Secure Integrated Sensing and Communications (S-ISAC) Network

Terry Guo and Husheng Li

2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall) | 979-8-3315-1778-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/VTC2024-Fall63153.2024.10757770

***Abstract*—This paper tries to raise awareness of security and privacy issues associated with Integrated Sensing and Communications (ISAC). In the context of ISAC, sensing (or radar) and communication functionalities can work synergically, i.e., the two functionalities can benefit each other, which is both exciting and worrisome. Our concern is that ISAC exposes increased vulnerability and faces threats we never experienced before, while it offers tremendous opportunity. In the ISAC system not only can an attacker wirelessly sniff data transmitted by legitimate users, but can also locate them passively or actively via illuminating. For instance, sensing-assisted eavesdropping in ISAC is much easier than traditional eavesdropping. With the availability of precise sensing at sub-centimeter accuracy, an attacker gains much more information than just a MAC address. The stolen information can include location, speed and ambient condition, and may be in the format of images. Consequently, attacks can be more targeted and effective. In addition, as sensing becomes ubiquitous and collaborative sensing becomes easier, it is harder to preserve privacy and to manage the trustworthiness of a large number of participants. We introduce a secure ISAC (S-ISAC) framework and propose a number of solutions. In contrast to some information-theoretic works on ISAC security, we emphasize practical countermeasures from an ISAC-network perspective. We also propose a number of research topics that need to be addressed before the ISAC concept is fully adopted by the industry.**

***Index Terms*—Security, privacy, Integrated Sensing and Communication (ISAC).**

I. Introduction

Integrated Sensing and Communication (ISAC) or Joint Communication & Sensing (JC&S) is expected to support more functionality without requiring additional spectrum or infrastructure [1], The increased capabilities are both exciting and worrisome, as ISAC enlarges the attack surface (a sum of all security vulnerabilities) and enables new threats we have never experienced before, though it offers attractive opportunities. In contrast to traditional communication or sensing networks, ISAC also opens new dimensions for both attacking and defending wireless networks. It is not clear whether the new ‘armaments’ have greater benefit for the attacker or defender. **As the game changes, traditional threats have to be re-evaluated and defensive strategies have to be revised.**

Nevertheless, we are forced to join an attack-defense game and new defensive strategies against threats to ISAC are needed *before* the technology is widely adopted. These issues are closely related to very low-level information, such as user and target locations, propagation environment, and even circuit-level phenomena. These issues have not been well addressed in traditional cyber security research. Furthermore, practical constraints in ISAC are different from those in radar and communication systems, Special constraints in commercial applications include low-cost, run-time limit and limited resources (transmit power, battery supplies, computing power, etc.), given that the dedicated defense strategies used for the military are not feasible for commercial applications. However, in a commercial ISAC system, there are ubiquitous user equipments (UEs) and base stations (BSs) that can act collaboratively; i.e., they can help each other by acting as verifiers, noise jammers and deceptive jammers, etc. This collaboration potential naturalizes the negative impact imposed by the constraints on resources and cost.

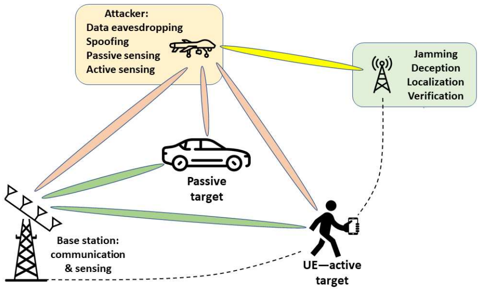


Fig. 1. An exemplary ISAC system with offense and defense.

There have been some works on ISAC security exploiting either spatial characteristics [2]–[9] or memoryless state-dependent ISAC channels [10], [11]. However, these works deal with data eavesdropping at the physical-layer security from an information theoretic perspective. They do not consider the practical solutions to security and privacy issues in ISAC from a holistic ISAC network perspective. In response to the urgent need for securing systems incorporating the emerging ISAC technology, in this paper we raise the awareness of security and privacy threats to ISAC by proposing a defensive framework with different countermeasures, leveraging multi-format sensing ability, and considering practical constraints and conditions (e.g., varying environment and insufficient knowledge about the attackers).

The rest of this paper is organized as follows. A secure ISAC (S-ISAC) framework is provided in the next section. Section III describes some practical techniques for proactive protection. Dynamic S-ISAC user trust is discussed in Section IV, followed by remarks along with future research topics in Section V.

T. Guo is with the Center for Manufacturing Research, Tennessee Technological University, Cookeville, TN (email: nguo@tntech.edu). H. Li is with Purdue University, West Lafayette, IN 47907, USA (email: husheng@purdue.edu). This work is supported by the National Science Foundation under grant #2135275.

979-8-3315-1778-6/24/$31.00 ©2024 IEEE

II. S-ISAC Framework

From a physics point of view, radio sensing and communication happen in an electromagnetic (EM) field that can be specified in strength, frequency and phase. In many practical situations there is a limited capability to confine the EM field within a space of interest, possibly resulting in information leakage to unintended parties with comprehensive inference ability. In particular, a target can block and/or reflect the incoming EM wave, which can give additional hints to nearby attackers to eavesdrop the transmitted data and infer the state (e.g., location, velocity, pose, etc.) of the target. In other words, in addition to the data eavesdropping, there could be one more type of eavesdropping in an ISAC system—location eavesdropping, or more general, target-state eavesdropping that has not been adequately studied.

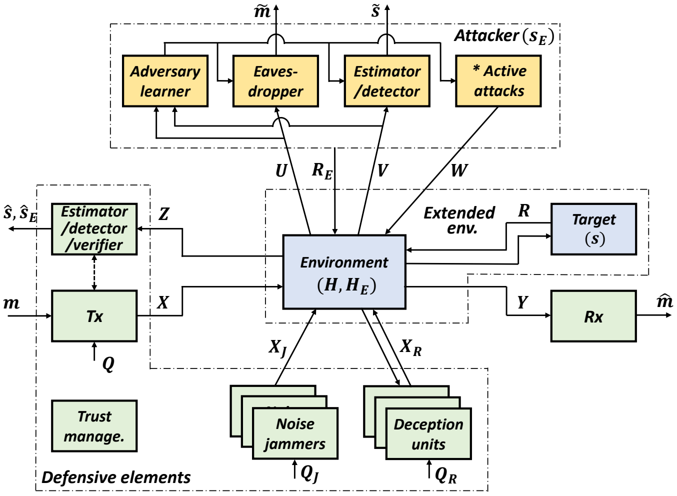


Fig. 2. Analytic diagram of simplified S-ISAC system (Active attacks: jamming, illuminating and various spoofing attacks like Sybil and replay attack).

A. System Model

We consider an S-ISAC system where the users can be regarded as targets with certain radar cross section (RCS) from the perspective of sensing and they can be classified into two types: 1) passive user/target, a physical object that does not emit any EM signals but may be able to receive EM signals; and 2) active user/target, a device that can transmit and reflect EM signals. In such a system, two types of information are involved: communication data and target states (location, speed, size, shape, etc.) The following **threat models** are considered: **data eavesdropping, illegal illuminating, target state eavesdropping or sensing, target state spoofing** and **jamming**.

Shown in Figure 2 is a high-level analytical diagram of a simplified S-ISAC system consisting of a sophisticated attacker and defensive elements–there can be multiple transmitters, receivers, targets and eavesdroppers in reality. The parameters Q, Q_J and Q_R represent transmitter precoding, jamming setting and deception setting, respectively; H and H_E refer to environments for legal users and attackers, respectively. $\hat{m}$ and $\tilde{m}$ are intended and adversarial estimates of communication data m; $\hat{s}$ and $\tilde{s}$ are intended and adversarial estimates of target's state s; and $\hat{s}_E$ is the intended estimates of attacker's state s_E. This simplified analytical diagram does not imply a limited scope. The primary task of this ISAC system is to transmit data wirelessly and sense the state of the target simultaneously. The transmitter plays a role in both data transmission and radar illumination. The transmitter and state estimator (or detector) can be co-located (acting as a mono-static radar) or separated (acting as a bi-static radar; or a multi-static radar if there are more than one state estimator or detector). The attacker is located at position p and includes the following malicious functions: data eavesdropping (passive), state estimation or detection of targets, active attacks including jamming, illuminating, and various spoofing attacks such as Sybil and replay attack. At least four types of countermeasures are considered here to combat the attacks jointly: 1) transmitter-side process that may combine beamforming, frequency sub-band selection and power allocation, base-band precoder, etc., 2) protective jamming, 3) protective deception, and 4) trust management. Both the jammer and deceptive units use antenna directivity to reduce interference to the communication receiver. Also, these units could be co-located with or separated from the transmitter. The target shown in Fig. 2 is an individual passive (no emission of EM signal) object, while it could be the transmitter itself, in which case it is an active target (signal source). One-way communication is considered here. However, it can be extended to two-way communications, and the transceiver itself may be an active target.

B. Problem Formulation

Collectively, a number of techniques can be regarded as high-dimensional **S**pace-**T**ime-**F**requency **P**recoding (**STFP**) with an extended parameter $\{Q, Q_J, Q_R\}$. N_R deceptive units generate fake target echo signals to confuse the adversarial estimator. To win the attack-defense game, we need to design the system optimally; i.e., choosing the optimal STFP parameter $\{Q, Q_J, Q_R\}$ with respect to the following quality-of-service (QoS) metrics: **secrecy rate (or capacity)** $I(X;Y|H) - I(X;U|H_E)$ for communications; **distortion ratio** $\mathbb{E}[d(s,\hat{s})]/\mathbb{E}[d(s,\tilde{s})]$ for state estimation; and **detection probability ratio** $p/\tilde{p}$ for target detection; where H and H_E represent channels for the legitimate user and the attacker, respectively; $I(\ )$ denotes mutual information, and $I(X;Y|H) - I(X;U|H_E)$ is the secrecy rate; $d(\ )$ is the distortion function; p is the detection probability of the target known by the legitimate users, and $\tilde{p}$ is the target detection probability inferred by the attacker, reflecting the **covertness level**. Extended from the formulation in [10]–[13], the optimization considering the worst case can be formulated conceptually as:

$$
\begin{aligned}
&\max\ \min\big\{I(X;Y|H) - I(X;U|H_E)\big\} \qquad (1)\\
&\quad \text{s.t. } \mathbb{E}[b(X)] \le B,\ \mathbb{E}[b(X_J)] \le B_J,\ \mathbb{E}[b(X_R)] \le B_R\\
&\qquad\quad \mathbb{E}[d(s,\hat{s})]/\mathbb{E}[d(s,\tilde{s})] < \beta,\ \beta > 1\\
&\qquad\quad p/\tilde{p} > \gamma,\ 0 < \gamma < 1
\end{aligned}
$$

where $b(\ )$ is the function of transmit power, and B, B_J and B_R are transmit power limits; β is the threshold of distortion ratio; and γ is the threshold of detection probability ratio. Our analysis can also be extended to other possible formulations of the problem.

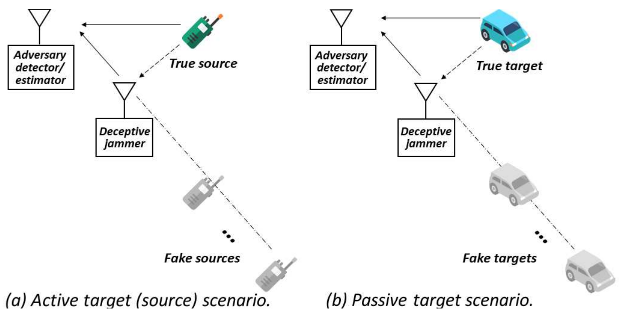
Although the above formulation can guide us toward the optimal goal, in practice it is unlikely to solve the very complicated problem that looks for global robust optimization, especially when the knowledge about the attackers is not sufficient. Therefore, we have to consider some practically achievable (possibly suboptimal) solutions.

III. Practical Techniques for Proactive Protection

Recalling Fig. 1 and Fig. 2, assume that an attacker conducts adversarial detection and estimation via sniffing and actively illumination[1]. Target-state sensing/eavesdropping is part of these adversarial actions. This section covers three defensive techniques against adversarial illumination, target detection, and target estimation: 1) identify suspicious illumination signal sources via authentication with predefined secrecy and localization result; 2) proactively deceive the attacker to reduce the chance of being detected; and 3) physical-layer protection of ISAC users' privacy. We consider two types of targets under protection: i) a signal source as an active target being monitored by the adversarial sensors, where the signal source transmits dual-function (sensing & communication) waveforms for simultaneous sensing and communication; and ii) a physical object (not actively emitting EM signals) with certain RCS as a passive target under adversarial illuminating.

A. Identification of Adversarial Illumination and Detection

Traditionally, a target being illuminated has no way to prevent itself from being "seen" and to know whether or not the illuminator is legitimate. Adversarial detection and estimation of legal targets can lead to unwanted consequences. Fortunately, users in an ISAC system can agree on a predefined secrecy for identifying signals emitted from participating entities. Unlike a traditional radar user, an ISAC user with the dual-function mechanism can easily do so. There can be various ways to convey secrecy for authentication [14]–[17], and we are more interested in approaches that can be embedded in the dual-function waveforms and do not consume significant resources. Formally, the secrecy is formed as a **watermark** carried by a dual-function waveform, then legitimate ISAC users can perform authentication based on it. A watermark can be in different formats; e.g., small variations in amplitude and/or phase [14], [17] at a level near to circuit noise. The natural frequency drift [16] or I/Q imbalance [18], [19] can be directly used as unique watermarks too. Many of these watermarks are essentially I/Q variations and can be easily mixed with regularly modulated data symbols.



(a) Active target (source) scenario. (b) Passive target scenario.

Fig. 3. Illustration of deceptive jamming.

B. Deception Solutions in Commercial Infrastructure

For active targets to hide their emissions, a straightforward protection is to use traditional low probability of detection (LPD) and low probability of intercept (LPI) techniques, such as spread spectrum [20], [21]. However, there are limited degrees of freedom to improve the LPI/LPD of active targets, especially when dual-function waveforms are employed in an ISAC system with cellular configuration. Also, there are no inexpensive ways to reduce the target RCS. In contrast to passive countermeasures, the ideas explored below are proactive countermeasures against adversarial target detection and estimation. Deceptive jamming is a traditional electronic warfare technology used by the military. A false-target jammer or deceptive jammer is typically an intelligent full-duplex transceiver that is able to relay an incoming illumination signal with predefined amplitude and delay to imitate a fake target echo, distracting the adversarial detector/estimator [22]–[24]. Fig. 3 shows such an idea for both types of targets. By using multiple pairs of amplitudes and delays, multiple fake targets can be generated by a single deceptive jammer. Employing such dedicated jammers can be costly and infeasible in a commercial wireless system, and low-cost deception solutions are desired.

C. Physical-Layer Protection of ISAC Users' Privacy

Because of ubiquitous sensing in ISAC systems, privacy violations become easy. Fortunately, many existing anti-privacy thieving can be applied to protect ISAC users' privacy. Assume that a privacy sniffer is capable of using a classification algorithm, such as the k-nearest neighbors, to guess who is currently sending packets, where N transmitters represent N classes. It is assumed that the sniffer knows the exact number of the transmitters and can obtain a training dataset of received signal strength (RSS) in advance. This assumption is impractically strong in reality since without legitimate users' cooperation the sniffer is not able to acquire the training dataset. Nevertheless, with this assumption, the worst-case outcome can be observed.

Practical countermeasures in the physical-layer include: **cooperative jamming**, **directional antennas or beamforming**, **sending redundant packages smartly**, and **transmit power**

[1] This assumption is for the sake of easy explanation but the scheme can be extended to more sophisticated scenarios.

dithering. The last countermeasure selects a transmit power randomly between $P_{Tx} - \Delta P$ and $P_{Tx} + \Delta P$, where P_{Tx} is the regular transmit power in dBm and ΔP is the power dithering range in dB.

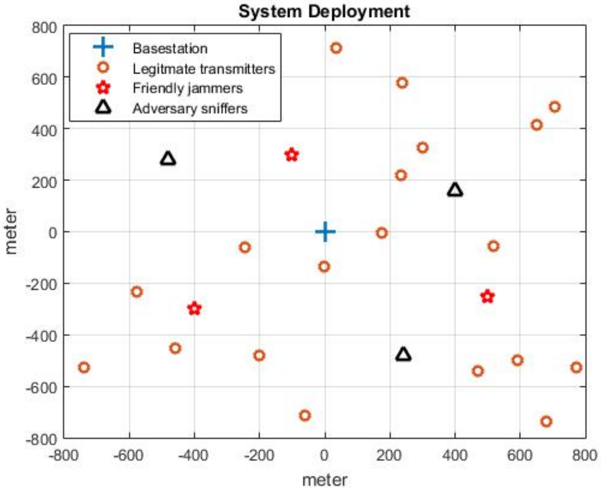


Fig. 4. An example of system deployment.

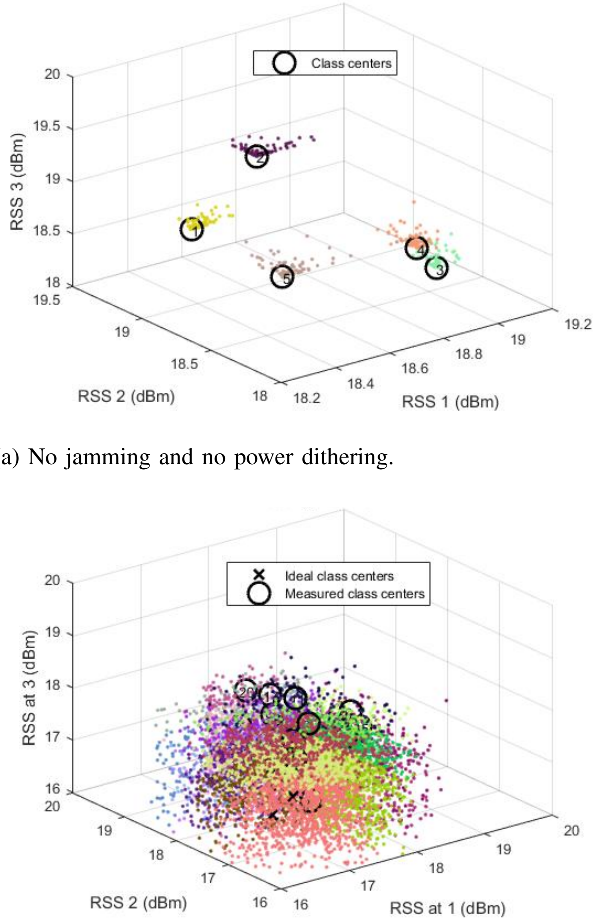
To demonstrate the effectiveness of , we conduct a simulation with the following setup. N transmitters are randomly deployed in a 1600 m × 1600 m area and the base station is located at the center; N_{sniff} sniffing receivers and N_{jam} cooperative jammers are randomly deployed in the same area. Such a deployment is shown in Fig. 4. The cooperative jammers transmit Gaussian noise cooperatively so that the base station would not be interfered thanks to **beam nulling**. Each of the jammers transmits the same amount of average power and the total average jamming power is given. The antenna patterns of legitimate transmitters are either omni-directional or directional. Fig.5 is a visual demonstration of the effectiveness of the countermeasures, where only five transmitters and three sniffers are shown for better visualization. From a view of sniffers, each user's presence is represented by its RF fingerprint. One can see from Fig.5 (b) that jamming and power dithering can confuse the sniffers effectively.

IV. Dynamic S-ISAC User Trust Management

This section is concerned with location-sensitive spoofing attacks in ISAC systems, including **Sybil attack** [25]–[27], **replay attack** [28]–[30], and **radar spoofing** [31]–[33]. Many existing techniques for spoofer detection exploit the spoofers' location fingerprinting [34], [35]. However, due to poor sensing ability, they do not work well, especially when the spoofer is close to the imitated object and the environment is changing. A **dual-ID** (a pair of digital IDs and physical IDs) mechanism is exploited against location-sensitive attacks in the ISAC systems.

A. Dual-ID in S-ISAC Network

The presence of a spoofing attack in an ISAC system is one or multiple fake objects associated with true physical locations.



(a) No jamming and no power dithering.

(b) With jamming and power dithering.

Fig. 5. RF fingerprint based on RSS values at three sniffing receivers under condition: -85 dBm receive power at the base station, omni-directional antennas.

Traditionally, user identities are digital, such as MAC addresses, unique keys, watermarks, and RF fingerprints. Digital ID based authentication is relatively simple but ineffective under some spoofing attacks like Sybil attacks, since they are independent of users' locations. Fortunately, any type of object in a real-world environment is associated with a set of location-related physical characteristics and environmental information, such as *velocity, mechanical dynamics, CSI, RCS characteristic, and radar clutter*. They can be **used collectively as a physical ID** that cannot be easily generated by an attacker. By pairing a digital ID with a physical ID, we have a **dual-ID** that is much stronger against spoofing.

Physical ID is equivalent to some fingerprinting. It has been a term used by [36], being named in contrast to regular "digital" ID. It is named in contrast to regular "digital" ID. Yes, physical ID is equivalent to some fingerprinting.

B. Detecting Spoofing Attacks via Physical ID Verification

Consider an ISAC system with one or more verifiers, an identity spoofer, and at least one fake object. Each fake object can be one of three types: 1) an object that does not (or is not able to) transmit and receive data; 2) a signal source; and 3) an object that is able to transmit and receive data. To detect a potential spoofing attack, we propose two verification methods as follows, assuming a distance metric (e.g. $\boldsymbol{l_2}$ **vector norm**) has been defined to measure the similarity between two dual-IDs.

Verification Method 1 (for all types of objects): Estimate the physical ID via illuminating and echo analyzing, and then compare the measured dual-ID with the one claimed by the ISAC user.

Verification Method 2 (for type-3 objects): Use a spatial-temporal challenge-response process (nonce-message exchange + return signal analysis)—send a probing nonce-message, wait for a return message within a certain time window, analyze the return message signal, and then verify both of the nonce and dual-ID.

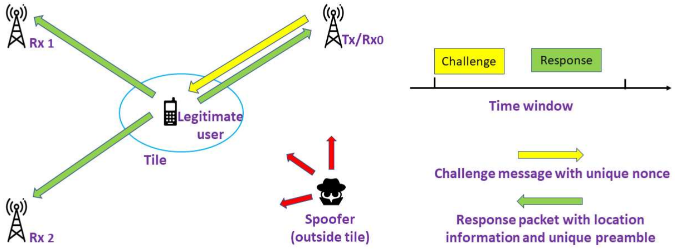

Rx 1
Tx/Rx0
Legitimate user
Tile
Rx 2
Spoofer (outside tile)
Challenge
Response
Time window
Challenge message with unique nonce
Response packet with location information and unique preamble

Fig. 6. Spatial-temporal challenge-response verification (method 2).

The key action in both verification methods is to extract and verify the physical ID by taking advantage of ISAC sensing functionality, but method 2 has an extra enhancement mechanism, i.e., a timely nonce verification, exploiting both sensing and communication functionalities of a transceiver. Fig. 6 is a conceptual illustration of verification method 2. Its procedure (protocol) is as follows, assuming an area of interest is divided into a number of tiles. For each predefined tile, 1) the verifier transmits a challenge message with a **nonce** (one-time-use random number); 2) if a legitimate ISAC user is in that tile and receives the challenge message, the user is supposed to send back within a given time window a response packet containing i) a preamble generated using the nonce and ii) (optional) a message with current ambient information; 3) if the verifier receives the response message, i) it is used to extract the physical ID, and ii) the received message is analyzed to verify the dual-ID and timely nonce. The above process is performed for each tile by following an ordered tile sequence known only by the system authority, and there can be multiple verifiers working cooperatively.

C. Joint Tx-Rx Multi-Beam Sweeping to Enhance User Verification

According to [37], the beamforming gain is approximately inversely proportional to the beamwidth. Beamforming leads to a few benefits, such as increase of detection sensitivity and interference reduction, at the cost of reduced space coverage at a time. In particular, verification can be further enhanced by beam sweeping, since a spoofer away from the targeted area is automatically out of the verification process. 2D beam sweeping has been part of 5G standards and used for initial user access [38]–[40]. It is possible to achieve joint transmitter-receiver (Tx-Rx) beam sweeping (Fig. 7) for both communication and sensing if the current protocols and processing at PHY and MAC layers can be revised. Beam sweeping can have three scenarios: joint illuminator (transmitter) receiver sweeping, illuminator sweeping and receiver sweeping; they can be denoted by Tx-Rx sweeping, Tx-sweeping and Rx-sweeping, respectively. With beam sweeping, predefined tiles (a piece of area)[2] in an area of interest can be screened by the radio beams sequentially.

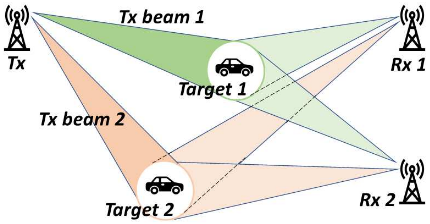


Fig. 7. Joint Tx-Rx multi-beam sweeping.

V. Conclusions

Security and privacy issues will be more and more problematic as ISAC advances from the concept to adoption by the telecommunication industry, to provision of ISAC services. Tackling security and privacy issues from an ISAC network perspective to enjoy massive collaboration for global optimization is desirable, but this approach will face many challenges in practice. Finding a globally optimal strategy is extremely complicated and difficult, thus some sort of workaround has to be considered. Recalling (1), the distortion is usually defined as the Cramer-Rao bound (CRB). However, the CRB is not practically convenient to use, which calls to reformulate and lose the optimization so that it only involves some practically measurable metrics like SINR and RSS. The optimization may involve unknown parameters such as H_E, and measurement as well as environment variation introduce additional uncertainties. To minimize these negative impacts, certain level of prior knowledge [8], [9] about the eavesdroppers (e.g., their locations, CSI) should be exploited.

Research on S-ISAC is demanding for reducing the gap between theory and practice before it is fully adopted by the industry. An non-exhaustive list of future research topics are as follows: collaborative and decentralized security approaches exploiting massive participation of ISAC users, robust security and privacy countermeasures considering uncertainties about the environment and attackers, suboptimal but practical solutions against malicious actions in ISAC, and real-time trust management of ISAC users.

[2] Their sizes do not have to be equal and shapes do not have to be identical.

References

[1] J. A. Zhang, M. L. Rahman, K. Wu, X. Huang, Y. J. Guo, S. Chen, and J. Yuan, "Enabling joint communication and radar sensing in mobile networks-a survey," *IEEE Communications Surveys & Tutorials*, 2021.

[2] N. Su, F. Liu, and C. Masouros, "Secure radar-communication systems with malicious targets: Integrating radar, communications and jamming functionalities," *IEEE Transactions on Wireless Communications*, vol. 20, no. 1, pp. 83–95, 2020.

[3] 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 Transactions on Wireless Communications*, vol. 21, no. 9, pp. 7238–7252, 2022.

[4] J. Chu, R. Liu, M. Li, Y. Liu, and Q. Liu, "Joint secure transmit beamforming designs for integrated sensing and communication systems," *IEEE Transactions on Vehicular Technology*, 2022.

[5] Z. Ren, L. Qiu, J. Xu, and D. W. K. Ng, "Robust transmit beamforming for secure integrated sensing and communication," *IEEE Transactions on Communications*, 2023.

[6] F. Dong, W. Wang, X. Li, F. Liu, S. Chen, and L. Hanzo, "Joint beamforming design for dual-functional MIMO radar and communication systems guaranteeing physical layer security," *IEEE Transactions on Green Communications and Networking*, vol. 7, no. 1, pp. 537–549, 2023.

[7] N. Su, F. Liu, and C. Masouros, "Sensing-assisted physical layer security," in *WSA & SCC 2023; 26th International ITG Workshop on Smart Antennas and 13th Conference on Systems, Communications, and Coding*. VDE, 2023, pp. 1–6.

[8] K. Hou and S. Zhang, "Secure integrated sensing and communication exploiting target location distribution," in *GLOBECOM 2023-2023 IEEE Global Communications Conference*. IEEE, 2023, pp. 4933–4938.

[9] H. Jia, X. Li, and L. Ma, "Physical layer security optimization with cramér-Rao bound metric in ISAC systems under sensing-specific imperfect CSI model," *IEEE Transactions on Vehicular Technology*, 2023.

[10] O. Günlü, M. R. Bloch, R. F. Schaefer, and A. Yener, "Secure integrated sensing and communication," *IEEE Journal on Selected Areas in Information Theory*, 2023.

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

[12] M. Kobayashi, H. Hamad, G. Kramer, and G. Caire, "Joint state sensing and communication over memoryless multiple access channels," in *2019 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2019, pp. 270–274.

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

[14] X. Xie, W. Chen, and Z. Xu, "A physical-layer watermarking scheme based on 5G NR," *Electronics*, vol. 11, no. 19, p. 3184, 2022.

[15] Y. Leng, R. Zhang, W. Wen, P. Wu, and M. Xia, "Physical-layer authentication based on spreading code watermarking for IoT networks," in *2022 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*. IEEE, 2022, pp. 434–438.

[16] W. Hou, X. Wang, and J.-Y. Chouinard, "Physical layer authentication in OFDM systems based on hypothesis testing of CFO estimates," in *2012 IEEE International Conference on Communications (ICC)*. IEEE, 2012, pp. 3559–3563.

[17] J. E. Kleider, S. Gifford, S. Chuprun, and B. Fette, "Radio frequency watermarking for OFDM wireless networks," in *2004 IEEE International Conference on Acoustics, Speech, and Signal Processing*, vol. 5. IEEE, 2004, pp. V–397.

[18] D. Roy, T. Mukherjee, M. Chatterjee, E. Blasch, and E. Pasiliao, "RFAL: Adversarial learning for RF transmitter identification and classification," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 2, pp. 783–801, 2020.

[19] T. Ding, L. Peng, Y. Qiu, Z. Wu, and H. Fu, "A research of I/Q imbalance based RF fingerprint identification with LTE-RACH signals," in *2021 IEEE 6th International Conference on Signal and Image Processing (ICSIP)*. IEEE, 2021, pp. 66–71.

[20] C. Shi, F. Wang, M. Sellathurai, J. Zhou, and S. Salous, "Low probability of intercept-based optimal power allocation scheme for an integrated multistatic radar and communication system," *IEEE Systems Journal*, vol. 14, no. 1, pp. 983–994, 2019.

[21] J. H. Booske, N. Behdad, and J. Zhao, "Low-probability-of-intercept/detect (LPI/LPD) secure communications using phased-arrays employing side-lobe time modulation," in *2022 United States National Committee of URSI National Radio Science Meeting (USNC-URSI NRSM)*. IEEE, 2022, pp. 100–101.

[22] C. Wen, J. Peng, Y. Zhou, and J. Wu, "Enhanced three-dimensional joint domain localized STAP for airborne FDA-MIMO radar under dense false-target jamming scenario," *IEEE Sensors Journal*, vol. 18, no. 10, pp. 4154–4166, 2018.

[23] F. Zhou, T. Tian, B. Zhao, X. Bai, and W. Fan, "Deception against near-field synthetic aperture radar using networked jammers," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 6, pp. 3365–3377, 2019.

[24] O. Šimon and T. Götthans, "A survey on the use of deep learning techniques for UAV jamming and deception," *Electronics*, vol. 11, no. 19, p. 3025, 2022.

[25] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Channel-based detection of Sybil attacks in wireless networks," *Information Forensics and Security, IEEE Transactions on*, vol. 4, no. 3, pp. 492–503, 2009.

[26] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 372–383, 2014.

[27] H. Yang, Y. Zhong, B. Yang, Y. Yang, Z. Xu, L. Wang, and Y. Zhang, "An overview of Sybil attack detection mechanisms in VFC," in *2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*. IEEE, 2022, pp. 117–122.

[28] Z. Feng, J. Ning, I. Broustis, K. Pelechrinis, S. V. Krishnamurthy, and M. Faloutsos, "Coping with packet replay attacks in wireless networks," in *2011 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*. IEEE, 2011, pp. 368–376.

[29] R. Merco, Z. A. Biron, and P. Pisu, "Replay attack detection in a platoon of connected vehicles with cooperative adaptive cruise control," in *2018 Annual American Control Conference (ACC)*. IEEE, 2018, pp. 5582–5587.

[30] M. A. Al-shareeda, M. Anbar, I. H. Hasbullah, S. Manickam, N. Abdullah, and M. M. Hamdi, "Review of prevention schemes for replay attack in vehicular ad hoc networks (VANETs)," in *2020 IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP)*. IEEE, 2020, pp. 394–398.

[31] R. Komissarov and A. Wool, "Spoofing attacks against vehicular FMCW radar," in *Proceedings of the 5th Workshop on Attacks and Solutions in Hardware Security*, 2021.

[32] P. Kapoor, A. Vora, and K. Kang, "Detecting and mitigating spoofing attack against an automotive radar," in *Proc. of 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, 2018.

[33] D. Rodriguez, J. Wang, and C. Li, "Spoofing attacks to radar motion sensors with portable RF devices," in *Proc. of 2021 IEEE Radio and Wireless Symposium (RWS)*, 2021.

[34] M. H. Yılmaz and H. Arslan, "A survey: Spoofing attacks in physical layer security," in *2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops)*. IEEE, 2015, pp. 812–817.

[35] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8169–8181, 2019.

[36] Y. Cui, Z. Feng, Q. Zhang, Z. Wei, C. Xu, and P. Zhang, "Toward trusted and swift UAV communication: ISAC-enabled dual identity mapping," *IEEE Wireless Communications*, vol. 30, no. 1, pp. 58–66, 2023.

[37] Y. Yaman and P. Spasojevic, "Analytical framework of beamwidth selection for RT-ICM millimeter-wave clusters," *arXiv preprint arXiv:2003.12947*, 2020.

[38] S. Tomasin, C. Mazzucco, D. De Donno, and F. Cappellaro, "Beam-sweeping design based on nearest users position and beam in 5G mmWave networks," *IEEE Access*, vol. 8, pp. 124 402–124 413, 2020.

[39] A. Mazin, M. Elkourdi, and R. D. Gitlin, "Accelerating beam sweeping in mmWave standalone 5G new radios using recurrent neural networks," in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*. IEEE, 2018, pp. 1–4.

[40] M. Giordani, M. Polese, A. Roy, D. Castor, and M. Zorzi, "A tutorial on beam management for 3GPP NR at mmWave frequencies," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 173–196, 2018.