OPEN CALL ARTICLE

Integrating Sensing and Communications in 6G? Not Until It Is Secure to Do So

Nanchi Su, *Member, IEEE*, Fan Liu, *Senior Member, IEEE*, Jiaqi Zou, *Graduate Student Member, IEEE*, Christos Masouros, *Fellow, IEEE*, George C. Alexandropoulos, *Senior Member, IEEE*, Alain Mourad, *Member, IEEE*, Javier Lorca Hernando, *Member, IEEE*, Qinyu Zhang, *Senior Member, IEEE*, and Tse-Tin Chan, *Member, IEEE*

Abstract

Integrated Sensing and Communication (ISAC) is emerging as a cornerstone technology for forthcoming 6G systems, significantly improving spectrum and energy efficiency. However, the commercial viability of ISAC hinges on addressing critical challenges surrounding security, privacy, and trustworthiness. These challenges necessitate an end-to-end framework to safeguard both communication data and sensing information, particularly in ultra-low-latency and highly connected environments. Conventional solutions, such as encryption and key management, often fall short when confronted with ISAC's dual-functional nature. In this context, the physical layer plays a pivotal role: this article reviews emerging physical-layer strategies, including artificial noise (AN) injection, cooperative jamming, and constructive interference (CI), which enhance security by mitigating eavesdropping risks and safeguarding both communication data and sensing information. We further highlight the unique privacy issues that ISAC introduces to cellular networks and outline future research directions aimed at transitioning from static protection to a "synergistic ISAC security" framework for 6G.

I. Introduction

The rapid evolution of communication systems toward 6G networks promises to deliver unprecedented connectivity, enabling a new era of intelligent, integrated services across diverse sectors, from healthcare to autonomous transportation. One of the core innovations expected in 6G is the integration of Sensing and Communications (ISAC), wherein communication networks seamlessly incorporate sensing capabilities to enhance not only system performance but also the services and applications built on top of these networks. This convergence introduces a range of transformative applications that go beyond traditional communication, creating new possibilities in fields such as autonomous driving, smart cities, environmental monitoring, public safety, and industrial IoT.

However, these technological advances have led to a growing volume and complexity of data exchange among devices, users, services, and network infrastructure in 6G ISAC systems, raising significant security and privacy concerns. With sensitive personal and operational data being generated and processed on an unprecedented scale, ensuring the confidentiality, integrity, and availability of this information has become critical. In this context, recent global developments in data protection regulations highlight the growing emphasis on security in digital ecosystems. For instance, while the European Data Act established clear and fair rules for accessing and using data within the European data economy, the European Union's General Data Protection Regulation (GDPR) continues to set the standard for privacy, imposing stringent rules on data processing and transfers. Similarly, China's Personal Information Protection Law (PIPL) enforces robust data protection practices, particularly concerning cross-border data flows, while the California Privacy Rights Act (CPRA) strengthens consumer rights to control sensitive personal information [1]. Crucially, these regulatory frameworks translate into tangible technical constraints for ISAC design. For instance, the "data minimization" principle prohibits the indiscriminate storage of fine-grained sensing data, encompassing both raw I/Q samples and high-fidelity representations like point clouds. Instead, systems must prioritize edge processing to extract key features while immediately discarding identifiable raw signals. Similarly, strict consent requirements under the CPRA necessitate privacy-preserving waveform designs, capable of selectively suppressing sensing performance for non-consenting users without compromising communication performance.

ISAC, along with its wide-ranging benefits, brings entirely new security vulnerabilities. First, as illustrated

Nanchi Su is with Guangdong Provincial Key Laboratory of Aerospace Communication and Networking Technology, Harbin Institute of Technology (Shenzhen), Shenzhen 518055, China, and also with The Education University of Hong Kong, Hong Kong, China; Fan Liu is with the Southeast University, Nanjing 210096, China; Jiaqi Zou is with Tsinghua University, Beijing 100084, China; Christos Masouros is with the University College London, WC1E 7JE London, U.K.; George C. Alexandropoulos is with the National and Kapodistrian University of Athens, 157 84 Athens, Greece; Alain Mourad and Javier Lorca Hernando are with InterDigital, EC3A 3DH London, U.K.; Qinyu Zhang is with Guangdong Provincial Key Laboratory of Aerospace Communication and Networking Technology, Harbin Institute of Technology (Shenzhen), Shenzhen 518055, China, and also with Peng Cheng Laboratory, Shenzhen 518055, China; Tse-Tin Chan (corresponding author) is with The Education University of Hong Kong, Hong Kong, China.

The work of Nanchi Su was supported in part by NSFC under Grant 62401181 and in part by the Research Matching Grant Scheme from the Research Grants Council of Hong Kong. The work of Fan Liu was supported by the National Natural Science Foundation of China (NSFC) under Grant 62522107 and Grant 62331023. The work of Christos Masouros and George C. Alexandropoulos was supported by the Smart Networks and Services Joint Undertaking (SNS JU) 6G MUSICAL and 6G-DISAC under the EU's Horizon Europe Research and Innovation Programme under Grant 101139176 and Grant 101139130, respectively. The work of Qinyu Zhang was supported in part by the Major Key Project of PCL of China under Grant PCL2024A01 and in part by NSFC under Grant 62027802. The work of Tse-Tin Chan was supported in part by the Research Matching Grant Scheme from the Research Grants Council of Hong Kong.

Digital Object Identifier: 10.1109/MWC.2026.3703015

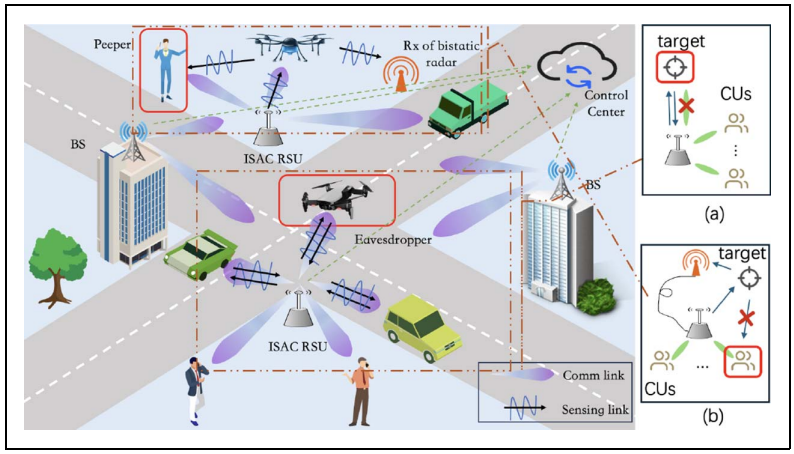

FIG. 1. Data security and sensing privacy threats caused by unauthorized receivers in ISAC systems: (a) Data security, addressed by AN and CI/DI designs in Section III. (b) Sensing privacy, addressed by beamforming and randomization designs in Section IV.

in Fig. 1, a critical challenge unique to ISAC arises when the sensing targets are non-cooperative or potentially malicious. In such cases, illuminating the targets with high-power information-carrying ISAC signals creates the opportunity for the targets to eavesdrop on confidential data within the ISAC signal (Fig. 1(a)). More critically, the new sensing functionality of the ISAC infrastructure makes private information, such as target location, size, shape, and mobility, vulnerable to eavesdropping from unauthorized sensors (Fig. 1(b)). While recent advances in lightweight encryption have addressed latency concerns, cryptography remains fundamentally insufficient for ISAC due to the unique nature of sensing. First, the sensing operation does not incorporate an explicit data transmission from A to B, and therefore there is nothing to encrypt. Security is therefore primarily addressed at the physical layer. Second, leakage of physical semantics: encryption secures bitstreams but leaves the waveform exposed. The beam's spatial signature itself may leak sensitive location or operational data, bypassing upper-layer protection. Consequently, PLS is an essential solution to protect across both functionalities of communication and sensing in the future ISAC networks. Commercial ISAC deployment hinges on adaptive security frameworks that simultaneously safeguard communication data and sensing privacy.

The aforementioned limitations have spurred a growing interest in physical layer security (PLS) research as an essential component of the security and privacy framework for ISAC networks. PLS can provide real-time security without the time delay resulting from the computational overhead, and it is inherently scalable as it does not rely on complex key management systems. Notably, the new sensing functionality brings new opportunities for ISAC security. With the enabling role of sensing in providing environment awareness, ISAC systems can estimate unauthorized sensing channels (i.e., channels used for illicit reception of communication data). This approach addresses the challenge of acquiring eavesdropping channel information [2], which has been a significant barrier in applying PLS in practice in the past. Additionally, the dual-functional waveform provides new avenues of privacy protection, where novel techniques can ensure that adversaries are unable to extract sensitive information through side-channel attacks or unintended signal leakage.

These integrated approaches can fundamentally reshape the security landscape of next generation wireless networks, making ISAC systems not only more efficient but also inherently more secure. In this article, we advocate for the necessity of a "Synergistic ISAC Security" framework. We critically analyze the fundamental Sensing-Communication-Security (S-C-S) trade-offs to propose a paradigm shift that transforms the sensing functionality from a privacy liability into a proactive security enabler. By synthesizing emerging physical-layer strategies for data security, such as Constructive Interference/Destructive Interference (CI/DI) precoding, and sensing-secure approaches, such as Ambiguity Function (AF) engineering and sensing-assisted PLS, we envision a pathway for PLS across communication and sensing, tuned for the sensing-aware multi-functional networks of the future.

II. Security and Privacy Threats in ISAC

Before discussing specific countermeasures, we distinguish data security from sensing privacy. Data security relates to the data *transfer* and primarily safeguards the digital domain, ensuring that information bits embedded in ISAC waveforms remain confidential during transmission. In contrast, sensing privacy relates to sensing data *acquisition* in the first place and protects the physical domain, aiming to prevent the acquisition of state parameters from unauthorized estimation, such as location, trajectory, and velocity. This distinction dictates the choice of physical layer techniques: Section III explores data security solutions, such as AN injection, while Section IV addresses sensing privacy through privacy-preserving beamforming and randomized precoding.

A. ISAC Basics

Given that ISAC has been extensively reviewed in the existing literature, this subsection provides a concise introduction, focusing on three key aspects: the physical layer, the network layer, and joint hardware design.

1) Physical layer techniques: Waveform designs for ISAC systems have been extensively explored and overviewed in the existing literature, encompassing communication-centric, sensing-centric, and joint waveform designs. These methodologies have been thoroughly reviewed in [3], demonstrating that the dual-functional waveforms have enabled complex implementations in vehicle-to-everything (V2X) communications, uncrewed aerial vehicles (UAVs), smart cities, etc. Recent work has also extended the study to the fundamental limits of ISAC, discussing fundamental tradeoffs between the Cramér-Rao Bound (CRB) and capacity distortion (C-D) [4].

2) Network layer schemes: ISAC research at the network level focuses on enhancing cooperation and synergy between S&C functionalities across multiple cellular sites while also providing inherent mechanisms to collect, process, and expose sensing data both within the network and to external applications. Key advancements in network-level ISAC include the development of cooperative multi-cell strategies building on communication-only methodologies such as coordinated multi-point (CoMP). Tailoring these for ISAC expands coverage and enhances the precision of both communication and sensing capabilities [5]. Moreover, integrating new sensing sources into the cellular infrastructure brings additional

challenges in data fusion, real-time analytics, resource management, and security. Addressing these complexities, along with considerations such as signaling overhead and synchronization, calls for innovative network architectures and protocols that balance the performance gains of ISAC against the increased overhead, while ensuring that sensing data is efficiently gathered, processed, and accessible for diverse use cases [6].

3) Hardware architectures for ISAC: The hardware design for ISAC systems emphasizes advanced radio frequency (RF) front-end architectures and antenna designs tailored for dual-functionality in S&C. This involves integrating wideband transceivers capable of supporting various signal types and modulation schemes to facilitate both high-resolution sensing and efficient data communication. Moreover, the design also considers low-latency signal processing hardware to manage the real-time requirements of ISAC systems, ensuring that the hardware can swiftly switch between S&C modes without performance degradation. These developments are crucial in pushing the boundaries of ISAC technology toward practical deployment in future communication networks.

In light of the above, ISAC systems have garnered considerable attention as a crucial enabler for future wireless networks. However, the deployment of ISAC hinges on ensuring robust security and privacy for both the communication data of users and the sensing information of targets. The potential data security and privacy threats in ISAC are elaborated in the following.

B. Data Security Threats in ISAC

The platform integration of the ISAC significantly heightens security vulnerabilities. The security of communication data in ISAC systems can be comprehensively analyzed by examining threats at both the physical and network layers, which can be specified as follows.

MAC layer and network layer: The shared data pathways between these dual functions increase the risk of routing integrity compromises, allowing attackers to exploit sensing-derived information for spoofing or impersonation attacks. This convergence also amplifies the likelihood of man-in-the-middle (MITM) attacks, where adversaries intercept or manipulate communication streams by leveraging sensing-related feedback or configurations. Furthermore, the joint management of S&C data complicates system configuration, increasing the risk of errors that can lead to data breaches and unauthorized access. These threats underscore the critical need for security mechanisms that address the dual-purpose nature of ISAC, ensuring both sensing-derived data and traditional communication streams are protected in complex, interconnected environments.

Physical layer: Fundamentally, PLS needs to be jointly designed with sensing operation, leading to new joint PLS and sensing metrics, methodologies, and entirely new performance tradeoffs. More importantly, different from the nature of communication-only scenarios, at the physical layer of ISAC systems, the transmission of electromagnetic waves presents a unique challenge. Unlike radar-only systems, the probing signal contains communication information, making it prone to potentially malicious targets acting as eavesdroppers to extract critical information. This happens because ISAC may employ the same directional beam for dual purposes: to facilitate communication with users and to illuminate the target for sensing functionality. As the beam is directed explicitly toward the target to capture reflected or scattered signals essential for sensing, the target, strategically located within the beam's path, may receive all transmitted data embedded within this beam. Therefore, ISAC inherently exposes vital communication data to potential interception. Classical PLS, such as secure beamforming and null-steering to the target, do not apply, as they would jeopardize the sensing functionality. This necessitates the conception of entirely new PLS approaches tailored for ISAC.

C. Sensing Privacy Threats in ISAC

On top of the new data security challenges, the privacy for sensing is also jeopardized due to the introduction of the sensing functionality, now inherent in the cellular network signals, architecture, and hardware. When sensing signals emitted by the dual-function base station are reflected by a target and subsequently intercepted by unauthorized receivers, there is a substantial likelihood that these users can obtain target-related information. This scenario presents a significant risk of sensitive target information leakage. Importantly, higher-layer encryption does not apply, as there is no data link to encrypt; it is merely the ability of a node to sense the environment in a passive manner, exploiting the enhanced sensing signaling of ISAC technologies.

In this subsection, we explore these sensing privacy risks in detail, highlighting the vulnerabilities associated with ISAC waveforms and the subsequent threats to sensing privacy.

Transmitter privacy: ISAC signals contain implicit geometrical information designed to mitigate interference. Adversaries can exploit this embedded structure to estimate the transmitter's location or operational parameters [15], bypassing upper-layer protections.

Target confidentiality: The enhanced sensing capabilities for ISAC signals open up opportunities for independent passive sensing from unauthorized nodes. Critically, this offers enhanced sensing eavesdropping performance since ISAC transmission is tuned for sensing. Sensing eavesdroppers can be both nodes external to the ISAC networks and nodes of the network that are not authorized for sensing. An example would be a communication user (CU) that is subscribed to communication services but not to sensing services.

Imaging and environment privacy: In existing and emerging network technologies, significant risks to location and environment privacy arise from exploiting unencrypted control signals, such as channel state information (CSI). Passive eavesdroppers can leverage unencrypted control signals, such as precoder index feedback, to deduce user positions or construct environmental maps. By matching feedback from multiple positions, attackers can achieve high localization accuracy, particularly in mmWave networks with fine-grained beams [11], [12].

In light of the above, ISAC systems are susceptible to various data security and sensing privacy threats, such as eavesdropping and adversarial sensing. To address these challenges, a range of countermeasures has been proposed, as summarized in Table I. The following sections provide a detailed analysis of these ISAC data security and sensing privacy solutions.

Category	Technique	Design Principles	Pros	Cons
ISAC Data Security Design	AN Injection [7]	Introduces artificially designed noise to degrade eavesdroppers' SNR while preserving legitimate communication.	Effective against eavesdroppers, adaptable to ISAC.	Requires accurate CSI for optimal interference placement.
	CI & DI [8]	CI enhances legitimate signal detection, while DI disrupts eavesdroppers' reception by steering signals into undecodable regions.	Energy-efficient alternative to AN, well-suited for mmWave ISAC due to angular dependency.	Requires precise angle estimation and channel state feedback.
ISAC Sensing Privacy Design	Privacy-Preserving Beamforming [9]	Limits the amount of information leaked to unauthorized sensing entities by minimizing mutual information.	Preserves legitimate sensing while restricting unauthorized sensing.	Requires real-time interference management for effective control.
	Transmitter Privacy Protection [10]	Prevents adversaries from extracting radar location information using waveform design and gradient-based precoding.	Prevents localization-based attacks and mitigates side-channel vulnerabilities.	May slightly reduce sensing accuracy in highly dynamic environments. No countermeasures against the training-based adversaries.
	RIS & Precoding Randomization [11], [12]	Prevents adversarial localization through CSI leakage mitigation techniques, such as randomized precoding.	Randomization reduces tracking accuracy without significantly affecting legitimate communication.	Requires additional processing to avoid unnecessary degradation in system performance.
ISAC-Enabled Privacy and Security	Sensing-Assisted PLS [13]	Uses ISAC's sensing capability to infer eavesdropper locations and adjust security measures dynamically.	Enhances proactive security by leveraging real-time sensing.	Performance depends on sensing accuracy and environmental stability.
	Sensing-Assisted Covert Communication [14]	Uses sensing data to predict adversary behavior and design undetectable communication strategies.	Achieves high confidentiality for secure transmissions.	Requires sophisticated environmental modeling and tracking.

TABLE I. Summary of ISAC data security and sensing privacy designs.

III. ISAC Data Security Solutions

A critical requirement for deploying these security schemes is the availability of CSI. In practical ISAC scenarios, legitimate users actively transmit pilot signals to facilitate channel estimation. Conversely, non-cooperative targets or eavesdroppers do not send pilots, meaning the transmitter must rely on sensing echoes to estimate parameters. This distinction implies that security schemes must be robust to the variable levels of channel knowledge.

A. ISAC-Tailored AN Design

AN is an interference-based technique that selectively degrades eavesdroppers' reception while legitimate receivers remain unaffected. By reducing the SNR at unauthorized users, AN prevents malicious interception without compromising authorized data transfer. AN-aided methods have proven effective in mitigating security vulnerabilities in ISAC systems, particularly against malicious targets attempting to eavesdrop on confidential information. By injecting carefully designed interference into legitimate communication channels, AN techniques degrade the signal-to-noise ratio (SNR) at potential eavesdroppers while ensuring reliable communication for authorized users, as illustrated in Fig. 1(a). Recent advancements, such as the optimization framework proposed in [7], employ dynamic AN power and spatial distribution adjustments based on CSI, achieving an optimal tradeoff between data security, communication performance, and sensing accuracy.

Nevertheless, the dependency on precise CSI poses challenges in practical deployments. In practical deployments, CSI uncertainty varies by link type. Legitimate user channels are typically subject to errors from pilot-based estimation, whereas wiretap channels are generally characterized by statistical information or sensing-derived bounded uncertainty regions. To overcome this challenge, robust optimization approaches and statistical CSI models have been developed to ensure consistent security performance despite CSI uncertainties. These innovations underline the significance of AN techniques as a cornerstone for secure and efficient communication in next generation ISAC systems.

B. Constructive-Destructive Interference

CI strengthens desired signals at legitimate receivers, while DI deliberately weakens signals in unwanted directions. Directional Modulation (DM) leverages CI and DI to ensure the QoS for authorized users, whereas it severely degrades signals for unauthorized receivers.

DM leverages CI by ensuring that received signals at legitimate users are pushed away from detection thresholds rather than aligning precisely with intended symbols, as illustrated in Fig. 2. Conversely, DI can be utilized to ensure that information-carrying signals used to illuminate targets are protected against potential eavesdropping [8]. This technique enhances PLS by limiting the ability of eavesdroppers to decode signals. In the ISAC context, this design must also accommodate sensing performance, ensuring that sensing tasks are not compromised while securing communication data. A critical distinction of CI-based schemes is the reliance on instantaneous, perfect CSI at the transmitter side. Unlike AN, CI requires precise knowledge of the legitimate user's phase to align interference at the symbol level. Nevertheless, robust CI designs to imperfect CSI exist in the literature. Conversely, for the DI aimed at targets, the system generally operates under imperfect CSI assumptions, relying on the estimated Angle of Arrival (AoA) from the sensing function to steer nulls or jamming signals. Consider, for example, an ISAC BS serving a user

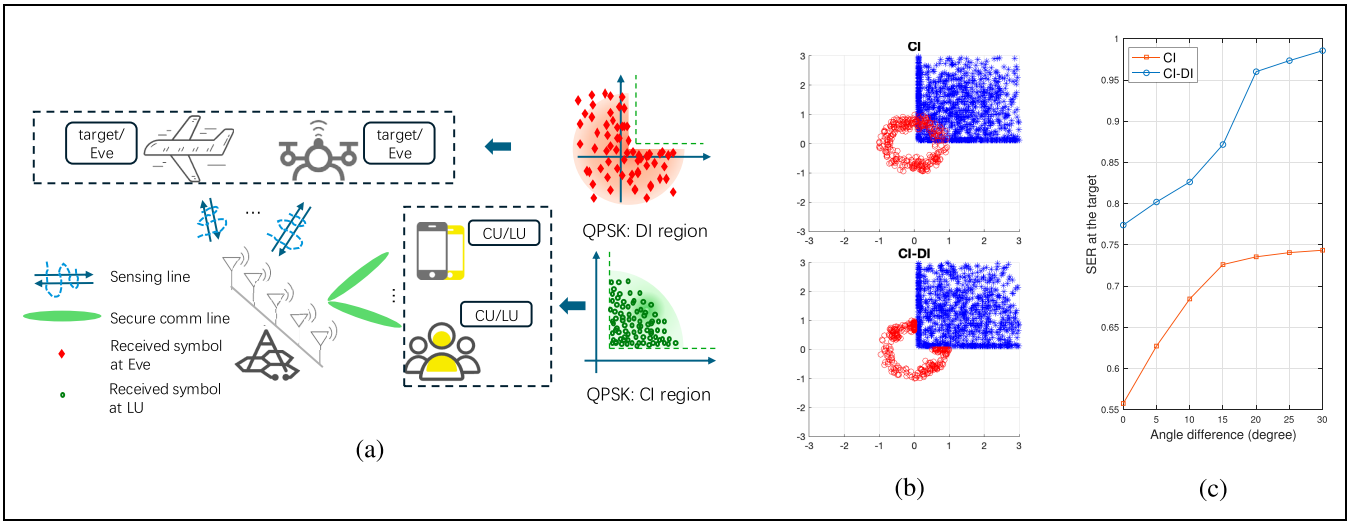

FIG. 2. Communication data security in ISAC systems: CI-DI technique, where each CU is regarded as a legitimate user (LU), and the target is regarded as a potential eavesdropper (Eve). (a) System model: the dual-functional AP ensures communication data security by deploying the symbol-level precoder. (b) Constellations for the CI technique (up) and the CI-DI technique (down). (c) The symbol error rate (SER) of deploying the CI and the CI-DI techniques when the S&C are correlated, where the correlation is depicted by the angle difference in mmWave frequency.

while sensing a suspicious target [8]. Unlike classical MISO CI schemes that typically steer nulls toward eavesdroppers, ISAC encounters a unique "high-power destructive" constraint, where it needs to illuminate the target with high power, but that signal containing minimal useful power for data decoding. The precoder must align signals constructively for the user and destructively for the target to inhibit decoding, yet simultaneously maintain high transmit power toward the target to guarantee the sensing performance. This dual requirement renders simple null-steering inapplicable, necessitating a strict joint optimization of security and sensing SNR.

A key challenge of CI-enabled PLS is the correlation between legitimate and wiretap channels, which constrains secure transmission rates. This issue is further pronounced in ISAC scenarios, where sensing and communication functionalities must be jointly optimized. In mmWave ISAC systems, the correlation between communication and sensing channels depends on angular differences, with the communication channel varying based on the CUs' angles. This necessitates careful joint optimization of PLS and sensing performance, considering angular correlation. Numerical results in Fig. 2(b) and (c) verify the effectiveness of the DI technique even when CUs and targets have small angular separations, demonstrating the feasibility of DM-based ISAC while addressing secure communication and robust sensing challenges.

IV. ISAC Sensing Privacy Solutions

A. Beamforming for Sensing Privacy

A particularly critical scenario arises when a CU subscribes only to communication services but attempts to exploit ISAC signals for unauthorized sensing activities. As illustrated in Fig. 3(a), CUs could potentially use the transmitted waveforms to gather information about surrounding targets or the environment, despite not being granted access to sensing services. This necessitates dedicated mechanisms to restrict their ability to perform unauthorized sensing.

To mitigate this security threat, the authors in [9] propose an innovative beamforming design that maximizes mutual information (MI) for legitimate radar sensing receivers while limiting the MI accessible to unauthorized sensors, including eavesdropping CUs. Unlike traditional AN-aided communication security schemes, which focus solely on protecting data transmission, the proposed approach leverages AN to enhance sensing privacy. Intuitively, AN is designed to be minimally coupled to the legitimate sensing receiver, while imposing additional interference on an unauthorized CU under a mismatched channel/spatial observation. This diminishes the CU's effective sensing SNR and thus reduces the MI available for target/environment inference. This dual-purpose strategy not only improves the sensing capabilities of legitimate receivers but also actively degrades the sensing performance of unauthorized users. The effectiveness of these methods is validated through simulations, as shown in Fig. 3(b), which demonstrate that AN significantly bolsters sensing security by increasing the MI gap between legitimate and unauthorized entities, all while maintaining the quality of service for CUs.

B. Transmitter Privacy

Recall Section II-C, radar privacy can be compromised in both non-training-based and training-based frameworks [15], in spectrum sharing ISAC scenarios. To bridge this gap, authors in [10] proposed leveraging channel characteristics as a defense mechanism against radar privacy interception. Specifically, in Fig. 4, interference from communication devices to radar can be mitigated via optimization-based precoding. The communication precoder is designed to minimize interference at the radar while meeting power and rate constraints. Meanwhile, an adversary with knowledge of the waveform covariance matrix can estimate radar angles by scanning for the minimum power consumption.

To counter radar privacy leakage, a privacy-preserving precoder design enforces a positive gradient for the term associated with radar angles in the optimization problem. This prevents adversaries from

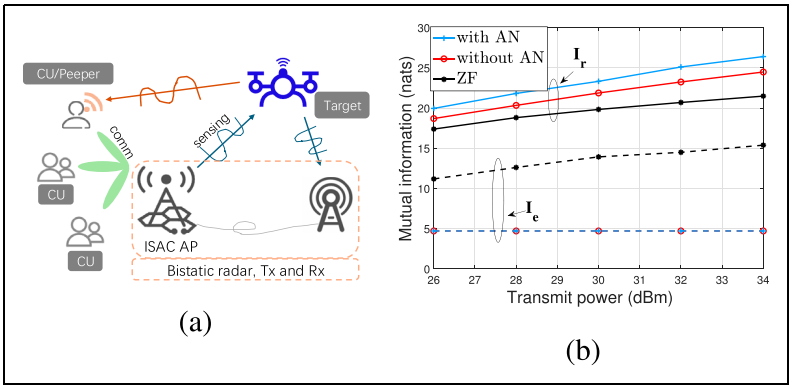

FIG. 3. Sensing privacy: parameter leakage risks of the sensing targets. (a) System model: In a bistatic ISAC system, a central AP transmits dual-functional waveforms intended for both a legitimate radar receiver and K single-antenna CUs. Meanwhile, one of the CUs, serving as an unauthorized peeper/Eve, has perfect knowledge of the transmitted signals. (b) The mutual information gap while deploying the ZF technique, with and without AN designs, where I_r is the MI of the legitimate radar receiver and I_e is the MI of the peeper.

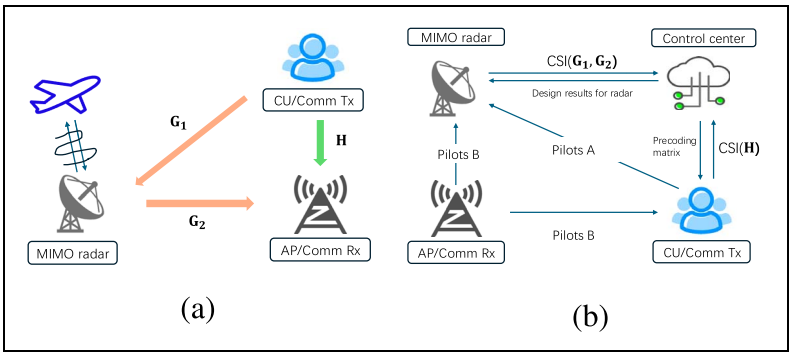

FIG. 4. Sensing privacy: radar information privacy. (a) Spectrum sharing between co-located MIMO radar and communication systems; (b) Spectrum sharing architecture aided by a control center. $\mathbf{G}_1$, $\mathbf{G}_2$, $\mathbf{H}$ denote channels: $\mathbf{G}_1$ from the radar to the CU, $\mathbf{G}_2$ from the radar to the access point (AP)/Comm receiver, and $\mathbf{H}$ from the CU to the AP/Comm receiver.

exploiting angular scans to extract radar information, thereby safeguarding radar privacy in ISAC systems.

C. User Location Privacy

To mitigate location leakage risks from precoder index eavesdropping, randomizing the precoder index selection has been proposed as an effective countermeasure. Rather than always selecting the optimal precoder, users randomly choose from several top-performing precoders, introducing unpredictability into the transmission process. This strategy significantly reduces the accuracy of location inference attacks with minimal impact on overall communication performance. Such measures are critical for enhancing user privacy in 5G networks, where the precise nature of localization techniques poses substantial privacy risks [11].

Balancing user location privacy with high-precision localization is a complex challenge. [12] proposes solutions such as the integration of Reconfigurable Intelligent Surfaces (RISs) and the strategic manipulation of precoder feedback. RISs dynamically optimize signal paths during localization, restricting the precision of location data to legitimate users while obscuring it from potential adversaries. By focusing signals in specific directions, RIS configurations enhance the desired signal quality for user equipment (UE) while distorting or nullifying locational clues, thereby reducing the risk of location leakage.

V. ISAC-Enabled Privacy and Security

Practical ISAC deployments will encounter data security and sensing privacy threats simultaneously and often face conflicting resource demands. For instance, high-power jamming improves security but pollutes the sensing spectrum, whereas stealthy transmission aids privacy but compromises communication reliability. To bridge this gap, we propose a unified framework centered on synergy. Instead of treating sensing, communication and security as competing tasks, we prioritize designs where sensing proactively enhances security through mechanisms like eavesdropper detection and channel estimation. This approach effectively harmonizes the conflicting tradeoffs, as detailed in the following techniques.

A. Sensing- Assisted PLS

Leveraging the inherent advantages of ISAC, the BS can extract the amplitude and phase of each target within the line-of-sight (LoS) distance through reflected echoes. When this is used to sense potential eavesdroppers, it enables the acquisition of wiretap channel information. By recognizing that the angle of the target/Eve cannot always be estimated accurately, one effective design of secure dual-functional transmission is to maximize the secrecy rate, while shaping the radar beampattern such that the main beam may cover all possible angles of each target so as to ensure the sensing performance. This beamformer design effectively ensures the sensing performance and communication data security, where the detailed discussion can be found in [7].

A two-stage sensing-assisted PLS technique was proposed in [13] to alleviate the dependence on the knowledge of the channel conditions, as shown in Fig. 5. In this case, the sensing performance is measured by the Cramér-Rao Lower Bound (CRLB), and the PLS is measured by the secrecy rate. The unique insight of this work is that even without *a priori* knowledge of the wiretap channel, the sensing functionality can still obtain eavesdropping information. A major limitation of traditional PLS is the reliance on prior knowledge of the eavesdropper's CSI. The sensing functionality of ISAC offers an enabling role here by utilizing reflected echoes to estimate the potential eavesdroppers' parameters and synthesize the wiretap channel. Consequently, the design paradigm shifts from assuming "perfectly known" to "imperfectly estimated" CSI, where the estimation accuracy is theoretically lower bounded by the CRB. The first stage aims to obtain the channel information of each target/eavesdropper. Specifically, the dual-functional BS estimates the direction of each target (potential eavesdropper) via emitting an omnidirectional waveform, which accordingly obtains the estimated target/eavesdropper channel. Then, the secrecy rate and the estimation accuracy can be optimized by formulating the weighted problem iteratively until convergence. Fig. 5(b) and 5(c) illustrate that as the direction of each target/eavesdropper estimation improves, so does the data secrecy rate, revealing a key synergy between sensing and security.

B. Covert Communication in ISAC

Extending the sensing-aided secure transmission strategies, sensing-assisted covert communication leverages the sensing capabilities of ISAC systems to achieve undetectable communication. This approach capitalizes on the integration of S&C to design

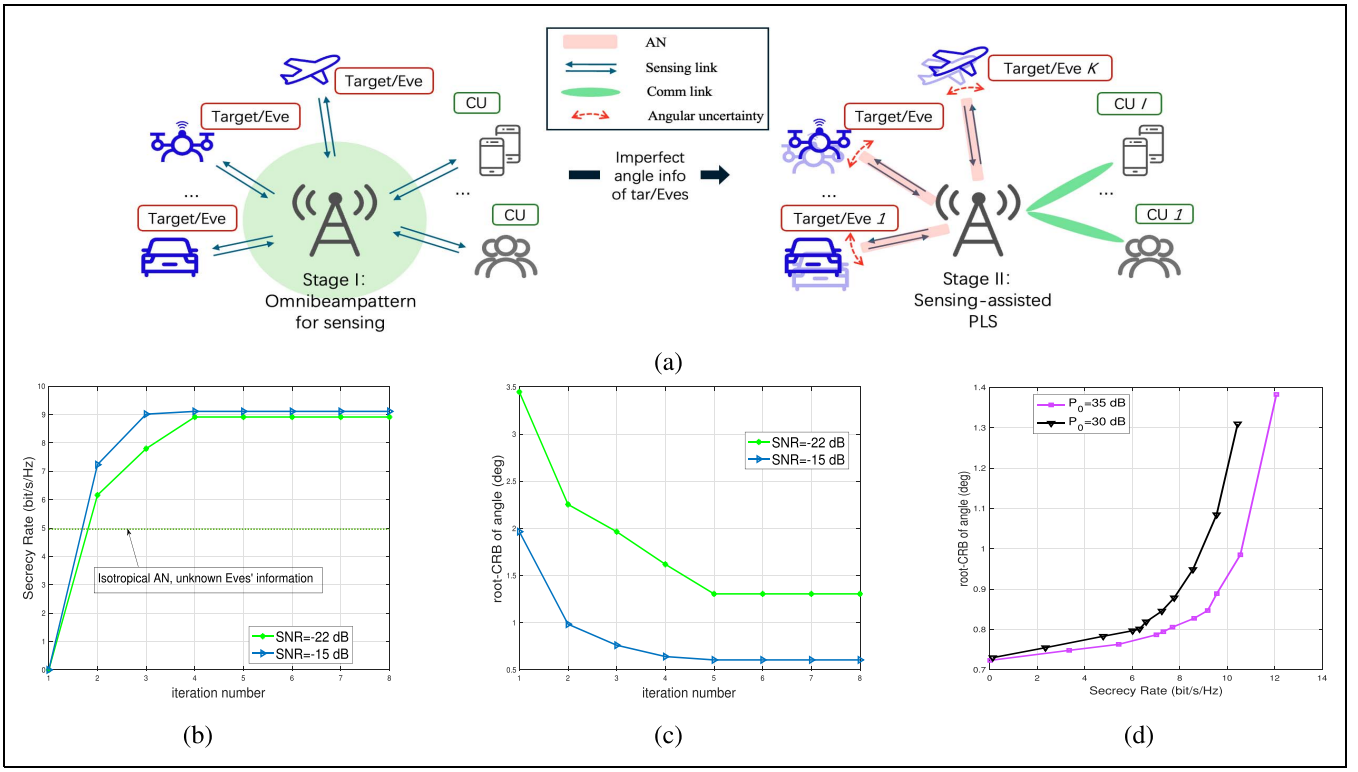

FIG. 5. The two-stage sensing-assisted PLS technique in ISAC and the corresponding performance analysis. (a) The two-stage sensing-assisted PLS; (b) Secrecy rate convergence; (c) CRB convergence; (d) Tradeoff between the PLS and the sensing performance.

transmission schemes that exploit environmental complexities and adversary behavior for improved covertness.

In [14], by employing extended Kalman filtering (EKF), adversarial movements and channel conditions are accurately tracked, enabling the prediction of target behavior and the design of covert transmission strategies. In deterministic scenarios, the optimization problem is formulated to design radar and communication signals, ensuring undetectability while meeting system constraints. For uncertain multi-path environments, robust fractional programming integrates probabilistic covert constraints, maintaining reliable transmission while obfuscating communication activity.

This approach transforms environmental challenges into opportunities, enabling ISAC systems to achieve secure and efficient covert communication in adversarial settings.

VI. Open Challenges and Future Work

A. Passive Target/Eve Classification

In ISAC scenarios, the detection of passive eavesdroppers faces a unique signal-level ambiguity that differs from generic wireless threats. While a passive eavesdropper acts as a silent receiver, its physical reflection characteristics often mimic the Radar Cross Section (RCS) of static clutter like buildings or trees. Consequently, the ISAC system struggles to distinguish a hovering malicious drone from environmental background scatterers. Solving this requires advanced signal processing and AI-driven techniques that exploit subtle features beyond just mobility. These include detecting faint electromagnetic (EM) emissions, such as local oscillator leakage, analyzing micro-Doppler signatures, and identifying distinct behavioral patterns to separate legitimate clutter from stationary threats.

B. Cross-Layer Security

Current research on network security often focuses on individual layers, such as the physical, MAC, and network layers, addressing security concerns in isolation. However, as we move towards the development of next generation networks, 6G and beyond, it is increasingly evident that this fragmented approach may be insufficient to address the complex and dynamic security challenges these networks will face. To establish a robust and secure paradigm for 6G and beyond, it is essential to adopt a cross-layer security strategy that integrates and harmonizes security measures across all layers of the network stack. This comprehensive approach is crucial for maintaining the integrity, confidentiality, and availability of data in future networks, where the convergence of communication, sensing, and computing will require unprecedented levels of security coordination across multiple layers.

C. Sensing Privacy Solutions Are Still Scarce

Most current research in ISAC systems primarily focuses on securing communication data, including sensed data that is being transmitted, with relatively few studies addressing the critical issue of sensing privacy. Passive radar sensing from sensing eavesdroppers can reveal sensitive information about environments, locations, and even individuals, posing significant privacy risks if not adequately secured. Despite the importance of this issue, research in radar and sensing information privacy remains far from sufficient. To ensure the security and privacy of future networks, it is imperative that future work prioritizes the development of robust frameworks and methodologies to safeguard sensing data, thereby preventing

unauthorized access and exploitation. Expanding research in this area will be essential to meet the evolving demands of next generation ISAC systems and to protect users' privacy in increasingly complex and data-rich environments.

VII. Conclusion

While ISAC introduces complex privacy vulnerabilities, this article argues that its sensing capability is ultimately the key to unlocking robust PLS. By navigating the fundamental S-C-S trade-offs, we demonstrate that emerging strategies such as DI for data security, AF engineering for sensing privacy, and sensing-assisted transmission can transform sensing from a liability into a proactive defense mechanism. This paradigm shift charts a clear pathway for future research to move beyond static protection toward dynamic, sensing-aware protection in 6G. As ISAC systems are further implemented in future networks, ongoing research into passive eavesdropper detection, cross-layer security strategies, and privacy-preserving mechanisms will be essential to ensure both efficient and secure deployments.

References

[1] L. Determann and J. Tam, "The California privacy rights act of 2020: A broad and complex data processing regulation that applies to businesses worldwide," *J. Data Protection & Privacy*, vol. 4, no. 1, pp. 7–21, 2020.

[2] G. C. Alexandropoulos, K. D. Katsanos, M. Wen, and D. B. Da Costa, "Counteracting eavesdropper attacks through reconfigurable intelligent surfaces: A new threat model and secrecy rate optimization," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 1285–1302, 2023.

[3] S. Lu et al., "Integrated sensing and communications: Recent advances and ten open challenges," *IEEE Internet Things J.*, vol. 11, no. 11, pp. 19094–19120, Jun. 2024.

[4] Y. Xiong, F. Liu, K. Wan, W. Yuan, Y. Cui, and G. Caire, "From torch to projector: Fundamental tradeoff of integrated sensing and communications," *IEEE BITS Inf. Theory Mag.*, vol. 4, no. 1, pp. 73–90, Mar. 2024.

[5] K. Meng, C. Masouros, A. P. Petropulu, and L. Hanzo, "Cooperative ISAC networks: Opportunities and challenges," *IEEE Wireless Commun.*, vol. 32, no. 3, pp. 212–219, Jun. 2025.

[6] E. Calvanese Strinati et al., "Toward distributed and intelligent integrated sensing and communications for 6G networks," *IEEE Wireless Commun.*, vol. 32, no. 1, pp. 60–67, Feb. 2025.

[7] N. Su, F. Liu, and C. Masouros, "Secure radar-communication systems with malicious targets: Integrating radar, communications and jamming functionalities," *IEEE Trans. Wireless Commun*, vol. 20, no. 1, pp. 83–95, Jan. 2021.

[8] N. Su, F. Liu, Z. Wei, Y.-F. Liu, and C. Masouros, "Secure dual-functional radar-communication transmission: Exploiting interference for resilience against target eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 21, no. 9, pp. 7238–7252, Sep. 2022.

[9] J. Zou, C. Masouros, F. Liu, and S. Sun, "Securing the sensing functionality in ISAC networks: An artificial noise design," *IEEE Trans. Veh. Technol.*, vol. 73, no. 11, pp. 17800–17805, Nov. 2024.

[10] A. Al Hilli, A. Petropulu, and K. Psounis, "MIMO radar privacy protection through gradient enforcement in shared spectrum scenarios," in *Proc. IEEE Int. Symp. Dyn. Spectr. Access Netw.*, Newark, USA, 2019, pp. 1–5.

[11] S. Roth, S. Tomasin, M. Maso, and A. Sezgin, "Localization attack by precoder feedback overhearing in 5G networks and countermeasures," *IEEE Trans. Wireless Commun.*, vol. 20, no. 7, pp. 4100–4112, Jul. 2021.

[12] S. Roth, R. Bessel, and A. Sezgin, "Privacy-aware localization enhancement based on intelligent reconfigurable surfaces," in *Proc. 17th Int. Symp. Wireless Commun. Sys. (ISWCS)*, 2021, pp. 1–6.

[13] N. Su, F. Liu, and C. Masouros, "Sensing-assisted eavesdropper estimation: An ISAC breakthrough in physical layer security," *IEEE Trans. Wireless Commun.*, vol. 23, no. 4, pp. 3162–3174, Apr. 2024.

[14] X. Wang, Z. Fei, P. Liu, J. A. Zhang, Q. Wu, and N. Wu, "Sensing-aided covert communications: Turning interference into allies," *IEEE Trans. Wireless Commun.*, vol. 23, no. 9, pp. 10726–10739, Sep. 2024.

[15] A. Dimas, B. Li, M. Clark, K. Psounis, and A. Petropulu, "Spectrum sharing between radar and communication systems: Can the privacy of the radar be preserved?," in *Proc. Asilomar Asilomar Conf. Signals Syst. Comput.*, Pacific Grove, CA, USA, Oct. 2017, pp. 1285–1289.

Biographies

Nanchi Su (Member, IEEE) is a Postdoctoral Research Associate with Guangdong Provincial Key Laboratory of Aerospace Communication and Networking Technology, Harbin Institute of Technology (Shenzhen), China, and with The Education University of Hong Kong, Hong Kong, China. Her research interests span ISAC, network security, green communications, convex optimization, as well as aerospace communications and networks. She serves as a TPC Member for IEEE flagship conferences.

Fan Liu (Senior Member, IEEE) is currently a Professor with the Southeast University, Nanjing, China. He is the Founding Academic Chair of the IEEE ComSoc ISAC Emerging Technology Initiative (ISAC-ETI), a Vice Chair and Founding Member of the IEEE SPS ISAC Technical Working Group (ISAC-TWG), an Elected Member of the IEEE SPS Sensor Array and Multichannel Technical Committee (SAM-TC), an Associate Editor of IEEE Transactions on Communications, IEEE Transactions on Mobile Computing, and IEEE Open Journal of Signal Processing, and a Guest Editor of IEEE Journal on Selected Areas in Communications, IEEE Wireless Communications, and IEEE Vehicular Technology Magazine. He was a recipient of numerous Best Paper Awards, including the 2024 IEEE SPS Best Paper Award, 2024 IEEE SPS Donald G. Fink Overview Paper Award, 2024 IEEE ComSoc Asia-Pacific Outstanding Paper Award, 2023 IEEE Communications Society Stephan O. Rice Prize, and 2021 IEEE SPS Young Author Best Paper Award.

Jiaqi Zou (Graduate Student Member, IEEE) received the B.Eng. and Ph.D. degrees from Beijing University of Posts and Telecommunications, China, in 2020 and 2024. She is an Engineer with the Department of Electronic Engineering, Tsinghua University. She won the Best Paper Award from IEEE VCIP 2020. Her current research interests include wireless communications and machine learning.

Christos Masouros (Fellow, IEEE) is a Full Professor with the University College London, U.K. He received the 2023 IEEE ComSoc Stephen O. Rice Prize, the 2021 IEEE SPS Young Author Best Paper Award, and Best Paper Awards at IEEE GlobeCom 2015 and IEEE WCNC 2019. He is an Editor for IEEE Transactions on Wireless Communications, IEEE Open Journal of Signal Processing, and IEEE OJ-COMS. He has been an Editor for IEEE Transactions on Communications, IEEE Communications Letters, and a Guest Editor for a number of IEEE Journal of Selected Topics in Signal Processing and IEEE Journal on Selected Areas in Communications issues.

George C. Alexandropoulos (Senior Member, IEEE) is an Associate Professor with the Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, Greece, and an Adjunct Professor with the Department of Electrical and Computer Engineering, University of Illinois Chicago, USA. His research interests span the general areas of algorithmic design and performance analysis for wireless networks with emphasis on multiantenna transceiver hardware architectures, full duplex MIMO, active and passive multifunctional RISs, ISAC, and millimeter-wave/THz communications, as well as distributed machine learning algorithms.

Alain Mourad (Member, IEEE) received the engineering and Ph.D. degrees in telecommunications from the University of Rennes 1 and IMT Atlantique, France. He is the Senior Director and the Head of Wireless Labs Europe, InterDigital, where he leads advanced wireless research and innovation with a strong focus on global standardisation. He actively contributes to international research and standards bodies, shaping next-generation wireless technologies. He has held senior leadership roles at InterDigital, Samsung Electronics, and Mitsubishi Electric, as well as within global organisations including ETSI and WWRF. A Prolific Inventor and a Recognised Thought Leader, he has received Multiple Industry and Corporate Awards. He serves on the ETSI Board and chairs the ETSI ISAC Industry Specification Group.

JAVIER LORCA HERNANDO (Member, IEEE) received the M.Sc. degree in telecommunications from UPM, Madrid, in 1998, and the Ph.D. degree from UC3M, Madrid, in 2026. He is a Consultant for Wireless Labs Europe, Interdigital. He is a Secretary and an Active Contributor of the ETSI ISG ISAC, and was a Secretary of ETSI ISG THz from 2022 to 2024. In his 25 years' experience, he has occupied different positions in the wireless industry and research ecosystem, and led the Radio Innovation, Open RAN and Standards at Telefonica where he received several Innovation Awards. He is a Guest Editor for IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS and served as a TPC Member of major conferences.

QINYU ZHANG (Senior Member, IEEE) is a Professor with Guangdong Provincial Key Laboratory of Aerospace Communication and Networking Technology, Harbin Institute of Technology (Shenzhen), China. His research interests encompass aerospace communications and networks, wireless communications and networks, cognitive radios, signal processing, and biomedical engineering. He has served as a TPC or a Symposium Co-Chair at major IEEE conferences and was the Founding Chair of the IEEE ComSoc Shenzhen Chapter.

TSE-TIN CHAN (Member, IEEE) (tsetinchan@eduhk.hk) is an Assistant Professor with the Department of Mathematics and Information Technology, The Education University of Hong Kong (EdUHK), Hong Kong, China. His research interests include wireless communications and networking, age of information (AoI), and AI-native wireless systems. He has served as a Guest Editor for IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING and IEEE Open Journal of the Communications Society. He has also served on the Organizing Committees and Technical Program Committees of various flagship conferences and workshops, including IEEE ICC and IEEE GLOBECOM.