Secure Hybrid Digital-Analog Wyner-Ziv Coding

Ghadamali Bagherikaram, Konstantinos N. Plataniotis
The Edward S. Rogers Sr. Department of ECE, University of Toronto,
10 Kings College Road, Toronto, Ontario, Canada M5S 3G4
Emails: {gbagheri, kostas}@comm.utoronto.ca

Abstract—In this work, the problem of transmitting an i.i.d Gaussian source over an i.i.d Gaussian wiretap channel with an i.i.d Gaussian side information at the intended receiver is considered. The intended receiver is assumed to have a certain minimum SNR and the eavesdropper is assumed to have a strictly lower SNR compared to the intended receiver. The objective is minimizing the distortion of source reconstruction at the intended receiver. In this work, it is shown that the source-channel separation coding scheme is optimum in the sense of achieving the minimum distortion. A hybrid digital-analog Wyner-Ziv coding scheme is then proposed which achieve the minimum distortion. This secure joint source channel coding scheme is based on Wyner-Ziv coding scheme and wiretap channel coding scheme when the analog source is not explicitly quantized. The proposed secure hybrid digital-analog scheme is analyzed under the main channel SNR mismatch. It is proven that the proposed scheme can give a graceful degradation of distortion with SNR under SNR mismatch, i.e., when the actual SNR is larger than the designed SNR.

I. INTRODUCTION

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 [2] and [3] which have studied the wiretap channel, many extensions of the wiretap channel model have been considered from a perfect secrecy point of view (see e.g., [4]–[8]). Particularly, in [9], [10], the Gaussian wiretap channel of [11] is extended to the Gaussian wiretap channel with side information available at the transmitter.

All extensions of the wiretap channel model have considered communicating a discrete source with perfect secrecy constraint. In many applications, however, a bandlimited analog source needs to be transmitted on a bandlimited Gaussian wiretap channel with side information available at the receiver. 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: Quantize the analog source and then transmit the result discrete source by the digital secret wiretap channel coding 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” [12], [13]. 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 [14]. 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 [15]–[19].

In [17], several hybrid digital-analog joint source channel coding scheme are proposed for transmitting a Gaussian source over a (non-secure) Gaussian channel (without side information). The main idea in [17] for increasing robustness is to reduce the number of quantization intervals, and thereby increase the distance between the decision lines of the quantization levels. This will increase the distortion, however, to compensate the coarser representation, the quantization error is sent as an analog symbol using a linear coder (see also [20]). In [21], different coding schemes are analyzed for transmitting a Gaussian source over a Gaussian wiretap channel (without side information). For a fixed information leakage rate to the eavesdropper, [21] has shown that superimposing the secure digital signal with the analog (quantization error) part has better performance compared to the separation based scheme and the uncoded scheme. In [22], the problem of transmitting a Gaussian source over a (non-secure) Gaussian channel with side information (either at transmitter or at receiver) is studied. [22] has introduced several hybrid digital-analog forms of the Costa and Wyner-Ziv coding ( [23]) schemes. In [22], the results of [24] 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 the work of [25], we considered the problem of transmitting a Gaussian source over a secure Gaussian channel with side information available at the transmitter and proposed different secure joint source channel coding schemes based on the secret dirty paper coding and wiretap channel coding scheme.

In this paper, we consider the problem of transmitting an i.i.d Gaussian source over an i.i.d Gaussian wiretap channel with side information available at the intended receiver. 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 minimizing the distortion of source reconstruction at the intended receiver. We show that, here, like the Gaussian wiretap channel without side information, Shannon’s source-channel separation coding scheme is optimum in the sense of achieving the minimum distortion. We then propose a hybrid digital-analog secure joint source channel coding scheme which achieve the minimum distortion. Our coding scheme is based on the Wyner Ziv coding scheme and wiretap channel coding scheme when the analog source is not explicitly quantized. We will illustrate that this scheme achieves the optimum distortion. We analyze our secure hybrid digital-analog scheme under the main channel SNR mismatch. We will show that our proposed scheme can give a graceful degradation of distortion with SNR under SNR mismatch, i.e., when the actual SNR is larger than the designed SNR.

II. PRELIMINARIES AND RELATED WORKS

A. Notation

In this paper, random variables are denoted by capital letters (e.g. $X$) and their realizations 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 $P(x)$. Similarly, the function $P(x,y)$ represents the joint probability distribution function of the random variables $X$ and $Y$. The vectors will be written as $x^n = (x_1, x_2, ..., x_n)$, where subscripted letters denote the components and superscripted letters denote the vector. The notation $x^n_j$ denotes the vector $(x_i, x_{i+1}, ..., x_j)$ for $j \geq i$. A Gaussian Random variable $X$ with a mean of $\mu$ and variance of $\sigma^2$ is denoted by $X \sim \mathcal{N}(\mu, \sigma^2)$. The function $E[.]$ represents a statistical expectation. The function $I(X;Y)$ represents mutual information between random variables $X$ and $Y$ and $A^n_\epsilon$ denotes the set of strongly jointly typical sequences.

B. System Model And Problem Statement

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

Channel Model: The source is transmitted over an Additive White Gaussian Noise (AWGN) wiretap channel when the intended receiver has some side information about the source. The channel therefore is modeled as follows:

$$Y_i = X_i + W_i,$$

$$Z_i = X_i + W'_i,$$

$$V_i = \hat{V}_i + T_i,$$

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 $E[X_i^2] \leq P$, and $W_i \sim \mathcal{N}(0, N_1)$, $W'_i \sim \mathcal{N}(0, N_2)$, where $N_2 > N_1$. Furthermore, assume that $T_i$’s are a sequence of real i.i.d Gaussian random variables with zero mean and variance $\sigma^2$, i.e. $T_i \sim \mathcal{N}(0, \sigma^2_i)$. Here $V_i$ and $T_i$ are mutually independent Gaussian random variables. As the source, side information 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 wiretap channel with bandwidth $W_c(Hz)$. The equivalent discrete-time channel is used at a rate of $2W_c$ channel uses per second. The block diagram of the system is depicted in Fig.1.

Coding Scheme: The source samples are grouped into blocks of size $m$

$$V^m = (V_1, V_2, ..., V_m),$$

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

$$Y^n = X^n + W^n,$$

$$Z^n = X^n + W'_n,$$

where $X^n = f_n(V^n)$, $W^n \sim \mathcal{N}(0, N_1 I_n)$, $W'_n \sim \mathcal{N}(0, N_2 I_n)$, and $I_n$ is the $n \times n$ identity matrix. The decoder at the intended receiver is a mapping $g_n : \mathbb{R}^n \rightarrow \mathbb{R}^n$. The secrecy of the system is measured by the information leaked to the eavesdropper and is expressed as $I_e = \frac{1}{n} I(V^n; Z^n)$. Note that $I_e$ is 0 corresponds to perfect secrecy condition and implies that the eavesdropper obtains no information about the source. In this paper we consider the situation in which the leaked information is fixed, i.e., $I_e = \text{cte}$. The average squared-error distortion of the coding scheme at the intended receiver is given by

$$\tilde{D}_n(f_n, g_n, N_1, N_2) = \frac{1}{n} E[\|V^n - \hat{V}^n\|^2],$$

where $\hat{V}^n = g_n(Y^n)$. For the purpose of analysis, we will consider sequences of codes $(f_n, g_n)$, where $n$ is increasing. The asymptotic performance of the code is given by

$$\tilde{D}(N_1, N_2) = \lim_{n \rightarrow \infty} \tilde{D}_n(f_n, g_n, N_1, N_2).$$

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

Distortion Exponent: In practical scenarios, the transmitter usually does not have an exact knowledge of the actual $N_1$ but knows that $N_1 \geq N_{1a}$, where $N_{1a}$ is the actual noise variance corresponding to the actual $SNR_{1a} = \frac{P}{N_2}$. The eavesdropper channel is still a degraded version of the main channel and is assumed to have the lowest $SNR_2 < SNR_1 < SNR_{1a}$, where $SNR_2 = \frac{P}{N_2}$ and $SNR_1 = \frac{P}{N_1}$. The receiver is assumed to have a perfect estimate of $SNR_{1a}$, but the transmitter communicates at a lower designed $SNR_1$. In this scenario, we expect a graceful degradation of distortion $D(SNR_{1a})$ with $SNR_{1a}$ compared with $D(SNR_1)$ when the actual $SNR_{1a} > SNR_1$. Let us define the distortion exponent as follows:

**Definition 1:** For a fixed $SNR_2$, the distortion exponent of $D(SNR_{1a})$ is given by

$$\zeta \triangleq - \lim_{SNR_{1a} \to \infty} \frac{\log D(SNR_{1a})}{\log SNR_1}. \quad (5)$$

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 against the case of $SNR$ mismatch where we design the scheme to be optimal for a channel noise variance of $N_1$, but the actual noise variance is $N_{1a}$. In this paper, we propose a robust coding scheme which achieve the optimum mean-squared distortion and analyze it for $SNR$ mismatch. Before introducing our proposed scheme, we need to review some related works in this area.

C. Related Works

1) Digital Wiretap Channel: In a digital wiretap channel (without any side information $V'$), a digital message $M \in \{1, 2, ..., 2^{nC_s}\}$ is transmitted to the intended receiver while the eavesdropper is kept ignorant. Wyner in [2] characterized the secrecy capacity of this channel when the eavesdropper's channel is degraded with respect to the main channel. Csiszar et. al. in [3] considered the general wiretap 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 wiretap channel is given by

$$C_s = 2W_c \left[I(U; Y) - I(U; Z)\right], \quad (6)$$

where $U \rightarrow X \rightarrow Y Z$ forms a Markov chain. When the channels are AWGN, [11] has shown that the secrecy capacity is given by

$$C_s = W_c \left[\log \left(1 + \frac{P}{N_1}\right) - \log \left(1 + \frac{P}{N_2}\right)\right]. \quad (7)$$

Here, we briefly explain the coding scheme. We generate $2^{nI(U; Y)}$ Gaussian codewords $U^n$ and throw them uniformly at random into $2^{nC_s}$ bins. Each bin thus contains $2^{nI(U; Z)}$ codeword $U^n$. To encode the message $M \in \{1, 2, ..., 2^{nC_s}\}$ 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, i.e., $\lim_{n \to \infty} P_e(M \neq M) \to 0$. The information leakage is $\lim_{n \to \infty} \frac{1}{n} I(M; Z^n) = 0$.

2) Digital Wyner-Ziv Coding: Consider a (non-secure) source coding problem with side information known at the receiver. The rate distortion function with side information $R_{V'}(D)$ is defined as the minimum rate required to achieve distortion $D$ if the side information $V'$ is available to the decoder. Precisely, $R_{V'}(D)$ is the infimum of rates $R$ such that there exist maps in $f_{n} : \mathcal{V} \to \{1, ..., 2^{nR}\}$, and $g_{n} : \mathcal{V}' \times \{1, ..., 2^{nR}\} \to \mathcal{V}$ such that

$$\lim_{n \to \infty} \inf \sup Ed(V^n, g_{n}(V^n, f_{n}(V^n))) \leq D. \quad (8)$$

Wyner-Ziv coding scheme achieved the entire curve $R_{V'}(D)$ as in the following theorem.

**Theorem 1:** [2] \[ Rate distortion with side information \]
Let $(V, V')$ be drawn i.i.d. according to the joint distribution $p(v, v')$ and let $d(v^n, \hat{v}^n) = \frac{1}{n} \sum_{i=1}^{n} d(i, \hat{i})$ be given. The rate distortion function with side information is given by

$$R_{V'}(D) = \min_{p(u|v)} \min_{y} \left\{ I(U; V) - I(U; V') \right\} \quad (9)$$

where the minimization is over all functions $g : V' \times U \to \hat{V}$ and conditional probability mass functions $p(u|v), |U| \leq |V| + 1$, such that

$$\sum_{v} \sum_{u} \sum_{v'} p(u, v') p(u|v) d(v, g(v', u)) \leq D. \quad (10)$$

The function $g$ in the theorem corresponds to the decoding map that maps the encoded version of the $V$ symbols and the side information $V'$ to the output alphabet. We minimize over all conditional distributions on $U$ and functions $g$ such that the expected distortion for the joint distribution is less than $D$. Here, we briefly explain the Wyner-Ziv achievability scheme: Fix $p(u|v)$ and the function $g(u, v')$. Calculate $p(u) = \sum_{v} p(v) p(u|v)$.

**Codebook Generation:** Let $R_1 = I(V; U) + \epsilon$. Generate $2^{nR_1}$ i.i.d. codewords $U^n(s) \sim \prod_{i=1}^{n} p(u_i)$, and index them by $s \in \{1, 2, ..., 2^{nR_1}\}$. Let $R_2 = I(U; V) - I(U; V') + 5\epsilon$. Randomly assign the indices $s \in \{1, 2, ..., 2^{nR_1}\}$ to one of $2^{nR_2}$ bins using a uniform distribution over the bins. Let $B(i)$ denote the indices assigned to bin $i$. There are approximately $2^{n(R_1-R_2)}$ indices in each bin.

**Decoding:** The decoder looks for a $U^n(s)$ such that $s \in B(i)$ and $(U^n(s), V^n) \in A^n(\epsilon)$. If $s$ is not unique, it then calculates $V^n$, where $\hat{V}_i = f(U_i, V'_i)$. If it does not find any such $s$ or more than one such $s$, it sets $\hat{V}_i = \check{v}^n$, where $\check{v}^n$ is an arbitrary sequence in $V^n$. It does not matter which default sequence is used; it is shown that the probability of this event is small.
III. SEPARATION BASED SCHEME

In this section we consider the problem described in Fig. 1. We use a separation scheme with an optimum Wyner-Ziv code followed by an optimum channel code. We refer to this scheme as “secure digital Wyner-Ziv coding scheme”. We show that this scheme achieves the optimum possible distortion.

If we suppose that the side information $V$ is also available at the encode, the transmitter therefore requires to send the remaining information $T$. In [6] the rate distortion problem for Shannon cipher system is considered. It can be seen from Theorem 1 in [6] by setting $R_k = 0$, the Shannon cipher system reduces to the wiretap channel setup and the optimum distortion can be achieved by separate source coding followed by digital wiretap channel coding scheme. Therefore, for a fixed leaked information $I$, we first need to quantize the source $T^n$ to $T'_q$ at a rate $C_s + I_e = \frac{1}{2} \log \left(1 + \frac{P}{N_t} \right) - \frac{1}{2} \log \left(1 + \frac{P}{N_s} \right) + I_e$ and then transmit $V_q^n$. Thus, we can achieve the optimum distortion of

$$D^* = \sigma_t^2 2^{-2(C_s + I_e)}$$

In the problem of Fig.1, assume that a genie informs the transmitter about the side information $V$. Therefore, the above distortion is an upperbound for the problem of Fig.1, i.e., $D^*$ is the minimum possible value for distortion $D = E \left[|V - \hat{V}|^2 \right]$. We show that the same distortion can be achieved in the setup of Fig.1 by using the secure digital Wyner-Ziv coding scheme. The following theorem illustrates this result.

Theorem 2: In the problem of secure transmitting a discrete-time Gaussian analog source over a Gaussian wiretap channel with side information known at the intended decoder, a separation based scheme can achieve the optimum distortion of $D^*$.

Proof: The achievability scheme is secure digital Wyner-Ziv coding scheme. Let $U$ be an auxiliary random variable given by

$$U = \sqrt{\alpha} V + F,$$  (12)

where $F \sim N(0, D)$. We generate an $n$-length i.i.d Gaussian codebook $\mathcal{U}$ with $2^{n I(U;V)}$ codewords, where each component of a codeword is Gaussian with zero mean and variance $\alpha \sigma_v^2 + D$. We then evenly distribute them into $2^n R_{v'}(D)$ bins, where $R_{v'}(D) = I(U;V) - I(U;V')$. Let $i(u^n)$ be the index of the bin containing $u^n$. For each $v^n$, find a $u^n$ such that $(u^n, v^n)$ are strongly jointly typical, i.e., $(u^n, v^n) \in A_v^{\epsilon}(n)$. The index $i(u^n)$ is the Wyner-Ziv source coding index. The transmitter then encoded the index $i(u^n)$ using an optimal secure channel code of rate arbitrary close to $C_s$ and transmit it over the channel. The receiver decodes the index $i(u^n)$ with high probability. Next for the decoded $i(u^n)$ we look for an $u^n$ in the bin whose index is $i(u^n)$ such that $(u^n, v^n) \in A_v^{\epsilon}(n)$. We make an estimate for source $v^n$ from the decoded $u^n$ and $v^n$ as follows:

$$\hat{v}^n = \left( \lambda_1 \lambda_2 \right) \left( \begin{array}{c} u^n \\ v^n \end{array} \right),$$  (13)

where we need to determine $\lambda_1$ and $\lambda_2$ such that the distortion $D = E \{|v^n - \hat{v}^n|^2 \}$ is minimized. After some math, the optimum values for $\lambda_1$ and $\lambda_2$ are as follows:

$$\lambda_1 = \sqrt{\alpha}$$

(14)

$$\lambda_2 = 1 - \alpha,$$

(15)

and the related distortion is given by

$$D = (1 - \alpha) \sigma_t^2.$$  (16)

To calculate the coefficient $\alpha$, note that

$$R_{v'}(D) = I(U;V') - I(U;V')$$

$$= \frac{1}{2} \log \left(1 + \frac{\alpha \sigma_v^2}{D} \right) - \frac{1}{2} \log \left(1 + \frac{\alpha \sigma_t^2}{D} \right)$$

$$= \frac{1}{2} \log \left( \frac{D + \alpha \sigma_v^2}{\alpha \sigma_t^2 + \alpha \sigma_v^2 + D} \right)$$

$$= \frac{1}{2} \log \left( \frac{\alpha \sigma_t^2 + \sigma_v^2 + D}{D} \right).$$

where $(a)$ follows from the fact that $\sigma_v^2 = \sigma_{v'}^2 + \sigma_t^2$. According to the fact that $R_{v'}(D)$ must be equal to $C_s + I_e$ we have,

$$\alpha = \frac{D}{\sigma_t^2} \left[ 2^{2I_e} P + N_1 N_2 \right. \left. \frac{P + N_2}{P + N_2 N_1} \right].$$  (17)

From (15) and (17) the achieved distortion is given by

$$D = \frac{\sigma_t^2}{2^{2I_e} P + N_1 N_2 \frac{P + N_2}{P + N_2 N_1}} = D^*.$$  (18)

IV. SECURE HYBRID DIGITAL-ANALOG WYNER-ZIV CODING

In this section, we propose a secure joint source channel coding scheme that does not involve quantizing the source explicitly. We generate the auxiliary random variable $U$ as follows:

$$U = X + kV,$$  (19)

where $k$ is defined as $k^2 = \frac{1}{\sigma_t^2} \left[ \frac{P N_1}{P + N_2} 2^{2I_e} - \frac{P N_2}{P + N_1} \right]$ and $X \sim N(0, P)$.

Codebook Generation: We generate a random i.i.d codebook $\mathcal{U}$ with $2^{n I(U;V)}$ sequences, where the components of the codewords are zero mean Gaussian random variables with variance $P + k^2 \sigma_v^2$. We then distribute the generated codewords into $2^n R_{v'}$ bins. This codebook is shared between the encoder and the intended receiver’s decoder.

Encoding: For a given $v^n$ the transmitter finds $u^n$’s such that $(u^n, v^n)$ are strongly jointly typical, i.e., $(u^n, v^n) \in A_v^{\epsilon}(n)$. Transmitter randomly chooses one of $u^n$ and then sends $x^n = \sqrt{\alpha} v^n + F$. 

\[1164\]
\( u^n - kv^n \). This is possible with arbitrary high probability if \( R > I(U; V) - I(U; V') \).

**Decoding:** The intended receiver’s signal is \( y^n = x^n + u^n \). The intended decoder finds a \( u^n \) such that \( (u^n, y^n, u^n) \in \mathcal{A}^{(n)} \). A unique such \( u^n \) can be found with high probability if \( R < I(U; V'; Y) - I(U; Z) \). We next show that we can choose \( R \) to satisfy \( I(U; V) - I(U; V') < R < I(U; V'; Y) - I(U; Z) \). Equivalently, we show that with \( k^2 = \frac{1}{\sigma_t^2} \left[ \frac{P N_2}{P + N_2} 2^{2I_t} - \frac{P N_1}{P + N_1} \right] \), we have \( I(U; V) - I(U; V') < I(U; V'; Y) - I(U; Z) \). Note that after some manipulation

\[
I(U; V) - I(U; V') = \frac{1}{2} \log \left( \frac{P + k^2 \sigma^2_u}{P} \right) - \frac{1}{2} \log \left( \frac{P + k^2 \sigma^2_v}{P} \right),
\]

and

\[
I(U; V'; Y) - I(U; Z) = \frac{1}{2} \log \left( 1 + P \sigma^2_u \frac{N_2 - N_1}{\sigma_t^4 N_2 (P + N_1)} \right).
\]

It is easy to see that for \( k^2 = \frac{1}{\sigma_t^2} \left[ \frac{P N_2}{P + N_2} 2^{2I_t} - \frac{P N_1}{P + N_1} \right] \), always we have \( I(U; V) - I(U; V') < I(U; V'; Y) - I(U; Z) \). The intended decoder therefore can estimate the transmitted signal \( v^n \) from \( u^n, v^n, \) and \( y^n \) as follows:

\[
v = (\lambda_1 \lambda_2 \lambda_3) \begin{pmatrix} u^n \\ v^n \\ y^n \end{pmatrix},
\]

where \( (\lambda_1 \lambda_2 \lambda_3) \) are the coefficients of the linear MMSE estimate which minimize \( D = E \left[ \| V - \hat{V} \|^2 \right] \). After some math, the optimal choices for the coefficients the the related distortion given as

\[
\lambda_1 = -\frac{k \sigma^2_u}{k \sigma^2_t + P N_1},
\]

\[
\lambda_2 = -P k \sigma^2_u,\]

\[
\lambda_3 = k^2 \sigma^2_t (P + N_1) + P N_1
\]

\[
D = \frac{\sigma^2}{P + N_1 N_2 2^{2I_t}} \frac{PN_2}{P + N_2 N_1}.
\]

**V. SNR MISMATCH ANALYSIS**

In this section, we evaluate the performance of the above secure hybrid digital-analog Wyner-Ziv scheme for the case of SNR mismatch where we design the scheme to be optimal for a designed \( SNR_{1a} \); \( SNR_2 < SNR_{1b} < SNR_{1a} \), but the actual \( SNR \) is \( SNR_{1a} \). It is well known that separation based scheme suffers from a pronounced threshold effect; When the actual \( SNR \) is worse than the designed \( SNR \), the index cannot be decoded and when the actual \( SNR \) is better than the designed \( SNR \), the distortion is limited by quantization and therefore, the distortion dose not. We show that however our proposed secure joint source-channel coding scheme offer better performance in this situation.

Let us consider the secure joint source-channel coding scheme with side information the receiver, where \( N_{1a} < N_1 < N_2 \). The intended receiver can decode \( u^n \) when the \( SNR_{1a} \) is better than the designed \( SNR_1 \) and make an estimate of the source from the observations at the receiver. The various signals are as follows:

\[
U = X + kV
\]

\[
V = V' + T
\]

\[
Y = X + W_a
\]

\[
Z = X + W'.
\]

where \( k = \sqrt{\frac{1}{\sigma_t^2} \left[ \frac{P N_2}{P + N_2} 2^{2I_t} - \frac{P N_1}{P + N_1} \right] \} \). The intended receiver uses an optimal linear MMSE to estimate the transmitted signal \( V \) from the observations of \( [U, V', Y] \). Note that this receiver knows the exact value of \( N_{1a} \), but the transmitter chooses the parameter \( k \) based on designed \( N_1 \). Let \( \Lambda \) be the covariance matrix of \( (U, V', Y)^T \) and \( \Gamma \) be the correlation between \( V \) and \( (U, V', Y)^T \). Thus,

\[
\Lambda = \begin{pmatrix} P + k^2 \sigma^2_u & k(\sigma^2_v - \sigma^2_t) & P \\ k(\sigma^2_v - \sigma^2_t) & \sigma^2_v - \sigma^2_t & 0 \\ P & 0 & P + N_{1a} \end{pmatrix}
\]

and

\[
\Gamma = \begin{pmatrix} k \sigma^2_v & \sigma^2_v - \sigma^2_t & 0 \end{pmatrix}^T.
\]

The coefficients of the linear MMSE estimate are given by \( \Lambda^{-1} \Gamma \). After some math, the actual distortion is then given by

\[
D_a = \sigma^2_v - \Gamma^T \Lambda^{-1} \Gamma
\]

\[
= \sigma^2_v - k^2 \sigma^2_v \left( P + N_{1a} \right) + (\sigma^2_v - \sigma^2_t) \left( P + N_{1a} \right) + PN_{1a}
\]

\[
= \sigma^2_v \left( P + N_{1a} \right) + PN_{1a}
\]

\[
(a) = \frac{P N_2}{P + N_2} 2^{2I_t} - \frac{P N_1}{P + N_1} \left[ P + N_{1a} \right] + N_{1a}.
\]

where \((a)\) follows by substituting \( k \).

Fig. 2 Compares the performance of the secure hybrid coding scheme with the separation based scheme. In this figure, \( P = 10, SNR_{1a} = 10, SNR_2 = 7, 10 \leq SNR_{1a} \leq 50, P_e = 0, \) and \( \sigma^2_t = 5 \). As shown in this figure, our proposed hybrid Wyner-ziv scheme provides the optimum distortion when the transmitter has the exact value of the \( SNR_1 \) and is more robust against the \( SNR \) mismatch compared with digital Wyner-Ziv Coding scheme.

**VI. CONCLUSIONS**

we considered the problem of transmitting an i.i.d Gaussian source over an i.i.d Gaussian wiretap channel with side information available at the intended receiver. We showed that Shannon’s source-channel separation coding scheme is
optimum in the sense of achieving the minimum distortion. We then proposed a hybrid digital-analog secure joint source coding scheme which achieve the minimum distortion. Our coding scheme was based on the Wyner Ziv coding scheme and wiretap channel coding scheme when the analog source is not explicitly quantized. We analyzed our secure hybrid digital-analog scheme under the main channel SNR mismatch and showed that that our proposed scheme can give a graceful degradation of distortion with SNR under SNR mismatch, i.e., when the actual SNR is larger than the designed SNR.

REFERENCES


