# Low-latency Secure Integrated Sensing and Communication with Transmitter Actions

Truman Welling[1], Onur Günlü[2], and Aylin Yener[1]
[1]Department of Electrical and Computer Engineering, The Ohio State University, USA
[2]Information Theory and Security Laboratory (ITSL), Linköping University, Sweden
welling.78@buckeyemail.osu.edu, onur.gunlu@liu.se, yener@ece.osu.edu

*Abstract*—This paper considers an information theoretic model of secure integrated sensing and communication, represented as a wiretap channel with action dependent states. This model allows one to secure a part of the transmitted message against a sensed target that eavesdrops the communication, while allowing transmitter actions to change the channel statistics. An exact secrecy-distortion region is given for a physically-degraded channel. Moreover, a finite-length achievability region is established for the model using an output statistics of random binning method, giving an achievable bound for low-latency applications.

*Index Terms*—integrated sensing and communication, wiretap channel, finite blocklength analysis

## I. INTRODUCTION

The importance of connectivity is increasing, in terms of both communication and sensing in applications such as self driving cars, giving natural rise to Integrated Sensing and Communication (ISAC) [1]. The integration of sensing and communication also allows for more efficient usage of bandwidth than independent sensing and communication [2]. This increase in efficiency introduces an inherent secrecy issue. If a target is sensed using an ISAC waveform, then the target has potentially observed the waveform, making the target also an eavesdropper.

Standard cryptographic methods are not a practical solution in all communication scenarios, such as Internet of Things (IoT) settings where the devices have few computing resources or are designed for low power consumption. In these cases, physical layer security is a potential alternative [3]. Recently, information theoretic models have been proposed to explore the theoretical limits of physical layer security for ISAC channels. In [4], an ISAC channel was modeled as a state-dependent broadcast channel with feedback. Physical layer security was explored for this model in [5]. A similar model characterizes the secrecy-distortion region for Rayleigh fading channels [6]. All of these models assume that the channel output feedback is available to the transmitter while encoding.

The secure ISAC model in [7] simplifies the model of [5] by using the feedback for state estimation but not encoding. The lack of dependence in encoding on feedback allows the model to meet low-latency requirements. Our model performs the same simplification on the model in [8], allowing us to find results relevant in a low-latency setting. Our contributions are an exact secrecy-distortion region and an inner bound on the finite blocklength secrecy-distortion region.

First, the specific theoretical model is introduced following which we establish the exact asymptotic secrecy distortion region for the physically-degraded ISAC channel with transmitter actions. We then analyze the finite blocklength performance using nonasymptotic output statistics of random binning (OSRB) method [9], [10] to derive an inner bound for the ISAC channel with transmitter actions.

## II. PROBLEM DEFINITION

Consider the channel model depicted in Figure 1, a state dependent broadcast channel with feedback, consisting of a transmitter who wants to communicate reliably with the legitimate receiver and sense a target while keeping part of the message secret from the target (thus also treating the target as an eavesdropper). The transmitter, observing a uniformly distributed message $M = (M_1, M_2) \in \mathcal{M} = \mathcal{M}_1 \times \mathcal{M}_2$ computes the action sequence $A^n = \mathsf{Enc}_{Act}(M) \in \mathcal{A}^n$ and the channel input sequence $X^n = \mathsf{Enc}(M, A^n) \in \mathcal{X}^n$ where $\mathsf{Enc}_{Act}(\cdot)$ and $\mathsf{Enc}(\cdot, \cdot)$ are (random) encoding functions for the action and channel inputs, respectively. The states are determined by nature according to $(S_1^n, S_2^n)|\{A^n = a^n\} \sim \prod_{i=1}^n P_{S_1 S_2 | A}(s_{1,i}, s_{2,i}|a_i)$. For each channel use $i \in [1 : n]$, $(X_i, S_{1,i}, S_{2,i})$ are inputs to the discrete memoryless channel $P_{Y_1 Y_2 | S_1 S_2 X}$ during which the legitimate receiver observes $Y_{1,i} \in \mathcal{Y}_1$ and $S_{1,i} \in \mathcal{S}_1$ and the target (eavesdropper) observes $Y_{2,i} \in \mathcal{Y}_2$ and $S_{2,i} \in \mathcal{S}_2$. After the $n^{th}$ transmission, the legitimate receiver forms an estimate $\widehat{M}$ of $M$ by $\widehat{M} = \mathsf{Dec}(Y_1^n, S_1^n)$ where $\mathsf{Dec}(\cdot, \cdot)$ is a decoding function. We denote the feedback to the transmitter by $Z_i \in \mathcal{Z}$. The sensing is abstracted as the estimates $(\widehat{S}_1^n, \widehat{S}_2^n)$ of the states, which is done with the estimators $\widehat{S}_j = \mathsf{Est}_j(A^n, X^n, Z^n) \in \widehat{\mathcal{S}}_j^n$ for $j = 1, 2$ where $\mathsf{Est}_j(\cdot, \cdot, \cdot)$ is an estimation function. All sets $\mathcal{A}, \mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2, \mathcal{S}_1, \mathcal{S}_2, \widehat{\mathcal{S}}_1, \widehat{\mathcal{S}}_2$ and $\mathcal{Z}$ are assumed to be finite.

To simplify the analysis, we assume that the transmitter feedback is noiseless channel feedback, i.e., $Z_i = (Y_{1,i}, Y_{2,i})$ for all $i \in [1 : n]$, which provides an outer bound for the performance of the noisy feedback scenario.

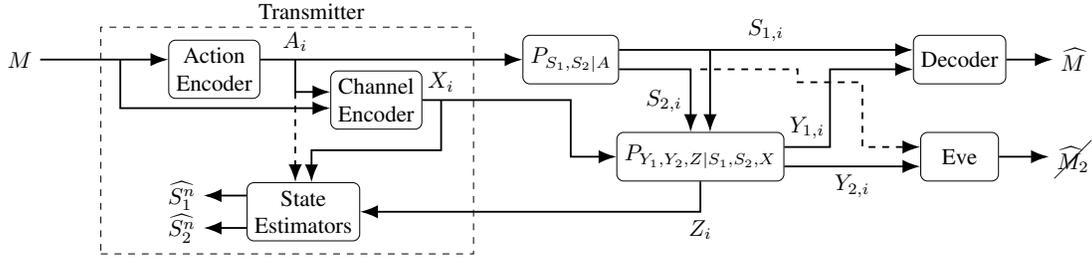Now we define physical degradation for an ISAC channel with transmitter actions.

Fig. 1. Secure ISAC model with transmitter action-dependent states under partial secrecy, where we have $M = (M_1, M_2)$ and only $M_2$ should be kept secret from Eve, for $i = [1:n]$. The channel input $X_i$ is a function of $(M, A_i)$.

*Definition 1:* An ISAC channel with transmitter actions as depicted in Fig.1 is *physically-degraded* if

$$P_{AXY_1Y_2S_1S_2} = P_{AX}P_{Y_1S_1Y_2S_2|AX}$$
$$= P_{AX}P_{S_1|A}P_{Y_1|S_1X}P_{Y_2S_2|S_1Y_1}. \quad (1)$$

$\diamond$

## III. ASYMPTOTIC PERFORMANCE LIMITS UNDER PARTIAL SECRECY

We first define an achievable tuple and the achievable secrecy distortion region.

*Definition 2:* Under partial secrecy, a secrecy-distortion tuple of the form $(R_1, R_2, D_1, D_2)$, with $\log|\mathcal{M}_j| = nR_j$ for $j = 1, 2$ is achievable if for any $\delta > 0$ there exists a channel encoder, action encoder, decoder, $n \geq 1$, and two state estimators $\widehat{S}_j^n = \mathsf{Est}_j(X^n, A^n, Z^n)$ such that

$$\Pr\left[(M_1, M_2) \neq (\widehat{M}_1, \widehat{M}_2)\right] \leq \delta \quad \text{(reliability)} \quad (2)$$
$$I(M_2; Y_2^n, S_2^n) \leq \delta \quad \text{(strong secrecy)} \quad (3)$$
$$\mathbb{E}\left[d_j(S_j^n, \widehat{S_j^n})\right] \leq D_j + \delta \quad \text{for } j = 1, 2 \quad \text{(distortion)} \quad (4)$$

and we have per letter distortion metrics $d_j(\widehat{s}_j^n, s_j^n) = \frac{1}{n}\sum_{i=1}^n d_j(\widehat{s}_{j,i}, s_{j,i})$ for $j = 1, 2$ that are bounded from above by some value $d_{\max}$. The secrecy-distortion region $\mathcal{R}_{PS,Act}$ is the closure of all achievable tuples under partial secrecy. $\diamond$

Now we give the asymptotic secrecy-distortion region for a physically-degraded ISAC channel.

*Theorem 1:* (Physically-degraded): For a physically-degraded ISAC channel, $\mathcal{R}_{PS,Act}$ is the union over all joint distributions $P_{VAX}$ of the rate tuples $(R_1, R_2, D_1, D_2)$ satisfying

$$R_1 + R_2 \leq I(V; Y_1, S_1) \quad (5)$$
$$R_2 \leq I(V; Y_1, S_1) - I(V; Y_2, S_2) \quad (6)$$
$$D_j \geq \mathbb{E}[d_j(S_j, \widehat{S}_j))] \quad \text{for } j = 1, 2 \quad (7)$$

where we have

$$P_{VAXY_1Y_2S_1S_2} = P_{V|AX}P_{AX}P_{S_1|A}P_{Y_1|S_1X}P_{Y_2S_2|S_1Y_1} \quad (8)$$

and one can use the deterministic per-letter estimators $\mathsf{Est}_j(a, x, y_1, y_2) = \widehat{s}_j$ for $j = 1, 2$ such that

$$\mathsf{Est}_j(a, x, y_1, y_2)$$
$$= \underset{\tilde{s}\in\widehat{\mathcal{S}}_j}{\arg\min} \sum_{s_j\in\mathcal{S}_j} P_{S_j|AXY_1Y_2}(s_j|a, x, y_1, y_2)\, d_j(s_j, \tilde{s}). \quad (9)$$

One can also bound $|\mathcal{V}|$ by

$$(|\mathcal{X}|\cdot|\mathcal{A}|+1). \quad (10)$$

$\diamond$

*Proof Sketch:* The cardinality bound follows from [11, Lemma 15.4], where $|\mathcal{X}|\cdot|\mathcal{A}|-1$, letters are needed to preserve $P_{XA}$ with two additional letters to preserve $I(V; Y_1, S_1)$ and $I(V; Y_2, S_2)$.

Achievability Proof: We use the OSRB method [9] for the achievability proof. To this end, we consider two problems, the channel coding problem assisted with shared randomness and the source coding problem that is operationally dual to the former. We find conditions for which the source coding protocol is reliable and secure, then we find conditions for which the probability distributions induced by the two protocols are arbitrarily close, providing a reliable, secure solution to the channel coding problem assisted with shared randomness. Finally, we remove the shared randomness by showing that the protocol remains secure and reliable for a specific realization of the shared randomness.

Fix $P_{VAX}(v, a, x)$ for which there exist per-letter estimators $\mathsf{Est}_j(A, X, Y_1, Y_2) = \widehat{S}_j$ for $j = 1, 2$ that satisfy $\mathbb{E}\left[d_j(S_j, \widehat{S}_j)\right] \leq D_j + \epsilon_n$ for $j = 1, 2$ and $0 < \epsilon_n \to 0$ as $n \to \infty$.

*Protocol A:* We first generate a tuple of random variables $(V^n, A^n, X^n, Y_1^n, S_1^n, Y_2^n, S_2^n)$ according to $P_{VAXY_1S_1Y_2S_2}$ as defined in (8). The source encoder, observing $V^n$, uniformly and independently assigns random bin indices $\mathcal{B}_{M_1}(V^n) = M_1 \in \mathcal{M}_1[1 : 2^{nR_1}]$, $\mathcal{B}_{M_2}(V^n) = M_2 \in \mathcal{M}_1 = [1 : 2^{nR_2}]$, and $\mathcal{B}_F(V^n) = F \in [1 : 2^{n\widetilde{R}}]$. The decoder employs a Slepian-Wolf decoder [12] to recover $\widehat{V}^n$ from $(Y_1^n, S_1^n, F)$, which we denote $P_{\widehat{V}^n|Y_1^n S_1^n F}^{SW}$.

The random binning induces the following random pmf

$$P^{RB} = P_{M_1 M_2 F}^{RB} P_{V^n|M_1 M_2 F}^{RB} P_{A^n X^n Y_1^n S_1^n Y_2^n S_2^n|V^n} P_{\widehat{V}^n|Y_1^n S_1^n F}^{SW}. \quad (11)$$

*Protocol B:* We assume $F$ is uniformly and independently selected from $[1 : 2^{n\widetilde{R}_v}]$ and is shared with all parties prior to transmission. The transmitter selects a message $M = (M_1, M_2)$ uniformly from $(\mathcal{M}_1 \times \mathcal{M}_2)$ independent of $F$. Using $P_{V^n|M_1 M_2 F}^{RB}$ from Protocol A, the transmitter generates $V^n$. The

channel inputs $(A_i, X_i)$ for the $i^{th}$ channel use are produced by the transmitter according to $P_{XA|V}$. The legitimate receiver uses its observations $(Y_1^n, S_1^n)$ and the common randomness $F$ to form an estimate $\widehat{V}^n$ via $P^{SW}_{\widehat{V}^n|Y_1^n S_1^n F}$ from Protocol A.

The pmf induced by Protocol B is

$$P^{RC} = P^U_{M_1 M_2} P^U_F P^{RB}_{V^n|M_1 M_2 F} P_{A^n X^n Y_1^n S_1^n Y_2^n S_2^n|V^n} P^{SW}_{\widehat{V}^n|Y_1^n S_1^n F}. \tag{12}$$

A sufficient condition for the Slepian-Wolf decoder to correctly estimate $V^n$ in Protocol A [9, Lemma 1] is

$$\widetilde{R} > H(V|Y_1, S_1). \tag{13}$$

Partial secrecy requires almost independence of $M_2$ and $F$ with the eavesdropper's observation $(Y_1^n, S_1^n)$. Privacy amplification [9, Theorem 1] ensures almost independence of mentioned random variables for Protocol A if

$$\widetilde{R}_v + R_2 < H(V|Y_2, S_2). \tag{14}$$

Finally, using [9, Theorem 1], the induced distributions (11) and (12) are arbitrarily close in variational distance when

$$R_1 + R_2 + \widetilde{R}_v < H(V) \tag{15}$$

which gives the desired reliability and security guarantees for Protocol B. A coding scheme for the original channel coding problem is obtained by finding a specific realization f of the common randomness $F$ for which the reliability and security conditions continue to hold as in [9].

Using Fourier-Motzkin elimination [13] to simplify (13)-(15) gives (5) and

$$R_2 < \left[H(V|Y_2, S_2) - H(V|Y_1, S_1)\right]^+$$
$$= \left[I(V; Y_2, S_2) - I(V; Y_1, S_1)\right]^+ \tag{16}$$

where $[a]^+ = \max(0, a)$. Application of the Markov chain $V - (A, X) - (Y_1, S_1) - (Y_2, S_2)$, which follows from channel degradation, and the data processing inequality to (16) recovers (6). The distortion constraints in (7) and the viability of the deterministic per-letter estimators in (9) follow as in [5], [8].

Converse Proof: Suppose for some $n \geq 1$, $\delta_n > 0$, there exists a channel encoder, action encoder, decoder, and state estimators such that

$$P\{M \neq \widehat{M} \leq \delta_n \tag{17}$$
$$I(M_2; Y_2^n, S_2^n) \leq \delta_n \tag{18}$$
$$\mathbb{E}\left[d_j(S_j^n, \widehat{S}_j^n)\right] \leq D_j + \delta_n \tag{19}$$

are satisfied for some tuple $(R_1, R_2, D_1, D_2)$.

We have

$$H(M_1, M_2|Y_1^n, S_1^n) \overset{(a)}{\leq} H(M_1, M_2|\widehat{M_1}, \widehat{M_2}) \overset{(b)}{\leq} n\epsilon_n \tag{20}$$

where $(a)$ follows by allowing randomized decoding and $(b)$ follows from Fano's inequality with $\epsilon_n = \frac{H_b(\delta_n)}{n} + \delta_n(R_1 + R_2)$. Note that $\epsilon_n \to 0$ as $\delta_n \to 0$.

We also define $V_i \triangleq (M_1, M_2, Y_1^{i-1}, S_1^{i-1}, Y_2^{i-1}, S_2^{i-1})$ such that the Markov chain $V_i - (A_i, X_i) - (Y_{1,i}, S_{1,i}, Y_{2,i}, S_{2,i})$ holds.

Bound on $n(R_1 + R_2)$:

$$n(R_1 + R_2) \overset{(a)}{\leq} I(M_1, M_2; Y_1^n, S_1^n) + n\epsilon_n$$
$$\leq \sum_{i=1}^{n} \left[H(Y_{1,i} S_{1,i}) - H(Y_{1,i}, S_{1,i}|M_1, M_2, Y_1^{i-1}, S_1^{i-1}, Y_2^{i-1}, S_2^{i-1})\right] + n\epsilon_n$$
$$\overset{(b)}{=} \sum_{i=1}^{n} I(V_i; Y_{1,i}, S_{1,i}) + n\epsilon_n \tag{21}$$

where $(a)$ follows from (20) and $(b)$ follows from the definition of $V_i$.

Bound on $nR_2$:

$$nR_2 \overset{(a)}{\leq} H(M_2|Y_2^n, S_2^n) + \delta_n$$
$$= I(M_2; Y_1^n, S_1^n|Y_2^n, S_2^n) + H(M_2|Y_1^n, Y_2^n, S_1^n, S_2^n) + \delta_n$$
$$\leq I(M_2; Y_1^n, S_1^n|Y_2^n, S_2^n) + H(M_1, M_2|Y_1^n, S_1^n) + \delta_n$$
$$\overset{(b)}{\leq} I(M_2; Y_1^n, S_1^n|Y_2^n, S_2^n) + n\epsilon_n + \delta_n$$
$$\leq \sum_{i=1}^{n} \left[H(Y_{1,i}, S_{1,i}|Y_{2,i}, S_{2,i}) - H(Y_{1,i}, S_{1,i}|Y_1^{i-1}, S_1^{i-1}, M_1, M_2, Y_2^n, S_2^n)\right] + n\epsilon_n + \delta_n$$
$$\overset{(c)}{=} \sum_{i=1}^{n} \left[H(Y_{1,i}, S_{1,i}|Y_{2,i}, S_{2,i}) - H(Y_{1,i}, S_{1,i}|Y_1^{i-1}, S_1^{i-1}, M_1, M_2, Y_2^i, S_2^i)\right] + n\epsilon_n + \delta_n$$
$$\overset{(d)}{=} \sum_{i=1}^{n} \left[I(V_i; Y_{1,i}, S_{1,i}|Y_{2,i}, S_{2,i})\right] + n\epsilon_n + \delta_n$$
$$\overset{(e)}{=} \sum_{i=1}^{n} \left[I(V_i; Y_{1,i}, S_{1,i}) - I(V_i; Y_{2,i}, S_{2,i})\right] + n\epsilon_n + \delta_n \tag{22}$$

where $(a)$ follows from (18), $(b)$ follows from (20), $(c)$ follows by application of the Markov chain $(Y_{1,i}, S_{1,i}) - (Y_1^{i-1}, S_1^{i-1}, M_1, M_2, Y_2^i, S_2^i) - (Y_{2,i+1}^n, S_{2,i+1}^n)$, $(d)$ follows from the definition of $V_i$, and $(e)$ follows because of the channel degradation (1).

By introducing a time sharing random variable Q uniformly distributed over $[1 : n]$ and independent of all other random variables and following the standard time sharing argument applied to (21) and (22), letting $V = (V_Q, Q)$, $X = X_Q$, $A = A_Q$, $Y_1 = Y_{1,Q}$, $S_1 = S_{1,Q}$, $Y_2 = Y_{2,Q}$, and $S_2 = S_{2,Q}$ such that $V - (A, X) - (Y_1, S_1) - (Y_2, S_2)$ forms a Markov chain, we recover the rate conditions (5) and (6). ∎

## IV. Inner Bound on Nonasymptotic Performance under Partial Secrecy

We now consider the achievable performance of our model for a finite block length $n$. We first adjust Definition 2 to a fixed

blocklength $n$. Following that we define some quantities that will be useful in the statement and proof of the nonasymptotic achievable region.

*Definition 3:* Under partial secrecy and for fixed $\delta_r, \delta_D, \delta_{\sec} > 0$ and $n \geq 1$, a nonasymptotic secrecy-distortion tuple $(R_1, R_2, D_1, D_2)$, with $\log |M_j| = nR_j$ for $j = 1, 2$, is $(\delta_r, \delta_D, \delta_{\sec}, n)$-achievable if there exists an action encoder, channel encoder, decoder, and two per-letter state estimators $\widehat{S}_j = \mathsf{Est}_j(X, A, Y_1, Y_2)$ such that we have (4) with per-letter distortion metrics bounded by a value $d_{\max}$ and

$$\Pr\left[(M_1, M_2) \neq (\widehat{M}_1, \widehat{M}_2)\right] \leq \delta_r \quad \text{(reliability)} \tag{23}$$

$$\| P_{M_2 Y_2^n S_2^n} - P^U_{M_2} P^n_{S_2 Y_2} \|_1 \leq \delta_{\sec} \quad \text{(strong secrecy)} \tag{24}$$

$$\mathbb{E}\left[d_j(S_j^n, \widehat{S_j^n})\right] \leq \delta_D \quad \text{for } j = 1, 2 \quad \text{(distortion)}. \tag{25}$$

The nonasymptotic secrecy-distortion region $\mathcal{R}_{Act}(\delta_r, \delta_d, \delta_{\sec}, n)$ is the closure of all $(\delta_r, \delta_d, \delta_{\sec}, n)$-achievable tuples under partial secrecy. ◇

We define the information of a probability distribution $P_A$ as

$$h_{P_A} = \log \frac{1}{P_A(a)} \tag{26}$$

and the information density of a distribution $P_{AB}$ as

$$\imath(A, B) = \log \frac{P_{AB}(a, b)}{P_A(a) P_B(b)}. \tag{27}$$

Next, we define the dispersion of the channels

$$\mathcal{V}_{Y_1 S_1} = \min_{P_{V|Y_1 S_1}} \left[\mathrm{Var}_{P_{V Y_1 S_1}}[\imath(V, Y_1 S_1)|V]\right] \tag{28}$$

$$\mathcal{V}_{Y_2 S_2} = \min_{P_{V|Y_2 S_2}} \left[\mathrm{Var}_{P_{V Y_2 S_2}}[\imath(V, Y_2 S_2)|V]\right] \tag{29}$$

where $\mathrm{Var}[\cdot]$ is the variance. $Q(\cdot)$ denotes the standard normal tail probability. Define

$$\mu_{s\widehat{s}} = \min_{(s\widehat{s}) \in \mathrm{supp}(P_{S\widehat{S}})} P_{S\widehat{S}}(s, \widehat{s}). \tag{30}$$

We next establish an inner bound on the nonasymptotic secrecy-distortion region for the secure ISAC model considered.

*Theorem 2:* For an ISAC channel with transmitter actions, a $(R_1, R_2, D_1, D_2)$ tuple is $(\delta_r, \delta_D, \delta_{\sec}, n)$-achievable if, for any $\theta \in [0, 1]$, we have

$$R_1 + R_2 \leq \left[ I(V; Y_1, S_1) - \mathcal{O}\left(\frac{\log n}{n}\right) \right.$$
$$\left. - Q^{-1}\left(\theta\left(\delta_r + \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)\right)\right)\sqrt{\frac{\mathcal{V}_{Y_1 S_1}}{n}} \right]^+ \tag{31}$$

$$R_2 \leq \left[ I(V; Y_1, S_1) - I(V; Y_2, S_2) - \mathcal{O}\left(\frac{\log n}{n}\right) \right.$$
$$- Q^{-1}\left((1 - \theta)\left(\delta_{\sec} + \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)\right)\right)\sqrt{\frac{\mathcal{V}_{Y_2 S_2}}{n}}$$
$$\left. - Q^{-1}\left(\theta\left(\delta_r + \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)\right)\right)\sqrt{\frac{\mathcal{V}_{Y_1 S_1}}{n}} \right]^+ \tag{32}$$

$$D_j \geq \mathbb{E}[d_j(S_j, \widehat{S}_j)] - \epsilon_D \quad \text{for } j = 1, 2 \tag{33}$$

such that

$$\delta_D = \epsilon_D(1 + D_j + \epsilon_D) + 2|\mathcal{S}||\widehat{\mathcal{S}}|e^{-2n\epsilon_D^2 \mu_{s_j \widehat{s}_j}} d_{\max} \tag{34}$$

where we have

$$P_{VAXY_1 Y_2 S_1 S_2} = P_{V|AX} P_{AX} P_{S_1 S_1|A} P_{Y_1 Y_2|S_1 S_2 X} \tag{35}$$

and the per-letter estimators in (9).

*Proof Sketch:* The proof sketch will proceed as follows:
1) We define Protocols A and B and we establish a bound on the reliability and security.
2) We combine the bounds on reliability and security to bound the expected variational distance between the distribution induced by the channel coding problem and the distribution that satisfies the reliability and security constraints.
3) We establish rate conditions such that the reliability and security constraints are satisfied for $\theta\delta_r$ and $(1 - \theta)\delta_{\sec}$, for any $\theta \in [0, 1]$. The rate conditions come from the minimization of the measure of atypical sets using the Berry-Esseen CLT.

Fix a distribution $P_{VAX}$ such that $\mathbb{E}[d_j(S_i, \widehat{S}_j)] \leq D_j + \epsilon_D$.

*Protocol A:* We define the random binning as in the proof of Theorem 1 with the exception that we use (35) and the stochastic likelihood decoder, as defined in [10], [14], associated with probability distribution

$$T(\widehat{v}^n | y_1^n, s_1^n, f) = \frac{t(\widehat{v}^n | y_1^n, s_1^n)\mathbb{1}\{\mathcal{B}_F(\widehat{v}^n) = f\}}{\sum_{\bar{v}^n \in \mathcal{V}^n} t(\bar{v}^n | y_1^n, s_1^n)\mathbb{1}\{\mathcal{B}_F(\bar{v}^n) = f\}} \tag{36}$$

using an arbitrary pmf $t_{\widehat{V}^n Y_1^n S_1^n}$ selected by the legitimate receiver.

*Protocol B:* We define Protocol B as in the proof of Theorem 1 with the exception of the decoder, for which we choose the stochastic likelihood decoder associated with $T_{\widehat{V}^n | Y_1^n S_1^n F}$ used in Protocol A.

We define the following atypical sets. For $\gamma_1, \gamma_2, \gamma_3$ positive real numbers, we have

$$S_{\gamma_1} = \{v^n : h_{P_{V^n}}(v^n) - n(R_1 + R_2 + \widetilde{R}) > \gamma_1\} \tag{37}$$

$$S_{\gamma_2} = \{(v^n, y_1^n, s_1^n) : n\widetilde{R} - h_t(v^n | y_1^n, s_1^n) > \gamma_2\} \tag{38}$$

$$S_{\gamma_3} = \{(v^n, y_2^n, s_2^n) : h_{P_{V}^n | Y_2^n S_2^n}(v^n | y_2^n, s_2^n) - n(R_2 + \widetilde{R}) > \gamma_3\}. \tag{39}$$

We first establish a bound on the probability of error of Protocol A. The expected variational distance between the distributions induced by Protocols A and B is bounded by [10, Theorem1], i.e.,

$$\mathbb{E}\left\| P^{RB} - P^{RC} \right\|_1 \leq \epsilon_{\mathrm{apx}} \tag{40}$$

where $\epsilon_{\mathrm{apx}} = P_{V^n}(S_{\gamma_1}^c) + 2^{-\frac{1}{2}(\gamma_1 + 1)}$. By [10, Theorem 2], the probability of error for the Protocol A is bounded by $\epsilon_{\mathrm{dec}}$ where where $\epsilon_{\mathrm{dec}} = P_{V^n Y_1^n S_1^n}(S_{\gamma_2}^c) + 2^{-\gamma_2}$. Then for Protocol B, we have

$$\mathbb{E}\left[P^{RC}\{V^n \neq \widehat{V}^n\}\right] < \epsilon_{\mathrm{apx}} + \epsilon_{\mathrm{dec}}. \tag{41}$$

The triangle inequality and [14, Theorems 1 and 2] give

$$\mathbb{E}\big\|P^{RC}_{M_2FY_2^nS_2^n} - P^U_{M_2}P^U_F P_{Y_2^nS_2^n}\big\|_1 \leq \epsilon_{\text{apx}} + \epsilon_{\text{sec}} \qquad (42)$$

where $\epsilon_{\text{sec}} = P_{V^nY_2^nS_2^n}(S_{\gamma_3}^c) + 2^{-\frac{1}{2}(\gamma_3+1)}$. We let $\theta\delta_r = (1/8)\epsilon_{\text{apx}} + \epsilon_{\text{dec}}$ and $(1-\theta)\delta_{\text{sec}} = (1/2)\epsilon_{\text{apx}} + \epsilon_{\text{sec}}$.

Now we combine the bounds on reliability and security. By the triangle inequality and $(b)$ follows from (41) and [14, Proposition 1] and (42) we have

$$\mathbb{E}\big\|P^{RC}_{M_2FY_2^nS_2^n\widehat{V}^n} - P^U_{M_2}P^U_F P_{Y_2^nS_2^n}\mathbb{1}\{\widehat{V}^n = V^n\}\big\|_1$$
$$\leq 2\epsilon_{\text{apx}} + \epsilon_{\text{sec}} + 4\epsilon_{\text{dec}} = \epsilon_{\text{tot}}. \qquad (43)$$

We now eliminate the common randomness $F$ by conditioning on a specific realization $f$. Specifically, [9, Lemma 3] allows us to bound (43) by $2\epsilon_{\text{tot}}$.

We now establish the rate conditions through minimizing $2\epsilon_{\text{tot}}$ as follows

$$2\epsilon_{\text{tot}} \leq 8\big(P_{V^n}(S_{\gamma_1^c}) + P_{V^nY_1^nS_1^n}(S_{\gamma_2^c}) + P_{V^nY_2^nS_2^n}(S_{\gamma_3^c})\big)$$
$$+ 2\big(2^{-\frac{1}{2}(\gamma_1+1)} + 4 \cdot 2^{-\gamma_2} + 2^{-\frac{1}{2}(\gamma_3+1)}\big)$$
$$\overset{(a)}{\leq} 32\big(P_{V^nY_1^nS_1^nY_2^nS_2^n}(S_{\gamma_1}^c \cup S_{\gamma_2}^c \cup S_{\gamma_3}^c)$$
$$+ 2\big(2^{-\frac{1}{2}(\gamma_1+1)} + 4 \cdot 2^{-\gamma_2} + 2^{-\frac{1}{2}(\gamma_3+1)}\big)$$
$$\overset{(b)}{\leq} 32\big(P_{V^nY_1^nS_1^nY_2^nS_2^n}((S_{\gamma_1} \cap S_{\gamma_2} \cap S_{\gamma_3})^c)$$
$$+ 2\big(2^{-\frac{1}{2}(\gamma_1+1)} + 4 \cdot 2^{-\gamma_2} + 2^{-\frac{1}{2}(\gamma_3+1)}\big) \qquad (44)$$

where $(a)$ follows as $P_{V^nY_1^nS_1^nY_2^nS_2^n}(S_{\gamma_1}^c \cup S_{\gamma_2}^c \cup S_{\gamma_3}^c) > P_{V^nY_1^nS_1^nY_2^nS_2^n}(S_{\gamma_j}^c \cap S_{\gamma_i}^c)$ for $i \neq j$ and $(b)$ follows from De Morgan's laws. What remains is to minimize the measure of the set $(S_{\gamma_1} \cap S_{\gamma_2} \cap S_{\gamma_3})^c$ and prudent selection of $\gamma_1$, $\gamma_2$, and $\gamma_3$.

Following the steps in [14] and letting $t(v^ny_1^ns_1^n) = \prod_{i=1}^n P_{V|Y_1S_1}(v_i, y_{1,i}, s_{1,i})$, we have that bounding the measure of $(S_{\gamma_1} \cap S_{\gamma_2} \cap S_{\gamma_3})^c$ is equivalent to bounding the measure of $S_1 \cup S_2$ where

$$S_1 = \{(v^n, y_1^n, s_1^n, y_2^n, s_2^n) : n(R_1 + R_2) \geq \imath(v^n, y_1^ns_1^n) - \gamma_1 - \gamma_2\}$$
$$S_2 = \{(v^n, y_1^n, s_1^n, y_2^n, s_2^n) :$$
$$nR_2 \geq \imath(v^n, y_1^ns_1^n) - \imath(v^n, y_2^ns_2^n) - \gamma_2 - \gamma_3\}. \qquad (45)$$

We outline the bound on $P(S_1 \cup S_2)$. Since the tuple of random variables $(v^n, y_1^n, s_1^n, y_2^n, s_2^n)$ are i.i.d., the terms $Z_i = \imath(v_i, y_{1,i}s_{1,i})$ are also independent for $i = 1, \ldots, n$. Defining $\mu_n = 1/n \sum_{i=1}^n \mathbb{E}[Z_i]$ and $V_n = 1/n \sum_{i=1}^n \text{Var}[Z_i]$, if we assume that

$$n(R_1 + R_2) < n\mu_n - Q^{-1}(\theta\delta_r)n\sqrt{\frac{V_n}{n}} - \gamma_1 - \gamma_2 \qquad (46)$$

then we can define the set

$$\left\{(v^n, y_1^n, s_1^n, y_2^n, s_2^n) : \sum_{i=1}^n \imath(V; Y_1S_1) < n\Big(\mu_n - t\sqrt{\frac{V_n}{n}}\Big)\right\}. \qquad (47)$$

which contains $S_1$. Thus bounding (47) will also bound $S_1$. Application of the Berry Esseen CLT, see [10], gives that the

measure of (47) is upper bounded by $\theta\delta_r + \mathcal{O}\big(\frac{1}{\sqrt{n}}\big)$, we obtain $P(S_1) \leq \theta\delta_r + \mathcal{O}\big(\frac{1}{\sqrt{n}}\big)$. Since $(v_i, y_{1,i}, s_{1,i})$ are generated i.i.d. according to $P_{VY_1S_1}$ for all $i = 1, \ldots, n$, we have

$$\mu_n = I(V; Y_1, S_1) \qquad (48)$$
$$V_n \geq \mathcal{V}_{V|Y_1S_1}, \qquad (49)$$

which in combination with prudent selection of $(\gamma_1, \gamma_2)$ results in (31). The bound on $P(S_2)$ follows similarly, resulting in (32). The distortion constraints follow as in the proof of [7, Theorem 1]. ∎

In conclusion, Theorem 1 provides the exact asymptotic result for the secure ISAC model considered, whereas Theorem 2 provides an achievable region for low-latency secure ISAC with a fixed blocklength and specific bounds on the reliability, strong secrecy, and distortion measures. While the results of Theorem 1 assume that the channel is physically degraded, Theorem 2 is more general and holds for all channels described by Fig. 1.

### References

[1] H. Andersson, "Joint communication and sensing in 6G networks," *Ericsson Blog*, 2021.

[2] T. Wild, V. Braun, and H. Viswanathan, "Joint design of communication and sensing for beyond 5G and 6G systems," *IEEE Access*, vol. 9, pp. 30 845–30 857, Feb. 2021.

[3] Z. Wei, F. Liu, C. Masouros, N. Su, and A. P. Petropulu, "Toward multifunctional 6g wireless networks: Integrating sensing, communication, and security," *IEEE Communications Magazine*, vol. 60, no. 4, pp. 65–71, 2022.

[4] M. Kobayashi, H. Hamad, G. Kramer, and G. Caire, "Joint state sensing and communication over memoryless multiple access channels," in *Proc. of IEEE Int. Symp. Inf. Theory*, Paris, France, July 2019, pp. 270–274.

[5] O. Günlü, M. R. Bloch, R. F. Schaefer, and A. Yener, "Secure integrated sensing and communication," *IEEE J. Sel. Areas Inf. Theory*, 2023.

[6] M. Mittelbach *et al.*, "Secure integrated sensing and communication under correlated Rayleigh fading," *Cryptology ePrint Archive*, 2024.

[7] O. Günlü, M. Bloch, R. F. Schaefer, and A. Yener, "Nonasymptotic performance limits of low-latency secure integrated sensing and communication systems," in *IEEE Int. Conf. Acoustics Speech Sign. Process.*, 2024, pp. 12 971–12 975.

[8] T. Welling, O. Günlü, and A. Yener, "Transmitter actions for secure integrated sensing and communication," *Cryptology ePrint Archive*, 2024.

[9] M. H. Yassaee, M. R. Aref, and A. Gohari, "Achievability proof via output statistics of random binning," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6760–6786, Nov. 2014.

[10] ——, "Non-asymptotic output statistics of random binning and its applications," in *IEEE Int. Symp. Inf. Theory*, 2013, pp. 1849–1853.

[11] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge, U.K.: Cambridge University Press, 2011.

[12] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, July 1973.

[13] A. Schrijver, *Theory of Linear and Integer Programming*. Chichester, England: John Wiley & Sons, June 1998.

[14] G. Cervia, T. J. Oechtering, and M. Skoglund, "($\epsilon$, n) fixed-length strong coordination capacity," in *IEEE Inf. Theory Workshop*, 2021, pp. 1–6.