Benefits of Multiple Transmit Antennas in Secure Communication: A Secrecy Outage Viewpoint

Xi Zhang*, Xiangyun Zhou†, Matthew R. McKay*
*Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology, Hong Kong
†Research School of Engineering, The Australian National University, Canberra, Australia

***Abstract*—This paper investigates secure multi-antenna transmission in slow fading channels without the eavesdropper's channel state information. The use of multiple transmit antennas enables the transmitter to strengthen the signal reception at the intended receiver while simultaneously confusing the eavesdropper by delivering artificial noise. A recently developed secrecy outage formulation, which can separately measure the quality of service and the level of security, is used to characterize the security performance. We show that an arbitrarily low secrecy outage probability cannot be achieved by adding more transmit antennas alone without optimizing other system parameters. To facilitate the practical system design, we present an on-off transmission scheme with optimal artificial noise power allocation, which minimizes the secrecy outage probability whilst guaranteeing a minimum required quality of service.**

I. Introduction

Secrecy is one of the most important concerns in wireless communication. Currently, the primary method for keeping broadcasted messages confidential is to use high complexity encryption algorithms, which are typically designed without regard to the physical properties of the wireless medium. For such techniques, although the expenditure on interception may be very high, with the rapid development of the computing devices, providing robust security algorithms is becoming ever more challenging. A recent strong focus has thus been directed at developing physical-layer techniques, which can *guarantee* secret transmission in an information-theoretic sense.

Drawing upon the classical work of Shannon [1], it was proved in [2] that perfect secrecy can indeed be achieved in the physical layer by employing a proper encoder-decoder pair. Many recent papers have expanded upon this early work, considering various system configurations and assumptions. In particular, a major focus has been on studying the secrecy capacity under the assumption that the eavesdropper's instantaneous channel state information (CSI) is available at the transmitter; something which is usually impractical. Some notable exceptions, presented in [3, 4], introduced a secrecy outage formulation to give a probabilistic measure of security in slow fading channels, which is applicable to the case that the transmitter does not have the instantaneous CSI of the eavesdropper. This commonly used secrecy outage formulation gives a fundamental characterization of the possibility of having a reliable and secure transmission without distinguishing reliability and security. In our recent work [5], we revised the secrecy outage formulation in [3, 4] to give a more explicit measure of secrecy, which further allows a trade-off between the secrecy performance and the quality of service (QoS).

In this paper, we extend our earlier work [5] to the case of multi-antenna transmission. We consider a transmitter structure similar to [6, 7], for which the CSI feedback from the dedicated receiver is used to specify a beamforming vector to maximize the received signal strength, whilst simultaneously projecting artificial noise in the associated null space in order to protect against eavesdropping.

A primary objective of our work is to investigate the benefits of multi-antenna transmission in terms of reducing the secrecy outage probability. To this end, we start by analyzing the impact of varying the number of transmit antennas on the secrecy outage probability, keeping all the other parameters fixed. Our analysis demonstrates that, whilst some gain is observed by the addition of more antennas, an arbitrarily low secrecy outage probability cannot be achieved without adjusting the other parameters. In fact, we then show that by properly adjusting the amount of power which is allocated for artificial noise generation, any secrecy outage probability can indeed be obtained. We also investigate the secrecy performance under a constraint on the QoS performance, and derive the optimal system parameters to achieve the minimal secrecy outage probability.

We make use of the following notations: Boldface upper and lower case symbols denote matrices and vectors, respectively. $[\cdot]^T$ denotes the matrix transpose operation and $[\cdot]^*$ denotes the complex conjugate operation. We use $|\cdot|$ to denote the absolute value of a scalar, $||\cdot||$ to denote the norm of a vector, and $\mathbb{P}(\cdot)$ to denote the probability of an event.

II. System Model

We consider the transmission from Alice to Bob in the presence of an eavesdropper, Eve. Alice is equipped with N transmit antennas whilst Bob and Eve each has one receive antenna. Quasi-static Rayleigh fading is used to model the wireless channels.

The N dimensional symbol vector to be transmitted is defined as $\boldsymbol{x}$ and the received signal at Bob is given by

$$y_b = \boldsymbol{h}^T \boldsymbol{x} + n_b \,, \tag{1}$$

where the $N \times 1$ vector $\boldsymbol{h}$ is the channel fading gain from Alice to Bob and n_b is the receiver noise at Bob. The entries

X. Zhou was previously with UNIK - University Graduate Center, University of Oslo, Norway. This work was partially supported by the Research Council of Norway through the project 197565/V30.

of $\boldsymbol{h}$ are assumed to be independent and identically distributed (i.i.d.) zero-mean complex Gaussian variables with unit variance. The noise at Bob is zero-mean complex Gaussian with variance σ_b^2.

Similarly, the received signal at Eve is given by

$$y_e = \boldsymbol{g}^T \boldsymbol{x} + n_e \ , \tag{2}$$

where the $N \times 1$ vector $\boldsymbol{g}$ is the channel fading gain from Alice to Eve and n_e is the receiver noise at Eve. The entries of $\boldsymbol{g}$ are assumed to be i.i.d. zero-mean complex Gaussian variables with the same variance σ_g^2.

We assume that Bob can estimate the channel accurately and use a perfect feedback link to inform Alice about his instantaneous CSI. This link is not secure and can be intercepted by Eve. Assuming that Eve is a passive eavesdropper, the instantaneous CSI of Eve is unavailable to Alice.

A. On-Off Transmission and Secrecy Measure

Following the well-known encoding scheme of Wyner [2], the data is encoded in the physical layer before transmission in order to enhance the secrecy performance. The rate of transmitted codeword R_b and the rate of confidential information R_s are properly chosen by the encoder. The difference between these two rates $R_e = R_b - R_s$ indicates the sacrifice on the data rate to secure the communication against eavesdropping. If the channel capacity from Alice to Eve C_e is larger than the rate difference R_e, then perfect secrecy cannot be achieved and a secrecy outage occurs [5].

We consider an on-off transmission scheme, in which a transmit threshold on the signal-to-noise ratio (SNR) at Bob is used by Alice to decide to transmit or not. She transmits signals only when the instantaneous SNR at Bob γ_b exceeds the transmit threshold μ. The purpose of using the SNR threshold is to prevent possible information leakage due to unnecessary transmission. More specifically, when Bob's channel cannot support the codeword rate, Alice would suspend the transmission since it would ultimately lead to decoding errors at Bob, whilst simultaneously causing unnecessary information leakage to Eve.

For a given transmit threshold μ, the transmit probability is

$$p_{\text{tx}} = \mathbb{P}\left(\gamma_b \geq \mu\right) \ , \tag{3}$$

which can be treated as a QoS measure. For example, if messages are transmitted as soon as the channel condition allows, the quantity $p_{\text{tx}}^{-1} - 1$ can serve as an indication of the average delay of transmission.

According to [5], the secrecy outage probability can be written as

$$p_{\text{so}} = \mathbb{P}\left(C_e > R_b - R_s \mid \text{message transmission}\right) \ . \tag{4}$$

B. Transmit Beamforming with Artificial Noise

In [6], Goel and Negi introduced the concept of generating artificial noise to guarantee secure transmission. The key idea is outlined as follows. Alice can generate a matrix $\boldsymbol{W} = [\boldsymbol{w}_1 \ \boldsymbol{W}_2]$, which is an orthonormal basis of $\mathbb{C}^N$ and $\boldsymbol{w}_1 = \boldsymbol{h}^*/||\boldsymbol{h}||$. Then she can mix the artificial noise with the message symbol to be transmitted u as

$$\boldsymbol{x} = \boldsymbol{w}_1 u + \boldsymbol{W}_2 \boldsymbol{v} \ , \tag{5}$$

where u is zero-mean complex Gaussian variable with variance σ_u^2. The $N-1$ entries of the column vector $\boldsymbol{v}$, which is the artificial noise, are i.i.d. zero-mean complex Gaussian variables.

Using maximum ratio transmission with the added artificial noise in the null space of Bob's channel, by (1) and (2), the received signal at Bob becomes

$$\begin{aligned} y_b &= \boldsymbol{h}^T \boldsymbol{w}_1 u + \boldsymbol{h}^T \boldsymbol{W}_2 \boldsymbol{v} + n_b \\ &= ||\boldsymbol{h}|| u + n_b \ , \end{aligned} \tag{6}$$

whilst the received signal at Eve becomes

$$\begin{aligned} y_e &= \boldsymbol{g}^T \boldsymbol{w}_1 u + \boldsymbol{g}^T \boldsymbol{W}_2 \boldsymbol{v} + n_e \\ &= g_1 u + \boldsymbol{g}_2^T \boldsymbol{v} + n_e \ , \end{aligned} \tag{7}$$

where $g_1 = \boldsymbol{g}^T \boldsymbol{w}_1$ and $\boldsymbol{g}_2^T = \boldsymbol{g}^T \boldsymbol{W}_2$.

The total transmit power of Alice is fixed to its maximal level P. Part of the transmit power is given to the information-bearing signal. We define the power allocation ratio as the fraction of the information-bearing signal power to the total transmit power:

$$\Phi = \frac{\sigma_u^2}{P} \ . \tag{8}$$

The rest of the transmit power is used to generate artificial noise and is equally assigned to the $N-1$ entries of the artificial noise vector $\boldsymbol{v}$. Thus the variance of each entry of $\boldsymbol{v}$ is given as

$$\sigma_v^2 = \frac{(1-\Phi)\, P}{N-1} \ . \tag{9}$$

With such a power splitting, the transmitted signal-to-artificial-noise ratio (SANR) is given by $\frac{\Phi}{1-\Phi}$.

With the normalization of the noise power at Bob, i.e., $\sigma_b^2 = 1$, the instantaneous received SNR at Bob is given as

$$\gamma_b = P\Phi ||\boldsymbol{h}||^2 \ , \tag{10}$$

where $||\boldsymbol{h}||^2$ follows a Gamma distribution with parameters $(N, 1)$. Hence the complementary cumulative density function (c.c.d.f.) of γ_b can be characterized as

$$\bar{F}_{\gamma_b}\left(\gamma_b\right) = \Gamma_R\left(N, \frac{\gamma_b}{P\Phi}\right) \ , \tag{11}$$

where $\Gamma_R\left(\cdot,\cdot\right)$ is the regularized upper incomplete Gamma function. Thereby, the transmit probability in (3) can be evaluated.

To facilitate our subsequent analysis, we define a function $\Gamma_R^{-1}(N, X)$ to represent the inverse function of the regularized upper incomplete Gamma function, taken w.r.t. the second parameter X. A closed-form expression for $\Gamma_R^{-1}(N, X)$ is not available, but it can be computed easily numerically. We can see that $\Gamma_R^{-1}(N, X)$ decreases with X and increases with N.

The noise power at Eve may not be known to Alice and hence a robust approach, as done in [6, 7], is to assume that

there is no receiver noise at Eve, i.e., $n_e = 0$. Therefore, the instantaneous received SNR at Eve is given as

$$\gamma_e = \frac{|g_1|^2\sigma_u^2}{||\boldsymbol{g}_2||^2\sigma_v^2} = \frac{N-1}{\Phi^{-1}-1}\frac{|g_1|^2}{||\boldsymbol{g}_2||^2} \ . \tag{12}$$

Since $\boldsymbol{g}$ has i.i.d. complex Gaussian entries each with variance σ_g^2 and $\boldsymbol{W}$ is a unitary matrix, $\boldsymbol{g}^T\boldsymbol{W} = [g_1\ \boldsymbol{g}_2]$ also has i.i.d. complex Gaussian entries with variance σ_g^2. Consequently, the quantity $|g_1|^2/||\boldsymbol{g}_2||^2$ is equivalent to the signal-to-interference ratio of a minimum mean-squared error estimator with $N-1$ interferers. Hence we can use the result in [8, Eq. 19] to characterize the c.c.d.f. of γ_e as

$$\bar{F}_{\gamma_e}(\gamma_e) = \left(1+\gamma_e\left(\frac{\Phi^{-1}-1}{N-1}\right)\right)^{1-N} \ . \tag{13}$$

Note that when the number of transmit antennas goes to infinity, the received SNR at Eve becomes exponentially distributed with the transmitted SANR as its mean.

III. Secrecy Outage Probability

In this section, we consider the secrecy performance under the assumption that the encoder at the transmitter is "fixed"; i.e., all the rates and the transmit threshold have been chosen carefully and do not change with the instantaneous CSI. By the independence of Bob's and Eve's channels, the secrecy outage probability in (4) reduces to the unconditional probability:

$$p_{\text{so}} = \mathbb{P}\left(C_e > R_b - R_s\right) \ . \tag{14}$$

For a given power allocation ratio, recalling that

$$C_e = \log_2\left(1+\gamma_e\right) , \tag{15}$$

we further evaluate (14) as

$$\begin{aligned} p_{\text{so}} &= \bar{F}_{\gamma_e}\left(2^{R_b-R_s}-1\right) \\ &= \left(1+\left(2^{R_b-R_s}-1\right)\left(\frac{\Phi^{-1}-1}{N-1}\right)\right)^{1-N} \ . \end{aligned} \tag{16}$$

Note that since we assumed that there is no receiver noise at Eve, the secrecy outage probability above serves as an upper bound to the actual secrecy outage probability and we use it to measure the secrecy performance. By ignoring the receiver noise at Eve, we see that the secrecy outage probability becomes independent of the total transmit power, and depends only on the power allocation ratio. In other words, increasing the total transmit power without adjusting the power allocation ratio cannot improve the secrecy performance.

A. Effects of Transmit Antenna Number

For a given power allocation ratio, it can be proved by using the binomial theorem that the secrecy performance will be enhanced when the transmit antenna number increases. The underlying reason is that the added transmit antennas give Alice more directions in the complex space to confuse Eve. From (3) and (11), we can see that the added transmit antennas guarantee a better QoS performance.

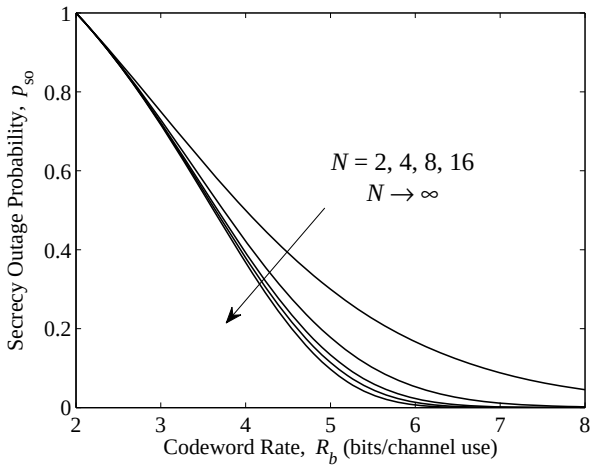

Fig. 1. Secrecy outage probability versus the codeword rate for different numbers of transmit antennas, with $\Phi = 0.75$, and $R_s = 2$ bits/channel use.

By taking the number of transmit antennas to infinity, the secrecy outage probability in (16) converges to

$$\lim_{N\to\infty} p_{\text{so}} = \exp\left(-\frac{2^{R_b-R_s}-1}{\frac{\Phi}{1-\Phi}}\right) \ . \tag{17}$$

From the limit above, we can see that the improvements on the secrecy performance brought by extra transmit antennas is limited, i.e., an arbitrarily low secrecy outage probability cannot be obtained by increasing the number of transmit antennas while other parameters remain unchanged. This is explained by noting that, with more transmit antennas and a fixed power allocation ratio, the received artificial noise becomes "more random", with the received SNR at Eve eventually following an exponential distribution as N goes to infinity. These comments are corroborated in Fig. 1.

B. Effects of Power Allocation Ratio

From (16), we can see that the secrecy outage probability increases with increasing the power allocation ratio. When less power is used to confuse the eavesdropper, the risk of secrecy outage would naturally increase. Furthermore, we see that any secrecy outage probability can be achieved by choosing a proper power allocation ratio, and this is a direct benefit of using multi-antenna beamforming transmission with artificial noise, as opposed to single antenna transmission. However, it should be noted that by lowering the power allocation ratio, the improvement in terms of secrecy performance comes at the cost of reducing the QoS performance, i.e., the transmit probability is also lowered. The relationship between the secrecy outage probability and the power allocation ratio is clearly shown in Fig. 2.

The previous discussions indicates that, with a fixed encoder at the transmitter, there are two methods to obtain a lower secrecy outage probability: one is increasing the number of transmit antennas, the other one is reducing the power allocation ratio. The first method can improve the secrecy

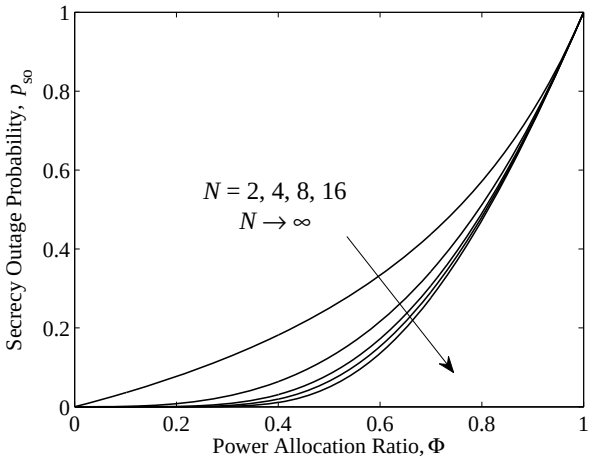

Fig. 2. Secrecy outage probability versus the power allocation ratio for different numbers of transmit antennas, with $R_s = 2$ bits/channel use, and $R_b = 4$ bits/channel use.

and QoS performance simultaneously, but the gain on the secrecy performance is limited. On the other hand, the second method can make sure that any arbitrarily low secrecy outage probability is realizable, but pays a price in terms of the QoS performance.

IV. Secrecy Performance Optimization

In this section, we consider the minimization of the secrecy outage probability with a prescribed data rate R_s and a QoS requirement given by a minimum acceptable transmit probability δ, which guarantees the maximum average delay. The optimization problem can be written as

$$\min_{\mu,R_b,\Phi} \; p_{\rm so}\left(R_b,\Phi\right) \quad \text{s.t.} \quad p_{\rm tx}\left(\mu,\Phi\right) \geq \delta \; . \tag{18}$$

Although the codeword rate R_b is the same for all transmissions, it will be carefully chosen to give the best possible secrecy performance. We first optimize the transmit threshold and the codeword rate jointly for any given power allocation ratio, then derive the optimal power allocation ratio to minimize the secrecy outage probability.

A. Optimization of Transmit Threshold and Codeword Rate

From (3) and (11), the QoS requirement can be expressed as

$$p_{\rm tx}\left(\mu,\Phi\right) = \Gamma_R\left(N, \frac{\mu}{P\Phi}\right) \geq \delta \; . \tag{19}$$

By the inverse regularized upper incomplete Gamma function we defined, the possible range of the transmit threshold can be determined by

$$\frac{\mu}{P\Phi} \leq \Gamma_R^{-1}(N,\delta) \; . \tag{20}$$

Thus the maximal transmit threshold can be given as

$$\mu_{\max} = P\Phi\,\Gamma_R^{-1}(N,\delta) \; . \tag{21}$$

By choosing a proper transmit threshold, which is no larger than $\mu_{\max}$, the QoS requirement can be guaranteed.

To ensure the successful decoding at Bob, the inequality $R_b \leq \log_2\left(1+\mu\right)$ must stand. From (14), we see that the secrecy outage probability decreases with the codeword rate. To obtain the best possible secrecy performance, the codeword rate and thereby the transmit threshold will be set to their maximal acceptable values. Therefore, the optimal transmit threshold is $\mu_{\max}$ and the optimal codeword rate is given as

$$R_b^{\max} = \log_2\left(1 + P\Phi\,\Gamma_R^{-1}(N,\delta)\right) \; . \tag{22}$$

Since the codeword rate must be larger than the secrecy rate, there is an intrinsical constraint on our system as

$$\frac{2^{R_s}-1}{\Gamma_R^{-1}(N,\delta)P} < 1 \; . \tag{23}$$

In the following, we assume that this constraint is satisfied.

By using the optimal codeword rate, from (16), the secrecy outage probability in this case can be written as

$$p_{\rm so}\left(\Phi\right) = \left(1 + \left(\frac{1+P\Phi\,\Gamma_R^{-1}(N,\delta)}{2^{R_s}} - 1\right)\left(\frac{\Phi^{-1}-1}{N-1}\right)\right)^{1-N} \; , \tag{24}$$

where the power allocation ratio can be adjusted to achieve the minimal secrecy outage probability.

B. Optimization of Power Allocation Ratio

We can rewrite (24) as

$$p_{\rm so}\left(\Phi\right) = \left(\frac{A\Phi + B\Phi^{-1} + C}{2^{R_s}(N-1)}\right)^{1-N} \; , \tag{25}$$

where

$$\begin{aligned} A &= -\Gamma_R^{-1}(N,\delta)P \; , \\ B &= 1 - 2^{R_s} \; , \\ C &= 2^{R_s}N + \Gamma_R^{-1}(N,\delta)P - 1 \; . \end{aligned}$$

It can be shown that the secrecy outage probability with a QoS requirement is a convex function of the power allocation ratio (the proof is omitted due to space limitation). We can see that the minimal secrecy outage probability can be achieved when the numerator inside the bracket in (25) reaches its maximal value. By setting the derivative of $A\Phi + B\Phi^{-1} + C$ w.r.t. Φ to zero, we can give the optimal power allocation ratio as

$$\Phi_{\rm opt} = \sqrt{\frac{2^{R_s}-1}{\Gamma_R^{-1}(N,\delta)P}} \; , \tag{26}$$

and the minimal secrecy outage probability as

$$p_{\rm so}^{\min} = \left(1 + \frac{\left(\sqrt{\Gamma_R^{-1}(N,\delta)P} - \sqrt{2^{R_s}-1}\right)^2}{2^{R_s}(N-1)}\right)^{1-N} \; . \tag{27}$$

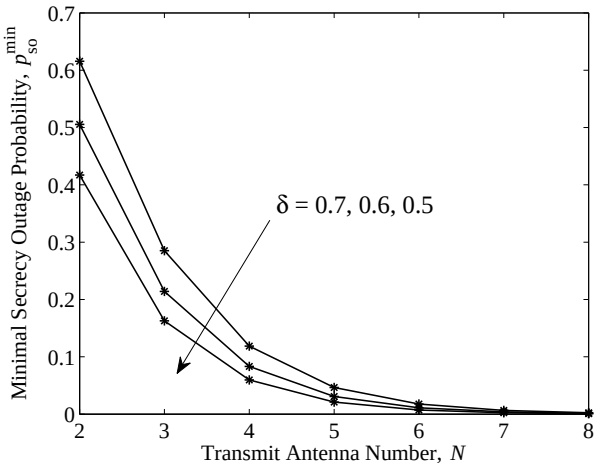

Fig. 3. Minimal secrecy outage probability versus the number of transmit antennas for different QoS requirements, with $P = 10$ dB, and $R_s = 2$ bits/channel use.

Note that different from the system without optimization in Section III, the minimal secrecy outage probability in this case is related to the transmit power. It can be proved that the minimal secrecy outage probability under QoS constraint can be reduced by increasing the number of transmit antennas. The underlying reason is that the benefits brought by extra transmit antennas is used to fight against eavesdropping, i.e., the power allocation ratio Φ is adjusted to be smaller and the rate difference R_e is reasonably enlarged. From (26), we can see that the optimal power allocation ratio converges to zero as N goes to infinity. In the Appendix, we show that the secrecy outage probability under a QoS constraint converges to zero when N goes to infinity.

Fig. 3 illustrates the optimized secrecy performance w.r.t. the number of transmit antennas for different QoS requirements. The secrecy improvements brought by extra transmit antennas turn to be very appreciable. Moreover, the tradeoff between the secrecy performance and the QoS requirement can be observed, i.e., when the QoS requirement gets stronger, the optimized secrecy performance becomes worse.

V. Conclusion

In this paper, we investigated the secrecy outage probability of a system in which beamforming is performed at the transmitter to strengthen the communication with the intended receiver and artificial noise is intentionally delivered to confuse the potential eavesdropper. We found that an arbitrarily low secrecy outage probability cannot be obtained by adding more transmit antennas alone without adjusting other system parameters. After that, the secrecy outage probability with a QoS requirement was minimized and the optimal system parameters were given. We revealed that with the optimal power splitting between the information-bearing signal and the artificial noise, the minimal secrecy outage probability under a QoS constraint converges to zero as the number of transmit antennas goes large.

Appendix

It is not easy to show the convergence directly since that there is no closed-form expression for $\Gamma_R^{-1}(N,\delta)$. Instead, we use a lower bound of $\Gamma_R^{-1}(N,\delta)$ to show the convergence.

For $N \geq 2$, define

$$\Delta\left(X\right) := \Gamma_R\left(N, X\right) - \left(1 - \frac{X}{N-1}\right) , \tag{28}$$

which is larger than zero when $X \geq N-1$.

The second order derivative of $\Delta\left(X\right)$ w.r.t. X is given by

$$\frac{d^2\Delta(X)}{dX} = \mathrm{e}^{-X}\frac{X^{N-2}}{(N-2)!}\left(\frac{X}{N-1} - 1\right) , \tag{29}$$

which is smaller than zero in $(0, N-1)$.

Since $\Delta\left(0\right)$ and $\Delta\left(N-1\right)$ are both no less than zero, by concavity, we can show that $\Delta\left(X\right) \geq 0$ holds when X is in $[0, N-1]$.

Conclusively, the following inequality:

$$\Gamma_R(N,X) \geq 1 - \frac{X}{N-1} , \tag{30}$$

stands for any $X \geq 0$ when $N \geq 2$.

When $X = \Gamma_R^{-1}(N,\delta)$, the inequality above changes to

$$\Gamma_R^{-1}(N,\delta) \geq (N-1)(1-\delta) , \tag{31}$$

which serves as a lower bound of $\Gamma_R^{-1}(N,\delta)$.

From (27), when N is sufficiently large, we can see that

$$p_{\mathrm{so}}^{\min} \leq \left(1 + \frac{\left(\sqrt{(N-1)(1-\delta)P} - \sqrt{2^{R_s}-1}\right)^2}{2^{R_s}(N-1)}\right)^{1-N} , \tag{32}$$

where it can be shown that the right part converges to zero as N goes to infinity. Thus we can see that $p_{\mathrm{so}}^{\min}$ in (27) also converges to zero as N goes to infinity.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Technol. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Technol. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[4] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Symp. Inform. Theory*, Adelaide, Australia, Sep. 2005, pp. 2152–2155.

[5] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[6] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[7] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[8] H. Gao, P. J. Smith, and M. V. Clark, "Theoretical reliability of MMSE linear diversity combining in Rayleigh-fading additive interference channels," *IEEE Trans. Commun.*, vol. 46, no. 5, pp. 666–672, May 1998.