Secure joint source–channel coding with interference known at the transmitter

G. Bagherikaram  K.N. Plataniotis

The Edward S. Rogers Sr. Department of ECE, University of Toronto, 10 King’s College Road, Toronto, Ontario, Canada M5S 3G4
E-mail: gbagheri@comm.utoronto.ca

Abstract: In this study, the problem of transmitting an independent and identically distributed (i.i.d.) Gaussian source over an i.i.d. Gaussian wire-tap channel, with an i.i.d. Gaussian known interference available at the transmitter is considered. The intended receiver is assumed to have a certain minimum signal-to-noise ratio (SNR) and the eavesdropper is assumed to have a strictly lower SNR compared to the intended receiver. The objective is to minimise the distortion of source reconstruction at the intended receiver. In this study, an achievable distortion is derived when Shannon’s source–channel separation coding scheme is used. Three hybrid digital–analogue secure joint source–channel coding schemes are then proposed, which achieve the same distortion. The first coding scheme is based on Costa’s dirty-paper-coding scheme and wire-tap channel coding scheme, when the analogue source is not explicitly quantised. The second coding scheme is based on the superposition of the secure digital signal and the hybrid digital–analogue signal. It is shown that for the problem of communicating a Gaussian source over a Gaussian wire-tap channel with side information, there exists an infinite family of secure joint source–channel coding schemes. In the third coding scheme, the quantised signal and the analogue error signal are explicitly superimposed. It is shown that this scheme provides an infinite family of secure joint source–channel coding schemes with a variable number of binning. Finally, the proposed secure hybrid digital–analogue schemes are analysed under the main channel SNR mismatch. It is proven that the proposed schemes can give a graceful degradation of distortion with SNR under SNR mismatch, that is, when the actual SNR is larger than the designed SNR.

1 Introduction

Security protocols are the most critical elements involved in enabling the growth of the wide range of wireless data networks and applications. The broadcast nature of wireless communications, however, makes them particularly vulnerable to eavesdropping. With the proliferation of more complex modern infrastructure systems, there is an increasing need for secure communication solutions. Cryptography is a traditional field that provides ‘computationally secure’ protocols at the application layer. The goal of cryptography has recently expanded from providing the critical confidentiality service, to other issues including authentication, key exchange and management, digital signature and more. Unlike the cryptographic approaches, the recently reintroduced ‘physical-layer’ security aims to develop effective secure communication schemes exploiting the properties of the physical layer. This new paradigm can strengthen the security of existing systems by introducing a level of ‘information-theoretic’ security, which has provable security, as compared with computational security. The notion of information theoretic secrecy in communication systems was first introduced in [1]. The information-theoretic secrecy requires that the received signal by an eavesdropper not provide any information about the transmitted messages. Following the pioneering works of the authors [2, 3], which have studied the wire-tap channel, many extensions of the wire-tap channel model have been considered from a perfect secrecy point of view (see e.g. [4–8]).

In [9–12], the Gaussian wire-tap channel of Leung-Yan-Cheong and Hellman [13] is extended to the Gaussian wire-tap channel with side information available at the transmitter. In the Gaussian wire-tap channel with side information, an independent and identically distributed (i.i.d.) additive white Gaussian interference is added to the transmitted signal. The interference is completely known at the transmitter and can be used as a covert communication channel. The authors of [9–12] have proposed an achievable perfect secrecy rate for the Gaussian wire-tap channel with side information. The achievable coding scheme of [9–12] is a combination of Costa’s dirty-paper coding (DPC) [14] and the wire-tap channel coding, and the source is assumed to be digital. We refer to this coding scheme as the digital-secret-DPC (DS-DPC) scheme. The main difference between these works and our work here is that we have considered transmitting an ‘analogue’ source with joint source and channel coding design.

The other works that are related to our work here are [15, 16]. In [15], the authors considered Shannon’s secrecy system in which the legitimate receiver and the wire-tapper have access to side information sequences correlated to the
source, but the wire-tapper receives both the coded information and the side information via channels that are more noisy than the legitimate channel. In the model of Merhav [15], the transmitter and the intended receiver also share a secret key. The key difference between the work of Merhav [15] and our work here is that unlike [15], we have considered a situation in which a known interference available at the transmitter (known also as side information) is disturbing both the legitimate and the eavesdropper channels while in [15] both the intended receiver and the eavesdropper have access to side information correlated with the source. In [16], the rate–distortion theorem is considered for the Shannon cipher system in which there exists no known interference at the transmitter, but the transmitter and the intended receiver share a secret key with rate $R_k$. In the special case of Yamamoto [16], where $R_k = 0$ and the special case in our work where $Q = 0$ ($Q$ is the variance of the known interference), our problem configuration coincides with the model of Yamamoto [16]. In [16], the admissible region of cryptogram rate and the legitimate receiver’s distortion is determined. In our work here, however, we propose several schemes that achieve the lowest known distortion.

Almost all extensions of the wire-tap channel model have considered communicating a ‘discrete’ source with perfect secrecy constraint. In many applications, however, a bandlimited analogue source needs to be transmitted on a bandlimited Gaussian wire-tap channel with side information. In many situations, the exact signal-to-noise ratio (SNR) of the main channel may not be known at the transmitter. Usually, a range of the main channel SNR is known but the true SNR value is unknown. Given a range of main channel SNR, such that the eavesdropper’s signal is degraded with respect to the legitimate receiver’s signal, it is desirable to design a single transmitter, which has a robust performance for all range of SNRs. A common method of designing such a system is based on Shannon’s source–channel separation coding: Quantise the analogue source and then transmit the result discrete source by the DS-DPC scheme. The main advantage of a digital system is that it is more reliable and cost-efficient.

The inherent problem of digital systems is that they suffer from a severe form of ‘threshold effect’ [17, 18]. This effect can be briefly described as follows: the system achieves a certain performance at a certain designed SNR. When the SNR is increased, however, the system performance does not improve and it degrades drastically when the true SNR falls below the designed SNR. The severity of the threshold effect in digital systems is related to Shannon’s source–channel separation principle [19]. Recent works on non-secure communication systems, however, have proven that joint source–channel coding schemes not only can outperform the digital systems for a fixed complexity and delay, they are also more robust against the SNR variations [20–24].

In [22], several hybrid digital–analogue joint source–channel coding scheme are proposed for transmitting a Gaussian source over a (non-secure) Gaussian channel (without side information). The key differences between the work of Mittal and Phamdo [22] and our work are, therefore security and availability of side information. The main idea in [22] for increasing robustness is to reduce the number of quantisation intervals, and thereby increase the distance between the decision lines of the quantisation levels. This will increase the distortion, however, and to compensate the coarser representation, the quantisation error is sent as an analogue symbol using a linear coder (see also [25]). In [26], different coding schemes are analysed for transmitting a Gaussian source over a Gaussian wire-tap channel (without side information). For a fixed information leakage rate to the eavesdropper, [26] has shown that superimposing the secure digital signal with the analogue (quantisation error) part has better performance compared with the separation-based scheme and the uncoded scheme. In [27], the problem of transmitting a Gaussian source over a (non-secure) Gaussian channel with side information is studied. Wilson and Narayan [27] has introduced several hybrid digital–analogue forms of the Costa and Wyner–Ziv coding [28] schemes. In [27], the results of Bross et al. [29] are extended to the case in which the transmitter or receiver has side information, and have shown that there are infinitely many schemes for achieving the optimal distortion.

In this paper, motivated by a covert communication system, we consider the problem of transmitting an i.i.d. Gaussian source over an i.i.d. Gaussian wire-tap channel with known interference available at the transmitter. We assume that the intended receiver has a certain minimum SNR and the eavesdropper has a strictly lower SNR compared to the intended receiver. We are interested in minimising the distortion of source reconstruction at the intended receiver. Here, we derive an achievable distortion when Shannon’s source–channel separation coding scheme is used. We then propose three hybrid digital–analogue secure joint source–channel coding schemes, which achieve the same distortion. Our first coding schemes are based on Costa’s DPC scheme and wire-tap channel coding scheme when the analogue source is not explicitly quantised. Our second coding scheme is based on the superposition of secure digital and hybrid digital–analogue signals. We will show that for the problem of communicating a Gaussian source over a Gaussian wire-tap channel with side information, there exists an infinite family of secure joint source–channel coding scheme. We explicitly superimpose the quantised and analogue signals in our third coding scheme. We will show that this scheme provides an infinite family of secure joint source–channel coding schemes with a variable number of binning. Finally, we analyse our secure hybrid digital–analogue schemes under the main channel SNR mismatch. We will show that our proposed schemes can give a graceful degradation of distortion with SNR under SNR mismatch, that is, when the actual SNR is larger than the designed SNR.

Besides the aforementioned benefits of our proposed schemes, the major limitations of our hybrid digital–analogue secure joint source–channel coding methods can be listed as follows:

- In our schemes, the intended receiver is assumed to have a certain minimum SNR and the eavesdropper is assumed to have a strictly lower SNR compared with the intended receiver.
- Our proposed schemes have more complexity in both encoding and decoding parts compared with Shannon’s source–channel separation coding scheme.

2 Preliminaries and related works

2.1 Notation

In this paper, random variables are denoted by capital letters (e.g. $X$) and their realisations are denoted by corresponding lower case letters (e.g. $x$). The finite alphabet of a random
variable is denoted by a script letter (e.g. $X$) and its probability distribution is denoted by $P(x)$. The vectors will be written as $x^n = (x_1, x_2, \ldots, x_n)$, where subscripted letters denote the components and superscripted letters denote the vector. The notation $x'_i$ denotes the vector $(x_1, x_{i+1}, \ldots, x_n)$ for $j \geq i$. A Gaussian random variable $X$ with a mean of $m$ and variance of $\sigma^2$ is denoted by $X \sim N(m, \sigma^2)$. The function $E[.]$ represents a statistical expectation.

### 2.2 System model and problem statement

#### 2.2.1 Source model: Consider a memoryless Gaussian source of $\{V_i\}_{i=1}^\infty$ with zero mean and variance $\sigma^2$. Thus, $V_i \sim N(0, \sigma^2)$ and we assume that the sequence $V_i$ is the i.i.d. We assume that the source is obtained from uniform sampling of a continuous-time Gaussian process with bandwidth $W_s(\text{Hz})$. Furthermore, we assume that the sampling rate is $2W_s$ samples per second.

#### 2.2.2 Channel model: The source is transmitted over an additive white Gaussian noise (AWGN) wire-tap channel in the presence of an interference $S$, which is known to the transmitter but unknown to the receivers. The channel is modelled as follows

$$
Y_i = X_i + S_i + W_i \\
Z_i = X_i + S_i + W'_i
$$

where $X_i$, $Y_i$, and $Z_i$ are the channel input, the received signal by the intended receiver and the received signal by the eavesdropper, respectively. We assume that $E[Y_i] = P$, and $W_i \sim N(0, N_s)$. $W'_i \sim N(0, N_s)$. Furthermore, assume that $S_i$s are a sequence of real i.i.d. Gaussian random variables with zero mean and variance $Q$, that is, $S_i \sim N(0, Q)$. As the source, interference and the channel are i.i.d. over the time, we will omit the index $i$ throughout the rest of the paper. The channel is derived from a continuous-time AWGN wire-tap channel with bandwidth $W_s(\text{Hz})$. The equivalent discrete-time channel is used at a rate of $2W_s$ channel uses per second. The block diagram of the system is depicted in Fig. 1.

#### 2.2.3 Coding scheme: The source samples are grouped into blocks of size $m$

$$
V^n = (V_1, V_2, \ldots, V_m)
$$

and the encoder is a mapping $f_m: \mathbb{R}^m \times \mathbb{R}^m \rightarrow \mathbb{R}^n$ which satisfies the power constraint $E[\|f_m(V^n, S^n)\|^2] \leq nP$. Let us define the parameter $\rho = n/m = W_s/W_c$. In this paper, we assume that $\rho = 1$. The received signals by the intended receiver and the eavesdropper are given by

$$
Y^n = X^n + S^n + W^n \\
Z^n = X^n + S^n + W'^n
$$

where $X^n = f_m(V^n, S^n)$, $W^n \sim N(0, N_sI_n)$, $W'^n \sim N(0, N_sI_n)$ and $I_n$ is the $n \times n$ identity matrix. The decoder at the intended receiver is a mapping $g_m: \mathbb{R}^n \rightarrow \mathbb{R}^m$. The average squared-error distortion of the coding scheme at the intended receiver is given by

$$
D_{\text{ave, m}}(f_m, g_m, N_1, N_2) = \frac{1}{m} E[\|\hat{V}^m - V^m\|^2]
$$

where $\hat{V}^m = g_m(Y^n)$. For the purpose of analysis, we will consider sequences of codes $(f_m, g_m)$, where $m$ is increasing but the ratio $\rho = n/m$ is fixed. The asymptotic performance of the code is given by

$$
D_{\text{ave}}(N_1, N_2) = \lim_{m \rightarrow \infty} D_{\text{ave, m}}(f_m, g_m, N_1, N_2)
$$

Note that the above $D_{\text{ave}}$ is also a function of $\sigma^2 > 0$, $P > 0$, $Q > 0$ and $\rho > 0$, but we assume that these parameters are known and fixed, and therefore express $D_{\text{ave}}$ as a function of $(N_1, N_2)$. In subsequent sections, we refer to $D_{\text{ave}}$ as mean-squared distortion and omit the superscript ‘ave’ and denote it by $D$, that is, $D = D_{\text{ave}}$.

#### 2.2.4 Secrecy requirements: The eavesdropper observes $Z^n$. The secrecy of the system is measured by the information leaked to the eavesdropper and is expressed as follows

$$
I_e = \frac{1}{n} I(V^n; Z^n)
$$

Note that $I_e = 0$ corresponds to the perfect secrecy condition and implies that the eavesdropper obtains no information about the source. In this paper, we consider the situation in which the leakage information $I_e$ is known and is a fixed constant.

#### 2.2.5 Distortion exponent: In practical scenarios, the transmitter usually does not have an exact knowledge of $N_1$ but knows that $N_1 \leq N_2$, where $N_2$ is the noise variance corresponding to the design $\text{SNR}_d = (P/N_2)$. The eavesdropper channel is still a degraded version of the main channel and is assumed to have the lowest $\text{SNR}_2 < \text{SNR}_d < \text{SNR}_1$, where $\text{SNR}_2 = (P/N_2)$ and $\text{SNR}_1 = (P/N_1)$. The receiver is assumed to have a perfect estimate of $\text{SNR}_1$, but the transmitter communicates at a lower designed $\text{SNR}_d$. In this scenario, we expect a graceful degradation of distortion $D(\text{SNR}_1)$ with $\text{SNR}_1$.

![Fig. 1 Block diagram of the secure joint source-channel coding problem with interference known only at the transmitter](image-url)
The secrecy capacity of a wire-tap channel is given by

\[ C \triangleq \lim_{\text{SNR}_1 \rightarrow \infty} \frac{\log D(\text{SNR}_1)}{\log \text{SNR}_1} \]  

(6)

The highest possible distortion exponent is \( \rho \) and therefore \( 0 \leq \zeta \leq \rho \). The distortion exponent can be used as a criterion for the robustness of a coding scheme. A high distortion exponent means that the coding scheme is more robust. In this paper, we propose different robust coding schemes. Before introducing our proposed schemes, we need to review some related works in this area.

2.3 Related works

2.3.1 Digital wire-tap channel: In a digital wire-tap channel (without any interference \( S \)), a digital message \( M \in \{1, 2, \ldots, N_C\} \) is transmitted to the intended receiver while the eavesdropper is kept ignorant. Wyner [2] characterised the secrecy capacity of this channel when the eavesdropper’s channel is degraded with respect to the main channel. Csiszar and Korner [3] considered the general wire-tap channel and established its secrecy capacity. Let us assume \( X, Y \) and \( Z \) to be the channel input, intended receiver’s signal and eavesdropper’s signal, respectively. The secrecy capacity of a wire-tap channel is given by

\[ C_s = \max_{P(x,u)} 2W_e[I(U; Y) - I(U; Z)] \]  

(7)

where \( U \rightarrow X \rightarrow YZ \) forms a Markov chain. When the channels are AWGN, Leung-Yan-Cheong and Hellman [13] have shown that the secrecy capacity is given by

\[ C_s = W_e \left[ \log \left( 1 + \frac{P}{N_1} \right) - \log \left( 1 + \frac{P}{N_2} \right) \right] \]  

(8)

Here, we briefly explain the coding scheme. We generate \( 2^{nW_e} \) Gaussian codewords \( U^n \) and throw them uniformly at random into \( 2^{nC_1} \) bins. Each bin thus contains \( 2^{nW_e} \) codewords. To encode the message \( M \in \{1, 2, \ldots, 2^{C_1}\} \) randomly choose a \( U^n \) from the bin, which is indicated by \( M \) and send it. The intended receiver seeks for a \( U^n \) which is jointly typical with \( Y^n \) and declares the bin index as the transmitted message. The probability of error asymptotically tends to be zero, that is, \( \lim_{n \rightarrow \infty} P_e(M \neq M) \rightarrow 0 \). The information leakage is \( \lim_{n \rightarrow \infty} 1/n I(M; Z^n) = 0 \). When \( I_e \) is not zero but is a fixed known constant, we have the following lemma:

Lemma 1: In a digital wire-tap channel (without any interference \( S \)), the information leakage rate to the eavesdropper is \( I_e \), for the rate of

\[ R_{I_e} = C_s + I_e \]

\[ = W_e \left[ \log \left( 1 + \frac{P}{N_1} \right) - \log \left( 1 + \frac{P}{N_2} \right) \right] + I_e \]  

(9)

Proof: Let \( M \) be the secret message. The transmission rate is then given by

\[ R_{I_e} = \frac{H(M)}{n} \]  

(10)

According to the security analysis of Leung-Yan-Cheong and Hellman [13], by applying Theorem 1 of Leung-Yan-Cheong and Hellman [13] to our problem setup, we obtain the following inequality

\[ \frac{H(M|Z^n)}{n} \leq W_e \left[ \log \left( 1 + \frac{P}{N_1} \right) - \log \left( 1 + \frac{P}{N_2} \right) \right] \]  

(11)

By combining (10) and (11), we have

\[ R_{I_e} \frac{H(M|Z^n)}{H(M)} \leq \frac{H(M) - n I_e}{H(M)} \]

\[ \leq R_{I_e} - I_e \]  

(12)

The left-hand side of the above inequality can be simplified as follows

\[ R_{I_e} \frac{H(M|Z^n)}{H(M)} = R_{I_e} \frac{H(M) - H(M) + H(M)}{H(M)} \]

\[ \overset{(a)}{=} R_{I_e} \frac{H(M) - n I_e}{H(M)} \]

\[ \overset{(b)}{=} R_{I_e} - I_e \]  

(13)

where (a) follows from the definition of \( I_e \) in (5), and (b) follows from (10). Thus, we can bound \( R_{I_e} \) as

\[ R_{I_e} \leq W_e \left[ \log \left( 1 + \frac{P}{N_1} \right) - \log \left( 1 + \frac{P}{N_2} \right) \right] + I_e \]  

(14)

Therefore the maximum rate for \( R_{I_e} \) can be obtained by choosing

\[ R_{I_e} = W_e \left[ \log \left( 1 + \frac{P}{N_1} \right) - \log \left( 1 + \frac{P}{N_2} \right) \right] + I_e \]  

(15)

2.3.2 Digital DPC: Consider transmitting a quantised (digital) source over a point-to-point AWGN channel (without any eavesdropper) with side information known at the transmitter. The received signal in this model can therefore be written as \( Y = X + S + W \). Costa [14] showed that the capacity of this channel is given by

\[ C = W_e \log \left( 1 + \frac{P}{N_1} \right) \]  

(16)

which is equal to the capacity of an AWGN channel without the interferer \( S \). The achievability scheme – which is called DPC – is as follows

Let

\[ R = \max_{P(u|y), P(u|s)} 2W_e[I(U; Y) - I(U; S)] \]  

(17)

where \( U \rightarrow X \rightarrow Y \) forms a Markov chain. We generate \( 2^{nW_e} \) Gaussian codewords \( U^n \) and throw them into \( 2^{nC_1} \) bins. In each bin, there exist \( 2^{nW_e} \) codewords. To transmit
a message $M \in \{1, 2, \ldots, 2^{|M|}\}$, we choose a $U^n$ in the bin, which is indicated by the message $M$, such that $(U^n, S^n)$ are jointly typical. The channel input $X$ is generated as a function of $U$ and $S$ as follows

$$ U = X + aS $$

(18)

where $X \sim \mathcal{N}(0, P)$ is independent of $S$ and $\alpha = (P/(P + N_i))$. The decoder seeks for a $U^n$ which is jointly typical with $Y^n$ and declares the bin number as the transmitted message. The channel output is $Y = X + S + W = U + (1 - \alpha)S + W$ and it is easy to show that with $\alpha = (P/(P + N_i))$, the achievable rate $R = C$.

**2.3.3 Digital-secret-DPC:** Consider transmitting a digital source over a Gaussian wire-tap channel in the presence of the interference $S$ known only at the transmitter. The received signals by the intended user and eavesdropper are given by

$$ Y = X + S + W $$

$$ Z = X + S + W' $$

(19)

Even in a Gaussian case, the secrecy capacity of this problem is still unknown. We can obtain an achievable rate by combining the secrecy coding of the wire-tap channel with Costa’s DPC. We refer to this coding scheme as DS-DPC. The following theorem characterises the best-known achievable secure rate for the Gaussian wire-tap channel with side information using DS-DPC scheme.

**Theorem 1 ([9–12]):** For the Gaussian wire-tap channel with side information, an achievable secrecy rate is given by

$$ R_s = 2W_e \max_{\alpha} \min \{ I(U_a; Y) - I(U_a; S), I(U_a; Y) - I(U_a; Z) \} $$

(20)

where $0 \leq \alpha \leq 1$ is a real number, $U_a = X + \alpha S$ and $X \sim \mathcal{N}(0, P)$. The above optimisation is further analysed in [9–12] to provide the more explicit expression for the secrecy rate.

Let

$$ R(\alpha) = I(U_a; Y) - I(U_a; S) $$

(21)

and

$$ R_s(\alpha) = I(U_a; Y) - I(U_a; Z) $$

(22)

The function $R(\alpha)$ is maximised at $\alpha^* = (P/(P + N_i))$ and

$$ R(\alpha^*) = \frac{1}{2} \log \left( 1 + \frac{P}{N_i} \right) $$

(23)

The function $R_s(\alpha)$ is maximised at $\alpha = 1$ and

$$ R_s(1) = \frac{1}{2} \log \left( \frac{P + Q + N_i N_2}{P + Q + N_i N_2} \right) $$

(24)

It is easy to show that $R(\alpha_0) = R_s(\alpha_0)$, where

$$ \alpha_0 = \frac{PQ + P\sqrt{Q(P + Q + N_2)}}{Q(P + N_2)} $$

(25)

Let

$$ P_L = -\frac{Q}{2} + \frac{\sqrt{Q^2 + 4QN_i}}{2} $$

(26)

$$ P_H = -\frac{Q}{2} + \frac{\sqrt{Q^2 + 4QN_2}}{2} $$

(27)

then the secrecy rate of (20) may be written as

$$ R_s = \begin{cases} R(\alpha^*), & \text{if } P \leq P_L \\ R(\alpha_0), & \text{if } P_L \leq P \leq P_H \\ R_s(1), & \text{if } P \geq P_H \end{cases} $$

(28)

The above three cases correspond to the three possible cases of the optimisation problem

$$ \max_{\alpha} \{ R(\alpha), R_s(\alpha) \} $$

(29)

(i) $R(\alpha)$ is optimised at $\alpha = \alpha^*$, and $R(\alpha^*) < R_s(\alpha^*)$; (ii) $R_s(\alpha)$ is optimised at $\alpha = 1$, and $R(1) > R_s(1)$; and (iii) $R(\alpha)$ is optimised subject to $R(\alpha) = R_s(\alpha)$.

It can be seen from the above equation that the Gaussian wire-tap channel with side information has larger secrecy capacity than the Gaussian wire-tap channel without the interferer. The side information, therefore helps to improve the secrecy capacity. This is in contrast to the point-to-point channel without the secrecy constraint, in which the side information does not affect the capacity.

As shown in [9–12], the achievable secrecy rate given in (28) is indeed the secrecy capacity for the cases when $P \leq P_L$ and when $P \geq P_H$. The secrecy rate in the former case is the capacity of the channel without secrecy constraint and with the transmitter knowing the state sequence (DPC). The secrecy rate in the latter case is the secrecy capacity of an enhanced wire-tap channel, in which the state variable is used as the channel input instead of the channel interference. Both of these two secrecy capacities are clearly upper bounds on the secrecy capacity for the original wire-tap channel with side information. Hence, achieving these two bounds imply achieving the secrecy capacity.

### 3 Separation-based scheme and a simple scaling scheme

Let us consider our problem of transmitting a Gaussian source over the Gaussian wire-tap channel with side information as depicted in Fig. 1. In this model $L$ leakage information rate is allowed for the eavesdropper. As assumed in this paper $\rho = n/m = 1$.

**3.1 Separation-based scheme**

In this section, we characterise the achievable distortion when the source $V^n$ is first quantised using an optimum quantiser to produce an index $m \in \{1, 2, \ldots, 2^{|V^n|} \}$, where $R_s$ is given in (28). Then, the index $m$ is transmitted using the secret DPC scheme. As the quantiser output is digital
information, we refer to this scheme as digital-secret-dirty-paper-coding. We briefly review this scheme here. Let 
\( U^a = X + \alpha S \), we first generate \( 2^{nR}(U^a) \) i.i.d. Gaussian sequences \( U^a \) and randomly distribute them into \( 2^n \max{(U^a, S)} \) bins such that each bin contains \( 2^n \max{(U^a, S)} \). We index each by 
the associated transmitter signal is given by 

3.2 Simple scaling scheme

For transmitting a Gaussian source over a

Theorem 2: For transmitting a Gaussian source over a 
Gaussian wire-tap channel with side information knowing at 
the transmitter, the separation-based scheme is not 
optimum, unless for \( P \leq P_I \).

In the following section we show that a number of secure 
joint source–channel coding schemes exist, which all 
achieve the same distortion of the separation-based scheme. 
Besides achieving the same distortion, we will show that 
our proposed secure joint source–channel coding are robust 
when there is an SNR_1 mismatch. We will analyse the 
robustness of these schemes later on.

3.2 Simple scaling scheme

Let us consider a simple scaling scheme in which the 
transmitter signal is given by \( X = k_1 V + k_2 S \). The received signals at the intended receiver and the eavesdropper are therefore given by

\[
Y = k_1 V + (k_2 + 1)S + W
\]
\[
Z = k_1 V + (k_2 + 1)S + W^
\]

For a fixed leakage information of \( I_e \), the parameters \( k_1 \) and \( k_2 \) 
are related as follows

\[
I_e = \frac{1}{2} \log \left( 1 + \frac{k_1^2 \sigma_v^2}{(k_2 + 1)^2 Q + N_2} \right)
\]

The power of the transmitter is limited by \( P \). Thus 

\[
k_1^2 \sigma_v^2 + k_2^2 Q \leq P
\]

The intended receiver estimates the transmitted source by 
\( \hat{Y} = \lambda Y \), where \( \lambda \) is chosen such that it minimises 
\( D = E[\|Y - \hat{Y}\|^2] \). After some algebra, the achieved 
distortion in this scheme is given by

\[
D = \frac{\sigma_v^2}{1 + (2^{2L_e} - 1)((k_2 + 1)^2 Q + N_2)/(2^{2L_e} + N_2)}
\]

where (a) follows from (32), and \( k_2 \) can be calculated to 
minimise \( D \) subject to the constraint of (33). It is easy to 
verify that the solution of this constraint optimisation 
problems is as follows

\[
D = \frac{\sigma_v^2}{1 + (2^{2L_e} - 1)((k_2 + 1)^2 Q + N_2)/(2^{2L_e} + N_2)}
\]
In this figure, $\sigma_r^2 = 20$, $I_e = 0.1$, $Q = 10$, $N_1 = 1$ and $N_2 = 4$. Using these values
\[ \text{SNR}_L = 10\log \frac{P_L}{N_1} = 1.52 \quad \text{and} \quad \text{SNR}_{hh} = 10\log \frac{P_{hh}}{N_1} = 4.86 \]

4 Secure hybrid digital–anologue DPC

4.1 Scheme 1

In this section, we propose a secure joint source–channel coding scheme, where the analogue source $V^n$ is not explicitly quantised. The code construction, encoding and decoding procedures are as follows.

Let us define an auxiliary Gaussian random variable $U_{n,k}$ as follows
\[ U_{n,k} = X + aS + kV \] (36)
where $X \sim N(0, P)$, and $X, S$ and $V$ are pairwise independent.

4.1.1 Codebook generation: We generate $2^{nH(U_{n,k};Y)+I_e}$ i.i.d. sequences $U_{n,k}^n$, where each component of each sequence is Gaussian with zero mean and variance $P + \alpha^2 Q + k^2 \sigma_r^2$. We then distribute these codewords into $2^R$ bins, where $R > 0$.

4.1.2 Encoding: Given the interference sequence $S^n$ and the source sequence $V^n$, the encoder finds $U_{n,k}^n$’s such that $(U_{n,k}^n, S^n, V^n)$ are jointly typical. The encoder then randomly chooses one of them and transmits $X^n = U^n - aS^n - kV^n$. If such $U^n$’s cannot be found, the encoder declares failure. Let $P_{c1}$ be the probability of an encoder failure.

From the extensions of typicality to infinite alphabet case [30], we have $\lim_{n \rightarrow \infty} P_{c1} = 0$ provided that
\[ I(U_{n,k}; Y) + I_e - R > \max \{ I(U_{n,k}; Z), I(U_{n,k}; SV) \} \] (37)
for any $R > 0$. Therefore the following condition must be satisfied:
\[ I(U_{n,k}; Y) + I_e > \max \{ I(U_{n,k}; Z), I(U_{n,k}; SV) \} \] (38)

4.1.3 Decoding: The legitimate receiver looks for a unique $U_{n,k}$ such that $(U_{n,k}^n, Y^n)$ is jointly typical and declares $U_{n,k}$ as the decoder output. It is easy to show that if the condition of (38) is satisfied the probability that the decoder output is not equal to the encoded $U_{n,k}^n$ goes to zero when $n \rightarrow \infty$. The legitimate receiver then estimates the source $V_n$ by using the pair $(U_{n,k}^n, Y^n)$ as follows
\[ \hat{V}_n = \lambda_1 Y_n + \lambda_2 U_{n,k} \] (39)
where $\lambda_1$ and $\lambda_2$ are such that minimise the distortion $D = \mathbb{E}[\| V - \hat{V} \|_2]$. After conducting some algebraic calculations, we can see that the optimum values for $(\lambda_1, \lambda_2)$ are given by
\[ \lambda_1 = \frac{-k^2 \sigma_r^2 (P + \alpha Q)}{k^2 \sigma_r^2 (P + Q + N_1) + (1 - \alpha)^2 PQ + N_1 (P + \alpha^2 Q)} \] (40)
\[ \lambda_2 = \frac{k \sigma_r^2 (P + Q + N_1)}{k^2 \sigma_r^2 (P + Q + N_1) + (1 - \alpha)^2 PQ + N_1 (P + \alpha^2 Q)} \] (41)

The minimum mean square error (MMSE) estimation therefore leads to the following distortion
\[ D(\alpha, k) = \frac{\sigma_r^2}{1 + ((k^2 \sigma_r^2) / \mu)} \] (42)
where $\mu$ is given by
\[ \mu = \frac{(1 - \alpha)^2 PQ + N_1 (P + \alpha^2 Q)}{P + Q + N_1} \] (43)

We need to find the optimum values of $(\alpha, k)$ which minimise the distortion $D$ with the constraint of (38). First, we assume that max $I(U_{n,k}; SV), I(U_{n,k}; Z) = I(U_{n,k}; SV)$. We choose $(\alpha, k)$ such that $I(U_{n,k}; Y) + I_e > I(U_{n,k}; SV) > I(U_{n,k}; Z)$. Our optimisation problem can therefore be written as the following constraint optimisation problem
\[ \min D(\alpha, k) \] (44)
\[ \text{s.t.} \quad I(U_{n,k}; Y) + I_e > I(U_{n,k}; SV) > I(U_{n,k}; Z) \]

After some manipulation, it is easy to see that the valid region of $(\alpha, k)$ is as follows (see Fig. 3. for a typical valid region. In this figure, $\sigma_c^2 = 10$, $P = 10$, $Q = 5$, $N_1 = 1$, $N_2 = 4$ and $I_e = 0.01$):
\[ k^2 \sigma_r^2 (P + Q + N_2) \geq -Q(P + N_2) \alpha^2 + 2PQ \alpha + P^2 \]
\[ k^2 \sigma_r^2 (P + Q + N_1) \leq -(1 - \alpha)^2 PQ - N_1 (P + \alpha^2 Q) \]
\[ + P(P + Q + N_1) \alpha^2 \]

In this region, the optimum values of $(\alpha, k)$ and the related $D(\alpha, k)$ are as follows.

\[ \text{Fig. 3 Typical valid region for choosing } (\alpha, k) \text{ in scheme 1} \]
In this case, the achievable distortion \( D \) is indeed optimum and is equal to the distortion of a Gaussian AWGN with side information and without the secrecy constraint. Similarly, if \( \max(I(U_{s,k};SV), I(U_{a,k};Z)) \equiv I(U_{a,k};Z) \), the achievable distortion \( D \) may be calculated as

\[
D = \frac{\sigma_i^2}{P + Q + N_1}/((P + Q + N_1)/2^{2I})
\]  

(48)

Again, in this case the achievable distortion \( D \) is indeed optimum and is equal to the distortion of an enhanced wire-tap channel, in which the state variable is used as the channel input instead of the channel interference.

Finally, when \( I(U_{a,k};SV) = I(U_{a,k};Z) \), the achievable distortion is given by

\[
D = \frac{\sigma_i^2}{2^{2I}((P + Q + N_1)/2^{2I})}
\]  

(49)

where \( \alpha_0 \) is given in (25). The distortions in (47)–(49) are the achievable distortions when \( P \leq P_L, P_L \leq P \leq P_H \) and \( P \geq P_H \), respectively, in which \( P_L \) and \( P_H \) are given in (26) and (27), respectively.

Therefore this proposed scheme has the same distortion of the separation scheme. Note that the proposed secure hybrid digital–analogue DPC is not entirely analogue in the sense that the auxiliary random variable \( U_{a,k} \) is from a discrete codebook. In contrast to secure digital DPC, however, the source is not explicitly quantised and is embedded into the transmitted signal \( X \) in an analogue method. Another feature of the secure analogue DPC is that there is no need for double binning the codewords. In the digital scheme, however, double binning is necessary: one binning is used

\[
\alpha = \frac{P}{P + N_1}
\]  

(45)

\[
k^2 = \frac{P}{\sigma_i^2} \left( 2^{2I} - \frac{N_1}{P + N_1} \right)
\]  

(46)

\[
D = \frac{\sigma_i^2}{(P + N_1/2^{2I})}
\]  

(47)

Fig. 4 Typical achievable distortion \( D \) against leakage information \( I_e \) for \( P \leq P_L \).
We first quantise the source at a rate \( R < R_s \), where \( R_s \) is given in (28). Let the quantiser error be \( E^s = V^s - V^{s^n} \), where \( V^{s^n} \) is the reconstruction of \( V^s \). The quantisation error has a variance of \( \sigma_e^2 = \sigma^2s^n \). We encode the quantised digital part using a secure digital dirty-paper--encoder, which treats \( S^n \) as the interference and \( X^n_h \) as the channel noise. The output signal of this section is denoted by \( X^n_h \) which has a power of \( P_1 \). The second part of the encoder is the same as scheme 1, which treats \( S^n \) and \( X^n_s \) as interference. The output of this part is denoted by \( X^n_s \), which has a power of \( P_2 = P - P_1 \). The transmitted signal is the superposition of \( X^n_s \) and \( X^n_h \), that is, \( X^n = X^n_s + X^n_h \).

Let first assume that \( P \leq P_{\text{th}} \). The auxiliary random variable of the digital encoder as \( U_1 = X_1 + \alpha_1 S \), where \( X_1 \) is independent of \( S \). The power \( P_1 \) and \( \alpha_1 \) of this encoder are chosen as follows

\[
P_1 = (P + N_1)(1 - 2^{-2R})
\]

\[
\alpha_1 = \frac{P_1}{P_1 + P_h + N_1}
\] (55)

Note that \( P_1 > 0 \) and the above choice for \( \alpha_1 \) corresponds to treating \( X_h \) as noise, in addition to the channel noise \( W \).

In the second encoder, we encode the quantisation error \( E^s \) using the coding scheme 1. Here, we treat \( X_1 + S \) as interference. In this case, we choose the parameters of this scheme as follows

\[
P_h = (P + N_1)2^{-2R} - N_1
\]

\[
\alpha_h = \frac{P_h}{P_h + N_1}
\]

\[
k^2 = \frac{P_h}{\sigma_e^2} \left( 2^{2R} - \frac{N_1}{P_h + N_1} \right)
\] (56)

Note that as \( R \leq (1/2)\log(P + N_1/(N_1)) \), the power \( P_h \) is always positive. The auxiliary random is chosen as \( U_{a,k} = X_h + \alpha_1 (X_1 + S) + kE \), where \( X_1 + S \) is considered as the net interference. Thus, we choose \( X_h \) independent of \( X_1, S \) and \( E \).

The intended decoder first decodes the quantisation index according to the decoding rule of the secure digital DPC scheme. Then it reconstructs \( V^{s^n} \). The overall distortion in this case is the distortion in estimating \( E^s \). According to the analysis of scheme 1, the overall distortion in this case is given by

\[
D = \frac{\sigma_e^2}{2^{2R}((P + N_1)2^{-2R} - N_1)/N_1)}
\]

\[
= \frac{\sigma_e^2}{2^{2R}((P + N_1)/N_1)}
\] (57)

As we can see, for any coding rate \( R \) of the first encoder such that \( R < R_s \), this scheme is valid and leads to the optimal distortion in this case. Similarly, when \( P \geq P_{\text{th}} \), we chose \( P_1 \) and \( P_h \) as follows

\[
P_1 = (P + Q + N_1)(1 - 2^{-2R})
\]

\[
P_h = (P + Q + N_1)2^{-2R} - (Q + N_1)
\] (58)

In this case, as the intended decoder can subtract \( X^n_h \) from \( Y^{s^n} \) and \( U_{a,k} \), the overall distortion is given by

\[
D = \frac{\sigma_e^2}{2^{2R}((P_h + Q + N_1)/(P + Q + N_2)(N_2/N_1))}
\]

\[
= \frac{\sigma_e^2}{2^{2R}((P + Q + N_1)/(P + Q + N_2)(N_2/N_1))}
\] (59)

Finally, when \( P_{\text{th}} \leq P \leq P_{h} \), the overall distortion can be calculated as

\[
D = \frac{\sigma_e^2}{2^{2R}((P_h + Q + N_1)/(P + Q + N_1))}
\]

\[
= \frac{\sigma_e^2}{2^{2R}((P + Q + N_1)/(P + Q + N_1))}
\] (60)

For any \( R < R_s \), this scheme is valid and we subsequently have the following theorem.

**Theorem 3:** For the problem of transmitting a Gaussian source over a Gaussian wire-tap channel with side information known at the transmitter, there exists an infinite family of secure joint source–channel coding schemes.

4.2.1 **Secrecy analysis:** Since in this scheme the quantisation rate is \( R < R_s \), the digital part is perfectly secure. However, we used scheme 1 to transmit the quantisation error. Therefore using Lemma 2, the maximum information leakage to the eavesdropper is limited by \( (1/n)I(V;Z^n) = (1/n)I(E;Z^n) \leq I_e \).

4.3 **Scheme 3**

This scheme is a combination of schemes 1 and 2. In this scheme, the quantised signal and the analogue part are explicitly superimposed.

First, we quantise the source \( V^n \) using an optimal quantiser at rate \( R < R_s \). Let \( V^{s^n} \) and \( E^n \) be the digital reconstruction of \( V^n \), and the quantisation error vector, respectively. According to the rate–distortion theorem, the quantisation error \( E^n \) is an i.i.d. Gaussian vector.

We next define an auxiliary random variable \( U_{a,k} \) as follows

\[
U_{a,k} = X + \alpha S + kE
\] (61)

where \( X \sim \mathcal{N}(0, P) \), \( E \sim \mathcal{N}(0, \sigma^2_s 2^{-2R}) \), and \( X, S \) and \( E \) are independent of each other. The coding/decoding procedure is as follows.

4.3.1 **Codebook generation:** We generate \( 2^nI(U_{a,k};Y) \) i.i.d. Gaussian sequences where each component has zero mean and variance of \( P + \sigma^2_s 2^{-2R} + k^2 \sigma^2_s 2^{-2R} \). We then distribute these codewords into \( 2^n \) bins and this is shared between the encoder and the decoder. The rate \( R \) must be chosen such that each bin contains

\[
N_b = 2^n\max\{I(U_{a,k};E|U_{a,k};Z)\}
\] (62)

codewords. We then randomly distribute the \( N_b \) codewords of
each bin into $N_{sb}$ subbins, where $N_{sb}$ is given by
\[ N_{sb} = 2^{n \max \{I(U_{a,k}; SE), I(U_{a,k}; Z)\} - nI(U_{a,k}; Z)} \]  

4.3.2 Encoding: Let $m \in \{1, 2, \ldots, 2^{nR}\}$ be the quantisation index corresponding to the quantised vector $V^n$. To send the message $m$ with an interference $S^n$, the encoder looks for $U^n_{a,k}$ sequences in the bin $m$ such that $(U^n_{a,k}, S^n, E^n)$ are jointly typical with respect to the distribution of (61). If such $U^n_{a,k}$ cannot be found, encoder declares a failure. Let $P_{e1}$ be the probability of an encoding failure. The encoder then randomly chooses one of the $U^n_{a,k}$ and transmits $X^n = U^n_{a,k} - aS^n - kE^n$.

4.3.3 Decoding: The received signal by the legitimate receiver is $Y^n = X^n + S^n + W^n$. The legitimate receiver looks for a unique $U^n_{a,k}$ such that it is jointly typical with $Y^n$. If such a unique $U^n_{a,k}$ can be found, the decoder declares $X^n$ as the decoder output, otherwise, it declares a failure. Let $P_{e2}$ be the probability of the decoding failure. Then, the legitimate receiver estimates $E^n$ from $U^n_{a,k}$ and $Y^n$.

We can see by similar Gelfand–Pinsker coding argument and wire-tap coding argument that
\[ 0 \leq R \leq I(U_{a,k}; Y) - \max\{I(U_{a,k}; SE), I(U_{a,k}; Z)\} + I_e \]  
then, $P_{e1}$ and $P_{e2}$ goes to zero when $n \to \infty$, and the leakage information to the eavesdropper is $I_e$.

4.3.4 Estimation: The legitimate receiver makes an MMSE estimate of $V^n$ from the observations $(Y^n, U^n_{a,k}, Y^n)$, where
\[ V = V^n + E \]
\[ U_{a,k} = X + aS + kE \]
\[ Y = X + S + W \]  
Let $\sigma_e^2 = \sigma_Y^2 2^{-2R}$. The optimum linear MMSE estimation is given by
\[ \hat{V} = \lambda_1 V^n + \lambda_2 U_{a,k} + \lambda_3 Y \]  
where $[\lambda_1, \lambda_2, \lambda_3]$ are chosen such that the distortion $D = \mathbb{E}[\|V - \hat{V}\|^2]$ is minimised. When $P \leq P_L$, we choose the parameters $(\alpha, k)$ as follows
\[ \alpha = \frac{P}{P + N_0}, \quad k = \frac{P}{\sigma_e^2} \left( \frac{2 I_{U_{a,k}} - N_0 2^{2R}}{P + N_0} \right) \]  
We can see the the above choice for $(\alpha, k)$ satisfies the condition of (64) when $\max\{I(U_{a,k}; SE), I(U_{a,k}; Z)\} = I(U_{a,k}; SE)$. Let $\Lambda$ be the covariance matrix of $(V^n, U^n_{a,k}, Y^n)$ and let $\Gamma$ be the correlation vector between $V$ and $(V^n, U^n_{a,k}, Y^n)^T$. The matrices of $\Lambda$ and $\Gamma$ are then given by
\[ \Lambda = \begin{pmatrix} \sigma_e^2 & \alpha & 0 \\ \alpha & P + \alpha^2 Q + k^2 \alpha_e^2 & P + \alpha Q \\ 0 & P + \alpha Q & P + Q + N_1 \end{pmatrix} \]  
and
\[ \Gamma = (\alpha_e^2 - \sigma_e^2, k \alpha_e^2, 0)^T \]  
The coefficients of the linear MMSE estimation are given by $(\Lambda_1, \Lambda_2, \Lambda_3)^T = \Lambda^{-1} \Gamma$ and the minimum distortion is given by
\[ D = \sigma_e^2 - \Gamma^T \Lambda^{-1} \Gamma = \frac{\sigma_e^2}{2I(P + N_1/N_0)} \]

Similarly, when $P \geq P_H$ or $P_L \leq P \leq P_H$, the overall distortion is given by (59) and (60), respectively. Note that this scheme is an intermediate scheme between the secure digital DPC with the maximum possible binning and the hybrid digital–analogue scheme 1 with minimum possible binning. We can, therefore have a family of schemes with varying bings by changing $R$ such that the condition of (64) is satisfied.

Theorem 4: For the problem of transmitting a Gaussian source over a Gaussian wire-tap channel with side information known at the transmitter, there exists an infinite family of secure joint source–channel coding schemes with a variable number of bingings.

Note that Scheme 3 is closely related to the secure digital DPC and Scheme 2. The difference, however, is that in Scheme 3 the transmitted signal is not a superposition of the two signals as seen in Scheme 2.

4.3.5 Secrecy analysis: Similar to Scheme 2, since in this scheme the quantisation rate is $R \leq R_s$, the digital part is perfectly secure. However, we used Scheme 2 to transmit the quantisation error. Therefore using Lemma 2, the maximum information leakage to the eavesdropper is limited by $(1/n)I(V; Z') = (1/n)I(E; Z') \leq I_e$.

5 Performance analysis of the schemes with SNR mismatch

In this section, we analyse the performance of the proposed secure joint source–channel coding schemes in the presence of SNR mismatch. Here, we assume that we have designed the schemes for a designed channel SNRd, but the actual SNR1 is such that SNR2 < SNRd < SNR1. As the analysis for the cases that $P \geq P_H$, and $P_L \leq P \leq P_H$ are messy, we only focus on the case in which $P \leq P_L$. Separation-based digital schemes suffer from the threshold effect. When the actual channel SNR1 is worse than the designed SNRd, the index cannot be decoded and therefore the distortion drastically increases. When the actual channel SNR1 is better than the designed SNRd, the distortion is limited by the quantisation and does not improve. Thus, the distortion exponent of the separation-based scheme is $\zeta = 0$. Our proposed secure hybrid digital–analogue schemes, however, offer better performance in the presence of SNR1 mismatch.

5.1 Performance analysis of scheme 1

Let us consider the proposed scheme 1, which is designed for a SNRd while actual SNR is SNR1 > SNRd > SNR2. The receiver can estimate the actual noise power $N_1$. Since the receiver knows that the system is designed for SNRd,
the receiver estimates \( \hat{V} \) as follows
\[
\hat{V} = \lambda_{1d}Y + \lambda_{2d}U
\] (71)
where \( \lambda_{1d} \) and \( \lambda_{2d} \) are given in (40) and (41), respectively, when \((\alpha, k)\) are set as follows
\[
\alpha_d = \frac{P}{P + N_d}, \quad k_d^2 = \frac{P^2}{\sigma_d^2(P + N_d)}
\] (72)

The received signal is \( Y = X + S + W \), where \( W \sim N(0, N_1) \). The actual \( U \) is set by the transmitter as follows
\[
U = X + \alpha_d S + k_d V
\] (73)
The actual distortion is therefore given by
\[
D_d(\text{SNR}_1) = \frac{\sigma_d^2 (Q N_d^2 + (P + Q) + 2P N_d + N_d^2) N_1}{M}
\] (74)
where
\[
M = P^2 (P + Q) + (P + Q) N_d + Q N_d^2
\]
\[
+ (2P + Q) + 3P N_d + N_d^2 N_1
\] (75)

A useful measure for the robustness of a single coding scheme is the rate of the decay of the distortion as a function of the actual SNR \( \text{SNR}_1 \) when SNR \( \rightarrow \infty \) [see (6)]. An upper bound on the achievable \( \zeta \) can be obtained by assuming that a genie informs the transmitter of the actual SNR, and the transmitter chooses an optimum encoding scheme based on the actual SNR. The distortion for the genie-aided scheme is \( D = \frac{\sigma_d^2}{1 + \text{SNR}_1} \). Thus, the distortion exponent is \( \zeta = 1 \). Note that in the absence of any side information the distortion exponent of the genie-aided scheme is \( \zeta = 1 \). Also, in the absence of the eavesdropper, the distortion exponent is \( \zeta = 1 \). Therefore for any single encoding scheme, \( \zeta \leq 1 \).

From (6), the distortion exponent is given by
\[
\zeta = \lim_{\text{SNR}_1 \to \infty} \frac{\log D_d(\text{SNR}_1)}{\log \text{SNR}_1}
\] (76)

5.1.1 Absence of interference: When there is no interference at the transmitter, that is, \( Q = 0 \). We can see from (74) and (76) that \( \zeta = 1 \). Therefore scheme 1 achieves the optimum distortion \( D_{\text{opt}} \) as well as the optimum distortion exponent \( \zeta = 1 \).

5.1.2 Presence of interference: In the presence of interference, that is, \( Q \neq 0 \), we can see that \( \zeta = 0 \). This is because some residual interference exists in the received signal \( Y \), and therefore in high SNR, the distortion exponent is dominated by this residual interference. However, if optimal distortion is not desired at SNR \( \text{SNR}_1 \), we can achieve the optimum distortion exponent of \( \zeta = 1 \) by using a minor modification in scheme 1. Let us modify the auxiliary random variable \( U \) in scheme 1 as follows
\[
U = X + S + k' V
\] (77)
In this modified scheme, \( \alpha \) is chosen to be 1, which is not an optimum choice for SNR \( \text{SNR}_d \). According to the valid region of Fig. 3, the value of \( k' \) must be such that
\[
\sqrt{P^2 + PQ - Q N_d} < k' < \sqrt{P^2 + PQ - Q N_1}
\] (78)
Hence, \( k' \) can be chosen to be arbitrarily close to \( \sqrt{((P^2 + PQ - Q N_1))/\sigma_d^2(P + Q + N_1))} \). Now \( X \) is transmitted and the received signal by the legitimate receiver is \( Y \). Using an MMSE estimate for \( V \), the final distortion for an actual SNR \( \text{SNR}_1 \) when the system designed for SNR \( \text{SNR}_d \) is given by
\[
D_d(\text{SNR}_1) = \frac{\sigma_d^2 (P + Q) N_1}{(P + Q) N_1 + k_d^2 \sigma_d^2 (P + Q + N_1)}
\] (79)
where
\[
k_d' = \sqrt{P^2 + PQ - Q N_d}/\sigma_d^2 (P + Q + N_1)
\] Hence, for SNR \( \text{SNR}_1 \to \infty \), the distortion exponent is \( \zeta = 1 \). Fig. 6 shows the distortion of different schemes against SNR \( \text{SNR}_1 \). In this figure \( P = 0.7, Q = 2, \text{SNR}_d = 20 \text{ dB}, N_2 = 1, \sigma_2^2 = 1 \) and the quantisation rate is \( R = 1 \).

5.2 Performance analysis of Scheme 2

Let us consider the proposed Scheme 2, in this section. Again, we assume that the scheme is designed for SNR \( \text{SNR}_d \), but the actual is SNR \( \text{SNR}_d > \text{SNR}_d \) > SNR \( \text{SNR}_d \). Scheme 2 consists of two parts, namely secure digital part and secure hybrid digital–anologue part. The performance of the digital part remains constant by increasing the SNR \( \text{SNR}_d \). Thus, performance analysis of this scheme is exactly the same as scheme 1, when we replace \( \sigma_e^2 \) and \( P \) with \( \sigma_2^2 = \sigma_e^2 2^{-2k} \) and \( (P + N_d)2^{-2k} = N_d \), respectively.

5.3 Performance analysis of Scheme 3

Next, we analyse the performance of the secure hybrid digital–anologue of Scheme 3 under the main channel mismatch. The different random variables of this scheme
are given below
\[ U_d = X + \alpha_d S + k_d E \]
\[ Y = X + S + W \]
\[ V = V^* + E \] (80)

where
\[ \alpha_d = \frac{P}{P + N_d}, \quad k_d = P \left( \frac{P + \eta - N_d 2^{2R}}{\sigma_i^2 (P + N_d)} \right) \]

The receiver makes an MMSE estimate for \( V \) as follows
\[ \hat{V} = (\lambda_1d, \lambda_2d, \lambda_3d)(V^*, U_d, Y)^T \] (81)

where \((\lambda_1d, \lambda_2d, \lambda_3d)^T = A_d \Gamma_d\) and \( A_d \) and \( \Gamma_d \) are given in (68) and (69), respectively, when \((a, k)\) are replaced with \((\alpha_d, k_d)\). The actual distortion for the legitimate receiver can, therefore, be written as follows
\[ D_d(SNR_1) = \frac{\sigma_i^2}{\Gamma_d} \hat{V}^T A_d \hat{V} - \frac{1}{\Gamma_d} \]

After some math, the actual distortion is given by
\[ D_d(SNR_1) = \frac{\sigma_i^2 (Q N_d^2 + (P(Q + P) + 2P N_d + N_d^2) N_d)}{(P + N_d)^2 (P + Q + N_d) - 2^{2R} (N_d - N_d) P (P + Q + N_d)} \] (82)

Note that here the actual distortion depends on the quantisation rate \( R \) and for a special case of \( R = 0 \), the above equation is equivalent to the equation of (74). Similar to the performance analysis of scheme 1, we can see that when \( Q = 0 \), this scheme achieves the optimum distortion exponent of \( \zeta = 1 \). When \( Q \neq 0 \), the distortion exponent is \( \zeta = 0 \). However, if the optimum distortion at SNR1 is not required, we can modify Scheme 3 by choosing \( a = 1 \) to achieve the optimum distortion exponent \( \zeta = 1 \). As the analysis for this case is straightforward and similar to the analysis of scheme 1, we, therefore, omit it here.

6 Conclusion

In this work, we considered secure joint source–channel coding schemes for transmitting an analogue source over a Gaussian wire-tap channel with known interference at the transmitter. We derived the distortion that the separation-based coding scheme can achieve. We then proposed a few classes of schemes that achieved the same distortion as of separation-based coding scheme. Our proposed schemes are based on Costa’s DPA scheme and Wyner’s wire-tap channel coding in which the analogue source or analogue quantisation error is not explicitly quantised and embedded in the transmitted signal. We analysed the performance of the proposed schemes under SNR mismatch. We showed that the proposed schemes can obtain a graceful degradation of distortion with SNR under secrecy constraint which allows a leakage rate of \( I_e \) to the eavesdropper. The cost of achieving an optimum distortion exponent and secrecy constraint, is to design a system that has higher distortion for a designed SNR. A possible future problem can be whether it is still possible to obtain the optimum distortion exponent under secrecy constraint when we enforce obtaining the lowest possible distortion for a design SNR. Another possible future work is to design the secure joint source–channel coding schemes for the source–channel bandwidth mismatch \( (\rho \neq 1) \).

7 Acknowledgment

This work was supported in part by an Ontario Research Fund (ORF) project entitled ‘Self-Powered Sensor Networks’.

8 References

