Towards Multi-Functional 6G Wireless Networks: Integrating Sensing, Communication and Security

Zhongxiang Wei, *Member, IEEE,* Fan Liu, *Member, IEEE,* Christos Masouros, *Senior Member, IEEE,* Nanchi Su, *Student Member, IEEE,* and Athina P. Petropulu, *Fellow, IEEE*

***Abstract*—Integrated sensing and communication (ISAC) has recently emerged as a candidate 6G technology, aiming to unify the two key operations of the future network in a spectrum/energy/cost efficient way. ISAC systems communicate and sense for targets using a common waveform, a common hardware platform and ultimately the same network infrastructure. Nevertheless, the inclusion of information signalling into the probing waveform for target sensing raises challenges from the perspective of information security. At the same time, the sensing capability incorporated in the ISAC transmission offers unique opportunities to design secure ISAC techniques. This overview paper discusses these unique challenges and opportunities for next generation of ISAC networks. We first briefly discuss the fundamentals of waveform design for sensing and communication. Then, we detail the challenges and contradictory objectives involved in securing ISAC transmission, along with state-of-the-art approaches to ensure security. We then identify the new opportunity of using the sensing capability to obtain knowledge target information, as an enabling approach against the known weaknesses of PHY security. Finally, we illustrate some low-cost secure ISAC architectures, followed by a series of open research topics. This family of sensing-aided secure ISAC techniques brings a new insight on providing information security, with an eye on robust and hardware-constrained designs tailored for low-cost ISAC devices.**

I. Introduction

The 6G network, not only an improvement or extension of existing communication technology but also a great paradigm revolution, is envisioned as the new engine of the future intelligent world. In addition to connecting communication nodes, 6G will support ubiquitous sensing, connectivity, and intelligence. Among the exciting features of 6G, sensing will rise from an auxiliary functionality to a basic service, providing an extra dimension of capability of the network [1]. This has prompted the recent research interest of integrated sensing and communication (ISAC), a technology that enables the integration of sensing and communication functionalities with a single transmission, a single device, and ultimately a single network infrastructure. By exploiting a common spectral, hardware platform and signal processing framework, ISAC can improve spectral and energy efficiencies, thus addressing the problem of spectrum congestion and at the same time reducing hardware and signaling costs, referred to as integration gain. Further, by exploiting the possibility to the co-design of the two functionalities, ISAC can enable communication-aided sensing and sensing-aided communication. Hence, it can considerably improve sensing and communication performance, referred to as coordination gain. Benefiting from the above merits, ISAC can enable emerging applications, including enhanced localization and tracking, drone monitoring/management, human activity recognition, vehicle platooning, environmental monitoring, protocols and network-level sensing, sensing-aided beam training/tracking/prediction, sensing-aided resource allocation (such as cell handover, bandwidth/beamwidth/power allocation).

Nevertheless, ISAC comes with unique security challenges, arising due to the shared use of spectrum and the broadcast nature of the wireless transmission. The inclusion of information messages into the radar probing signal makes the communication susceptible to eavesdropping by the target. Indeed, the target that is being sensed can potentially exploit the information-bearing signal, and detect the confidential message intended for the communication destinations [2]. This raises a unique and very interesting tradeoff for the transmitter. On one hand, it wishes to illuminate the target by focusing power towards its direction, and on the other hand, it has to limit the useful signal power that reaches the target to prevent eavesdropping.

A possible solution to the aforementioned security challenge is to apply cryptographic techniques at high layers of the network stack to encrypt the confidential data prior to transmission. However, such solutions have several limitations, such as a tedious secret key management/maintenance process, unprovable security performance in the presence of a computationally strong eavesdropper (Eve), and difficulty in identifying a compromised secret key. Physical layer (PHY) security, an information theory-based methodology could be a complementary approach for securing wireless transmission. By exploiting the channel variability between the Eves and the legitimate users (LU)s, the signal quality that the Eves receive can be degraded to the degree that the Eves cannot extract the message even when they have full knowledge of the secret key [3]. Despite decades of research, the major limitation of a large class of PHY security solutions stems from the either extremely optimistic or overly pessimistic assumptions with regards to what can be known about the Eve. Some methods require full knowledge or statistical information of the Eves'

Zhongxiang Wei is with the College of Electronic and Information Engineering, at Tongji University, Shanghai, China. Email: z_wei@tongji.edu.cn

Fan Liu is with the Department of Electronic and Electrical Engineering, at Southern University of Science and Technology, Shenzhen, China. Email: liuf6@sustech.edu.cn

Nanchi Su and Christos Masouros are with the Department of Electronic and Electrical Engineering, at University College London, London, UK. Email: {nanchi.su.18, c.masouros}@ucl.ac.uk

Athina P. Petropulu is with the Department of Electrical and Computer Engineering, at Rutgers University, NJ, USA. Email: athinap@rutgers.edu

Correponding authors: Fan Liu and Zhongxiang Wei.

channels. Some methods do not require any knowledge on the Eves' channels, such as transmitting artificial noise to jam the entire space except the legitimate destination. However, such methods do not make good use of the available bandwidth by transmitting a signal that does not bear communication information, as summarized in in Table I. There has also been recent works that monitor the changes caused by Eves' interaction with the radio frequency electromagnetic wave field at the the PHY to infer Eves' positions [4]. However, the sensing and communication in [4] are performed separately, and hence the obtained information of the Eves may be outdated, especially in high mobility scenarios. This approach too is not spectrally efficient, as spectral resources are dedicated for sensing only.

Interestingly, the joint sensing and communication mechanism of ISAC ushers in new opportunities for secure design, where the additional sensing functionality can serve as a support to facilitate the provision of security. Motivated by the aforementioned issue, this article overviews the sensing-aided secure designs together with the characteristics of ISAC. Starting from the fundamentals of ISAC systems, we first examine a novel secure ISAC design. Then, we discuss a practical robust secure ISAC design, where knowledge of the target and communication users is imperfectly obtained. Further, some hardware-efficient secure ISAC architectures are reviewed. Open challenges are then identified, before concluding this article.

II. The Fundamentals of ISAC

As an early stage of ISAC, communication and radar spectrum sharing (CRSS) has been investigated from the perspective of spectrum sensing, dynamic spectrum access, and mutual interference mitigation [5], so that communication and radar systems can share the spectrum without significantly interfering with each other. As a further step, ISAC can realize not only spectral coexistence, but also the shared use of hardware platform and even network architecture, as shown in Fig. 1. In addition to providing communication and sensing functionalities, ISAC systems lend themselves to communication-aided sensing, and sensing-aided communication functionalities. Let us start by discussing the fundamentals of ISAC, and then elaborate on secure ISAC transmission.

A. Sensing Basics

While communication aims to accurately convey the information to a receiver, sensing aims to extract target information from the target echoes. Consequently, the useful information for sensing is not in the sensing waveform but in the target return. Interestingly, since that sensing and communication performances are evaluated by different key performance indicators, ISAC waveform design should take different metrics into consideration for implementing the dual functionalities. This typically incurs conflicting design objective between sensing and communications, which needs to be carefully balanced as detailed in the next subsection.

B. Waveform Design for ISAC

ISAC waveform designs can be categorized into sensing-centric, communication-centric, and joint designs, as summarized in Table I.

Sensing-Centric Design: Sensing-centirc design integrates communication messages into a classical sensing waveform, and hence has high compatibility to the radar architecture. Early sensing-centric design works include pulse interval modulation, where the interval between radar pulses is utilized for communication. There have also been designs that leverage the concepts of index modulation, or generalized spatial modulation for waveform design [6]. Another sensing-centric design approach is to sense the target in the mainlobe of the radar beampattern, while embedding information in the beampattern sidelobes [7]. Nevertheless, since the communication symbols are generally embedded into the radar pulses, the sensing-centric design results in a low data rate, limited by the pulse repetition frequency of the radar, which is well below 5G/6G requirements.

Communication-Centric Design: Communication-centric designs leverage the standardized communication waveforms, protocols and architectures for sensing. For example, pilot signals and frame preambles that have good auto-correlation properties and are typically used for channel estimation or multi-user access, have been recently employed for sensing targets [8] [9]. Also, standards-relevant communication waveforms, such as the IEEE 802.11p vehicular communication waveform, have been used for sensing targets in vehicular applications. These communication-centric ISAC designs can realize sensing functionality without sacrificing the communication performance, thereby obtaining high data rate. However, the pilot signal, frame preambles and communication waveforms are not dedicatedly designed for sensing. Accordingly, the main drawback of the communication-centric designs lies in the poor, scenario-dependent and difficult-to-tune sensing performance.

Joint Design: In joint-design ISAC approaches, the beampattern is designed to meet an ideal radar beampattern, while ensuring a high signal-to-interference-plus-noise ratio (SINR) at LUs' for communications [10]. Also, the sum-weighted sensing and communication quality can also be exploited as an objective function, further leading to a Pareto-optimality of the multi-objective optimization. Apart from the optimization-oriented research, the joint-design has also been investigated from the perspective of information theory, such as the channel coding design [11], as well as the theoretic trade-off between the transmission rate and sensing performance design [12]. Evidently, joint design involves dedicated optimization of both functionalities and enables scalable performance trade-offs between them. It enables flexible use of time, frequency, and spatial resources, thereby achieving both high throughput and sensing reliability.

In addition to academic research, there have been extensive industrial activities focusing on ISAC, including the 3GPP (such as S1-214036/214056/214100/214101, R1-2110894/2104724, and R2-210049), IEEE standards (such as 802.11bf WLAN Sensing, 802.15.22.3-2020, and 802.11-

TABLE I
A BRIEF SUMMARY OF THE EXISTING ISAC AND PHY SECURITY DESIGNS.

	Relevant Techniques	Design Principles		Pros	Cons	Remarks
ISAC Design	**Sensing-centric design**	Integrate communication into radar systems	Side-lobe based ISAC [7]	High compatibility to radar systems	Low data rate	(i) These security-agnostic techniques may not preserve the confidentiality of the data; (ii) Even high layer encryption/authentication can be applied, the PHY information contained in the probing waveform can be exploited by the Eve; (iii) Then the Eve is able to decipher the data.
			Index or generalized spatial modulation ISAC [6]			
	Communication-centric design	Leverage the existing communication waveform or protocols for sensing [8] [9]	Use 802.11p communication waveform, or single carrier PHY frame of 802.11ad for sensing	High compatibility to communication systems	Poor sensing performance	
			Use OFDM signals for detection			
	Joint design	Involves optimization of one system or the other, subject to certain constraints for communication or sensing accuracy [10]	Optimize sensing subject to communication quality	High performance of sensing and communication	Need dedicated waveform design	
			Optimize communication, and meanwhile realize the sensing functionality			
			Optimize sum-weighted function of communication and sensing			
		Performance analysis by information theory	Channel coding for improving reception and channel estimation performance at the destination [12]			
			Theoretic trade-off analysis between the communication and sensing [11]			
PHY Secure Design	**Sensing-aided secure design [4]**	Exploit the EM wave change caused by the Eve; then proactively and causally infer the Eve's path loss to assist secure design	Encoder design for providing secrecy even when the Eve moves to improve its eavesdropping capability	The secrecy rate can be close to that obtained with hindsight, had the transmitter obtained the Eve's condition non-causally	Only theoretic analysis is given	Though the sensing and communication are performed on the same channel use, the optimal secure waveform is still unknown
			Characterize the secrecy rate for any sequence of path loss for the Eve			
	Sensing-agnostic secure design [3]	Secure precoding	Exploit the channel disparity between the LU and Eve for sending signals	Adjustable secrecy rate	Need multiple antennas for exploiting spatial disparity	(i) Sensing is disabled; (ii) Rely either on extremely optimistic or pessimistic assumption with regards to the Eve's condition; (iii) The transmitter is not capable of proactively sensing the Eves.
		Artificial Noise	Send isotropic AN towards the null-space of LUs	No requirement of Eve's CSI	Impracticality of network-level interference control	
			Inject spatial AN towards the direction of Eves	More energy-efficient than isotropic AN	Need Eve's full or statistical CSI	
		PHY authentication	Use LUs' PHY attributes for authentication	Difficult for Eve to impersonate; No requirement of Eve's CSI	Need agreement among the communication parties	
		Other hardware-efficient secure design	Constellation rotation and noise aggregation	Low complexity; No requirement of Eve's CSI	Reduced throughput	

2020), and ITU recommendations (such as ITU-T Y.4809 and ITU-T X.1080.2).

III. FROM DUAL-FUNCTIONAL TO MULTI-FUNCTIONAL: INTEGRATING SECURITY INTO ISAC

In this section, we discuss security issues around ISAC and how the sensing functionality can be judiciously utilized for benefiting the provision of information security.

A. The Unique Security Challenges and Opportunities of ISAC

The ISAC transmitter needs to focus its power towards directions that contain targets and ensure that the target echo at the receiver has good enough signal-to-clutter-plus-noise ratio (SCNR) for achieving certain sensing performance. However, as the target might be an Eve, the angle of the sensing beam that enters the SCNR objective is the same as the angle of the Eve, as shown in Fig. 2. This implies that the target has high reception SINR on the embedded communication signal, which significantly increases the susceptibility of information to eavesdropping by the target. Therefore, one should carefully strike a trade-off between sending sufficient power towards the target's direction for sensing, while limiting the useful signal power at the target to prevent eavesdropping. In the following, we examine recent research results of sensing-aided secure ISAC techniques.

The ISAC transmitter is able to sense the angle of arrival (AoA) of the echo signal reflected from the target, and infer the target's position based on the received signal strength. Leveraging this round-trip channel, the wiretap channel from

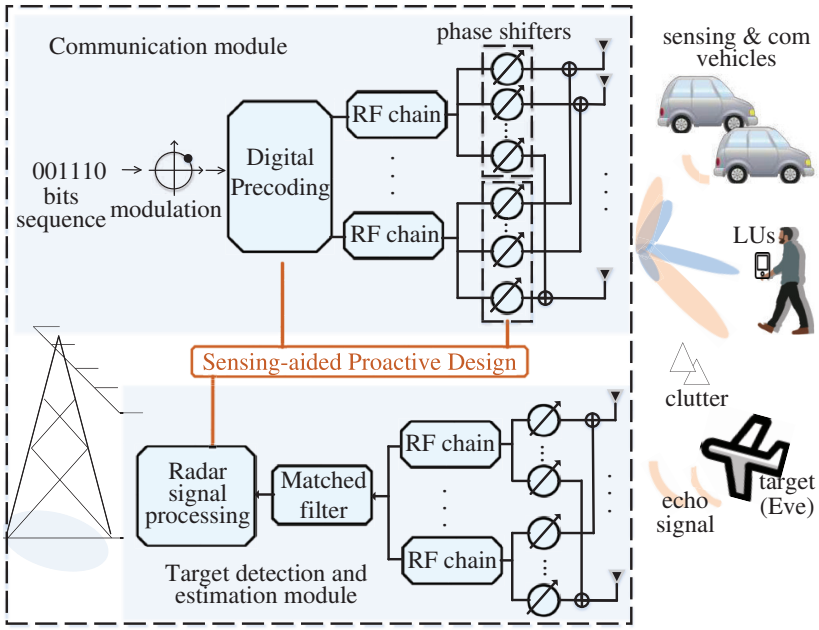

Fig. 1. A generic joint communication and sensing design for ISAC. At transmitter side, the modulated signal is manipulated by digital precoding at baseband, then passes through radio frequency (RF) chains, and finally is dissipated by antennas. On the other hand, while the reflected echo is analyzed for target detection, the sensing results also assist secure waveform design in a proactive and causal manner.

the ISAC transmitter to the target can be estimated. Hence, the proactively and casually obtained wiretap channel, or the target's AoA as a minimum, can be exploited to design a number of secure approaches such as secure beamforming, artificial noise, and cooperative jamming, amongst many others.

The unique ISAC transmission however requires the aforementioned approaches to be redesigned for achieving the "in-band" dual functionality. As an example, in designing a secure dual functional transmission, one can optimize the sensing performance by maximizing the echo signal's SCNR at the ISAC's receiver, while limiting the eavesdropping SINR at the target and at the same time guaranteeing the signal's SINR at LUs above a certain threshold. This equivalently improves the value of the secrecy rate, calculated as the achievable rate difference between the LUs and target. Alternatively, one can maximize the secrecy rate and meanwhile ensure the echo's SCNR at the ISAC receiver for guaranteeing the radar's functionality. Though designing of a sensing-aided secure waveform is not convex in nature, due to the fractional-structured SINR and SCNR constraints of the sensing and communication functionalities, there has been extensive optimization tools for handling these typical fractional-structured optimizations in ISAC systems. Detailed discussions can be found in [2] [5] [10]. Note that in the rare case that the target and LU are in the same direction and both have strong LOS channels, their channels are strongly correlated. In this context, ensuring security at the PHY layer is extremely challenging, where authentication and encryption secure techniques are still needed at the higher layers.

B. Robust Secure ISAC Waveform Design

In practice, a target's position may not be always perfectly obtained, due to sensing error and finite detection resolution. For example, given N antennas arranged in uniform linear structure with half-wavelength spacing, the angular resolution is approximately calculated as $\frac{2}{N}$ (in rad) [10], which means the targets within that angular interval can not be detected individually. When the target's position can only be roughly sensed within an angular region, a wider beam needs to be formulated towards that region to avoid missing the target. However, focusing the beam to a region of space inevitably leads to an increased possibility of the information leakage, giving rise to a need for robust secure waveform design.

When the target is only known to be located within a certain angular region of space, the robust secure waveform can be obtained by minimizing the sum of the target's reception SINR at the possible locations in this angular interval. In this way, the achievable rate of the target can be upper-bounded, thus guaranteeing information security. On the other hand, when the LUs' channels are also not perfectly known by the ISAC transmitter, the channel estimation error can be generally formulated using bounded or un-bounded error models [13]. With the bounded or un-bounded error model, ensuring the LUs' SINR can be further transformed into deterministic or probabilistic constraints, which can be readily handled by a series of established stochastic optimization tools [13].

Let us consider the scenario shown in Fig. 2, where the possible angular interval of the target is $[-5°, 5°]$, while the channel estimation error of the LUs follows Gaussian distribution with variance 0.05. There are 4 LUs and their SINR threshold is 40 dB. The power budget is 20 dBm. The objective of the secure waveform optimization is to suppress the targets' reception SINR, subject to per-LU's SINR requirement, while ensuring the resulting waveform approximates the desired sensing beampattern. As observed in Fig. 2(a), a narrow beampattern is obtained when the

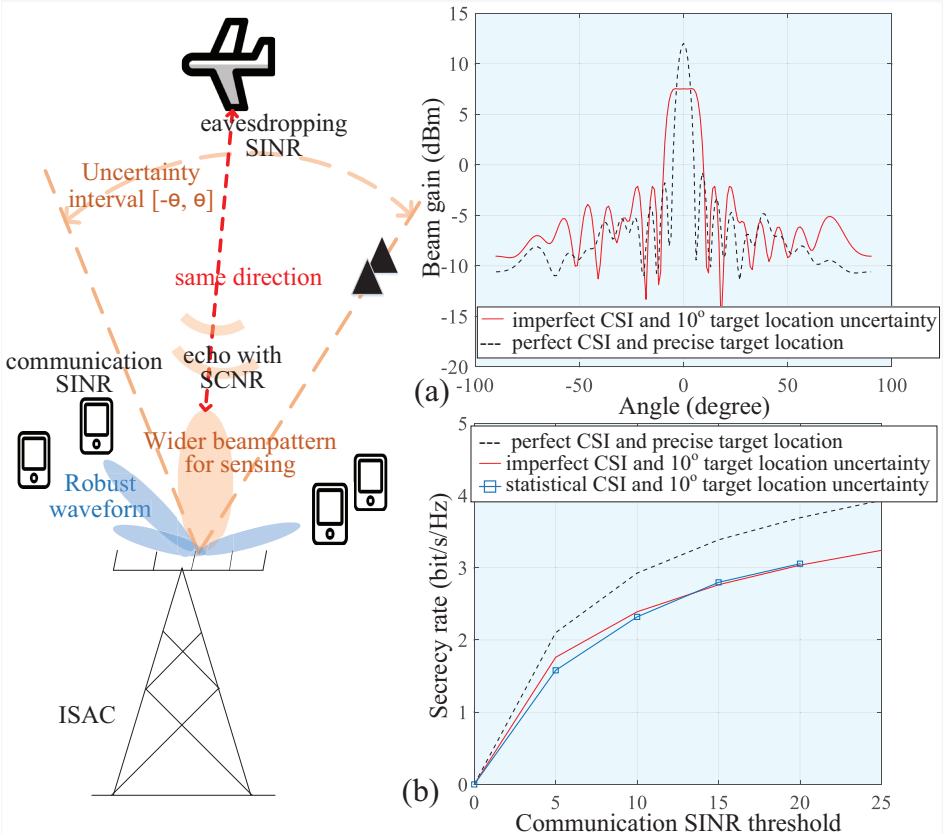

Fig. 2. A practical scenario, where the target's position is roughly sensed within an uncertainty interval, and the LUs' channels are also imperfectly known. (a) The width of the beampattern is adaptively manipulated in different scenarios for sensing the target. (b) By proactively sensing the target, a high level of secrecy rate is achieved.

target location is accurately sensed. Leveraging the proactively obtained location, the transmitter is able to manipulate the dissipated waveform to suppress the eavesdropping SINR of the target, thereby improving the secrecy rate in Fig. 2(b). When the target's location can only be imperfectly sensed, a wider beampattern is formed, directing the same power over the possible region, with reduced power gain of mainbeam. Nevertheless, by suppressing the sum of the target's SINR at the possible locations in the angular interval, a high level of secrecy rate is achieved, even if the ISAC transmitter only knows the statistics of the LUs' channels.

C. Hardware Efficient Secure ISAC Design

At millimeter wave band, a candidate frequency for 5G/6G systems, low-cost and -power consuming hardware is preferred. However, the hardware limitations may jeopardize the sensing and communication performance, and importantly the security of the transmission. A recent abundance of hardware efficient techniques that have been developed for communication-only systems can be leveraged to design hardware-informed secure ISAC transmission [14]. On the feasibility of secure waveform with high hardware efficiency, one approach is to reduce the RF chains through analog architectures that involve phase shifters (PS)s and/or switchers, as illustrated in Fig. 1. This hybrid ISAC involves low-dimensional digital beamforming and high-dimensional analogue beamforming. However, in both fully-digital or hybrid ISAC, the required number of RF chains is no smaller than the total number of data streams for multi-user communications.

To remove the expensive and power-consuming digital-to-analogue converters (DAC)s, a more hardware-efficient secure ISAC technique, built on the concept of directional modulation (DM) is emerging, where parasitic antennas are used as main components in the transmitter. Aided by the LU's channel state information (CSI), symbol modulation happens at the antenna level instead of the baseband level, and the received beam pattern at the LUs is treated as a spatial complex constellation point. In particular, the constructed signal of the LUs does not necessarily align with the desired symbols, but can be pushed away from the detection thresholds of de-modulation, built on the concept of constructive interference (CI) regions [13]. An example is illustrated by Fig. 3 for quadrature phase shift keying (QPSK). Since the decision thresholds for QPSK are the real and imaginary axes, the constructed symbols (denoted by blue dots) at the LUs can be judiciously pushed away from both the real and imaginary axes, where the resultant increased distance with respect to the detection threshold benefits the LUs' communication quality. In a similar vein, the symbols can be constructed for the LUs with higher-order modulations. On the other hand, with the proactively obtained Eve's information, one can intentionally locate the Eve's received symbols (denoted by red stars) into destructive

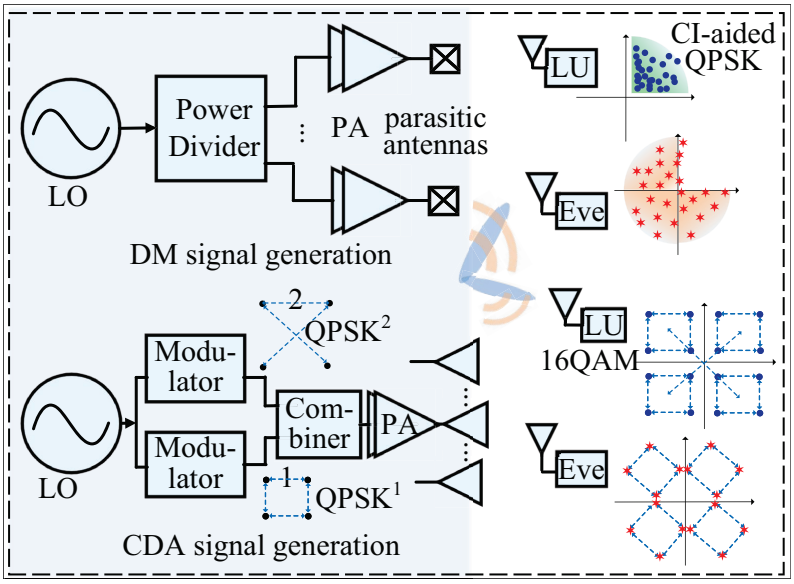

Fig. 3. The DM uses power amplifier (PA)s and parasitic antennas as main components, while CDA uses modulators, linear combiners and PAs as main components.

regions of the signal demodulation, which further impedes the Eve's intercepting behavior at a symbol level.

Another hardware-efficient architecture, namely constellation decomposition array (CDA), also has a high potential for securing ISAC. A simplified block of the CDA is shown in Fig. 3, including the local oscillators, modulators, linear combiners and PAs, but the costly DACs are completely avoided [14]. Evidently, a high-order quadrature amplitude modulation (QAM) can be treated as a vectorial combination of several low-order QAM/PSK signals. For example, a 16-QAM signal can be seen as a combination of a QPSK^1 and a QPSK^2 signals, where the superscript denotes the normalized Euclidean distance between two adjacent symbols. By properly controlling the array with the LU's CSI, a LU can see a correct combination of the intended signal, while any Eve (including the sensing target) located at a different angle will obtain a distorted signal in demodulation. Also, since the CDA transmits low-order modulation signals with a low level of peak-to-power-ratio, the stringent linearity requirement of the PAs is properly relaxed.

IV. Open Challenges and Future Works

ISAC-relevant design is still broadly open, and the remaining challenges can benefit from the communications literature.

Radar Location and Identity Privacy-Preserving Design: On the evolution road of ISAC design, the CRSS system still has its market. Designed to control mutual-interference, there are parameters transformed to one system that contain implicit information about the other. This raises privacy concerns for the two systems, and especially for the military radar. Recent research has unveiled some machine-learning based schemes, which exploit the information contained in the precoder to infer the radar's location [15]. As a result, how to exchange parameters between radar and communication units without loss of each other's privacy, while maintaining a minimum level of mutual interference remains an open challenge.

Secure ISAC Design for 5G/6G KPIs: In recent years, ultra-reliable and low-latency, and massive-device communications have received much attention in 5G/6G applications. Those applications involve new metrics and protocols, such as latency, reliability, grant-free massive access, short packets, and so on. Rethinking secure ISAC techniques to align with these stringent requirements, and also to maintain a low level of complexity and overhead is a fertile area of research.

On Compatibility of Secure ISAC and 5G NR: 5G new radio (NR) has standardized a series of waveforms, including but not limited to filter-OFDM, DFTS-OFDM, and FBMC-QAM. Also, 5G NR has also proposed adaptive wireless interface configuration, such as changeable frame structure and adaptive 15-120 KHz carrier spacing. With different communication environments and specific performance requirement, how to leverage the flexible waveform specification and wireless interface configuration? Essential work is needed to bridge the gap between theory and implementations.

Network Level ISAC Design and Secure Performance Analysis: Networking design has been investigated for cellular communication systems, where coverage probability and ergodic capacity are analyzed in a systematic manner. This network level investigation advises networking planing and engineering design with an eye to the interests of the whole system. While the existing ISAC-related research is investigated in simple scenarios, considering the heterogeneity and high nodes density in future communication systems, the systematic ISAC designs need fundamental research.

ISAC for New Security Metrics: Apart from data confidentiality, the concept of security has been greatly generalized in 5G/6G communications, such as covertness and privacy. In some scenarios, users want to communicate with others covertly, referred to as low-probability of detection communication. Coordinated with sensing, it becomes easier to detect an intruding adversary's information, which is then exploited

to design covert waveform to hide an ongoing communication. On the other hand, sensing may be leveraged by an adversary to violate users' privacy, such as sensing pedestrians' non-shared positions and trajectories, imaging users' indoor activities. Hence, it is demanding to rethink the role of ISAC from the perspective of new security metrics.

V. CONCLUSIONS

This article has discussed the exciting intersection of ISAC and security. Starting from the fundamentals of the ISAC, we first have introduced the methodology of the waveform design for joint sensing and communication. Then, we have examined the sensing-aided secure ISAC techniques to prevent the confidential signal embedded in the probing waveform from being eavesdropped upon by the sensing target. Finally, the recent interests in robust and hardware-efficient secure ISAC has been reviewed. This family of sensing-aided secure ISAC design offers a broad field of preserving information security in a proactive manner, which holds the promise of exciting research in the years to come.

ACKNOWLEDGEMENT

Z. Wei would like to acknowledge the financial support of the NSFC under Grant 62101384, as well as of the Chongqing Key Laboratory of Mobile Communication Technology under Grant cqupt-mct-202101. C. Masouros would like to acknowledge the financial support of the EPSRC under Grant EP/R007934/1. A. P. Petropulu would like to acknowledge the financial support of the ARO under Grant W911NF2110071.

REFERENCES

[1] Y. Cui *et al.*, "Integrating radio sensing and communications for ubiquitous IoT: applications, trends and challenges," *IEEE Network*, vol. 35, issue. 5, pp. 158-167, Oct. 2021.

[2] 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.

[3] M. Bloch *et al.*, "An overview of information-theoretic security and privacy: metrics, limits and applications," *IEEE J. Sel. Inf. Theory*, vol. 2, no. 1, pp. 5-22, Mar. 2021.

[4] M. Tahmasbi, M. Bloch, and A. Yener, "Learning an adversary's actions for secret communication," *IEEE Trans. Info. Theory,* vol. 66, no. 3, pp. 1607-1624, Mar. 2020.

[5] B. Li, A. P. Petropulu, W. Trappe, "Optimum co-design for spectrum sharing between matrix completion based MIMO radars and a MIMO communication system," *IEEE Trans. Sig. Process.,* vol. 64, no. 7, pp. 4562-4575, Jul. 2016.

[6] T. Huang *et al.*, "MAJoRCom: a dual-function radar communication system using index modulation," *IEEE Trans. Signal Process.*, vol. 68, no. 5, pp. 3423-3438, May 2020.

[7] A. Hassanien *et al.*, "Dual-function radar communications: Information embedding using sidelobe control and waveform diversity," *IEEE Trans. Signal Process.*, vol. 64, no. 8, pp. 2168–2181, Apr. 2016.

[8] P. Kumari, N. Myers, and R. W. Heath, "Adaptive and fast combined waveform beamforming design for mmWave automotive joint communication-radar," *IEEE J. Sel. Topics Sig. Process.,* vol. 15, no. 4, pp. 996-1012, Jun. 2021.

[9] P. Kumari *et al.*, "IEEE 802.11ad-based radar: an approach to joint vehicular communication-radar system, *in IEEE Trans. Veh. Tech.*, vol. 67, no. 4, pp. 3012-3027, Apr. 2018.

[10] F. Liu *et al.*, "Toward dual-functional radar-communication systems: optimal waveform design," *IEEE Trans. Signal Process.*, vol. 66, no. 16, pp. 4264–4279, Aug. 2018.

[11] M. Kobayashi, G. Caire, and G. Kramer, "Joint state sensing and communication: optimal tradeoff for a memory-less case," in *IEEE Proc. ISIT'18*, Vail, USA, pp. 111-115.

[12] W. Zhang, S. Vedantam, and U. Mitra, "Joint transmission and state estimation: a constrained channel coding approach," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 7084–7095, Oct. 2011.

[13] Z. Wei *et al.*, "Multi-cell interference exploitation: enhancing the power efficiency in cell coordination" *IEEE Trans. Wireless Commun.*, vol. 19, no. 1, pp. 547-562, Jan. 2020.

[14] N. S. Mannem *et al.*, "A mm-wave transmitter MIMO with constellation decomposition array for key-less physical secured high-throughput links," in *Proc. IEEE RFIC'21*, Denver, US, pp. 199-202.

[15] A. Dimas *et al.*, "On radar privacy in shared spectrum scenarios," in Proc. *IEEE ICASSP'19*, Brighton, UK.

Zhongxiang Wei is an associate professor of Electronic and Information Engineering at Tongji University. He received the Ph.D. from the University of Liverpool (2017). He was a postdoc researcher at the University College London (2018-2021), and was a Research Assistant at the A∗STAR Singapore (2016-2017). He has served as a TPC chair/member of various international flagship conferences. He was a recipient of an Exemplary Reviewer of the IEEE TWC, the Outstanding Self-Financed Students Abroad in 2018, and the A∗STAR Research Attachment Programme in 2016. His interests include MIMO systems, PHY security, and anonymous communication designs.

Fan Liu is an Assistant Professor of the Department of Electronic and Electrical Engineering, Southern University of Science and Technology. He received the Ph.D. and the BEng. degrees from Beijing Institute of Technology, China, in 2018 and 2013, respectively. He was a Marie Curie Research Fellow at University College London, UK, from 2018 to 2020. He is an Associate Editor of the IEEE OJSP and IEEE COMML, and a Guest Editor of the IEEE JSAC and IEEE WCM. He is also the Founding Academic Chair of the IEEE ComSoc ISAC Emerging Technology Initiative. He was the recipient of the 2021 IEEE SPS Young Author Best Paper Award, and the 2019 Chinese Institute of Electronics Best PhD Thesis Award. His research interests include ISAC, vehicular networks, and mmWave communications.

Christos Masouros is the Professor of Electrical and Electronic Engineering at UCL. He received his PhD from the University of Manchester, UK (2009). His interests include wireless communications and signal processing with specialty on Large Scale Antenna Systems and Interference Exploitation. He has held a Royal Academy of Engineering Research Fellowship (2011-2016). He is co-author of the 2021 IEEE SPS Young Author Best Paper Award (F. Liu). He is an Editor and Guest Editor for IEEE TWC/TCOM/JSTSP/JSAC and Vice-Chair of the IEEE ComSoc ISAC Emerging Technology Initiative.

Nanchi Su (S'18) received the B.E. and M.E. degrees from Harbin Institute of Technology, China, in 2015 and 2018, respectively. She is currently pursuing her Ph.D. degree at UCL, U.K. Her research interests include CI design, PHY security, and ISAC signal processing.

Athina P. Petropulu is a Distinguished Professor of Electrical and Computer Engineering at Rutgers University. Her interests include radar signal processing and PHY security. She received the Presidential Faculty Fellow Award (1995) from NSF and the US White House, and the 2012 IEEE Signal Processing Society (SPS) Meritorious Service Award. She is IEEE and AAAS Fellow. She is co-author of the 2005 IEEE Signal Processing Magazine Best Paper Award, the 2020 IEEE SPS Young Author Best Paper Award (B. Li), the 2021 IEEE SPS Young Author Best Paper Award (F. Liu), and the 2021 Aerospace and Electronic Systems Society Barry Carlton Best Paper Award. She is currently President-Elect of the IEEE SPS.