Apply Artificial Noise To Secure Fading Relay Networks: A SER-Based Approach

Ying Liu*, Liang Li*, George C. Alexandropoulos†, and Marius Pesavento*

*Communication Systems Group, Technische Universität Darmstadt, Darmstadt, Germany
†Mathematical and Algorithmic Sciences Lab, France Research Center, Huawei Technologies Co. Ltd.

Abstract—We apply the concept of artificial noise (AN) transmission in a relay network to enhance communication security between a source and a destination. In this network, the source transmits square quadrature amplitude modulated (QAM) signals to the destination via the assistance of an untrusted relay, and all wireless channels are assumed to be Rayleigh faded. In order to shield the signals from the untrusted relay, the destination applies its designed AN symbols to jam the relay. The objective of the AN design at the destination is to maximize the symbol error rate (SER) of the QAM signals at the relay based on different types of channel state information (CSI). Specifically, by assuming the knowledge of the instantaneous CSI of the source-to-relay and relay-to-destination links, we derive an analytical expression for the SER. Based on the assumption of an average power constraint at the destination, we find the optimal phase and power distribution of the AN that maximizes the SER at the untrusted relay. Furthermore, by assuming the the statistical CSI of the source-to-relay and relay-to-destination links, i.e., channel variances, the optimal AN design that maximizes the average SER at the untrusted relay is obtained. For both schemes, our study shows that the Gaussian distribution is generally not optimal to generate AN symbols. In particular, numerical results show that the Gaussian distributed AN is far from optimal when the instantaneous CSI is available. In addition, it is important to note that our SER-based approach takes practical communication issues into account, such as QAM signaling and maximum likelihood decoding. The results in this paper can be used as benchmarks for future analyses of AN-based techniques.

Index Terms—Physical layer security, artificial noise, Rayleigh fading, square quadrature amplitude modulation, symbol error rate, error maximization, KKT conditions.

I. INTRODUCTION

Today, secure data communications heavily rely on modern cryptography. In his seminal work [2], Shannon laid the foundation for mathematical cryptography, which has become the most popular means to secure data communications. However, the emergence of high-performance computers may challenge the existing cryptographic algorithms relying on computational hardness. As a complementary strategy to provide secure data communications, physical layer security has recently drawn considerable attention. Since preliminary works [3, 4] characterized the secrecy capacity for wiretap channels, secrecy communication has been extensively studied for various channel models and network setups, such as single-hop wiretap channels [5–10], multi-user networks [11, 12], and relay networks [13–17]. In relay networks, security issues can be categorized into two general types: trusted and untrusted relaying. Unlike trusted relaying, the transmit message from the source must be kept confidential from the untrusted relay, which performs as a helper in forwarding messages from the source to the destination, and yet also as an eavesdropper that tries to decode secret information, see e.g. [18–20] and references therein.

To shield the message from the untrusted relay, one popular physical layer scheme is to apply artificial noise (AN) to efficiently jam the signal reception at the relay. This technique has recently been studied from an information-theoretic perspective, such as secrecy rate and secrecy outage probability, see e.g., [20–25]. However, such metrics are in general valid for ideal communication assumptions of continuous input messages and random encoding schemes with asymptotically large block lengths. In order to take discrete modulation alphabets and finite block lengths into consideration, other secrecy performance metrics have also been proposed, such as bit error rate [26, 27]. The observation that in modern wireless communication systems square quadrature amplitude modulation (QAM) is widely used motivates us to address the problem of how to optimally apply AN to enhance the physical layer security in an untrusted relay network. The symbol error rate (SER) of the demodulated signal at the relay is used as a performance metric in this paper.

In the untrusted relay network of our interest, the relay simultaneously receives the QAM signals from the source and the AN, which is designed and transmitted by the destination. The destination has access to the instantaneous channel state information (CSI) of the source-to-relay and relay-to-destination links, both of which are assumed to be under independent Rayleigh fading. For this setup, we investigate the problem of how to optimally design the AN to maximize the SER of QAM signals at the relay. Based on the instantaneous CSI, we first derive the exact SER expression, which is then maximized to optimally design the phase and power of the AN symbols. For fading channels, an important performance metric is the average SER (ASER), which quantifies the average decoding error performance over fading channels.

This work was presented in part in IEEE 8th Sensor Array and Multichannel Signal Processing Workshop (SAM), 22-25 Jun. 2014, A Coruña [1].

Y. Liu, L. Li, and M. Pesavento acknowledge the financial support of the Seventh Framework Programme for Research of the European Commission under grant number: ADEL-619647. This work was partially performed within the LOEWE Priority Program Cocoon (http://www.cocoon.tu-darmstadt.de) supported by the LOEWE research initiative of the state of Hesse/Germany.
In this work, we further reveal the optimal AN design that maximizes the ASER of QAM signals at the relay based on statistical CSI, i.e., the channel variances. Interestingly, for both CSI schemes, our study shows that it is not optimal to generate AN from a Gaussian distribution. For example, based on instantaneous CSI, we note that a QAM or a rotated QAM AN generating method maximizes the SER at the relay. The results in this paper can be used as benchmarks for future analyses of AN-based techniques.

Furthermore, the AN-based scheme studied in this paper is formulated according to the framework of current cellular standards such as long-term evolution (LTE)/LTE-Advanced [28]. By applying an additional processing unit to generate AN, the studied scheme can be easily embedded in a practical system to secure wireless communications, e.g., key transmission or control signaling. Moreover, our study provides exact SER expressions of the QAM signals at the relay, which can be used as benchmarks for future extensions, e.g., deriving SER expressions for other modulation schemes, and designing AN signaling in other scenarios.

**Notation:** Throughout this paper, we use $\mathcal{CN}(b_1, b_2)$ to represent a complex circularly symmetric Gaussian distribution with mean $b_1$ and variance $b_2$. We use $\mathcal{E}\{\cdot\}$ and $\Pr(\cdot)$ to denote statistical expectation and probability. Moreover, $|b|$ and $b^*$ represent absolute value and complex conjugate of $b$, respectively.

## II. SYSTEM MODEL AND PROBLEM FORMULATION

Let us consider a relay channel as shown in Fig. 1. A legitimate transmitter (the source) sends information symbols to a legitimate receiver (the destination) assisted by an untrusted relay. We assume that a direct link between the legitimate terminals is not available. All the terminals are configured with a single antenna. We assume quasi-static Rayleigh fading channels and the channel coefficients for the source-to-relay and relay-to-destination links are respectively denoted by $h$ and $g$, where $h \sim \mathcal{CN}(0, \sigma^2_h)$ and $g \sim \mathcal{CN}(0, \sigma^2_g)$. All channels are assumed to be reciprocal and constant within one time block. The transmission from the source to destination can be partitioned into two time slots. During the first time slot, the source broadcasts the symbol $m$. Meanwhile, to prevent the relay from deciphering the information, the destination sends the AN symbol $z$ to increase the noise level at the relay. The received baseband signal at the relay can be mathematically expressed as

$$ y = hm + gz + n $$  \hspace{1cm} (1)

where the additive white Gaussian noise (AWGNN) symbol $n$ is zero mean and has the one-sided power spectral density $N_0$ in Watt/Hz. During the second time slot, the source is muted, and the relay applies the amplify-and-forward protocol [30] to forward a scaled version of the received signal to the destination. Upon receiving this signal, the destination removes the AN $z$ prior to decoding $m$. For this protocol, the destination is required to have the perfect CSI of $h$ and $g$ in order to maximize the system’s transmission rate [31].

While exploiting the untrusted relay to help the data transmission, the system is designed to make sure that the untrusted relay cannot decipher the source’s symbol $m$. In addition, we assume that the relay can obtain knowledge about the modulation scheme of the source, e.g., by tracking the common control channel of the network. Moreover, it is important to note that the AN in Eq. (1) is solely designed by the destination so that the relay is not aware of the existence of the AN, as well as the AN distribution. Therefore, when decoding the symbols transmitted by the source, the relay treats the AN from the destination as noise. Further, we assume that the source transmits demodulation reference signals (DM-RS) [28] so that the relay can perfectly estimate $h$ to perform ideal coherent demodulation as

$$ \hat{y} = \frac{h^*}{|h|} y = \frac{h^*}{|h|} m + \frac{h^*}{|h|} g z + \frac{h^*}{|h|} n. $$  \hspace{1cm} (2)

Forwarded by the relay, the destination also has access to $h$ and the DM-RS of the source. For the source’s symbol $m$, we consider square $M$-QAM modulation types with $M = 4^k$ and $k = 1, 2, \ldots$, which are frequently used in the current and upcoming communication standards [28]. We also make the common assumption that constellation points are uniformly distributed [32]. In addition, we use $E_m$ and $E_z$ to denote the average energy per symbol for the source’s signal $m$ and the AN sent by the destination $z$, respectively. Furthermore, $E_m$ is assumed to be known at the destination for the AN design.

Since the destination has perfect knowledge of the instantaneous channel coefficients $h$ and $g$, the AN symbol $z$ can be designed this. The relay uses the ideal coherent demodulation with minimum distance detection to recover the source’s signal $m$, and the corresponding SER is the performance metric used in this paper. The objective is to design the AN symbol $z$ at the destination in order to maximize the SER at the relay, which we address in Section III. To reduce the complexity of the AN design, the AN symbol $z$ can also be designed based on long-term CSI of $h$ and $g$, i.e., $\sigma^2_h$ and $\sigma^2_g$. In this case, the AN symbol $z$ can be designed in order to maximize the ASER at the relay, and this is investigated in Section IV.

## III. DESIGNING THE AN TO MAXIMIZE SER

The SER analysis in this section consists of three parts. In Section III-A, for given instantaneous channel realizations $h$ and $g$, we derive the SER expression at the relay for a...
given AN symbol \( z \) in the case of square \( M \)-QAM modulated signals. Based on this expression, in Section III-B, we further study the problem of how to select the phase of our SER analysis is based on the procedure presented in [32, Chapter 5].

As an example, the constellation diagram for the square 16-QAM is illustrated in Fig. 2. Denote the minimum distance between two constellation points as \( 2a \) \((a > 0)\), then for a general \( M \)-QAM constellation, the average energy per signal symbol \( E_m \) can be expressed as [33, p. 194]

\[
E_m = \frac{2}{3} a^2 T_m (M - 1)
\]

where \( T_m \) denotes the symbol duration.

Since the AN design in this section is based on \( h \) and \( g \), for simplicity of notation, we define \( s := \frac{b}{h^2} z \) and \( \tilde{n} := \frac{b}{h} n \) in Eq. (2), and denote the real and imaginary parts of \( s \) and \( \tilde{n} \) as \( s_r, s_i, \tilde{n}_r, \) and \( \tilde{n}_i \), respectively. Thus, we have \( s = s_r + js_i \) and \( \tilde{n} = \tilde{n}_r + j\tilde{n}_i \) with \( j = \sqrt{-1} \). Note that the equivalent noise \( \tilde{n} \) is identically distributed with \( n \), and thus \( \tilde{n} \sim C N(0, 2\sigma^2) \), where \( \sigma^2 = \frac{N_0}{2T_m} \). For a vertex such as the point “0” in Fig. 2, the received symbol \( \tilde{y} \) in Eq. (2) lies outside its decision region. Based on the assumption that the constellation points are uniformly distributed, for a given \( z \), or equivalently for a given \( s \), the SER for the square QAM signal at the relay can be derived by averaging the respective error probability expressions for all symbols under the assumption of a uniform symbol distribution, resulting in

\[
P_{e,0} = 1 - \left( 1 - Q \left( \frac{|h|a - s_r}{\sigma} \right) \right) \left( 1 - Q \left( \frac{|h|a + s_i}{\sigma} \right) \right)
\]

where \( Q(\cdot) \) is the Gaussian Q-function [33]. Similarly, the error probability for the \( i \)th constellation point \( P_{e,i} \) \((i = 0, 1, \ldots, M)\) is obtained by computing the probability that \( \tilde{y} \) in Eq. (2) lies outside its decision region. Based on the assumption that the constellation points are uniformly distributed, for a given \( z \), or equivalently for a given \( s \), the SER for the square QAM signal at the relay can be derived by averaging the respective error probability expressions for all symbols under the assumption of a uniform symbol distribution, resulting in

\[
\text{SER} (s) = c \left[ Q \left( \frac{|h|a - s_r}{\sigma} \right) + Q \left( \frac{|h|a + s_r}{\sigma} \right) - c^2 \left[ Q \left( \frac{|h|a - s_i}{\sigma} \right) + Q \left( \frac{|h|a + s_i}{\sigma} \right) \right] \right]
\]

where \( c = \frac{\sigma}{\sqrt{M}} \). Using Eq. (3), we have

\[
a = \sqrt{\frac{3E_m}{N_0 (M - 1)}}
\]

Note that in the case of \( z = 0 \), the SER expression in Eq. (5) coincides with that of the AWGN channel [33, Eq. (8.10)].

Before proceeding, it is interesting to note that the SER expression in Eq. (5) depends on the real and imaginary parts of \( s \), which motivates us to express \( s \) as

\[
s = |g||z| \exp(j\theta)
\]

where \( z = |z| \exp(j\theta_z), \ g = |g| \exp(j\theta_g), \ h = |h| \exp(j\theta_h), \) and \( \theta = \theta_g - \theta_h + \theta_z \), respectively. Now, inserting Eq. (7) into Eq. (5), the SER expression can be rewritten as a function of \( \theta \) and \( |z| \) as

\[
\text{SER} (\theta, |z|) = 
\]

\[
c \left[ Q \left( \frac{|h|a - |g||z| \cos \theta}{\sigma} \right) + Q \left( \frac{|h|a + |g||z| \cos \theta}{\sigma} \right) - c^2 \left[ Q \left( \frac{|h|a - |g||z| \sin \theta}{\sigma} \right) + Q \left( \frac{|h|a + |g||z| \sin \theta}{\sigma} \right) \right] \right]
\]

From Eq. (8), we can observe that the channel gains \( |h| \) and \( |g| \) play an important role on the SER performance, which we summarize in the following observations.

Observation 1 (SER Decreases in \( |h| \)): The SER in Eq. (8) is a monotonically decreasing function of \( |h| \).

Observation 2 (SER Increases in \( |g| \)): The SER in Eq. (8) is a monotonically increasing function of \( |g| \).
To prove these observations, we denote
\[ \xi(|h|, |g|) = \frac{1}{2\pi} \int_{-\pi}^{\pi} \frac{1}{\sigma^2} \exp \left( -\frac{x^2}{2\sigma^2} \right) \cos x \mathrm{d}x \]
and
\[ \eta(|h|, |g|) = \frac{1}{2\pi} \int_{-\pi}^{\pi} \frac{1}{\sigma^2} \exp \left( -\frac{x^2}{2\sigma^2} \right) \sin x \mathrm{d}x \].

We first focus on Observation 1. Since \( \xi(|h|, |g|) \) is a decreasing function of \( |h| \), the first derivative of \( \xi(|h|, |g|) \) with respect to \( |h| \) satisfies \( \frac{d\xi(|h|, |g|)}{d|h|} \leq 0 \), and for a given \( |g| \), \( \xi(|h|, |g|) \leq \xi(0, |g|) \). Similarly, \( \frac{d\eta(|h|, |g|)}{d|h|} \leq 0 \) and for a given \( |g| \), \( \eta(|h|, |g|) \leq 1 \). In addition, since \( 0 < c < 1 \), the first derivative of the SER expression on the right hand side of Eq. (8) with respect to \( |h| \) can be written as
\[ c(1 - \xi(|h|, |g|)) \frac{d\eta(|h|, |g|)}{d|h|} + c(1 - c\eta(|h|, |g|)) \frac{d\xi(|h|, |g|)}{d|h|} \leq 0 \]
which proves Observation 1. This observation agrees with the intuition that a stronger source-to-relay link improves the decoding performance at the relay.

Regarding Observation 2, for a given \( |h| \), we use the first derivative of the Q function
\[ \frac{dQ(x)}{dx} = \frac{1}{\sqrt{2\pi}} \exp \left( -\frac{x^2}{2} \right) \]
to obtain
\[ \frac{d\xi(|h|, |g|)}{d|g|} = \frac{|x|}{\sqrt{2\pi}} \cos x \left[ \exp \left( -\frac{1}{2} \left( \frac{|h|a}{\sigma} - \frac{|g|}{\sigma} \cos x \right)^2 \right) - \exp \left( -\frac{1}{2} \left( \frac{|h|a}{\sigma} + \frac{|g|}{\sigma} \cos x \right)^2 \right) \right] \geq 0 \]
which indicates that \( \xi(|h|, |g|) \) is an increasing function of \( |g| \). Thus, we have
\[ \xi(|h|, |g|) \leq \lim_{|g| \to \infty} \xi(|h|, |g|) = 1. \]

Therefore, since \( 0 < c < 1 \), the first derivative of the SER expression on the right hand side of Eq. (8) with respect to \( |g| \) can be written as
\[ c(1 - \xi(|h|, |g|)) \frac{d\eta(|h|, |g|)}{d|g|} + c(1 - c\eta(|h|, |g|)) \frac{d\xi(|h|, |g|)}{d|g|} \geq 0 \]
which proves Observation 2. This observation suggests that a stronger relay-to-destination link deteriorates the SER performance at the relay.

Note that \( \theta \) in Eq. (8) can be viewed as the equivalent phase of the AN. In the following subsection, we first derive the optimal rotation angle \( \theta \) that maximizes the SER in Eq. (8).

\section{B. Selecting the Phase of \( z \) for a Fixed \( |z| \)}

The focus of this subsection is to determine the optimal phase distribution of the AN. In this case, the power \( |z|^2 \) of the AN symbol \( z \), is assumed to be fixed. Then, we can for simplicity omit \( |z| \) in the argument of \( \text{SER}(\theta, |z|) \) in Eq. (8) and denote the SER expression as \( \text{SER}(\theta) \) in the remainder of this subsection.

Due to the \( \pi \)-periodicity of the function \( \text{SER}(\theta) \) and due to its symmetry, we only consider the interval \( \theta \in [0, \frac{\pi}{4}] \) to determine the maximum of \( \text{SER}(\theta) \). We first numerically verify that the following result.

\textbf{Result 1:} \( \text{SER}(\theta) \) is a quasi-convex function of \( \theta \) for all \( \theta \in [0, \frac{\pi}{4}] \), and either \( \theta = 0 \) or \( \theta = \frac{\pi}{4} \) maximizes the value of \( \text{SER}(\theta) \).

To illustrate this result, consider the constellation point “5” in Fig. 2 as an example. Given the power of the AN symbol \( z \), in order to maximize the expected SER at the relay according to \textbf{Result 1}, the destination can either allocate all the power \( |z|^2 \) to the direction of “12” or “13”, or equally distribute this power between the directions of “12” and “13”. Due to the similarity of this AN phase design to the constellation diagram, we refer to the case of \( \theta = 0 \) as the rotated QAM phase selection and the latter case of \( \theta = \frac{\pi}{4} \) as the QAM phase selection. Accordingly, the optimal phase selection of the AN \( z \) is computed as \( \theta = \theta_h - \theta_g \) or \( \theta = \frac{\pi}{4} + \theta_h - \theta_g \).

Next we address the question in which case using the rotated QAM constellation for the AN maximizes the SER at the relay and in which case the QAM constellation is optimal. Towards this aim, we plot Fig. 3. Each curve in this figure is plotted by numerically solving the equation \( \text{SER}(\pi/4) = \text{SER}(0) \) for \( |z|/\sigma \) for given values of \( a/\sigma \). The QAM region and the rotated QAM region denote the regions of \( \text{SER}(\pi/4) > \text{SER}(0) \) and \( \text{SER}(\pi/4) < \text{SER}(0) \), respectively. Therefore, Fig. 3 displays phase selection thresholds for different system parameters. In this figure, \( a/\sigma \) and \( |z|/\sigma \) indicate the energy of the source signal \( \sigma \) and the energy of the AN \( z \), respectively. We focus on the relation between the signal energy and the AN energy, and thus ignore the effect of channel gains by assuming \( h = 1 \) and \( g = 1 \).

The curves in Fig. 3 show that for a given signal power, there exists a threshold for the AN power, under which the optimal phase selection is \( \theta = 0 \), and above which the optimal phase selection is \( \theta = \pi/4 \). To explain the intuition behind this, consider the constellation point “5” in Fig. 2. With the purpose of maximizing the SER at the relay, if the power level of the AN \( |z|/\sigma \) is low (as compared to a given signal power \( E_m \)), the AN transmitted from the destination may deviate the equalized information signals received at the relay towards the adjacent constellation points “1”, “4”, “13”, and “15”, whilst if the power level of the AN \( |z|/\sigma \) is sufficiently high, the AN may shift the receive symbol towards the farther constellation points “0”, “12”, “3”, and “15”. From Fig. 3, one can also observe that for small values of \( a/\sigma \), the values of the threshold are very close to zero. This fact indicates that QAM phase selection is the preferable scheme if the received SNR at the relay is low.
In particular, from Eq. (8), we have
\[
\lim_{|z| \to \infty} \text{SER}(0, |z|) = c + 2c(1 - c)Q \left( \frac{|h|a}{\sigma} \right)
\leq \frac{\sqrt{M - 1}}{\sqrt{M}} + \frac{2(\sqrt{M - 1})}{M} \cdot \frac{1}{2}
= \frac{M - 1}{M} \tag{16}
\]
and
\[
\lim_{|z| \to \infty} \text{SER}(\pi/4, |z|) = 2e - c^2 = \frac{M - 1}{M} \tag{17}
\]
where the equality in (16) holds only when \(a = 0\), i.e., when no signal is transmitted. This indicates that when the signal is present, given sufficiently high AN noise power, the QAM phase selection yields a higher SER. This analysis can be confirmed by Fig. 3. Also note that \(\frac{M - 1}{M}\) is the SER when the relay does not have any prior information and randomly guesses the value of signal \(m\) for decoding, which serves as an upper bound on the SER of any AN scheme. In this work, we term this as non-informative error performance. Moreover, Eqs. (16) and (17) reveal that when the AN power is sufficiently high, the QAM selection asymptotically achieves the non-informative error performance.

**C. Assigning the Power of \(z\) for a Given \(E_z\)**

In Subsection III-B, we have shown how to select the phase \(\theta_z\) of \(z\) if the amplitude \(|z|\) is a fixed value. In general, however, it may be optimal to assign different powers to different AN symbols for a given average AN power. In this subsection, we assume that the average energy per AN symbol is limited to an average symbol energy \(\bar{E}\), i.e.,
\[
E_z = T_m \mathbb{E} \left\{ |z|^2 \right\} \leq \bar{E}. \tag{18}
\]
Furthermore, we denote \(\bar{P} = E/T_m\) as the average power of \(z\). Based on the results in Subsection III-B, the expected SER obtained from optimal phase selection is given by
\[
\text{SER}(|z|) = \max \{ \text{SER}(\pi/4, |z|), \text{SER}(0, |z|) \} \tag{19}
\]
where the \(\text{SER}(\theta, |z|)\) is defined according to Eq. (8). Following the proof of Observation 2, one can show that the first derivative of \(\text{SER}(\theta, |z|)\) in Eq. (8) with respect to \(|z|\) is non-negative, and thus \(\text{SER}(\theta, |z|)\) is a monotonically increasing function of \(|z|\) for a given \(\theta\). Accordingly, \(\text{SER}(\theta\ \bar{|z|})\) in Eq. (19) is also a monotonically increasing function of \(|z|\). Fig. 4 displays the values of \(\text{SER}(|z|)\) for 16-QAM and \(a/\sigma = 4\), where both the analytical and the simulated results are plotted. From the figure, we can see that as \(|z|/\sigma\) increases, the rotated QAM and the QAM phase selections alternatively achieve a better SER performance. Note that \(|z|^2 = \bar{P}\) can be viewed as a deterministic power usage.

The objective of this subsection is to derive the optimal distribution of the powers \(|z|^2\) to maximize the expected value of the SER in Eq. (19). Alternatively, the power needs to be smartly allocated to yield an upper bound on the SER performance with deterministic power usage. Denoting the probability density function (PDF) of \(|z|^2\) as \(f(x)\), the optimization problem can be formulated as
\[
\max_{f(x)} \int_0^\infty \text{SER}(\sqrt{x}) f(x) \, dx \tag{20a}
\]
subject to
\[
\int_0^\infty x f(x) \, dx \leq \bar{P} \quad \text{(average power)} \tag{20b}
\]
\[
\int_0^\infty f(x) \, dx = 1 \quad \text{(total probability)} \tag{20c}
\]
\[
f(x) \geq 0, \text{ for } x \geq 0 \quad \text{(non-negativity)} \tag{20d}
\]
where the average power constraint (20b) follows from (18). For computational tractability, we only consider PDFs \(f(x)\) for which all integrals in (20) exist.

The following theorem provides interesting insights into the power allocation problem and meanwhile can greatly simplify the calculation.

**Theorem 1 (Optimal Power Allocation):** Any PDF \(f(x)\) solving the problem (20) has the form
\[
f(x) = (1 - p) \delta(x - x_1) + p \delta(x - x_2) \tag{21}
\]
where $\delta(x)$ is the Dirac delta function defined by [34, Chapter 2]
\[
\int_{-\infty}^{\infty} \delta(t-\tau)g(t)dt = g(\tau)
\]
(22)
for any continuous function $g$ and any value of $\tau$, and
\[
p = \frac{\bar{P} - x_1}{x_2 - x_1}
\]
(23)
with $0 \leq x_1 \leq \bar{P} \leq x_2$.

Proof: See Appendix.

This theorem means that only two kinds of AN symbols are generated from the destination, one with probability $(1-p)$ and one with probability $p$, and the corresponding powers are $x_1$ and $x_2$, respectively.

Inserting Eq. (21) into Eq. (20), the expected SER in Eq. (20a) can be computed as
\[
\overline{\text{SER}}(x_1, x_2)
= \int_{0}^{\infty} \text{SER}(\sqrt{x}) f(x) dx
= (1-p)\text{SER}(\sqrt{x_1}) + p\text{SER}(\sqrt{x_2})
= \frac{x_2 - \bar{P}}{x_2 - x_1} \text{SER}(\sqrt{x_1}) + \frac{\bar{P} - x_1}{x_2 - x_1} \text{SER}(\sqrt{x_2}).
\]
(24)

From Eq. (24), at high average AN power, i.e., $\bar{P} \to \infty$, we observe that the expected SER in Eq. (24) approaches $M^{-1}/M$, which corresponds to the non-informative error performance. The proof can be sketched as follows. From Eqs. (16) and (17), we know that $\lim_{|z| \to \infty} \text{SER}(|z|) = M^{-1}/M$. Given $\bar{P} \to \infty$, by applying the Optimal Power Allocation Theorem, we have $x_2 \to \infty$ due to $x_2 \geq \bar{P}$. In this case, if $x_1 \to \infty$, we have $\lim_{x_1 \to \infty} \text{SER}(\sqrt{x_1}) = M^{-1}$ and $\lim_{x_2 \to \infty} \text{SER}(\sqrt{x_2}) = M^{-1}/M$, thereby $\text{SER}(x_1, x_2)$ in Eq. (24) approaches $M^{-1}/M$. If $x_1$ is a finite value, $x_2 \approx \bar{P}$, then the term $\frac{x_2 - \bar{P}}{x_2 - x_1} \text{SER}(\sqrt{x_1})$ in Eq. (21) approaches zero, and the term $\frac{\bar{P} - x_1}{x_2 - x_1} \text{SER}(\sqrt{x_2})$ in Eq. (21) converges to $M^{-1}/M$, which explains the above observation.

Another interesting observation is that the maximum $\overline{\text{SER}}(x_1, x_2)$ is a monotonically decreasing function in $[h]$. This is because $\text{SER}(x_1, x_2)$ in Eq. (24) is a linear combination of $\text{SER}(\sqrt{x_1})$ and $\text{SER}(\sqrt{x_2})$, each of which is a monotonically decreasing function of $|g|$ as shown below Eq. (19). Furthermore, maximizing $\text{SER}(x_1, x_2)$ with respect to $x_1$ and $x_2$ preserves the monotonicity. Similarly, it can be shown that $\text{SER}(x_1, x_2)$ in (24) is a monotonically increasing function of $|g|$. Therefore, by applying the optimal AN design, the SER at the relay increases with the relay-to-destination link quality, and decreases with the source-to-relay link quality.

The optimal values of $x_1$ and $x_2$ maximizing $\text{SER}(x_1, x_2)$ in Eq. (24), denoted by $x_1^*$ and $x_2^*$, can be computed numerically based on $g$, $\bar{P}$, $M$, $a$ and $\sigma$. Substituting $x_1^*$ and $x_2^*$ back into (24) yields the maximum expected SER, which is denoted as $\overline{\text{SER}}_{\text{max}}$. For example, in the case of $h = 1$, $g = 1$, $\bar{P} = 3.9811$, $M = 16$, $a = \sqrt{10}$ and $\sigma = 1/\sqrt{2}$, the optimal values can be computed as $x_1 = 0$ and $x_2 = 13.7098$, $\text{SER}(\sqrt{x_1}) = 0$ and $\text{SER}(\sqrt{x_2}) = 0.5832$. The corresponding maximum expected SER is $\overline{\text{SER}}_{\text{max}} = 0.1694$.

Interestingly, if we use a deterministic power usage $\bar{P}$, i.e., the AN PDF can be written as $f(x) = \delta(x - \bar{P})$, the corresponding expected SER is $0.0371$. Therefore, applying the Optimal power allocation theorem at the destination yields significantly higher SER values at the relay than the deterministic power usage.

### D. Relation Between Phase Selection and Power Allocation

Having determined the optimal phase selection and the optimal power distribution, it is interesting to examine the relation between them, which we illustrate in Figs. 5–7. Fig. 5 depicts the SER performance using a deterministic power level $|z|^2 = \bar{P}$ and the optimal power allocation. The line denoted as “Non-informative” represents the non-informative SER performance. In the case of 16-QAM, the non-informative SER is equal to $15/16$. Comparing Fig. 4 and Fig. 5, we observe that for a given SNR $E_m/N_0$, our derived power allocation approach yields an upper bound on the SER with the deterministic power usage. To take a deeper look, we depict in Fig. 6 the relation between the optimal power allocation $x_1^*$ and $x_2^*$. The corresponding phase selection $\theta_{x_1^*}$ and $\theta_{x_2^*}$ are obtained from evaluating $\text{SER}(\sqrt{x_1^*})$ and $\text{SER}(\sqrt{x_2^*})$ in Eq. (19), respectively. Fig. 7 plots the probability to transmit $x_2^*$, i.e., $p$ given in Eq. (23), noting that the probability to transmit $x_1^*$ is given by $(1-p)$.

In correspondence to Eq. (21), we observe from Fig. 6 and Fig. 7 that as the power of the AN $\bar{P}$ increases, either the probability $p$ remains constant and the powers $x_1^*$ or $x_2^*$ increase or the values of $x_1^*$ and $x_2^*$ remain constant (with $x_2^* > x_1^*$) and the probability $p$ of transmission with the larger power $x_2^*$ increases.

To simplify the discussion of Figs. 5–7, we partition the values of the artificial noise-to-natural noise ratio (ANR) into multiple regions by introducing the transition points $A–D$. From the figures, we have the following observations.

Region I ($0 \leq E_z/N_0 < A$): In this region we observe that when the ANR is low, the optimal AN design is to transmit a noise symbol with power $x_2^*$ and rotated QAM phase $\theta = 0$ at a constant probability $p_0$, and to transmit no AN ($x_1^* = 0$) with probability $(1-p_0)$. Thus, as $\bar{P}$ increases, the power $x_2^*$ increases while the probability of transmitting AN remains constant.

Region II ($A \leq E_z/N_0 < B$): When the ANR is medium, the power to transmit rotated QAM AN symbols $x_2^*$ reaches a constant, and the probability to transmit the AN symbols increases as $E_z/N_0$ increases. The corresponding SER in Fig. 5 is higher than those using the deterministic power $\bar{P}$.

Region III ($B \leq E_z/N_0 < C$): In this region, the probability to transmit AN symbols with the rotated QAM phase selection reaches 1, and the corresponding transmitting power reaches the highest $x_2^* = \bar{P}$. In other words, for the AN symbols, the deterministic power usage and the rotated QAM phase selection achieve the maximum SER, which can also be observed in Fig. 5.

Region IV ($C \leq E_z/N_0 < D$): The ANR arrives at a threshold $E_z/N_0 = C$, above which the optimal AN design is to use both of the two kinds of AN symbols: the rotated QAM
phase selection with power \( x_1^* \) and the QAM phase selection with power \( x_2^* \). The probability to transmit the QAM phase selection symbols increases as the ANR increases.

Region V (\( E_z/N_0 \geq D \)): When the ANR is large, the QAM phase selection with a deterministic power \( P \) achieves the maximum SER. In particular, when \( E_z/N_0 \) is sufficiently large, i.e., \( E_z/N_0 \geq 17 \) in Fig. 5, the SER converges to the non-informative SER, which was mathematically proved in Eq. (17).

To intuitively understand the above observations, again take the constellation point “5” in Fig. 2 as an example. When the AN power is low, the optimal AN generation scheme is to burst the limited power to move “5” towards the adjacent points “1”, “4”, “13” and “7” in order to introduce decoding errors. As the AN power goes sufficiently large, some of the power can be used to move “5” towards the points “0”, “12”, “3” and “15” in order to induce more decoding errors. Until when the AN power is significantly large, beaming all the power to the directions of points “0”, “12”, “3” and “15” yields the maximum SER.

IV. DESIGNING THE AN TO MAXIMIZE ASER

In Section III, we have obtained the optimal AN distributions based on the instantaneous channel knowledge of the source-to-relay and relay-to-destination links. In this section, we consider the optimal distribution of the AN power that maximizes the ASER at the relay provided that the long-term statistical CSI is known to the destination. Following a similar approach to Section III, we first present an analytical expression for the ASER over Rayleigh fading channels. The optimal phase and power distributions of the AN that maximizes this ASER are then determined.

A. Average SER Expression for a Given \( z \)

In this section, the channel coefficients \( h \) and \( g \) are assumed to be random variables. Moreover, the envelop of the relay-to-destination channel coefficient \( g \) is assumed to be Rayleigh distributed. For a given AN symbol \( z \), the received AN at the relay \( g z \) can be easily shown as \( g z \sim \mathcal{CN}(0, \sigma_z^2|z|^2) \). This indicates that the received AN at the relay is an extra source of AWGN. Hence, as can be observed from the signal model in Eq. (1), the overall received noise at the relay is a superposition of the AN and the natural AWGN. The relay-to-destination channel coefficient \( g \) and the AWGN symbols \( n \) are independent, and it can be easily shown that the received noise \( g z + n \) is distributed as \( g z + n \sim \mathcal{CN}(0, \sigma_z^2|z|^2 + 2\sigma^2) \), where \( 2\sigma^2 \) is the variance of the AWGN \( n \) as defined after Eq. (4). For Rayleigh faded source-to-relay channel gain \( |h| \) and the overall noise symbol \( g z + n \), the ASER of the QAM signals at the relay can be obtained using [35, Eq. (8.106)] as Eq. (25) at the top of the next page, where \( \tilde{\gamma}_s(z) = \frac{\sigma_z^2 E_m}{\sigma_h^2 |z|^2 + 2\sigma^2} \).

Similar to Observations 1 and 2 made on Eq. (8), the effects of channel statistics on the ASER given by Eq. (25) can be summarized as follows.

Observation 3 (ASER Monotonicity): The ASER in Eq. (25)
is a monotonically increasing function of $\sigma_g^2$, as well as a monotonically decreasing function of $\sigma_h^2$.

This observation is intuitive and is similar to Observations 1 and 2 in Section III: Stronger relay-to-destination channels help to deteriorate the ASER performance at the relay, whereas stronger source-to-relay channels improve the average decoding performance at the relay.

**Observation 4 (High Signal and AN Power Performance):** At high SNR and high ANR, i.e., $E_m \gg \sigma^2$ and $|z|^2 \gg \sigma^2$, $\gamma_s(z) \approx \frac{\sigma^2}{\gamma_m(z)}$.

Observation 4 reveals that provided an adequately high signal and AN power is available, the relative strength of the source-to-relay and relay-to-destination links affects the ASER performance of the QAM signals at the relay.

**Observation 5 (High AN Power Performance):** In the high AN power regime, i.e., for $|z|^2 \to \infty$, $\gamma_s \to 0$, we have

$$\lim_{|z|\to\infty} \text{ASER}(z) = 2e - c^2 = \frac{M-1}{M-2}.$$  

This observation shows that given sufficiently high AN power, the ASER at the relay is close to the non-informative error performance.

Furthermore, we observe that the ASER expression in Eq. (25) is independent of the phase of the AN, which is different from the AN design in Section III in the case of instantaneous CSI. Following a similar approach as in Section III-C, our objective in the following subsection is to derive the optimal power distribution for the AN under an average power constraint.

**B. Assigning Power of $z$ for a Given $E_z$**

We rewrite the function of the average symbol error rate ASER($z$) in Eq. (25) as $\text{ASER}(\sqrt{x})$ to reflect the effect of AN power, where $x = |z|^2$. Similar to Subsection III-C, the optimal power assignment problem is given by replacing $\text{SER}(\sqrt{x})$ in Eq. (20) by $\text{ASER}(\sqrt{x})$, and now $f(x)$ represents the PDF of $x$ for Rayleigh fading channels. Since one can see that $\text{ASER}(\sqrt{x})$ in Eq. (25) is a monotonically increasing function of $x$, the distribution of the optimal AN directly follows from the PDF expression derived in Eq. (21). Therefore, substituting Eq. (21) into Eq. (25) yields the expected ASER

$$\text{ASER}(x_1, x_2) = \frac{x_2 - \bar{P}}{x_2 - x_1} \text{ASER}(\sqrt{x_1}) + \frac{\bar{P} - x_1}{x_2 - x_1} \text{ASER}(\sqrt{x_2})$$  

(26)

where $\bar{P} = \frac{x_1}{x_2}$ is the average power constraint on the AN, and $0 \leq x_1 \leq \bar{P} \leq x_2$. The optimal values of $x_1$ and $x_2$ maximizing $\text{ASER}(x_1, x_2)$ in Eq. (26) are then derived numerically based on $\bar{P}$, $M$, $E_m$, $\sigma$, $\sigma_h$, and $\sigma_g^2$, where $\sigma^2$ and $\sigma_h^2$ represent the statistical/long-term CSI.

Similar to the analysis following Eq. (24), we can also show that as the AN power increases, the expected ASER in Eq. (26) converges to the non-informative SER performance.

**V. SIMULATION RESULTS**

In this section, we present simulation results to validate the obtained analytical results derived in the previous sections. In all figures, the average SNR is chosen as $E_m/N_0 = 10 \text{ dB}$. In order to depict the SER performance at the relay using the optimal AN design in Section III, we plot Fig. 8, where the signal symbol $m$ is randomly selected from the square 4-QAM constellation. We observe that all analytical results coincide very well with the corresponding simulation results. For the sake of comparison, the expected SER values for Gaussian AN are also plotted in Fig. 8. In the Gaussian case, we assume that the AN symbol $z$ is generated according to a complex Gaussian distribution with the same average symbol energy $E_z$. The line denoted as “Non-informative” represents the non-informative SER performance. The curve "w/o AN" in the figure depicts the SERs at the relay without AN, which lies a value of 0.0016 for the given parameters. Fig. 8 shows that the SER at the relay can be significantly increased by applying the AN. Even when the ANR $E_z/N_0$ is small, e.g., $E_z/N_0 = 2 \text{ dB}$, the SER is increased from 0.0016 to 0.05. Moreover, Fig. 8 clearly demonstrates that the Gaussian distribution is not optimal for AN generation and our scheme described in Section III can induce much larger SER at the relay. For the case shown in Fig. 8, if the ANR $E_z/N_0$ is above 16 dB, the maximum SER, i.e., $\text{SER}_{\text{max}}$, achieves 3/4. This fact indicates that if the AN $z$ is properly generated and $E_z$ is above a certain threshold, applying ideal coherent demodulation at the relay does not lead to better performance than the non-informative case, and secure data transmission can therefore be ensured by the proposed technique. Fig. 9 shows the SER performance for square 16-QAM constellations. Comparing Fig. 9 with Fig. 8, similar observations can be made as for the case of 4-QAM.

Now, we investigate the ASER performance at the relay using the optimal AN design in Section IV. Fig. 10 depicts the ASER performance for square 4-QAM and 16-QAM signals. In this figure, $\text{ASER}_{\text{max}}$ is computed by numerically maximizing $\text{ASER}(x_1, x_2)$ in (26) with respect to $x_1$ and $x_2$. For comparison, the ASER curves for various power distributions are plotted, i.e., the uniform and the exponential power distribution. For each curve, the numerical results are obtained from computing $\int_0^\infty \text{ASER}(\sqrt{x}) f(x) dx$, where

$$f(x) = \frac{1}{2\bar{P}} e^{-\frac{x}{\bar{P}}}, \quad \text{for } 0 \leq x \leq 2\bar{P}$$  

(27)

and

$$f(x) = \frac{1}{\bar{P}} \exp\left(-\frac{x}{\bar{P}}\right), \quad \text{for } x \geq 0$$  

(28)

are the PDFs of the AN power with uniform and exponential distributions, respectively. Note that there exists numerous AN designs with exponentially distributed power, such as the Gaussian AN. Fig. 10 shows that our proposed scheme with the optimal power distribution yields the largest ASER.
at the relay. Given sufficiently high ANR, all the ASER curves achieve the non-informative error performance, which confirms Observation 5. However, in contrast to the case with instantaneous CSI considered in Section III, the performance difference between different AN designs is not significant. This can be explained by the fact that the ASER expression in (25) does not consider the phase of the AN. Therefore, the degree of freedom of the phase design for the AN is not utilized.

Furthermore, it is interesting to compare the SER performance of the optimal AN designs in Sections III and IV. Fig. 11 compares the ASER performance of various AN designs. In the figure, “Instantaneous CSI Based Sim.” curve is plotted by computing $E_{h,g}[\text{SER}_{\text{max}}]$ using the Monte Carlo method, and the curve “Statistical CSI Based Ana.” is plotted using the same method as in Fig. 10. The curve “Gaussian Sim.” is plotted by numerically computing $E_{h,g}[\text{SER}(z)]$, with Gaussian distributed AN. From Fig. 11, we observe that the instantaneous CSI based AN design yields a higher ASER than the statistical CSI based AN design, which is consistent with our intuition. However, the performance difference between these two designs is not quite significant. Without optimal phase and power designs, the Gaussian distribution performs worse than both CSI based AN designs.

VI. Conclusion

We have investigated physical layer security in terms of the SER performance for a relay channel, where a source aims to transmit to a destination assisted by an untrusted relay. For this scenario, we apply the AN technique, where the AN is designed and generated by the destination. Based on the perfect instantaneous CSI of the source-to-relay and relay-to-destination links, we have derived exact analytical SER expressions for the relay and studied the optimal design of the AN signal to maximize the corresponding SER. In this work, the source uses QAM signaling as in modern cellular standards. It is interesting to note that the Gaussian distribution, which is
frequently used in the context of AN [6, 36, 37], is not optimal in general. In the considered setup, QAM or rotated QAM phase selection yields the optimal AN. Moreover, compared with the Gaussian AN, our optimal AN can yield remarkably higher SER at the relay. For the case when the AN design is based on the long-term CSI of the source-to-relay and relay-to-destination links, we present the corresponding ASER expression at the relay, and the optimal AN distribution to maximize the ASER is determined accordingly. Interestingly, the phase of the AN does not affect the ASER performance at the relay. Regarding the power design of the AN, our optimal power distribution still delivers higher ASERs than various distributions, such as uniform and exponential distributions. Finally, we mention that there are many directions for further work. For example, when the perfect CSI of the source-to-relay and relay-to-destination links is not available, opportunistic scheduling with low-rate CSI feedback might be applied [38].

**APPENDIX: PROOF OF THEOREM 1**

In the following, we base our proof on the concept of Linear Programming and the Karush-Kuhn-Tucker (KKT) optimality conditions [39, p. 243].

Before proceeding, note that for a discrete realization $x_1$ with probability $p$, one can express $f(x)$ at $x_1$ as

$$f(x) = p\delta(x - x_1).$$  \hspace{1cm} (29)

If a PDF $f(x)$, which solves the problem (20), has the form of $f(x) = \delta(x - x_0)$, we can easily obtain $x_0 = \bar{P}$, as $\text{SER}(x)$ in (19) is a monotonically increasing function. This case is trivially contained in Theorem 1. In the following, we will assume that $f(x) > 0$ for at least two different values of $x$. In this case, at the optimum, the constraint (20b) must be met with equality as otherwise we can further increase the objective function (20a) by increasing $f(x_1)$ and decreasing $f(x_2)$ for some $x_1 > x_2$ without violating any constraint, which contradicts to the optimality assumption.

If the optimal distribution $f(x)$ corresponds to that of a discrete random variable with $n$ realizations, $f(x)$ can be expressed as

$$f(x) = \sum_{i=1}^{n} p_i \delta(x - x_i)$$ \hspace{1cm} (30)

where $\sum_{i=1}^{n} p_i = 1$ and $p_i > 0$. Inserting (30) into (20a)-(20c), we can obtain the following system of linear equations

$$\alpha_1 p_1 + \alpha_2 p_2 + \cdots + \alpha_n p_n = b$$ \hspace{1cm} (31a)

$$\beta_1 p_1 + \beta_2 p_2 + \cdots + \beta_n p_n = \bar{P}$$ \hspace{1cm} (31b)

$$p_1 + p_2 + \cdots + p_n = 1$$ \hspace{1cm} (31c)

where $\alpha_i = \text{SER}(\sqrt{x_i})$, $\beta_i = x_i$, and $0 \leq p_i \leq 1$ with $i = 1, \cdots, n$. The achieved maximum value of the objective function (20a) is denoted as $b$.

If the optimal PDF $f(x)$ contains at least one interval $[x_a, x_b]$ with $f(x) > 0$ for any $x \in [x_a, x_b]$, we can divide $[x_a, x_b]$ into $m$ non-overlapping sub-intervals $[\tilde{x}_{m-1}, \tilde{x}_m]$ with $x_a = \tilde{x}_0 \leq \tilde{x}_1 \leq \cdots < \tilde{x}_m = x_b$. Then, following the first mean value theorem [40, Theorem 12.111], we can find some $\tilde{x}_i$ and $\hat{x}_i$ with $\tilde{x}_{i-1} \leq \tilde{x}_i \leq \hat{x}_i$ and $\hat{x}_{i-1} \leq \hat{x}_i \leq \tilde{x}_i$ such that

$$p_i = \int_{\tilde{x}_{i-1}}^{\hat{x}_i} f(x) \, dx$$ \hspace{1cm} (32)

$$\int_{x_a}^{x_b} \text{SER}(\sqrt{x}) \, f(x) \, dx = m \int_{x_a}^{x_b} \text{SER}(\sqrt{x}) \, f(x) \, dx$$ \hspace{1cm} (33)

and

$$\int_{x_a}^{x_b} x f(x) \, dx = m \sum_{i=1}^{m} \tilde{x}_i p_i.$$ \hspace{1cm} (34)

Denoting $\text{SER}(\sqrt{x})$ and $\hat{x}_i$ as $\alpha_i$ and $\beta_i$ in this case and repeating the approach for all intervals on which $f(x) > 0$, we can again obtain a system of linear equations in the form of (31). Note that $\hat{x}_i \approx \tilde{x}_i$ as the number of sub-intervals $m$ increases. In this case we have $\tilde{x}_i \approx \hat{x}_i \approx \tilde{x}_i \approx \tilde{x}_i$. Further, as $\text{SER}(x)$ is a monotonically increasing function, we can order the coefficients such that $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_n$ and $\beta_1 \leq \beta_2 \leq \cdots \leq \beta_n$. Then, as $0 \leq p_i \leq 1$ for all $i = 1, \cdots, n$, (31b) and (31c) indicate that $\beta_m \geq \bar{P}$.

As $f(x)$ is the optimal distribution and $b$ is the maximum of the objective function (20a), $p_i$ with $i = 1, 2, \cdots, n$ in (31) must be a solution of the following problem

$$\max_{y_1, i=1, \cdots, n} \alpha_1 y_1 + \alpha_2 y_2 + \cdots + \alpha_n y_n$$ \hspace{1cm} (35a)

s.t. $\beta_1 y_1 + \beta_2 y_2 + \cdots + \beta_n y_n = \bar{P}$ \hspace{1cm} (35b)

$y_1 + y_2 + \cdots + y_n = 1$ \hspace{1cm} (35c)

$0 \leq y_i \leq 1$ for $i = 1, 2, \cdots, n$ \hspace{1cm} (35d)

where $\alpha_i$ and $\beta_i$ with $i = 1, 2, \cdots, n$ are identical to the corresponding parameters in (31). Following the KKT conditions [39, p. 243], at the maximum of the problem (35), we must have

$$\lambda_0 = \frac{\alpha_i - \alpha_k}{\beta_i - \beta_k}$$ \hspace{1cm} (36)

for any $i \neq k$ with $0 < p_i < 1$ and $0 < p_k < 1$, where $\lambda_0$ is a constant (Lagrange multiplier). Without loss of generality, let us denote $k'$ as the first index such that $0 < p_i < 1$, i.e., $k' \leq i$ for any $0 < p_{k'} < 1$. Similarly, we can denote $k^*$ as the last index such that $0 < p_i < 1$, i.e., $k^* \geq i$ for any $0 < p_{k^*} < 1$. Clearly, we have $\beta_{k'} \leq \bar{P} \leq \beta_{k^*}$, as otherwise $p_i$ with $i = 1, \cdots, n$ cannot meet the constraints (35b)-(35d). Inserting (36) in (35) and eliminating all $\alpha_i$ and $\beta_i$ for $i \neq k'$, the optimum value of $b$ can be expressed as

$$b = \lambda_0 \bar{P} + \alpha_k \lambda_0 - \lambda_0 \beta_{k'}.$$ \hspace{1cm} (37)

Moreover, let

$$y_{k'} = \frac{\beta_{k'} - \bar{P}}{\beta_{k'} - \beta_{k'}}; \quad y_{k^*} = \frac{\bar{P} - \beta_{k^*}}{\beta_{k^*} - \beta_{k'}}; \quad \text{and} \quad y_i = 0 \text{ for } i \neq k', k^*$$ \hspace{1cm} (38)

and consider the following PDF $f(x)$

$$f(x) = \frac{\beta_{k'} - \bar{P}}{\beta_{k'} - \beta_{k'}} \delta(x - \beta_{k'}) + \frac{\bar{P} - \beta_{k^*}}{\beta_{k^*} - \beta_{k'}} \delta(x - \beta_{k^*}).$$ \hspace{1cm} (39)

Inserting (39) in (20), we obtain the same maximum value $b$ for the objective function (20a) as given in (37) while meeting all the constraints. Therefore, there exists a PDF $f(x)$ solving the problem (20) with $f(x) > 0$ for at most two values of $x$. \hfill \blacksquare
REFERENCES

[1] Y. Liu, L. Li, and M. Pesavento, “Enhancing physical layer security in untrusted relay networks with artificial noise: A symbol error rate based approach,” in Proc. of the 2014 IEEE 8th Sensor Array and Multichannel Signal Processing Workshop (SAM), A Coruña, Spain, 22-25 Jun. 2014, pp. 261–264.

[2] C. E. Shannon, “Communication theory of secrecy systems,” Bell System Technical Journal, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[3] A. D. Wyner, “The wire-tap channel,” Bell System Technical Journal, vol. 54, no. 8, pp. 1353–1387, Oct. 1975.

[4] I. Csiszár and J. Körner, “Broadcast channels with confidential messages,” IEEE Trans. Inform. Theory, vol. 24, no. 3, pp. 339–348, May 1978.

[5] Y. Liang, H. V. Poor, and S. Shamai, “Information theoretic security,” Foundations and Trends in Communications and Information Theory, vol. 5, no. 4-5, pp. 555–580, Mar. 2008.

[6] 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.

[7] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas I: The MISO wiretap channel,” IEEE Trans. Inform. Theory, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[8] D. W. K. Ng, E. S. Lo, and R. Schober, “Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks,” IEEE Trans. Wireless Commun., vol. 10, no. 10, pp. 3528–3540, Oct. 2011.

[9] F. Oggeri and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” IEEE Trans. Inform. Theory, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[10] R. Liu, T. Liu, H. V. Poor, and S. Shamai, “New results on multiple-input multiple-output broadcast channels with confidential messages,” IEEE Trans. Inform. Theory, vol. 59, no. 3, pp. 1346–1359, Mar. 2013.

[11] A. Mukherjee and A. L. Swindlehurst, “Utility of beamforming strategies for secrecy in multiuser MIMO wiretap channels,” in 17th Annual Allerton Conf. on Commun., Control, and Computing, Monticello, IL, USA, 30 Sep. - 02 Oct. 2009, pp. 1134–1141.

[12] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. B. Collings, “Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding,” IEEE Trans. Wireless Commun., vol. 60, no. 11, pp. 3472–3482, Nov. 2012.

[13] E. Tekin and A. Yener, “The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming,” IEEE Trans. Inform. Theory, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[14] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperative relaying,” IEEE Trans. Signal Processing, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[15] A. Mukherjee and A. L. Swindlehurst, “Securing multi-antenna two-way relay channels with analog network coding against eavesdroppers,” in Proc. IEEE Eleventh Int. Workshop on Signal Processing Advances in Wireless Commun. (SPAWC), Marrakech, Morocco, Jun. 2010, pp. 1–5.

[16] A. A. A. Fakoorian and A. L. Swindlehurst, “Solutions for the MIMO gaussian wiretap channel with a cooperative jammer,” IEEE Trans. Signal Processing, vol. 59, no. 10, pp. 5013–5022, Oct. 2011.

[17] A. Mukherjee and A. L. Swindlehurst, “Jamming games in the MIMO wiretap channel with an active eavesdropper,” IEEE Trans. Signal Processing, vol. 61, no. 1, pp. 82–91, Jan. 2013.

[18] Y. Oohama, “Capacity theorems for relay channels with confidential messages,” in Proc. of the IEEE Int. Symp. on Information Theory (ISIT), Nice, France, 24 - 29 Jun. 2007, pp. 926–930.

[19] X. He and A. Yener, “Cooperation with an untrusted relay: A secrecy perspective,” IEEE Trans. Inform. Theory, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[20] J. Huang, A. Mukherjee, and A. L. Swindlehurst, “Secure communication via an untrusted non-regenerative relay in fading channels,” IEEE Trans. Signal Processing, vol. 61, no. 10, pp. 2536–2550, May 2013.

[21] C. Jeong, I.-M. Kim, and D. I. Kim, “Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system,” IEEE Trans. Signal Processing, vol. 60, no. 1, pp. 310–325, Jan. 2012.

[22] L. Sun, T. Zhang, Y. Li, and H. Niu, “Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes,” IEEE Trans. Veh. Technol., vol. 61, no. 8, pp. 3801–3807, Oct. 2012.

[23] J. Mo, M. Tao, Y. Liu, B. Xia, and X. Ma, “Secure beamforming for MIMO two-way transmission with an untrusted relay,” in Proc. of IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, China, Apr. 2013, pp. 4180–4185.

[24] S. Vishwakarma and A. Chockalingam, “Amplify-and-forward relay beamforming for secrecy with cooperative jamming and imperfect CSI,” in Proc. of the 2013 IEEE Int. Conf. on Commun. (ICC), Budapest, Hungary, Jun. 2013, pp. 3047–3052.

[25] M. Pei, A. Swindlehurst, D. Ma, and J. Wei, “Adaptive limited feedback for MISO wiretap channels with cooperative jamming,” IEEE Trans. Signal Processing, vol. 62, no. 4, pp. 993–1004, Feb. 2014.

[26] D. Kline, J. Ha, S. W. MaLaughlin, J. Barros, and B.-J. Kwak, “LDPC codes for the Gaussian wiretap channel,” IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 532–540, Sep. 2011.

[27] A. Mukherjee, “Imbalanced beamforming by a multi-antenna source for secure utilization of an untrusted relay,” IEEE Communications Letters, vol. 17, no. 7, pp. 1309–1312, Jul. 2013.

[28] E. Dahlman, S. Parkvall, and J. Sköld, 4G: LTE/LTE-Advanced for Mobile Broadband. Elsevier Academic Press, 2011.

[29] M. Guillaud, D. T. M. Lock, and R. Knopp, “A practical method for wireless channel reciprocity exploitation through relative calibration,” in Proc. of the Eighth Int. Symp. on Signal Proc. and Its Appl., vol. 1, Sydney, Australia, Aug. 2005, pp. 403–406.

[30] T. Cover and A. El Gamal, “Capacity theorems for the relay channel,” IEEE Trans. Inform. Theory, vol. 25, no. 5, pp. 572–584, Sep. 1979.

[31] N. Laneman, D. N. C. Tse, and G. Wornell, “Cooperative diversity in wireless networks: Efficient protocols and outage behavior,” IEEE Trans. Inform. Theory, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[32] J. G. Proakis, Digital Communications, 4th ed. McGraw Hill, 2001.

[33] M. K. Simon and M.-S. Alouini, Digital Communication over Fading Channels: A Unified Approach to Performance Analysis. John Wiley & Sons, 2000.

[34] L. Meade and C. R. Dillon, Signals and Systems: Models and Behaviour, 2nd ed. Kluwer Academic Publishers, 1991.

[35] J. K. Sitchin and M.-S. Alouini, Digital Communication over Fading Channels. John Wiley & Sons, 2005, vol. 95.

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

[37] X. Zhang, M. McKay, X. Zhou, and R. Heath, “Artificial-noise-aided secure multi-antenna transmission with limited feedback,” IEEE Trans. Wireless Commun., vol. 9, no. 9, pp. 3062–3080, Dec. 2010.

[38] J. S. Gradshteyn and I. M. Ryzhik, Table of Integrals, Series and Products, 7th ed. New York: Academic Press, 2007.