Integrated Communication and Receiver Sensing with Security Constraints on Message and State

Mehrasa Ahmadipour, Michèle Wigger, Shlomo Shamai

2023 IEEE International Symposium on Information Theory (ISIT) | 978-1-6654-7554-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/ISIT54713.2023.10206763

Integrated Communication and Receiver Sensing with Security Constraints on Message and State

Mehrasa Ahmadipour*, Michèle Wigger†, Shlomo Shamai‡
*UMPA, ENS de Lyon, Email: mehrasa.ahmadipour@ens-lyon.fr
†LTCI Telecom Paris, IP Paris, 91120 Palaiseau, France, Email: michele.wigger@telecom-paris.fr
‡Technion, Haifa, Israel, Email: sshlomo@ee.technion.ac.il

***Abstract*—We study the state-dependent wiretap channel with non-causal channel state informations at the encoder in an integrated sensing and communications (ISAC) scenario. In this scenario, the transmitter communicates a message and a state sequence to a legitimate receiver while keeping the message and state-information secret from an external eavesdropper. This paper presents a new achievability result for this doubly-secret scenario, which recovers as special cases the best-known achievability results for the setups without security constraints or with only a security constraint on the message. The impact of the secrecy constraint (no secrecy-constraint, secrecy constraint only on the message, or on the message and the state) is analyzed at hand of a Gaussian-state and Gaussian-channel example.**

I. Introduction

Great scientific and technological efforts are currently being made to efficiently integrate sensing and communication (ISAC) into common hardware and bandwidth [1]–[7]. This trend is driven by spectrum scarcity, the enlargement of the communication spectrum closer to the traditional radar spectrum, the conceptual similarity between the two tasks (emitting specific waveforms and detecting parameters based on received signals), as well as economic pressure to reduce hardware costs. Radar systems can be divided into two families: *mono-static radar* where the same terminal emits the waveform and senses the environment based on the backscattered signal and *bi-static radar* where the sensing terminal exploits the scattered signals emitted by other terminals. Information-theoretic works have considered both types of systems, where in the literature on mono-static radar [8]–[10] the radar receivers typically have to reconstruct the channel's state sequence with the smallest possible distortion, while in the literature on bi-static radar [11]–[14] they aim to determine an underlying binary (or multi-valued) parameter with largest possible error exponent. This latter scenario has even been investigated for classical-quantum channels [15].

In this work, we consider an ISAC problem with bi-static sensing, where the sensing terminal coincides with the receiver of the data communication, see Figure 1. The receiver thus not only decodes the transmitted signal but also reconstructs the channel state-sequence up to a given distortion. We assume that the transmitter knows this state-sequence S^n perfectly and in advance (as in the famous Gel'fand-Pinsker [16] or dirty-paper setups [17]) and can thus actively help the receiver in his estimation. Bounds on the optimal rate-distortion tradeoff of the described setup have been derived in [18]–[20]. In the present work, we impose the additional security constraints that the transmitted message and part of the state S^n have to be kept secret from an external eavesdropper. In this sense, our model is an extension of the models in [18]–[20] but with an external eavesdropper that is not allowed to learn the message or the state. It can also be considered an extension of the wiretap channel with non-causal state-information [21] to include the sensing performance and the secrecy constraint on the state. The intriguing feature in our model is that the transmitter should describe the state to the legitimate receiver, but mask [22] it from the eavesdropper.

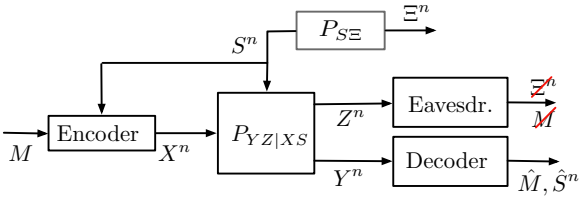

Fig. 1. State-dependent wiretap channel with non-causal channel state information at the transmitter and security constraints on the message and the state.

II. System Model

Formally, the model consists of the following elements.

- An independent and identically distriubuted (i.i.d.) state sequence $\{S_i\}_{i\geq 1}$ distributed according to the probability mass function (pmf) P_S over the finite state alphabet $\mathcal{S}$.
- Given that at time-i the Tx sends input $X_i = x$ and given state realization $S_i = s_i$, the Rx observes the time-i output Y_i and the eavesdropper observes signal Z_i distributed according to the stationary channel transition law $P_{YZ|SX}(\cdot,\cdot|s,x)$,
- Input and output alphabets $\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \mathcal{S}$ are assumed finite.

A rate-R_M and blocklength-n code consists of:

1) A message set $\mathcal{M}_n \stackrel{\triangle}{=} \{1, 2, \cdots, 2^{nR_M}\}$;
2) An encoder assigning codeword $x^n(m, s^n) \in \mathcal{X}^n$ to each $m \in \mathcal{M}_n$ and $s^n \in \mathcal{S}^n$;
3) A decoder that assigns a message estimate $\hat{m}$ and a state sequence estimate $\hat{s}^n \in \hat{\mathcal{S}}^n$ to each received sequence $y^n \in \mathcal{Y}^n$ where $\hat{\mathcal{S}}$ is a given reconstruction alphabet.
4) An encoding function: $f_n : \mathcal{M}_n \times \mathcal{S}^n \to \mathcal{X}^n$
5) A decoding function: $\phi_n : \mathcal{Y}^n \to \mathcal{M}_n$
6) A state estimator $\psi_n : \mathcal{Y}^n \to \hat{\mathcal{S}}^n$.

Message M is uniformly distributed over the message set so $P_M(m) = \frac{1}{2^{nR_M}}$. The probability of decoding error is:

$$P_e^{(n)} := \Pr\Big(\hat{M} \neq M\Big). \tag{1}$$

The fidelity of the state estimate at the Rx is measured by the expected distortion

$$\Delta^{(n)} := \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}[d_{\mathrm{R}}(S_i, \hat{S}_i)], \tag{2}$$

for a given bounded distortion function $d_{\mathrm{R}}(\cdot,\cdot)$.

The eavesdropper should not be able to learn a random sequence Ξ^n that is obtained by passing the state sequence S^n through a memoryless channel $P_{\Xi|S}$ independent of the message and the communication channel. The information leakage to the eavesdropper is measured by the mutual information

$$l_s^{(n)} \triangleq I(M, \Xi^n; Z^n). \tag{3}$$

Definition 1. *In the described setup, a rate-distortion pair* $(\mathsf{R}_M, \mathsf{D})$ *is called securely-achievable if there exists a sequence (in* n*) of rate-*R_M *and blocklength* n*-codes that simultaneously satisfy the three asymptotic constraints:*

$$\lim_{n\to\infty} P_e^{(n)} = 0 \tag{4a}$$

$$\lim_{n\to\infty} l_s^{(n)} = 0 \tag{4b}$$

$$\overline{\lim_{n\to\infty}}\, \Delta^{(n)} \leq \mathsf{D}. \tag{4c}$$

Remark 1. *Notice that Condition* (4b) *is equivalent to requiring that the sum of mutual informations* $I(M; Z^n)+I(\Xi^n; Z^n)$ *vanishes asymptotically as* $n \to \infty$.

III. Main Results

Our main result in Theorem 1 is based on the following coding idea. We employ a two-level superposition code with cloud-center codewords U^n and satellite codewords V^n. The transmitter uses the U^n-codewords to describe information about the state-sequence S^n to the receiver, where this cloud-center codeword can also be decoded by the eavesdropper. It further uses the V^n-codewords to send more refined information about S^n as well as the message M to the receiver. The receiver decodes both the U^n and V^n codewords so as to recover the transmitted message M. It also reconstructs the state-sequence based on the two decoded codewords and its own observed sequence of channel outputs. Security of the scheme against the external eavesdropper is obtained by choosing the U^n-codewords so that the decoded does not reveal information about the Ξ^n-sequence (because the U^n-codeword is also decoded by the eavesdropper). In fact, in our construction, only the V^n-codeword can contain information about Ξ^n and M, and they are chosen of sufficiently high rate so that the eavesdropper cannot decode them.

Theorem 1. *For any pmf* $P_{UVX|S}$ *so that for the associated tuple* $(S, \Xi, U, V, X, YZ) \sim P_S P_{\Xi|S} P_{UVX|S} P_{YZ|XS}$*, the random variable* Ξ *is independent of the pair* (U, Z)*,*

$$\Xi \perp (U, Z) \tag{5}$$

and any function $g(\cdot)$ *on appropriate domains, all pairs* (R_M, D) *satisfying the following inequalities*

$$R_M \leq I(U,V;Y) - I(U,V;S) \tag{6}$$

$$R_M \leq I(V;Y \mid U) - I(V;\Xi, Z \mid U) + \min\{0, I(U;Y) - I(U;S)\} \tag{7}$$

and

$$E[d(S, g(U,V,Y))] \leq D, \tag{8}$$

are securely achievable.

Proof. Choose a conditional distribution $P_{XUV|S}$ over $\mathcal{X} \times \mathcal{U} \times \mathcal{V}$ for auxiliary alphabets $\mathcal{U}$ and $\mathcal{V}$, and a reconstruction function $g\colon \mathcal{U} \times \mathcal{V} \times \mathcal{Y} \to \mathbb{R}_0^+$ so that for the tuple $(S, \Xi, U, V, X, Y, Z) \sim P_S P_{\Xi|S} P_{XUV|S} P_{YZ|XS}$ the random variable Ξ is independent of the pair (U, Z):

$$\Xi \perp (U, Z) \tag{9}$$

and the distortion constraint is satisfied:

$$\mathbb{E}[d_{\mathrm{R}}(S, g(U,V,Y))] \leq D_{\mathrm{R}}. \tag{10}$$

Fix a small number $\epsilon > 0$ and a large blocklength n. Pick auxiliary rates R_I, and R_J satisfying

$$R_I \geq I(U;S) \tag{11a}$$

$$R_I + R_J \geq I(UV;S) \tag{11b}$$

$$R_J \geq I(V;\Xi, Z|U) \tag{11c}$$

Construct a superposition code as follows.

- A lower-level code $\mathcal{C}_U$ consisting of 2^{nR_I} codewords $\{u^n(i)\}$ is constructed by drawing all entries i.i.d. according to the marginal pmf P_U of
$$P_{SUVXYZ} = P_S P_{XUV|S} P_{YZ|XS}. \tag{12}$$
- An upper-level code $\mathcal{C}_V(i)$ consisting of $2^{n(R_J+R_M)}$ codewords $\{v^n(m, j \mid i)\}$ is constructed for each $i \in [2^{nR_I}]$, by drawing the t-th entry of each codeword according to $P_{V|U}(\cdot \mid u_t(i))$ where $u_t(i)$ denotes the t-th entry of codeword $u^n(i)$.

The realization of the codebook is revealed to all parties.

The transmitter applies a likelihood encoder. That means, based on the state-sequence $S^n = s^n$ that it observes and the message $M = m$ that it wishes to convey, it randomly picks the indices (I^*, J^*) according to the conditional pmf

$$P_{\mathrm{LE}}(i, j \mid m, s^n) = \frac{P_{S|UV}(s^n|u^n(i), v^n(m, j \mid i))}{\sum\limits_{i\in[2^{nR_I}]}\sum\limits_{j\in[2^{nR_J}]} P_{S|UV}(s^n|u^n(i), v^n(m, j \mid i))}. \tag{13}$$

It then generates the random input sequence X^n by passing the pair of codewords $u^n(I^*)$ and $v^n(m, J^* \mid I^*)$ and the state sequence s^n through the memoryless channel $P_{X|UVS}$.

The receiver observes the channel outputs $Y^n = y^n$ and looks for a triple $(\hat{\imath}, \hat{\jmath}, \hat{m})$ so that

$$(u^n(\hat{\imath}),\ v^n(\hat{m}, \hat{\jmath}|\hat{\imath}),\ y^n) \in \mathcal{T}_\epsilon^{(n)}(P_{UVY}). \tag{14}$$

It randomly picks one of these triples and sets $(\hat{I}, \hat{J}, \hat{M}) = (\hat{i}, \hat{j}, \hat{m})$. Then it declares $\hat{M}$ as the transmitted message, and produces the state reconstruction sequence

$$\hat{S}^n = g^{\otimes n}(u^n(\hat{I}),\ v^n(\hat{M}, \hat{J} \mid \hat{I}),\ y^n). \tag{15}$$

If no triple was found, the receiver declares an error. Our scheme is analyzed in Section IV. □

Notice that when the entire state S has to be kept secret, $\Xi = S$, then U has to be chosen independently of S and thus $I(U;S) = 0$ and the minimum in the right-hand side of (7) evaluates to 0. Moreover, for $\Xi = S$ the right-hand side of (6) is larger than the right-hand side of (7) because $I(V;S,Z \mid U) \geq I(V;S \mid U)$. Thus, for $\nu(S) = S$, Constraint (6) is less stringent than Constraint (7) and we obtain the following corollary, after observing that U only plays the role of a convexification random variable.

Corollary 2 (Fully-Secret State)**.** *Assume $\Xi = S$. Then the convex hull of all rate-distortion pairs (R_M, D) is achievable that satisfy the constraints*

$$R_M \leq I(V;Y) - I(V;S,Z) \tag{16}$$

and

$$E[d(S, g(V,Y))] \leq D, \tag{17}$$

for some function $g(\cdot)$ on appropriate domains and pmf $P_{VX|S}$ where the associated tuple $(S, \Xi, V, X, YZ) \sim P_S P_{\Xi|S} P_{VX|S} P_{YZ|XS}$ has S independent of Z,

$$S \perp Z. \tag{18}$$

On the other extreme, we might only wish to keep the message secret but not the state, i.e. $\Xi =$const. In this case, Theorem 1 simplifies to (see the long version [23]):

Corollary 3 (No Secrecy Constraint on State)**.** *Assume $\Xi =$const. For any pmf $P_{UVX|S}$ and any function $g(\cdot)$ on appropriate domains, all pairs (R_M, D) satisfying*

$$\begin{aligned} R_M \leq \min\{&I(U,V;Y) - I(U,V;S), \\ &I(V;Y \mid U) - I(V;Z \mid U)\} \end{aligned} \tag{19}$$

and

$$E[d(S, g(U,V,Y))] \leq D, \tag{20}$$

are securely achievable rate-distortion pairs. It suffices to consider pmfs $P_{UVX|S}$ so that $I(U;Y) \geq I(U;S)$.

Notice that for sufficiently large distortion constraints D, Corollary 3 recovers the achievability result for the state-dependent wiretap channel with non-causal state-information at the encoder [21, Theorem 1].

Finally, we consider the special case where Z is independent of the input-state pair (X, S), which corresponds to the setup without secrecy constraint studied in [24]. In this special case, Theorem 1 can be simplified by choosing $U =$const., in which case Corollary 3 evaluates to:

Corollary 4 (No Eavesdropper, coincides with Theorem 1 in [24])**.** *Assume that Z is independent of the input-state pair (X, S). Then, for any pmf $P_{VX|S}$ and any function $g(\cdot)$ on appropriate domains, all non-negative rate-distortion pairs (R_M, D) are achievable that satisfy*

$$R_M \leq I(V;Y) - I(V;S) \tag{21}$$

and

$$E[d(S, g(V,Y))] \leq D. \tag{22}$$

Comparing Corollary 2 where both message and state have to be kept secret with Corollary 4 where no secrecy constraint is applied, we see that the price for achievable double state-and-message secrecy in our scheme is that S has to be independent of Z and that the rate has to be reduced by the mutual information quantity $I(V;Z|S) = I(SV;Z)$.

A. A Gaussian Example

Consider Gaussian channels both to the legitimate receiver

$$Y_i = X_i + S_i + N_i, \tag{23}$$

and to the eavesdropper

$$Z_i = aX_i + bS_i + N_{e,i}, \tag{24}$$

for given parameters $a = 0.7, b = 0.3$, where $\{S_i\}$ is an independently and identically distributed (i.i.d.) zero-mean Gaussian of power $Q = 3$ and the noise sequences are also i.i.d. zero-mean Gaussian of variances $\sigma^2 = 1$ and $\sigma_e^2 = 4$ and independent of each other and of the inputs and the states. The channel inputs are average blockpower constrained to power $P = 30$. Also, assume that

$$\Xi = S + A, \tag{25}$$

for A a zero-mean Gaussian random variable independent of all other random variables and of variance $\sigma_A^2 \geq 0$. This setup covers the scenario where the entire state-sequence has to be kept secret, with the choice $\sigma_A^2 = 0$. and (with a slight abuse of notation) the scenario where the state does not have be be kept secret at all, with the choice $\sigma_A^2 \to \infty$.

We use the squared error $d(s, \hat{s}) = (s - \hat{s})^2$ to measure the distortion at the receiver.

We shall numerically compare the achievability results in Corollaries 2, 3, 4 for this Gaussian example, to quantify the rate-penalty imposed by the various secrecy-constraints. To this end, we choose the following Gaussian auxiliaries:

$$U = F + \delta S + G \tag{26a}$$

$$V = T + \alpha S + G \tag{26b}$$

$$X = T + F + \epsilon G + \gamma S, \tag{26c}$$

where T, F, and G Gaussian random variable independent each of other and of the state S, and of variances $\sigma_T^2, \sigma_F^2 \geq 0$ so that $\sigma_T^2 + \sigma_F^2 + \epsilon^2 \sigma_G^2 + \gamma^2 Q \leq P$. Notice that for $\Xi = S$ we are obliged to choose $\gamma = -\frac{b}{a}$ to ensure that Z is independent of S. In this case, we can also choose U to be constant (i.e., F, G constants and $\delta = 0$), see Corollary 2.

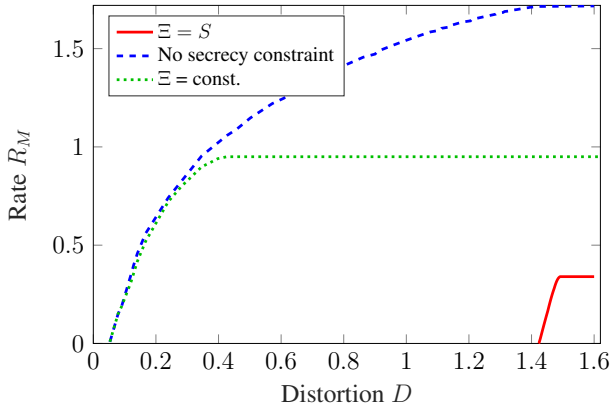

Fig. 2. Comparison of the achievable rate-distortion tradeoffs for a Gaussian channel with security constraints on both the message and the state and no security constraints at all.

Figure 2 illustrates the distortion-rate tradeoffs achieved by our Corollaries 2, 3, 4 for the described choice of auxiliaries. Notice that without any secrecy constraint, in the Gaussian case the achievability result in Corollary 4 is tight, as shown in [18]. The largest achievable rate equals the dirty-paper capacity [17] of the channel to the legitimate receiver $C = 1/2\log(1+P/\sigma_N^2) = 1.717$. In this no-secrecy setup the minimum distortion is achieved by simply sending a scaled version of the channel and equals

$$D_{\text{min,no-secrecy}} = Q\frac{\sigma_N^2}{(\sqrt{Q}+\sqrt{P})^2+\sigma_N^2} = 0.056. \tag{27}$$

Trivially, the same minimum distortion is also achievable in the classical wiretap setup where only the message but not the state have to be kept secret.

Finding the minimum distortion under a secrecy constraint on the state is more challenging, the same as finding the maximum rate when the message has to be kept secret (both in the scenarios with and without secrecy constraint on the state). We can however easily deduce that the minimum distortion under a secrecy constraint on the state cannot be achieved by an uncoded strategy. In fact, sending $X^n = -\frac{b}{a}S^n$ without any additional codeword (recall that the transmit signal X has to subtract the term $\frac{b}{a}S^n$ so as to keep the state S^n secret from the eavesdropper) achieves distortion

$$D_{\text{min,uncoded,secret}} = Q\frac{\sigma_N^2}{Q\left(1-\frac{b}{a}\right)^2+\sigma_N^2} = 1.516, \tag{28}$$

which exceeds the minimum distortion 1.423 achieved by Theorem 1 (see the red line in Figure 2) under the fully-secret state criterion $\Xi = S$ and with the auxiliaries in (26).

IV. Proof of Theorem 1: Analysis

1) Distortion and Error Probability: The encoding procedure is described in Fig. 3. We shall prove that the joint pmf $P_{MIJU^nV^nS^nX^nY^nZ^n}$ in this model is close in variational distance to an auxiliary distribution $\tilde{P}_{MIJU^nV^nS^nX^nY^nZ^n\hat{S}^n}$ implied by the diagramme in Fig. 4, where the the indices I and J are uniform over the sets $\{1,\dots,2^{nR_I}\}$ and $\{1,\dots,2^{nR_J}\}$, independent of each other and of the state sequence S^n and message M.

Notice that the joint pmfs $P_{MIJU^nV^nS^nX^nY^nZ^n\hat{S}^n}$ and $\tilde{P}_{MIJU^nV^nS^nX^nY^nZ^n\hat{S}^n}$ factorize in a similar way:

$$\begin{aligned}&P_{MIJU^nV^nS^nX^nY^nZ^n\hat{S}^n}(m,i,j,u^n,v^n,s^nx^n,y^n,z^n,\hat{s}^n)\\&=\frac{1}{2^{nR}}P_S^{\otimes n}(s^n)P_{\text{LE}}(i,j\mid m,s^n)\mathbb{1}\{u^n(i)=u^n\}\\&\cdot\mathbb{1}\{v^n(m,j\mid i)=v^n\}\cdot P_{XYZ|UVS}^{\otimes n}(x^n,y^n,z^n|u^n,v^n,s^n)\\&\qquad\mathbb{1}\{\hat{s}^n=g^{\otimes n}(u^n,v^n,y^n)\}\end{aligned} \tag{29}$$

where P_{LE} denotes the conditional marginal distribution induced by the likelihood encoder, and

$$\begin{aligned}&\tilde{P}_{MIJU^nV^nS^nX^nY^nZ^n}(m,i,j,u^n,v^n,s^n,x^n,y^n,z^n)=\\&\frac{1}{2^{n(R_M+R_I+R_J)}}\mathbb{1}\{u^n(i)=u^n\}\mathbb{1}\{v^n(m,j\mid i)=v^n\}\\&\cdot P_{S|UV}^{\otimes n}(s^n|u^n,v^n)P_{XYZ|UVS}^{\otimes n}(x^n,y^n,z^n\mid u^n,v^n,s^n)\\&\qquad\cdot\mathbb{1}\{\hat{s}^n=g^{\otimes n}(u^n,v^n,y^n)\}.\end{aligned} \tag{30}$$

By standard typicality arguments, if

$$R_I+R_J+R_M<I(U,V;Y) \tag{31a}$$
$$R_J+R_M<I(V;Y|U). \tag{31b}$$

the expected (over the random choice of the codebooks) probability of wrongly decoding indices (M,I,J) tends to 0 as $n\to\infty$. In fact, for any $M=m$, we have that

$$\mathbb{E}\left[p(\text{error}|M=m)\right]\to 0 \qquad \text{as } n\to\infty, \tag{32}$$

where expectation is with respect to the random codebook and

$$p(\text{error}|M=m) := \Pr\left[\hat{I}=I \text{ or } \hat{J}=J\middle|M=m\right]. \tag{33}$$

We now introduce the ideal system in Figure 5. It only differs from the system in Figure 4 in that error-free decoding is assumed. Notice that since under $\tilde{P}$ the decoding error probability vanishes as $n\to\infty$, we have:

$$\begin{aligned}&\mathbb{E}\Big[\Big\|Q_{MIJU^nV^nS^nX^nY^nZ^n\hat{S}^n}\\&\qquad-\tilde{P}_{MIJU^nV^nS^nX^nY^nZ^n\hat{S}^n}\Big\|_1\Big]\to 0,\end{aligned} \tag{34}$$

where expectation is over the random choice of the codebooks. By the boundedness of the distortion function, thus:

$$\lim_{n\to\infty}\mathbb{E}\left[\Delta^{(n)}\right] = d_{\text{R}}(S,g(U,V,Y)) \le D_{\text{R}}, \tag{35}$$

where $(U,V,S,Y)\sim P_{UV}P_{S|UV}P_{Y|UVS}$ and the last two equalities hold by the construction of the auxiliary system and by the choice of the auxiliary random variables.

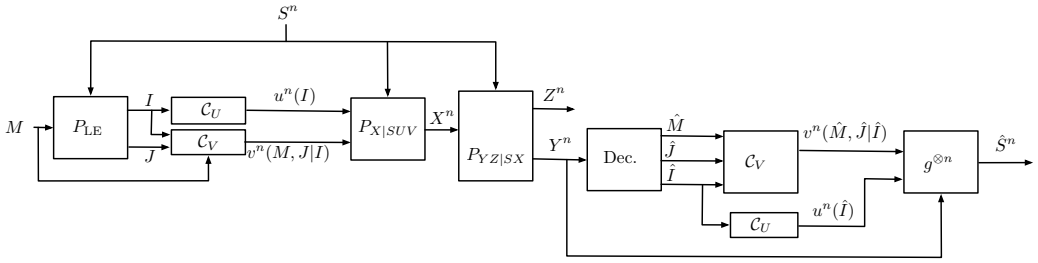

Fig. 3. Real system inducing distribution $P_{MIJU^nV^nS^nX^nY^nZ^n\hat{S}^n}$.

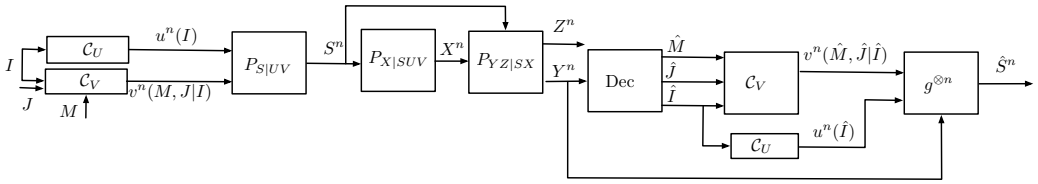

Fig. 4. Auxiliary System inducing distribution $\tilde{P}_{MIJU^nV^nS^nX^nY^nZ^n\hat{S}^n}$.

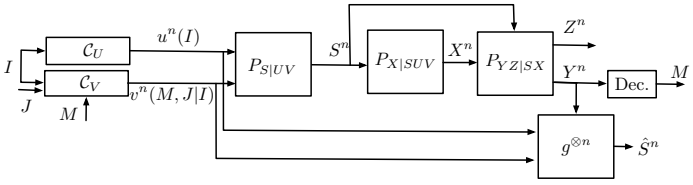

Fig. 5. Ideal System inducing distribution $Q_{MIJU^nV^nS^nX^nY^nZ^n\hat{S}^n}$.

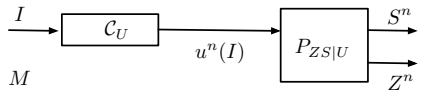

Fig. 6. Ideal system used for secrecy analysis, inducing joint pmf $\bar{Q}_{MIU^n\xi(S^n)Z^n}$.

2) Secrecy Analysis: Consider the system in Figure 6, implying distribution

$$\bar{Q}_{MIU^n\xi(S^n)Z^n}(m,i,u^n,\zeta^n,z^n) = \frac{1}{2^{nR_M}}\frac{1}{2^{nR_I}}\mathbb{1}\{u^n(i)=u^n\}P^{\otimes n}_{\nu(S)Z|U}(\zeta^n,z^n|u^n). \quad (36)$$

In this idealized secrecy system and for any choice of the codebook $\mathcal{C}_U$, the pair (M,Ξ^n) is independent of (U^n,Z^n) and $I_{\bar{Q}}(M,\Xi^n;u^n(I),Z^n)=0$.

Notice next that by the generalized superposition soft-covering lemma [25] and by choosing

$$R_J > I(V;\nu(S),Z|U), \quad (37)$$

the distribution $\bar{Q}_{MIU^n\xi(S^n)Z^n}$ is close to $Q_{MIU^n\xi(S^n)Z^n}$,

$$\Pr\left[\bar{Q}_{MIU^n\xi(S^n)Z^n} - Q_{MIU^n\xi(S^n)Z^n}\|_1 \le e^{-n\gamma}\right] \ge 1-e^{-n\delta}, \qquad \forall m\in\mathcal{M}, \quad (38)$$

where probability is over the random choice of the codebook.

By arguments similar to [26, Appendix D] (which use the boundedness of the alphabets), it also holds that for any pair of codebooks $\mathcal{C}_U$ and $\mathcal{C}_V$ satisfying

$$\left\|P_{MIU^n\xi(S^n)Z^n} - \bar{Q}_{MIU^n\xi(S^n)Z^n}\right\| \le e^{-n\gamma}, \quad (39)$$

we have that

$$\left|I_P(M,\xi(S^n);Z^n) - I_{\bar{Q}}(M,\xi(S^n);Z^n)\right| \to 0 \qquad \text{as } n\to\infty.$$

Combined with $I_{\bar{Q}}(M,\Xi^n;u^n(I),Z^n)=0$ this establishes the desired secrecy requirement.

V. Conclusions and Discussion

We introduced the concept of securing state-information (besides the message) from an external eavesdropper in an ISAC scenario. Notice that such a setup nicely unifies the models for state-communication [20] and state-masking [22] into a single problem. Specifically, we proposed a coding scheme for a state-dependent wiretap channel where the receiver wishes to estimate the state with predefined distortion, and information about this state-sequence has to be kept secret from an external eavesdropper. At hand of a Gaussian example, we numerically show the influence of the various security constraints on our achievable rate-distortion region.

Acknowledgement

The work of S. Shamai has been supported by the European Union's Horizon 2020 Research And Innovation Programme, grant agreement no. 694630.

REFERENCES

[1] Z. Wei, H. Qu, Y. Wang, X. Yuan, H. Wu, Y. Du, K. Han, N. Zhang, and Z. Feng, "Integrated sensing and communication signals towards 5g-a and 6g: A survey," *IEEE Internet of Things Journal*.

[2] Y. Liu, M. Li, A. Liu, J. Lu, and T. X. Han, "Information-theoretic limits of integrated sensing and communication with correlated sensing and channel states for vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 9, pp. 10 161–10 166, 2022.

[3] A. Liu, Z. Huang, M. Li, Y. Wan, W. Li, T. X. Han, C. Liu, R. Du, D. K. P. Tan, J. Lu, Y. Shen, F. Colone, and K. Chetty, "A survey on fundamental limits of integrated sensing and communication," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 994–1034, 2022.

[4] O. Li, J. He, K. Zeng, Z. Yu, X. Du, Z. Zhou, Y. Liang, G. Wang, Y. Chen, P. Zhu, W. Tong, D. Lister, and L. Ibbetson, "Integrated sensing and communication in 6G: a prototype of high resolution multichannel THz sensing on portable device," *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, no. 1, p. 106, 2022.

[5] F. Liu, Y. Cui, C. Masouros, J. Xu, T. X. Han, Y. C. Eldar, and S. Buzzi, "Integrated sensing and communications: Toward dual-functional wireless networks for 6G and beyond," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 6, pp. 1728–1767, 2022.

[6] L. Zheng, M. Lops, Y. C. Eldar, and X. Wang, "Radar and communication coexistence: An overview: A review of recent methods," *IEEE Signal Processing Magazine*, vol. 36, no. 5, pp. 85–99, 2019.

[7] S. H. Dokhanchi, M. B. Shankar, M. Alaee-Kerahroodi, T. Stifter, and B. Ottersten, "Adaptive waveform design for automotive joint radar-communications system," in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*. IEEE, 2019, pp. 4280–4284.

[8] M. Kobayashi, G. Caire, and G. Kramer, "Joint state sensing and communication: Optimal tradeoff for a memoryless case," 2018, pp. 111–115.

[9] M. Ahmadipour, M. Kobayashi, M. Wigger, and G. Caire, "An information-theoretic approach to joint sensing and communication," *IEEE Transactions on Information Theory*, 2022.

[10] M. Ahmadipour, M. Wigger, and M. Kobayashi, in *Proc. 2022 IEEE International Symposium on Information Theory (ISIT)*.

[11] H. Wu and H. Joudeh, "Joint communication and channel discrimination," 2022. [Online]. Available: https://arxiv.org/abs/2208.07450

[12] H. Joudeh and F. M. J. Willems, "Joint communication and binary state detection," *IEEE Journal on Selected Areas in Information Theory*, vol. 3, no. 1, pp. 113–124, 2022.

[13] M.-C. Chang, S.-Y. Wang, T. Erdogan, and M. R. Bloch, "Rate and detection-error exponent tradeoff for joint communication and sensing of fixed channel states," 2022. [Online]. Available: https://arxiv.org/abs/2210.07963

[14] M. Ahmadipour, M. Wigger, and S. Shamai (Shitz), "Strong converses for memoryless bi-static ISAC," Jan. 2023. [Online]. Available: https://arxiv.org/abs/2303.06636

[15] S.-Y. Wang, T. Erdoğan, U. Pereg, and M. R. Bloch, "Joint quantum communication and sensing," in *Proc. 2022 IEEE Information Theory Workshop (ITW)*, 2022, pp. 506–511.

[16] S. I. Gelfand and M. S. Pinsker, "Coding for channel with random parameters," *Problem Control Inf. Theory*, vol. 9, no. 1, p. 19–31, 1980.

[17] M. Costa, "Writing on dirty paper (corresp.)," *IEEE Transactions on Information Theory*, vol. 29, no. 3, pp. 439–441, 1983.

[18] A. Sutivong, M. Chiang, T. Cover, and Y.-H. Kim, "Channel capacity and state estimation for state-dependent gaussian channels," *IEEE Transactions on Information Theory*, vol. 51, no. 4, pp. 1486–1495, 2005.

[19] W. Zhang, S. Vedantam, and U. Mitra, "Joint transmission and state estimation: A constrained channel coding approach," vol. 57, no. 10, pp. 7084–7095, 2011.

[20] C. Choudhuri and U. M. Ming, "On non-causal side information at the encoder," in *2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2012, pp. 648–655.

[21] Z. Goldfeld, P. Cuff, and H. H. Permuter, "Wiretap channels with random states non-causally available at the encoder," *IEEE Transactions on Information Theory*, vol. 66, no. 3, pp. 1497–1519, 2020.

[22] N. Merhav and S. Shamai, "Information rates subject to state masking," *IEEE Transactions on Information Theory*, vol. 53, no. 6, pp. 2254–2261, 2007.

[23] M. Ahmadipour, M. Wigger, and S. Shamai (Shitz), "Strong converses for memoryless bi-static ISAC," Jan. 2023.

[24] C. Choudhuri and U. M. Ming, "On non-causal side information at the encoder," in *2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2012, pp. 648–655.

[25] C. Schieler and P. Cuff, "Rate-distortion theory for secrecy systems," *IEEE Transactions on Information Theory*, vol. 60, no. 12, pp. 7584–7605, 2014.

[26] A. Bunin, Z. Goldfeld, H. H. Permuter, S. Shamai Shitz, P. Cuff, and P. Piantanida, "Semantically-secured message-key tradeoff over wiretap channels with random parameters," *https://arxiv.org/abs/1708.04283.v1*, 2017.