ISAC under Security and Privacy Constraints – from Theory to Demonstrations

Holger Boche
Chair of Theoretical Information Technology
Technical University of Munich

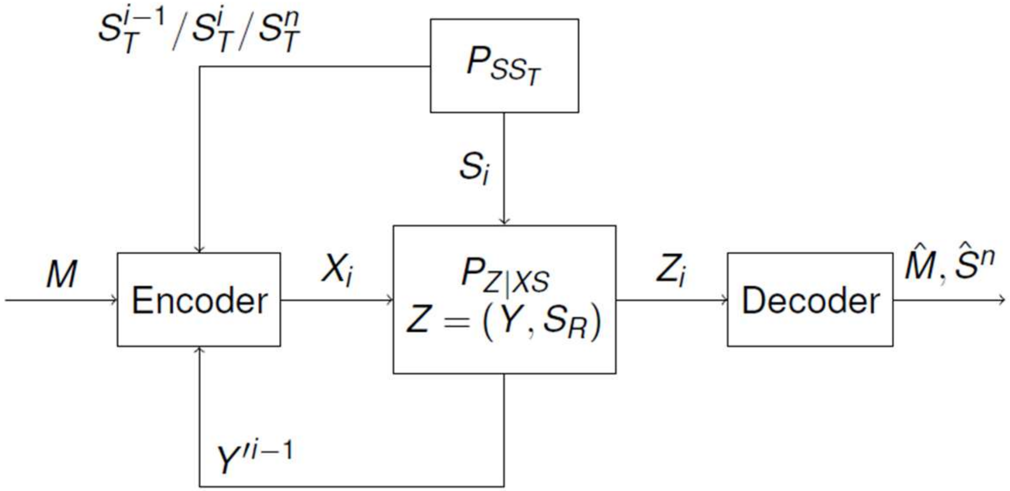
Thanks to Yiqi Chen#, Xinyang Li*, Vlad Andrei*, Dongxiao Xu*, Ullrich Mönich*
#TUM LTI, *ACES Lab at TUM

BMBF 6G Conference 2024, Berlin
July 3, 2024

Contents

Integrated Sensing and Communication (ISAC)

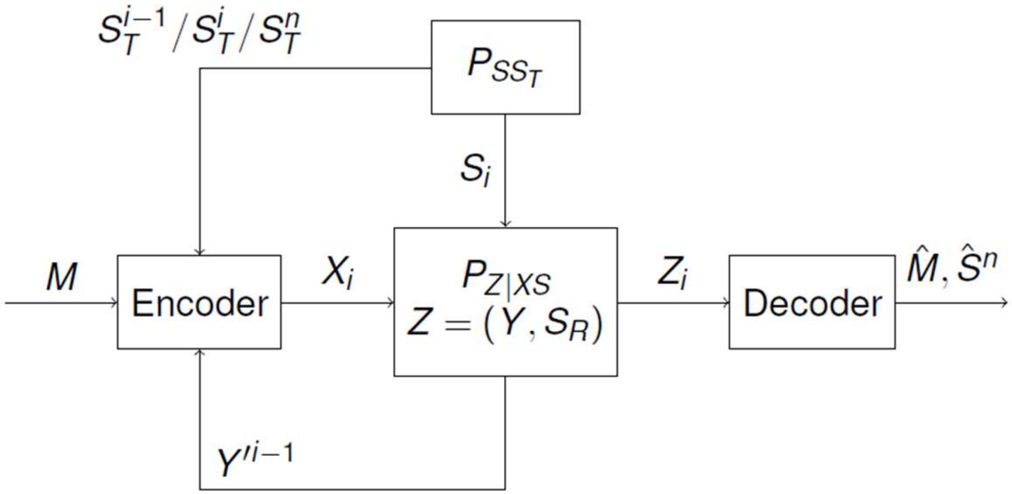
Point-to-point Channel



- State-dependent discrete memoryless channel (SD-DMC) with channel transition distribution $P_{Y|XS}$, state P_S
- Side information at transmitter (SI-T) $S_T \sim P_{S_T|S}$, strictly-causal, causal or non-causal available
- Side information at receiver (SI-R) S_R, treated as another channel output, $Z = (Y, S_R)$
- Feedback present $Y' = Y$ or absent $Y' = \varnothing$
- Message decoding $\hat{M} = f_d(Z^n)$
- State estimator $\hat{S}_i = h_i(S^n)$

[1] X. Li, V. C. Andrei, A. Djuhera, U, J. Mönich, H. Boche, “An Analysis of Capacity-Distortion Trade-Offs in Memoryless ISAC Systems,” arXiv preprint arXiv:2402.17058, 2024.

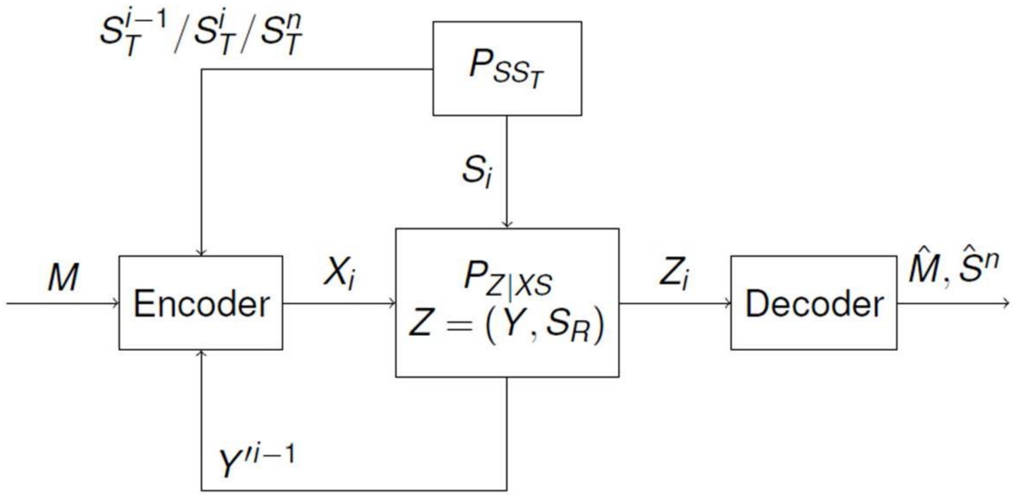
Point-to-point Channel



- Message decoding error probability $P_e^{(n)} \triangleq \frac{1}{2^{nR}} \sum_m \Pr\{f_d(Z^n) \neq M | M = m\}$
- Expected estimation distortion $D^{(n)} = \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}[d(S_i, \hat{S}_i)]$
- **Capacity-distortion function** $C(D)$: the supremum of code rate R such that $\lim_{n\to\infty} P_e^{(n)} = 0$ and $\limsup_{n\to\infty} D^{(n)} \leq D$
- GOAL: find the C-D functions for three causality levels: $C^{\mathrm{SC}}(D)$, $C^{\mathrm{C}}(D)$ and $C^{\mathrm{NC}}(D)$

[1] X. Li, V. C. Andrei, A. Djuhera, U, J. Mönich, H. Boche, "An Analysis of Capacity-Distortion Trade-Offs in Memoryless ISAC Systems," arXiv preprint arXiv:2402.17058, 2024.

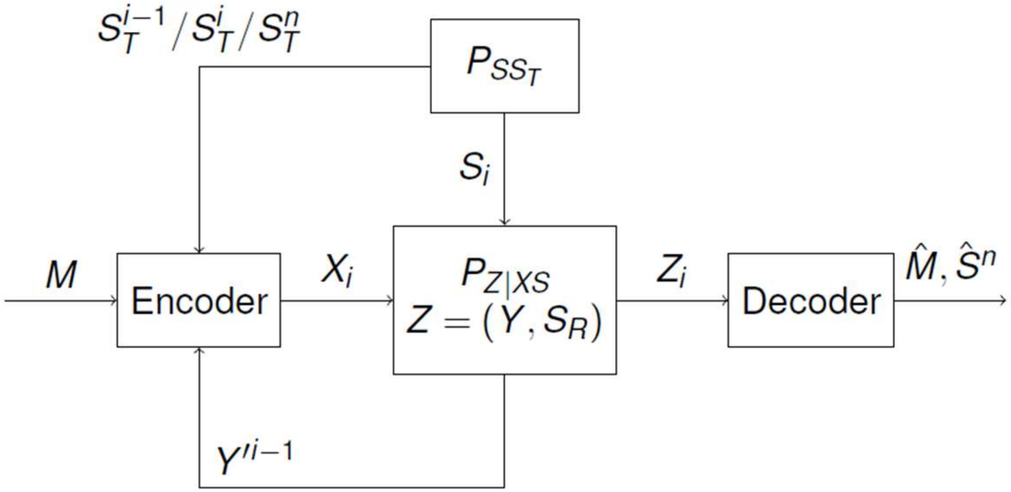
Point-to-point Channel



- Communication-only mode: $C(\infty)$, no state estimation task
- Sensing-only mode: $D_{\min}$, no message transfer task, but communication may happen to encode the SI-T
- Radar mode: special case of sensing-only mode, with $S_R = X$, $Y' = Y$ for monostatic and $Y' = \varnothing$ for bistatic
- Complicated systems modeled by combining multiple links at various modes $\rightarrow$ see BC channel later

[1] X. Li, V. C. Andrei, A. Djuhera, U, J. Mönich, H. Boche, "An Analysis of Capacity-Distortion Trade-Offs in Memoryless ISAC Systems," arXiv preprint arXiv:2402.17058, 2024.

C-D function for P2P Channel



Theorem 1

$$R(D) \triangleq \max_{P_{U|S_T},P_{X|US_T},P_{V|US_TY'}} I(U;Z)-I(U;S_T)-I(V;S_T|U,Z)$$
$$\text{s.t.} \quad \mathbb{E}[d(S,h^*(U,V,Z))] \leq D$$

with the optimal estimator h^* given by

$$h^*(u,v,z) = \arg\min_{\hat{s}\in\hat{\mathcal{S}}} \sum_{s\in\mathcal{S}} P_{S|UVZ}(s|u,v,z)d(s,\hat{s}).$$

The C-D functions for strictly causal case $C^{\mathrm{SC}}(D)$, causal case $C^{\mathrm{C}}(D)$, and non-causal case $C^{\mathrm{NC}}(D)$ satisfy

$$C^{\mathrm{SC}}(D) = R(D) \quad \text{s.t.} \quad P_{U|S_T}=P_U,\ P_{X|US_T}=P_{X|U},$$
$$C^{\mathrm{C}}(D) = R(D) \quad \text{s.t.} \quad P_{U|S_T}=P_U,$$
$$C^{\mathrm{NC}}(D) \geq R(D).$$

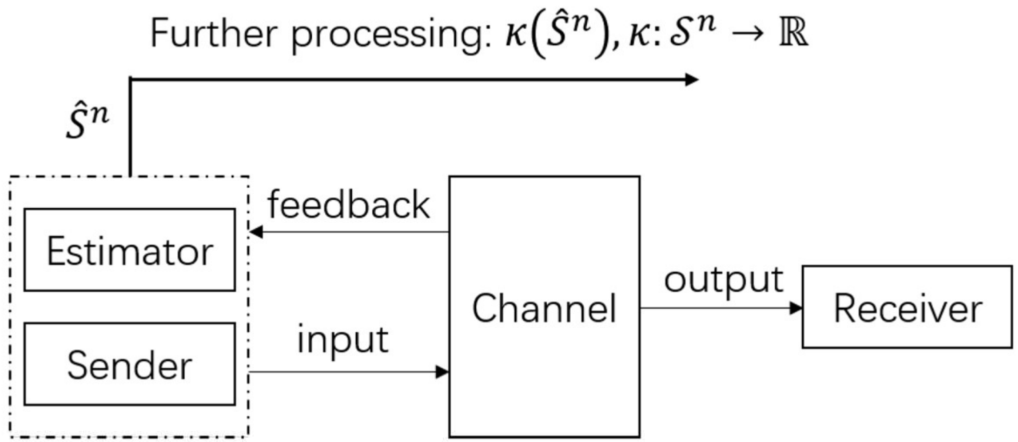
[1] X. Li, V. C. Andrei, A. Djuhera, U, J. Mönich, H. Boche, “An Analysis of Capacity-Distortion Trade-Offs in Memoryless ISAC Systems,” arXiv preprint arXiv:2402.17058, 2024.

Integrated Sensing and Communication with Trustworthiness

(Security, Privacy, and Integrity Part of Trustworthiness)

[2] G. Fettweis and H. Boche, “On 6G and trustworthiness,” Communications of the ACM, vol. 65, no. 4, pp. 48–49, Apr. 2022.
[3] G. Fettweis and H. Boche, “6G: The personal tactile internet—and open questions for information theory,” IEEE BITS the Information Theory Magazine, vol. 1, no. 1, pp. 71–82, 2021.

Motivation



- Estimation and decoding are not the end of the workflow.
- The further processing of the estimation result can be characterized by a function

$$\kappa : \mathcal{S}^n \to \mathbb{R}, \quad \text{s.t.} \max_{s^n \in \mathcal{S}^n} \kappa(s^n) = \Upsilon < \infty$$

[4] Y. Chen, T. Oechtering, H. Boche, M. Skoglund, Y. Luo, "Distribution-Preserving Integrated Sensing and Communication with Secure Reconstruction," in IEEE International Symposium on Information Theory (ISIT 2024), 2024.

Motivation

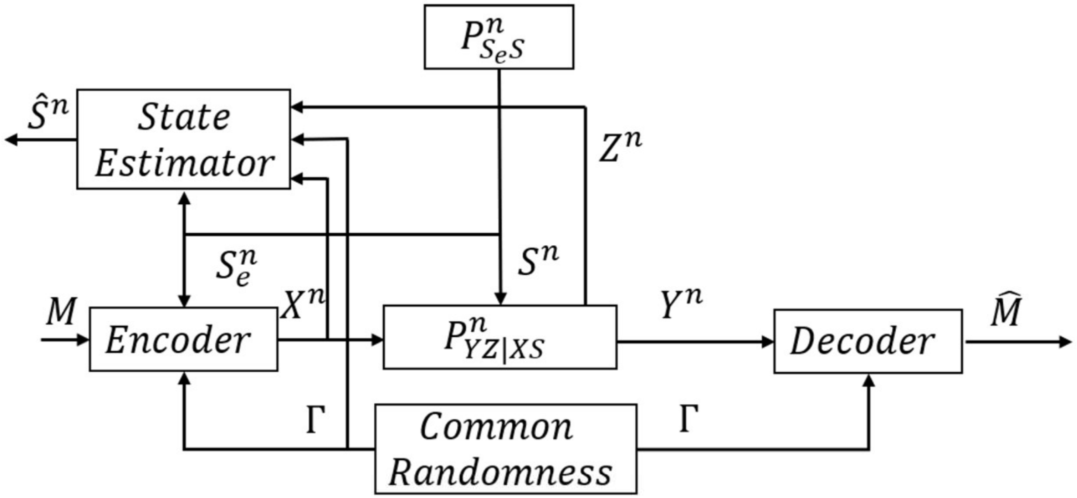
- The definition of κ depends on the objective of the system.
- What can we do?
  - By controlling the distribution of the estimation, we have

$$\max_{\kappa:\ \max_{\hat{s}^n} |\kappa(\hat{s}^n)| \leq \Upsilon} \left| \mathbb{E}_{P_S^n}[\kappa(S^n)] - \mathbb{E}_{P_{\hat{S}^n}}\left[\kappa(\hat{S}^n)\right] \right|$$
$$\leq \Upsilon \sum_{s^n \in \mathcal{S}^n} \left| P_S^n(s^n) - P_{\hat{S}^n}(s^n) \right|$$

  - The gap between the expectations is upper bounded by the distance between $P_{\hat{S}^n}$ and P_S^n no matter what processing function κ is selected.

⇒ This bound is sharp, i.e., $P_{\hat{S}^n} = P_S^n$ is the only way to achieve integrity.

Model Definition



- S_e^n represents some prior knowledge about the system.
- The decoder produces an estimation of the transmitted message $\hat{M}$.
- The state estimator produces an estimation of the channel state sequence $\hat{S}^n$. We only consider estimator with $P_{\hat{S}^n} = P_S^n$.
- The common randomness is shared between the encoder, decoder and estimator.

Main Result: Unlimited Randomness $\mathbf{R_c} = \infty$

Theorem (Capacity)

The distribution-preserving capacity-distortion function with unlimited common randomness is

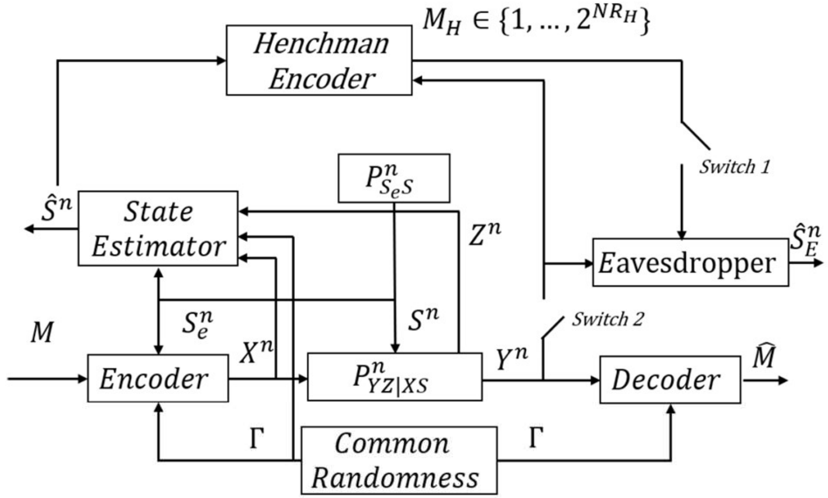
$$C^{\infty}(D,\Delta) = \begin{cases} (R,\infty) \in \mathbb{R}^2 : \exists P_{S_e S U X Y Z \hat{S}} \in \mathcal{P}_{UCR}, \\ \qquad R \leq I(U;Y) - I(U;S_e), \\ \qquad D \geq \mathbb{E}[d(S,\hat{S})], \end{cases}$$

where $\mathcal{P}_{UCR} = \{P_{S_e S U X Y Z \hat{S}} \in \mathcal{P}(U,X,\hat{S}) : ||P_S - P_{\hat{S}}|| \leq \Delta\}$

- The convexity of the function $C^{\infty}(D,\Delta)$ is still open due to the fact that the optimization runs over both $P_{U|S_e}$ and $P_{X|S_e U}$.

[4] Y. Chen, T. Oechtering, H. Boche, M. Skoglund, Y. Luo, “Distribution-Preserving Integrated Sensing and Communication with Secure Reconstruction,” in IEEE International Symposium on Information Theory (ISIT 2024), 2024.

ISAC with Secure Reconstruction



- A henchman observes the reconstructed sequence, and sends a message to the eavesdropper.
- The eavesdropper also receives the channel output, but has no access to the common randomness.
- Full results, see [1]

[4] Y. Chen, T. Oechtering, H. Boche, M. Skoglund, Y. Luo, "Distribution-Preserving Integrated Sensing and Communication with Secure Reconstruction," in IEEE International Symposium on Information Theory (ISIT 2024), 2024.

From Theory to Demonstrations and Resilience

From Theory to Demonstrations

- Results show that common randomness (CR) is needed
- Distillation of CR is important Post Shannon task [5], and very useful for physical layer security
- 6G-life Talk: “Achievability Schemes for Semantic Security” by Dr. M. Wiese
- 6G-life Demo: “Physical Layer Security for mmWave” by TUM ACES Lab
- The new result: CR is needed for ISAC
- Several patents with Deutsche Telekom AG have been filed [6], [7]
- A new 6G-life startup (SPRIN-D NCC Finalist) for Post Shannon tasks [5]

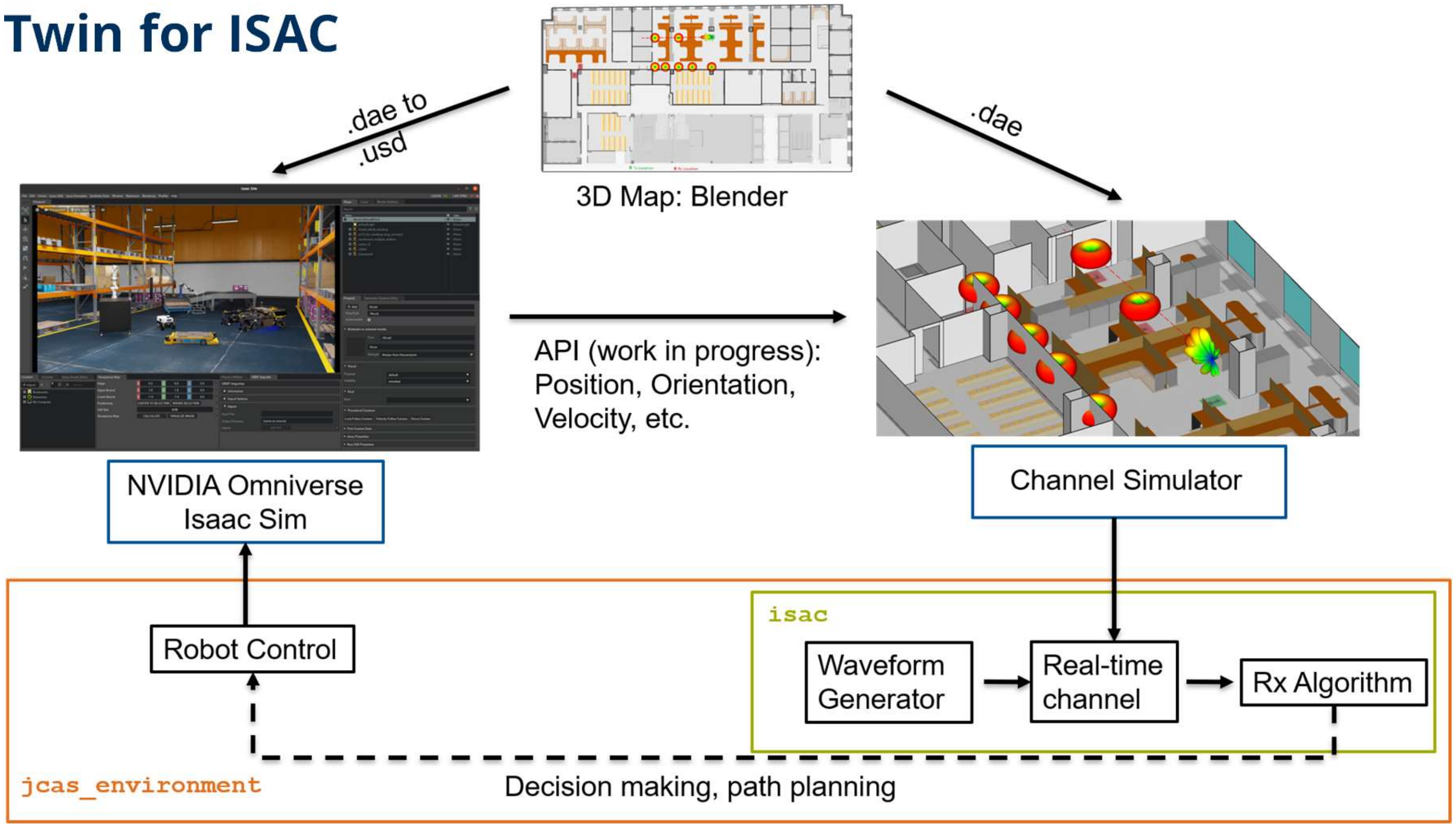
[5] J. A. Cabrera, H. Boche, C. Deppe, R. F. Schaefer, C. Scheunert, and F. H. P. Fitzek, “6G and the Post-Shannon Theory,” Shaping Future 6G Networks: Needs, Impacts, and Technologies, pp. 271–294, 2021.
[6] P. Schwenteck, G. T. Nguyen, H. Boche, W. Kellerer and F. H. P. Fitzek, “6G Perspective of Mobile Network Operators, Manufacturers, and Verticals,” IEEE Networking Letters, vol. 5, no. 3, pp. 169–172, 2023.
[7] R. Ezzine, M. Wiese, C. Deppe, H. Boche, “Common Randomness Generation from Finite Compound Sources,” IEEE International Symposium on Information Theory, IEEE, 2024.

ISAC for Resilience by Design in 6G

- Future 6G communication systems should be resilient against jamming
- Study of adversarial jamming (full knowledge)
- Transmitters are oblivious of jamming, resilience is generated by receiver; solution in [8]
- Neuromorphic hardware of a 6G-life startup (SPRIN-D NCC Finalist) is used to implement ISAC
- Neuromorphic hardware is necessary to detect denial-of-service attacks [9]

[8] V.-C. Andrei, X. Li, U. J. Mönich, and H. Boche, "Sensing-Assisted Receivers for Resilient-By-Design 6G MU-MIMO Uplink," in IEEE International Symposium on Joint Communications & Sensing, 2023. (Received the Best Paper Award).
[9] H. Boche, R.F. Schaefer, H.V. Poor, F.H.P. Fitzek, "On the Need of Neuromorphic Twins to Detect Denial-of-Service Attacks on Communication Networks," IEEE/ACM Transactions on Networking (Early Access), 2024.

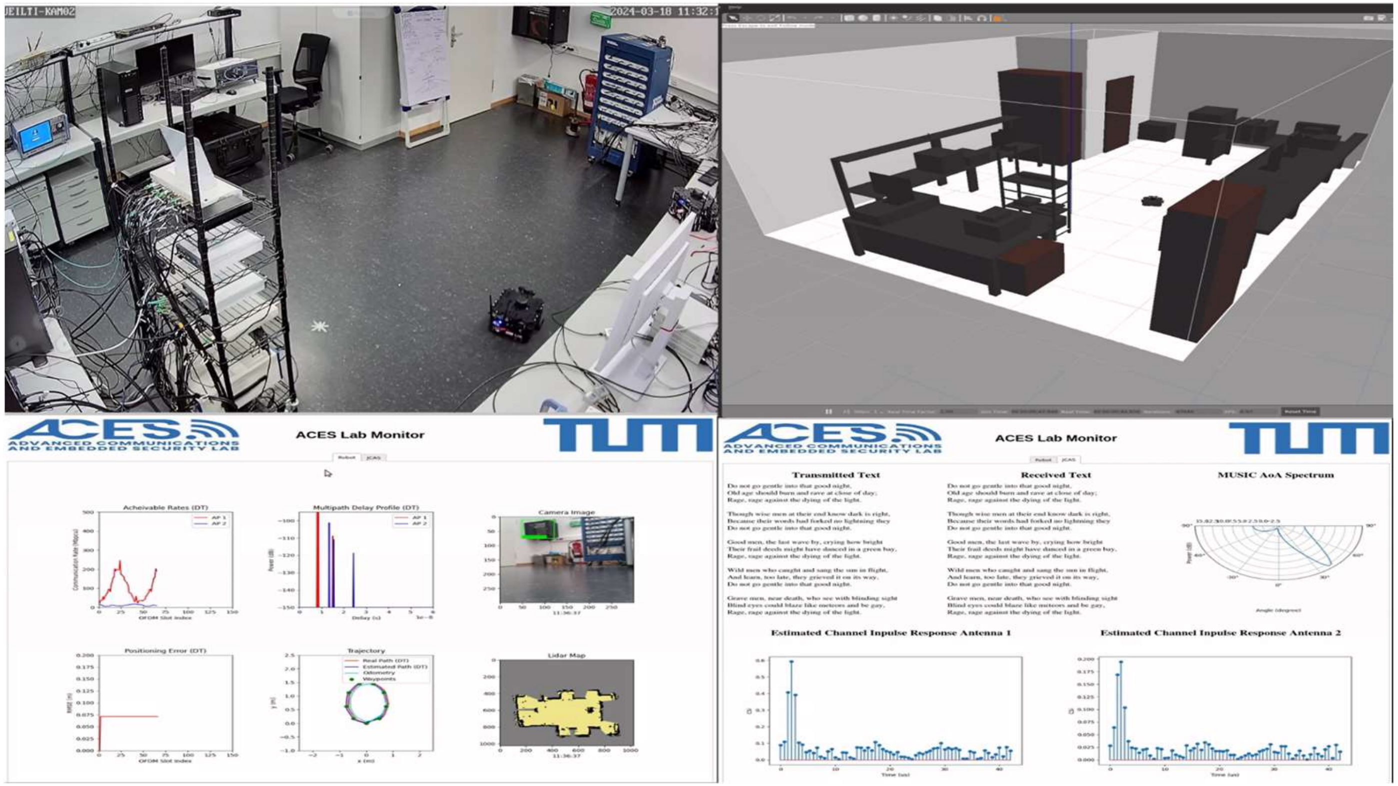
Digital Twin for ISAC

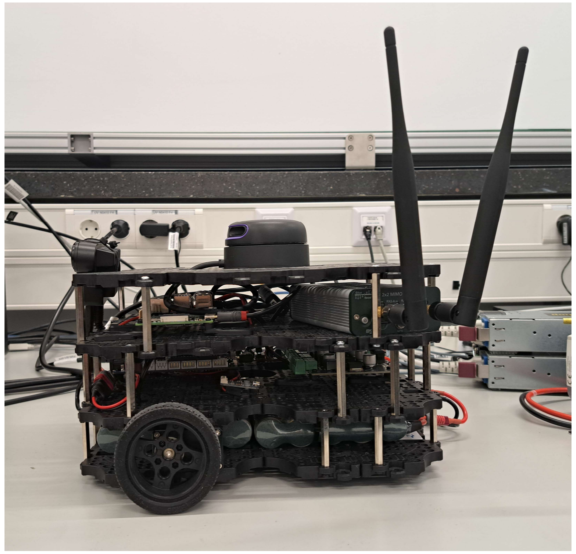


[10] V. Andrei, X. Li, “Demonstrator: A Digital Twinning Platform for Integrated Sensing, Communications and Robotics,” 4th IEEE Symposium on Joint Communications & Sensing, March 2024. (Received the Best Student Demo Award.)

ISAC in the Demo Session

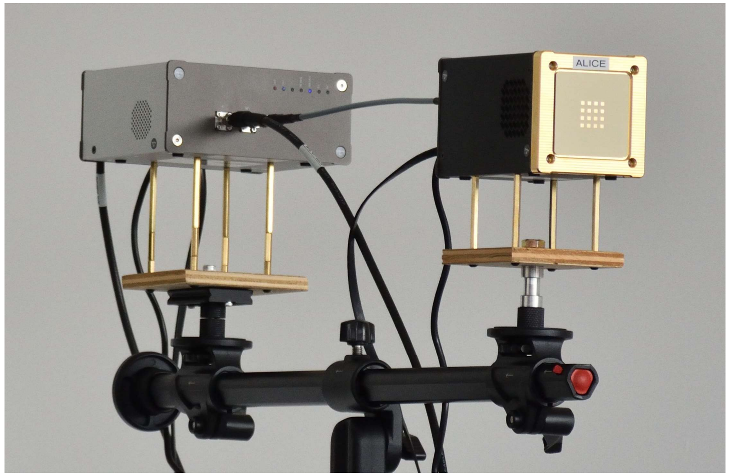
Demo: Digital-Twin Assisted Integrated Sensing and Communications





ISAC in mmWave for Robotic Applications

mmWave Experiental Setup



mmWave Antenna and Mixer (TMYTEK / NI)

BBox One 5G
26.5 - 29.5 GHz

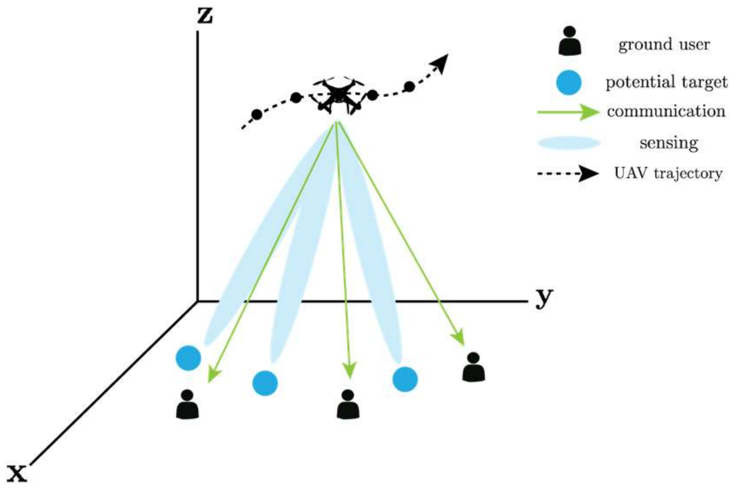
BBox Lite 5G
26.5 - 29.5 GHz

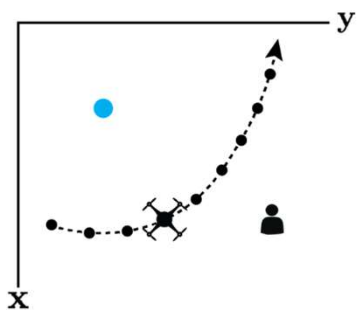
UD Box 5G

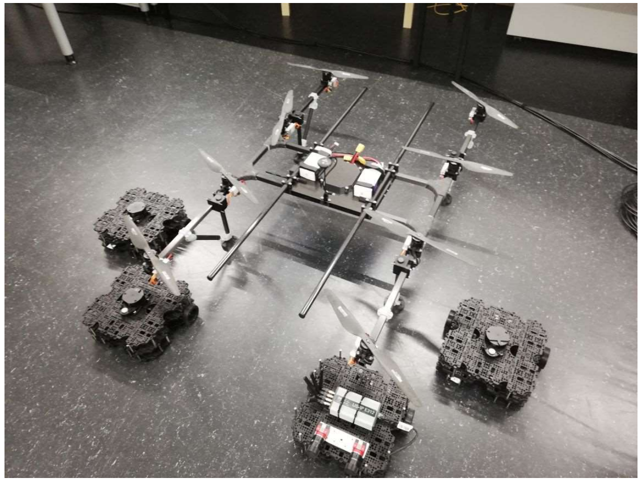
Source: TMYTEK / NI

Aerial Drones for ISAC and ISAC for Aerial Drones

- High mobility
- Multiantenna drones and robots
- Jamming and anti-jamming extensions







Further Directions, Conclusion and Outlook

Further Directions, Conclusion and Outlook

- mmWave for robotic applications
- Digital and neuromorphic twinning and Metaverse [11]
- Extension to high mobility drones with different frequencies and MIMO multiantenna beamforming
- Security and privacy extensions
- Integrated Sensing and Post Shannon Communication
- Integrated Quantum Sensing and Quantum Communication (see QUIET Talk)
- Complete new aspects to trustworthiness,
  inspired by European AI-Act and G7 Hiroshima Process on AI, i.e.,
  algorithmic transparency, right to explainability and algorithmic accountability [12]

[11] Y.N. Böck, H. Boche, R.F. Schaefer, F.H.P. Fitzek, H.V. Poor, "Virtual-Twin Technologies in Networking," IEEE Communications Magazine 61 (11), 2023, 136–141.
[12] H. Boche, A. Fono, G. Kutyniok, "A Mathematical Framework for Computability Aspects of Algorithmic Transparency," IEEE International Symposium on Information Theory, IEEE, 2024.

References

[1] X. Li, V. C. Andrei, A. Djuhera, U, J. Mönich, H. Boche, “An Analysis of Capacity-Distortion Trade-Offs in Memoryless ISAC Systems,” arXiv preprint arXiv:2402.17058, 2024.

[2] G. Fettweis and H. Boche, “On 6G and trustworthiness,” Communications of the ACM, vol. 65, no. 4, pp. 48–49, Apr. 2022.

[3] G. Fettweis and H. Boche, “6G: The personal tactile internet—and open questions for information theory,” IEEE BITS the Information Theory Magazine, vol. 1, no. 1, pp. 71–82, 2021.

[4] Y. Chen, T. Oechtering, H. Boche, M. Skoglund, Y. Luo, “Distribution-Preserving Integrated Sensing and Communication with Secure Reconstruction,” in IEEE International Symposium on Information Theory (ISIT 2024), 2024.

[5] J. A. Cabrera, H. Boche, C. Deppe, R. F. Schaefer, C. Scheunert, and F. H. P. Fitzek, “6G and the Post-Shannon Theory,” Shaping Future 6G Networks: Needs, Impacts, and Technologies, pp. 271–294, 2021.

[6] P. Schwenteck, G. T. Nguyen, H. Boche, W. Kellerer and F. H. P. Fitzek, “6G Perspective of Mobile Network Operators, Manufacturers, and Verticals,” IEEE Networking Letters, vol. 5, no. 3, pp. 169–172, 2023.

[7] R. Ezzine, M. Wiese, C. Deppe, H. Boche, “Common Randomness Generation from Finite Compound Sources,” IEEE International Symposium on Information Theory, IEEE, 2024.

[8] V.-C. Andrei, X. Li, U. J. Mönich, and H. Boche, “Sensing-Assisted Receivers for Resilient-By-Design 6G MU-MIMO Uplink,” in IEEE International Symposium on Joint Communications & Sensing, 2023. (Received the Best Paper Award).

[9] H. Boche, R.F. Schaefer, H.V. Poor, F.H.P. Fitzek, “On the Need of Neuromorphic Twins to Detect Denial-of-Service Attacks on Communication Networks,” IEEE/ACM Transactions on Networking (Early Access), 2024.

[10] V. Andrei, X. Li, “Demonstrator: A Digital Twinning Platform for Integrated Sensing, Communications and Robotics,” 4th IEEE Symposium on Joint Communications & Sensing, March 2024. (Received the Best Student Demo Award.)

[11] Y.N. Böck, H. Boche, R.F. Schaefer, F.H.P. Fitzek, H.V. Poor, “Virtual-Twin Technologies in Networking,” IEEE Communications Magazine 61 (11), 2023, 136–141.

[12] H. Boche, A. Fono, G. Kutyniok, “A Mathematical Framework for Computability Aspects of Algorithmic Transparency,” IEEE International Symposium on Information Theory, IEEE, 2024.

Thank you