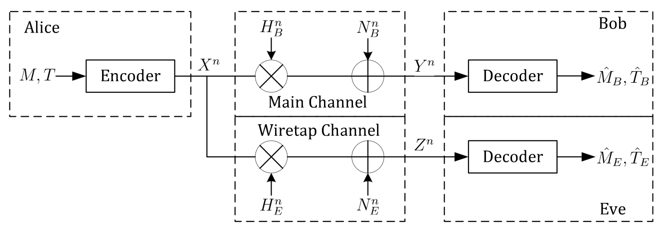


Figure 1. A covert communication channel model with one legitimate receiver and one passive eavesdropper. Both the main channel and the eavesdropper channel are slow fading.

After the sequence $\mathbf{x}$ goes through the wireless links, Bob observes the output of the slow fading channel as $\mathbf{y} = [Y(1), \cdots, Y(n)]$ with

$$Y(i) = d_B^{-\alpha/2} H_B(i) X(i) + N_B(i), \quad i = 1, 2, ..., n \tag{1}$$

where $i$ represents the channel use index, $N_B(i)$ is zero-mean circularly symmetric complex Gaussian noise, and $H_B(i) \in \mathbb{C}$ is the complex baseband equivalent channel coefficient of the *main* channel between Alice and Bob. Two real variables $d_B$ and $\alpha \in \mathbb{R}$ represent distance and pathloss exponent of the main channel. For example, free space microwave transmission has a pathloss exponent of $\alpha = 2$.

Eve observes the output of the symbols from the eavesdropper channel and receives a symbol sequence $\mathbf{z} = [Z(1), \cdots, Z(n)]^T$, where

$$Z(i) = d_E^{-\alpha/2} H_E(i) X(i) + N_E(i), \tag{2}$$

and $H_E(i) \in \mathbb{C}$ is a complex baseband channel gain of the eavesdropper. Two real variables $d_E, \alpha \in \mathbb{R}$ represent the distance and path loss exponent of the eavesdropper link, respectively. The noise on the Eve's receiver $N_E(i)$ also follows a zero-mean circularly symmetric complex Gaussian distribution. In this paper, we consider both the main channel and the eavesdropper channel to be quasi-static flat fading, corresponding to a large coherence time, so that the channel coefficients remain constant during the $n$ channel uses. Hence we can simplify the notations as $H_B(i) = H_B$, $H_E(i) = H_E$, $\forall i = 1, ..., n$.

The average transmission energy is defined as:

$$\mathcal{E} = \frac{1}{n} \sum_{i=1}^{n} E\left[|X(i)|^2\right] \tag{3}$$

where the expectation $E(\cdot)$ is taken over a time slot.

When $T = 0$, Alice switches off and the transmitted sequence $\mathbf{x} = \mathbf{0}$. Bob and Eve receive pure noises as $Y(i) = N_B(i)$ and $Z(i) = N_E(i)$, respectively.

### *B. Achievable rate region*

Bob decodes the message from $\mathbf{y}$ and the average error probability is:

$$P_b = \Pr(M \neq \hat{M}, \hat{T}_B = 1 | T = 1) + \Pr(\hat{T}_B = 0 | T = 1) \tag{4}$$

where $\hat{M}$ is the decoded message, $\hat{T}_B$ is Bob's detection whether a message is transmitted in the time block.

Eve tries to detect whether Alice transmits any message from the observed sequence $\mathbf{z}$. For every channel output, consider two hypotheses:

$$\begin{cases} H_0 : \mathbf{z} = \mathbf{n}_E \\ H_1 : \mathbf{z} = d_E^{-\alpha/2} H_E \mathbf{x} + \mathbf{n}_E \end{cases} \tag{5}$$

For simplicity, the distribution of the sequence $\mathbf{z}$ under the two hypotheses are denoted as $p_0(\mathbf{z})$ and $p_1(\mathbf{z})$, respectively. The probability of false alarm and mis-detection are given by

$$P_{FA} = \Pr(\hat{T}_E = 1 | T = 0), P_{MD} = \Pr(\hat{T}_E = 0 | T = 1),$$

respectively, where $\hat{T}_E$ is Eve's detection whether a message is transmitted in the time block. The probability of detection is measured by the sum of the probability of false alarm and the probability of miss-detection

$$P_\delta = |P_{FA} + P_{MD} - 1| \tag{6}$$

Set the bounds of the covert communication as the tolerable probability of detection $P_D$ and tolerable probability of decoding error $P_B$. A covert communication rate $R^*(n, P_B, P_D | H_B, H_E)$ is considered achievable if, under channel gains $H_B, H_E$, a transmission strategy exists such that the probability of decoding error and detection probability are respectively upper bounded by $P_b \leq P_B$ and $P_\delta \leq P_D$.

## III. SECURE TRANSMISSION RATE

Suppose Eve adopts the likelihood ratio test (LRT) to infer the binary hypothesis test in (5) with an LRT threshold $F$. Then we have

$$L(\mathbf{z}) = \frac{p_0(\mathbf{z})}{p_1(\mathbf{z})} \underset{H_1}{\overset{H_0}{\gtrless}} F \tag{7}$$

With the optimal detectors, the probability of false alarm and mis-detection is related with total variation distance between the two distributions [11]

$$P_{FA} + P_{MD} = 1 - V_t(\mathbb{P}_0, \mathbb{P}_1) = 1 - \frac{1}{2} \|p_0(\mathbf{z}) - p_1(\mathbf{z})\|_1 \tag{8}$$

where $\| \cdot \|_1$ is the $l_1$ norm. With Pinsker's Inequality, the relationship between the total variation distance and the informational divergence is

$$\frac{1}{2} \|p_0(\mathbf{z}) - p_1(\mathbf{z})\|_1 \leq \sqrt{\frac{1}{2} D(\mathbb{P}_1 || \mathbb{P}_0)} \tag{9}$$

where

$$D(\mathbb{P}_1 || \mathbb{P}_0) = \int_{\mathcal{Z}} p_1(\mathbf{z}) \log \frac{p_1(\mathbf{z})}{p_0(\mathbf{z})} d\mathbf{z}, \tag{10}$$

with $\mathcal{Z}$ being the support of $p_0(\mathbf{z})$. The informational divergence is also called the Kullback-Leibler (KL) divergence between two distributions. From the information geometry perspective, the KL divergence is a good approximation of the $l_1$ norm when the difference between two distributions is small.

By combining inequalities (6) and (9), the sufficient condition for communication with $P_\delta \leq P_D$ is then

$$D(\mathbb{P}_1||\mathbb{P}_0) \leq 2P_D^2. \tag{11}$$

**Covert Transmission Strategy:** *The best covert transmission scheme over $n$ channel uses with a total power $\mathcal{E}$ is to transmit independently with the expected power $\mathcal{E}/n$ in each channel use. The total power is upper bounded by*

$$\mathcal{E} \leq \sqrt{n} \cdot 2P_D d_E^\alpha \sigma_n^2/|H_E|^2. \tag{12}$$

The proof is provided in the appendix.

With this transmission strategy, the average SNR for Bob's receiver is:

$$\gamma_B = \frac{\mathcal{E}}{n}\frac{|H_B|^2}{d_B^\alpha \sigma_n^2} = \frac{2P_D}{\sqrt{n}}\frac{|H_B|^2}{|H_E|^2}\left(\frac{d_B}{d_E}\right)^{-\alpha}. \tag{13}$$

The channel throughput $L$ over $n$ channel uses with a tolerable probability of decoding error $P_B$ is hence [8, Eqn. 291]

$$L = nR = n\log(1+\gamma_B) - \sqrt{n\frac{\gamma_B}{2}\frac{\gamma_B+2}{(\gamma_B+1)^2}}Q^{-1}(P_B) + \mathcal{O}(\log n). \tag{14}$$

where $Q(x) = \frac{1}{2}\text{erfc}(x/\sqrt{2})$ is the Q-function, and $\mathcal{O}(\cdot)$ is the order operator.

## IV. Communication over uncertain WTC channels

In this section, we analyze the a more general case of fading wiretap channels. In most scenarios, CSI of the wiretap channel is unknown to the transmitter, and it can only be guaranteed that there is no eavesdropper within a certain distance range. Since the CSI of the wiretap channel is unknown, we cannot guarantee that the probability of detection must below a certain threshold. Alternatively, for flat fading scenarios, similar to the outage capacity, we measure the covert of communication systems in terms of the probability of outage detection. In this section, we assume both Alice and Bob have perfect knowledge of the main channel CSI but no knowledge of the wiretap channel CSI, while Eve knows the wiretap channel CSI. Assume Alice fix her total transmission power $\mathcal{E}$ and transmission block length $N$. In the previous section, we have proved that sending independently in all the channel uses with average power can reach the optimal transmission rate and the minimum probability of detection.

Denote the SNRs for Bob and Eve as $\gamma_B$ and $\gamma_E$, respectively. The distribution of $\gamma_B$ and $\gamma_E$ is hence exponential:

$$p(\gamma_B) = \frac{d_B^\alpha \sigma_n^2}{\mathcal{E}/n}\exp\left(-\frac{\gamma_B d_B^\alpha \sigma_n^2}{\mathcal{E}/n}\right), \quad \gamma_B > 0 \tag{15}$$

$$p(\gamma_E) = \frac{d_E^\alpha \sigma_n^2}{\mathcal{E}/n}\exp\left(-\frac{\gamma_E d_E^\alpha \sigma_n^2}{\mathcal{E}/n}\right), \quad \gamma_E > 0 \tag{16}$$

Assume the tolerable probability of detection is $P_D$, the outage probability of detection is defined as:

$$\mathcal{P}_{out}(P_D) = \text{Pr}\left[D(\mathbb{P}_1||\mathbb{P}_0) \geq 2P_D^2\right] \tag{17}$$

From inequality (12), the outage probability of detection beyond $P_D$ is obtained by:

$$\begin{aligned}\mathcal{P}_{out}(P_D) &= 1 - \int_0^{\frac{2P_D}{\sqrt{n}}} p(\gamma_E)d\gamma_E \\ &= 1 - \exp\left(-\frac{d_E^\alpha \sigma_n^2}{\mathcal{E}/n}2P_D/\sqrt{n}\right) \\ &= 1 - \exp\left(-\frac{d_E^\alpha \sigma_n^2}{\mathcal{E}}2P_D\sqrt{n}\right)\end{aligned} \tag{18}$$

## V. Simulations

In this section, we provide simulation results to show the covert transmission throughput under different communication settings, and the relationship with the square root law in covert communication.

In Fig. 2, we plot the achievable throughput for communication with detection probability $P_D \leq 0.1$ and decoding error rate less than $P_B \leq 0.1$. With a randomly generated channel $H_B = 0.6282 - 0.8111i$ and $H_E = 0.7558 - 0.5724i$, we study the achievable amount of covert message transformation under different attenuation exponent. We study the performance with $\alpha = 1.7$, $\alpha = 2$, and $\alpha = 3$, corresponding to the free space fading, urban cellular scenario and urban LoS scenario. From the simulation results, with larger $\alpha$, the more information that can be safely transmitted.

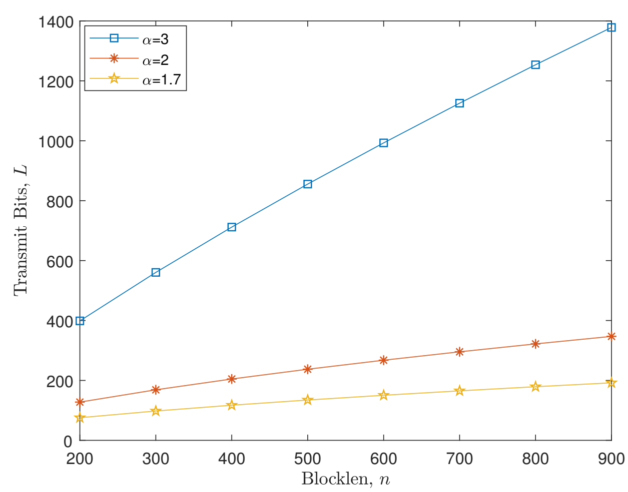


Figure 2. Number of achievable transmission messages $L = nR$ with various $\alpha$ and $d_B/d_E = 1/10, P_D \leq 0.1, P_B \leq 0.1$.

The bounds for communication with low probability of detection divide the number of transmission block length are depicted in Fig. 3. From the figure, when $\alpha = 2$ and 1.7, the ratio tends to be a constant with $n$ becomes bigger, indicating that the square root law holds true. For $\alpha = 3$, the increase speed of the curve keeps decreasing. Hence for $n$ becomes longer, it tends to reach a constant.

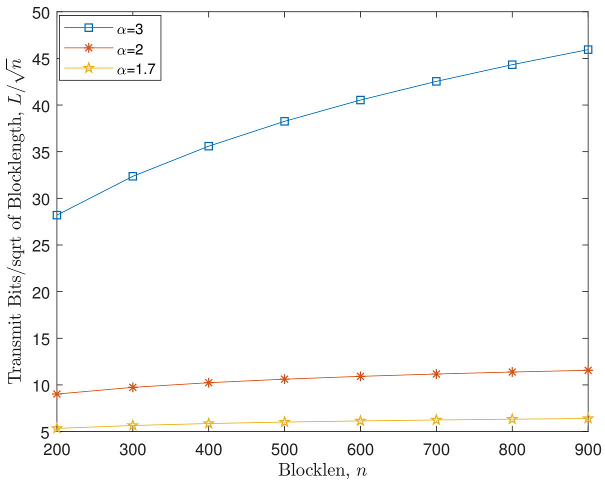


Figure 3. Relationship with square root law for covert communication with various $\alpha$ and $d_B/d_E = 1/10, P_D = 0.1, P_B = 0.1$.

## VI. Conclusions

With the novel metric effective security, we study the covert communication throughput under fading channel in this paper. Under both detection constraint and resolvability constraints, the channel throughput under finite block length is studied in the paper. Both theoretical analysis and simulation results reveal the relationship of the channel throughput with the previous result–*square root law*. Furthermore, the probability of outage detection is proposed as a metric for study the covert communication performance with the eavesdropper channel unknown.

## VII. Acknowledgement

This work was supported in part by the National Key R&D Program of China (Grant No.2017YFE0112300) and the National Natural Science Foundation of China under Grant 61471221, in part by the U.S.National Science Foundation under Grant ECCS-1646548 and the Wilkens Telecommunications Endowment at Missouri University of Science and Technology.

## Appendix A
## Proof of Covert Transmission Strategy

Denote $\mathbf{\Sigma}_X = E(\mathbf{x}\mathbf{x}^H)$ as the covariance matrix of transmit symbols $\mathbf{x}$ which satisfies the power constraint $\text{Tr}(\mathbf{\Sigma}_X) \leq \mathcal{E}$. Since the noise is assumed to be i.i.d. circularly symmetrical complex Gaussian over the $n$ channel uses, we have $p_0(\mathbf{z}) \sim \mathcal{CN}(\mathbf{0}, \sigma_n^2\mathbf{I})$ and $p_1(\mathbf{z}) \sim \mathcal{CN}(d_E^{-\alpha/2}H_E\mathbf{x}, \sigma_n^2\mathbf{I})$. The K-L divergence is then

$$\begin{aligned} & D(\mathbb{P}_1||\mathbb{P}_0) \qquad (19)\\ =\ & \int_{\mathcal{Z}} p_1(\mathbf{z}) \log \frac{p_1(\mathbf{z})}{p_0(\mathbf{z})} d\mathbf{z} \\ =\ & -H(\mathbb{P}_1) - \int_{\mathcal{Z}} p_1(\mathbf{z}) \log p_0(\mathbf{z}) d\mathbf{z} \\ =\ & -H(\mathbb{P}_1) - \int_{\mathcal{Z}} p_1(\mathbf{z}) \log \left( \frac{1}{(\pi\sigma_n^2)^n} \exp(-\frac{1}{\sigma_n^2}\mathbf{z}^H\mathbf{z}) \right) d\mathbf{z} \\ =\ & -H(\mathbb{P}_1) + n\log(\pi\sigma_n^2) + \frac{1}{\sigma_n^2} \int_{\mathcal{Z}} p_1(\mathbf{z})\mathbf{z}^H\mathbf{z}d\mathbf{z} \\ =\ & -H(\mathbb{P}_1) + n\log(\pi\sigma_n^2) + \frac{1}{\sigma_n^2}\left( \frac{|H_E|^2}{d_E^\alpha}\mathcal{E} + n\sigma_n^2 \right) \qquad (20) \end{aligned}$$

The integration in the last term of (20) is the correlation of $\mathbf{z}$ under the distribution of $p_1(\mathbf{z})$ which equals the total received signal power plus noise power $n\sigma_n^2$.

Minimizing the divergence $D(\mathbb{P}_1||\mathbb{P}_0)$ means to maximize the entropy of $\mathbb{P}_1$. When Alice transmits the message, the covariance of observation by Eve is

$$\begin{aligned} \mathbf{\Sigma}_Z = E[(d_E^{-\alpha/2}H_E\mathbf{x} + \mathbf{n}_E)(d_E^{-\alpha/2}H_E\mathbf{x} + \mathbf{n}_E)^H] \\ = \frac{|H_E|^2}{d_E^\alpha}\mathbf{\Sigma}_X + \sigma_n^2\mathbf{I}. \end{aligned} \qquad (21)$$

The maximum entropy is Gaussian distributed. Let the real part of the diagonal elements of $\mathbf{\Sigma}_Z$ be $\sigma_{Z(i)}^2$.

$$\begin{aligned} H(\mathbb{P}_1) &= -\int_{\mathcal{Z}} p_1(\mathbf{z}) \log p_1(\mathbf{z}) d\mathbf{z} \\ &\leq \log \left( (2\pi)^n \sqrt{\det \frac{1}{2} \begin{bmatrix} \Re(\mathbf{\Sigma}_Z) & \Im(\mathbf{\Sigma}_Z) \\ \Im(\mathbf{\Sigma}_Z) & \Re(\mathbf{\Sigma}_Z) \end{bmatrix}} \right) \\ &\leq \log \left( \pi^n \prod_i \sigma_{Z(i)}^2 \right) \\ &\leq \log \left( \pi^n \left( \frac{\sum_i \sigma_{Z(i)}^2}{n} \right)^n \right) \end{aligned} \qquad (22)$$

where the first inequality in (22) is obtained because Gaussian distribution maximizes the entropy under given covariance matrix. The second inequality in (22) is due to Hadamard inequality [12], which says the determinant of a positive semi-definite matrix is less than the product of its diagonal items. The third inequality in (22) is due to the geometric inequality, with equality achieved if and only if all the diagonal items are identical. Hence, to obtain the minimum divergence with a given total power constraint, the covariance of the received matrix is a diagonal matrix with identical entries, indicating that the best strategy is to use all the time slots independently and sending out symbols with equal power $\mathcal{E}/n$ in each slot.

Under the equal power transmission strategy, (22) becomes

$$H(\mathbb{P}_1) = n\log(\pi) + n\log\left( \frac{|H_E|^2}{d_E^\alpha}\mathcal{E} + n\sigma_n^2 \right) \qquad (23)$$

Substituting (23) into (20), the minimum divergence is then

$$\begin{aligned}
& D(\mathbb{P}_1||\mathbb{P}_0) \\
\geq \quad & -n\log\left(\pi\left(\frac{|H_E|^2}{nd_E^\alpha}\mathcal{E}+\sigma_n^2\right)\right)+n\log(\pi\sigma_n^2) \\
& +n\left(1+\frac{|H_E|^2}{nd_E^\alpha}\mathcal{E}\right) \\
= \quad & -n\log\left(1+\frac{|H_E|^2}{nd_E^\alpha\sigma_n^2}\mathcal{E}\right)+n\left(1+\frac{|H_E|^2}{d_E^\alpha\sigma_n^2}\mathcal{E}\right) \\
= \quad & -n\left\{1+\frac{|H_E|^2}{nd_E^\alpha\sigma_n^2}+\frac{1}{2}\left(\frac{|H_E|^2}{nd_E^\alpha\sigma_n^2}\right)^2+o\left(\left(\frac{|H_E|^2}{nd_E^\alpha\sigma_n^2}\right)^3\right)\right\} \\
& +n\left(1+\frac{|H_E|^2}{nd_E^\alpha\sigma_n^2}\right) \qquad (24)
\end{aligned}$$

The approximation in (24) are obtained using Taylor expansion with the assumption that $\frac{|H_B|^2}{nd_E^\alpha\sigma_n^2} << 1$, and hence the scaling item $o\left(\left(\frac{|H_E|^2}{nd_E^\alpha\sigma_n^2}\right)^3\right)$ can be omitted. Based on the above analysis, the minimum KL divergence is given by

$$D(\mathbb{P}_1||\mathbb{P}_0) \approx \frac{1}{2}n\left(\frac{|H_E|^2}{nd_E^\alpha\sigma_n^2}\mathcal{E}\right)^2. \qquad (25)$$

Substituting (25) into the inequality (11), the transmission power constraint must satisfy:

$$\frac{|H_E|^2\mathcal{E}}{d_E^\alpha\sigma_n^2} \leq 2P_D\sqrt{n} \qquad (26)$$

Then the result in (12) follows.

## REFERENCES


[1] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct 1949.

[2] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1921–1930, September 2013.

[3] G. D. Weeks, J. K. Townsend, and J. A. Freebersyer, "A method and metric for quantitatively defining low probability of detection," in *IEEE Military Communications Conference. Proceedings. MILCOM 98 (Cat. No.98CH36201)*, vol. 3, Oct 1998, pp. 821–826.

[4] T. S. Han, H. Endo, and M. Sasaki, "Reliability and secrecy functions of the wiretap channel under cost constraint," *IEEE Transactions on Information Theory*, vol. 60, no. 11, pp. 6819–6843, Nov 2014.

[5] J. Hou and G. Kramer, "Effective secrecy: Reliability, confusion and stealth," in *2014 IEEE International Symposium on Information Theory*, June 2014, pp. 601–605.

[6] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Transactions on Information Theory*, vol. 62, no. 6, pp. 3493–3503, June 2016.

[7] P. H. Che, M. Bakshi, and S. Jaggi, "Reliable deniable communication: Hiding messages in noise," in *Proceedings of the 2013 IEEE International Symposium on Information Theory, Istanbul, Turkey, July 7-12, 2013*, 2013, pp. 2945–2949.

[8] Y. Polyanskiy, H. V. Poor, and S. Verdu, "Channel coding rate in the finite blocklength regime," *IEEE Transactions on Information Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

[9] W. Yang, R. F. Schaefer, and H. V. Poor, "Wiretap channels: Nonasymptotic fundamental limits," [Online]. Available: http://arxiv.org/abs/1706.03866

[10] A. Abdelaziz and C. E. Koksal, "Fundamental limits of covert communication over MIMO AWGN channel," pp. 1–9, Oct 2017.

[11] E. L. Lehmann and J. P. Romano, *Testing statistical hypotheses*, 3rd ed. Springer Texts in Statistics. New York: Springer, 2005.

[12] M. Rozannski, R. Witula, E. Hetmaniok, "More subtle versions of the Hadamard inequality", Linear Algebra and its Applications, vol. 532, 2017, pp. 500–511