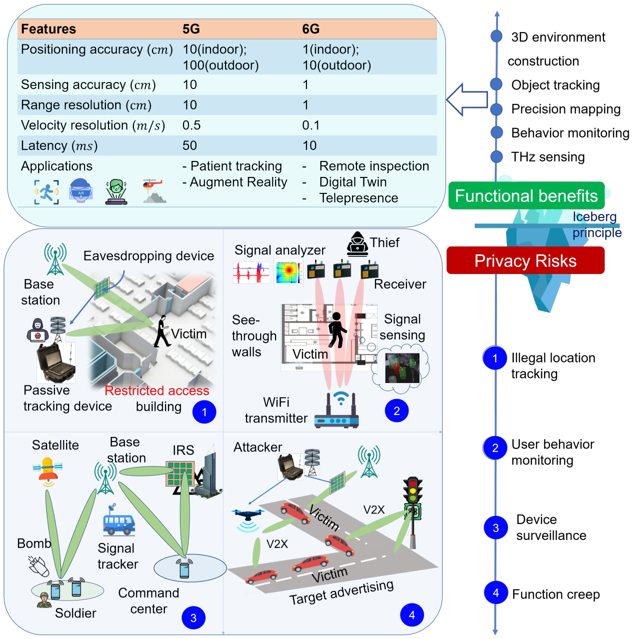
Understanding Privacy Risks of High-accuracy Radio Positioning and Sensing in Wireless Networks

Van-Linh Nguyen, *Member, IEEE*, Ren-Hung Hwang, *Senior Member, IEEE*, Bo-Chao Cheng, Ying-Dar Lin, *Fellow, IEEE*, Trung Q. Duong, *Fellow, IEEE*

***Abstract*—High-accuracy radio positioning and sensing technologies are crucial for many applications, including tracking hospital patients and identifying victims during emergency calls. However, these techniques present serious privacy concerns since malicious actors might use them to track users' activities and habits without their consent. This paper provides a systematic overview of the privacy risks posed by high-accuracy radio positioning and sensing, particularly from physical layer perspectives. To demonstrate a typical risk, we develop an intelligent tracking-without-consent model that can follow a target user in a restricted-access building with 94% accuracy reliability for less than $1m$. Our research reveals that none of the privacy-enhancing methods, such as channel state information (CSI) obfuscation and beamforming steering, can totally eliminate tracking, especially in coordinated attempts that use radio location and sensing simultaneously. Furthermore, there is currently no commercial implementation of these techniques integrated into civilian wireless chips that would enable users to be informed about ongoing radio-based surveillance, let alone grant them control over terminating the illegal tracking activity or secluding themselves. In addition, accurately detecting tracking activities by malicious actors in shared wireless networks with a high density of sensors or in advanced communication technologies like 6G mmWave/Terahertz beamforming, which utilizes rich CSI data, continues to pose a challenge. Given the difficulties of totally avoiding signal-based tracking threats, efficient signal encryption and access control mechanisms at the physical layer will be critical research topics for the coming years.**

***Index Terms*—Wireless security, Radio Surveillance, User Tracking, Privacy Risks, Privacy Preservation.**



Features	5G	6G

Positioning accuracy (cm)	10(indoor);
	100(outdoor)
		1(indoor);
		10(outdoor)

Sensing accuracy (cm)	10	1
Range resolution (cm)	10	1
Velocity resolution (m/s)	0.5	0.1
Latency (ms)	50	10
Applications	- Patient tracking - Augment Reality	- Remote inspection - Digital Twin - Telepresence

Fig. 1. An example of the functional benefits and the privacy risks of high-accuracy radio positioning and sensing in wireless networks. While the positive uses (e.g., patient tracking) are well-known to many users, the privacy dangers of monitoring without user authorization (illegal location tracking, extensive surveillance) have gotten little attention from the community.

I. Introduction

Radio positioning is a technique that exploits spatial-temporal information from the radio propagation channel to determine the location and movement of a wireless device. A related technique, radio sensing, refers to detecting and monitoring the object's orientation or gesture activity by measuring the reflected and emitted radiation at a distance. Unlike radio positioning, radio sensing can function without the user holding a cellular phone. The fifth-generation (5G) networks support radio positioning through the downlink positioning reference signal (DL-PRS) and uplink sound reference signal (UP-SRS) but they do not support radio sensing [1]. In general, radio positioning is crucial for location-based services, particularly in areas where Global Navigation Satellite System (GNSS) signals are blocked or degraded (due to satellite signal blockage by buildings, underground use, jamming attacks, solar storms, and satellite maintenance). The fundamental distinction between radio positioning and sensing in 5G and 6G lies in their accuracy and range resolution. As a result, by leveraging the high resolution of multipath components in large antenna arrays and high frequencies (e.g., Terahertz), the accuracy and range resolution of positioning and sensing in 6G are predicted to be ten times higher than in 5G [2], as shown at the top of **Figure 1**. The centimeter-level precision of the two technologies in 6G is essential to enable 3D environment reconstruction and precision mapping in many applications, including holographic telepresence [3] and digital twin [4].

However, the main concern for high-accuracy radio positioning and sensing is that they can be abused to violate user privacy. User privacy violations, in this context, refer to preventing the ability of individuals/groups from hiding their position/moving behavior information or disclosing the data without consent. In general, privacy violations can occur during the data collection and publishing process. While many previous studies have focused on how user privacy is violated in data publishing, for example, how to expose an individual/specific group from public/private datasets/taxi trajectory [5]–[8], this work is the first attempt to comprehensively

V.-L. Nguyen and B.-C. Cheng are with National Chung Cheng University, Chiayi, Taiwan. R.-H. Hwang and Y.-D. Lin are with National Yang Ming Chiao Tung University, Tainan, Taiwan. T. Q. Duong is with Queen's University Belfast, U.K. and also with Kyung Hee University, South Korea.

address the matters of how user data (location, trajectory) is illegally collected and abused through radio-based tracking without user consent. Before we delving technical insights of potential radio-based tracking-without-consent techniques, we summarize several typical privacy risks associated with radio positioning and sensing in **Figure 1**.

Case 1: **Illegal location tracking and profiling**. The attacker uses radio positioning to locate a target user in a restricted-access building, even without physical intrusion, as illustrated in **Figure 1**. The attacker can detect user movement and predict the next routines by connecting continuous data points from positioning results over time, i.e., tracking. This is particularly concerning when coupled with other obtained data, such as visited areas, as it could provide the attacker with the user's full profile or daily habits.

Case 2: **User behavior monitoring**. An attacker can utilize a wireless transmitter and signal analyzers to generate signals and examine the changes of channel state information (CSI) patterns with and without absorption from the human body [8]. By sensing such values, user actions (sleeping, walking) and habits can be collected for illegal physical building infiltration. In contrast to the prior method, the user does not carry any cellular phone but is still tracked. Other variations of this sensing approach, such as indoor crowd counting, can be used to track people in public places.

Case 3: **Device surveillance**. An attacker might target a group with special advertising or malware by exploiting radio signals to track specific devices. For example, when vehicles arrive in specified regions, the adversary may leverage positioning in Vehicle-to-Everything (V2X) communications to broadcast malicious data (fake map resolution updates, false maneuver information, malware link). When soldiers turn on their smartphones, the adversary can also locate the position of soldiers and launch missile attacks. On the other hand, this device tracking technology could be exploited to violate people's anonymity, making them identifiable in a public space. For example, a government may use radio positioning/sensing and unmanned aerial vehicles (UAV) to track the location of protest groups and suppress their movement.

Case 4: **Data retention and sharing without user consent**. Third-party developers or data-driven companies can exploit their high-accuracy radio positioning and sensing services (e.g., social network nearby friends, find my phone) to collect user location/trajectory information and share it with other parties for targeted advertising or other purposes without the consent of the individuals, i.e., a form of function creep.

Given the popularity of wireless signals everywhere and joint communication and sensing technologies in 6G, research efforts on privacy preservation against illegal radio-based tracking have become urgent. Unlike data anonymization in the application layer, dealing with privacy matters of tracking without consent at the physical layer of wireless networks is a challenge. Through extensive countermeasure analysis and a demonstration, we highlight the challenges of balancing high-quality connectivity guarantee and privacy protection when implementing such technologies in shared wireless networks.

II. Why privacy risks in radio positioning & sensing are high

The primary privacy risk in high-accuracy radio positioning and sensing is the risk of signal-based tracking without user consent. Another risk involves linkability, identifiability, and traceability based on user signals. The term "tracking without user consent" or "tracking without user approval" refers to the attacker silently locating and monitoring the user trajectory and behavior as described above while the user is unaware of or unable to get rid of that activity. The attacker has complete control over how signals are collected, data size, and sampling rate, allowing him to be proactive about data sources for high-accuracy tracking. A variety of factors cause this risk.

Shared networks create challenges to determine which receiver is a tracker: Since wireless networks are a 'shared' environment, it is impossible to tell whether the passive receivers are trackers collecting uplink and downlink angle of arrival (AoA), time of arrival (ToA)/time difference of arrival (TDoA), and time of flight (ToF) measurements for tracking. Note that such information from the wireless channel can be utilized to estimate the user's position via geometry, e.g., triangulation and trilateration [6]. In 6G, the advent of holographic radio technology [4] and dense radio units could even permit three dimensions of surveillance.

The introduction of multi-array antenna and beamforming technologies to enable precise single-station tracking: Multi-array antennas and beamforming techniques in new generation devices (e.g., 5G smartphones) can achieve peak data rates of up to dozens of gigabits per second (Gbps). But on the other side, the technologies also provide rich CSI data on the propagation environments. By using many available CSI extraction tools on the Internet, such as Nexmon and Atheros, attackers can extract phase, amplitude, and AoA and use multipath-based localization techniques [3], [6] to achieve user location accuracy under $1m$ without requiring many base stations. In scattering circumstances, the attacker can use a hybrid-based technique (radio fingerprint-based and multipath-based) with AI empowered to achieve the best accuracy performance [2]. Multi-array antennas and beamforming technology will continue to be significant in 6G. For example, to satisfy faster data rates and ultra-low latency, high-frequency wireless technologies (e.g., THz) and directional communications (holographic beamforming) are likely to prevail in 6G networks [4]. However, because of the rich CSI collection (angle-delay-azimuth information) and the resolvability of several beams of radio waves at different places, these technologies also provide high-precision tracking and capabilities.

There is a thin line between good tracking for civic applications and poor tracking by hostile actors: Many personalized-based features, such as location-based services (games/ads), patient tracking in hospitals, and emergency calls, rely on radio positioning [2]. In rare circumstances, police enforcement/emergency agencies can use tracking-without-consent technologies to provide essential help for safe intrusion in drug raid missions, rescuing attempted suicides, and so saving a life. Joint communication and tracking can also enable high-precision 3D reconstruction and mapping as a core 6G technology for digital twin/extended reality [7]. However, the line between good and bad usage (by civil apps, law enforcement organizations, and emergency response agencies) is thin. The most crucial problem is that there is no mechanism built into wireless chips to notify users that their communications are being monitored, nor is there a mechanism to stop illegal tracking.

A dense concentration of radio devices or antenna sites increases the risk of capturing valuable CSI data for tracking: Because high-frequency wireless technologies have short-range communications, the density of radio units or base stations in 6G, as well as aerial-assisted base stations, will be very high. This increases the risk that a grid of compromised radio equipment might be used to create a network of surveillance sensors.

The risks are posed by shared non-terrestrial wireless networks: The unique components of 6G networks are expected to be aerial-assisted communications from low-orbit commercial satellites. In contrast to traditional communications, 6G end-users may be able to access satellite Internet directly from their smartphones without the need to connect to base stations. In this instance, adversaries can leverage the previously mentioned tracking techniques and the availability of GNSS signals to track individuals remotely, regardless of their geographical location.

Table I summarizes our insights on typical user tracking techniques, data sources to exploit, privacy risk examples, and attack costs. As a result, unlawful tracking techniques are likely to become more intelligent with AI-aided models or, ironically, rich data from 6G-enabled devices.

III. Privacy-enhancing technologies in radio positioning and sensing

This section discusses numerous privacy-enhancing technologies (PET) of tracking approaches by targeting features of data sources (**Table I**) in tracking techniques. Basic techniques for preventing privacy issues at the physical layer include: (1) truncating exchange information in the wireless channel to prohibit linkability, identifiability, and traceability (LIT) to a specific user; (2) encrypting signals to eliminate CSI data for radio-based tracking. So far, the former strategy has had a lot of success in cellular networks by separating identities, such as the Subscription Concealed Identifier (SUCI) and the Subscription Permanent Identifier (SUPI), and Temporary Mobile Subscriber Identities. However, due to the hazards of linking SUPIs to a specific user during the initial authentication stage, the risks of radio-based monitoring remain considerable in 5G. Furthermore, even if linkability is not present, the attacker can still locate the unique user by collecting habit-moving patterns or visited places (i.e., personal gazetteer [5]) via radio positioning at the physical layer. The latter approach is promising due to its capability to jam source data of tracking. However, due to its expensive cost, immature hardware, and potentially negative impact on communication quality, the method has had limited success thus far.

Table II outlines key anti-tracking methods, limits, and future technologies in 6G, the majority of which belong to the second approach. We categorize five major privacy preservation strategies: (1) preventing CSI decoding; (2) preventing the attacker from getting any signals; (3) decreasing redundant broadcasting range; (4) directing the signals towards authorized users only; (5) employing laws and regulations to encourage good technology practices. In addition, we emphasize each method's signal target qualities and constraints in various scenarios each method's signal target qualities and constraints in various scenarios (e.g., additional data requirement, tested environment, build cost, deployment placement) as well as associated 6G enablers for increasing efficiency. "Additional data" refers to the fact that the PET method necessitates modulation to add additional specific noise/phases to signals before transmission. A tested environment denotes a list of wireless technologies that have been examined in existing research through proof-of-concept or theoretical analysis (e.g., [7], [9]–[11]). The build cost is determined by the expenditure (extra hardware) required to implement.

Method 1: **CSI obfuscation**. This technique is employed at the transmitter device. By distorting or altering the CSI data, such as adding random noise and phase shifts, it becomes difficult to link the device to a particular location. However, CSI obfuscation techniques can degrade signal quality, resulting in lesser throughput and shorter range for communications. It also necessitates the installation of additional hardware (signal modulation) and software to wireless devices for CSI manipulation, which can raise the system's cost. The majority of tested environments are WiFi-based [10]. Signal obfuscation for THz will be a promising area for research in 6G.

Method 2: **Beamforming steering**. This solution takes advantage of the important premise that "if the attacker receives no wireless signal or insufficient CSI information, the attacker has no way to perform related localization algorithms". Beamforming steering, in contrast to CSI obfuscation, tries to vary the wireless signal direction (e.g., main lobe beam) at random intervals. Note that collecting side lobe signals rather than main lobe signals will considerably reduce surveillance performance. This technique is often implemented at base stations/WiFi access points and is low-cost due to the lack of major hardware requirements. This strategy, however, is only possible on beamforming-capable wireless devices, such as WiFi 5 (IEEE 802.11ac), mmWave networks, and beyond.

Method 3: **Artificial noise generation**. In general, noise is a signal that interferes with the target signal, making it difficult to understand or interpret. Taking use of this trait, fake noise is inserted into the downlink training signals (before they are transmitted) to prevent the passive eavesdropper from acquiring the accurate CSI or RSS data [4]. In contrast to CSI obfuscation, noise production impacts the signal-to-noise ratio and frequently makes information extraction in fingerprint-based tracking techniques more difficult. However, this technology requires additional hardware and much more energy for operation, raising its overall cost.

Method 4: **Signal reflecting utilization and duplicate signals**. The primary idea behind this technology is that the wireless signal is reflected off surfaces in the surroundings, resulting in numerous copies of the signal being received by the receiver [12], [13]. This makes determining the exact

TABLE I
SUMMARY OF FIVE MAIN STATE-OF-THE-ART RADIO POSITIONING AND SENSING TECHNIQUES, PRIVACY RISKS, AND 6G TECHNOLOGY ENABLERS

Technique type	**Accuracy (cm)**	**Attack cost**	**Prerequisite**	**Active device**	**Tracking type**	**Data sources**	**Privacy risks**	**Limitations**	**6G enablers**
Geometric-based	up to 5m	High	Three base stations	Yes	Passive	AoA, TDoA, ToA, ToF	► Location tracking, Device surveillance	Require the presence of three base stations	► Holographic radio
Fingerprint-based	< 100	Medium	Ground truth fingerprints	Yes	Passive	RSS, CSI	► Location tracking, Device surveillance	Ground truth training requirement	► Ultra-wideband THz
Multipath-based	10-50	Medium	Ground truth CSI data	Yes	Passive	CSI	► Location tracking, Device surveillance Function creep	Devices with multi-array antennas	► Large antenna arrays, Large intelligent surface
Hybrid-based	10	Medium	Rich data source	Yes	Passive	RSS, CSI, AoA, ToF	► Location tracking, Device surveillance Function creep	High computation	► Large antenna arrays, Heterogeneous networks
RF sensing	10-50	High	Ground truth CSI data	No	Active	RSS, CSI, RF reflectors	► Location tracking, User behavior monitor	Performance degraded due to the absorption or reflection of obstacles/victim body	► Joint communication and sensing, THz imaging

TABLE II
SUMMARY OF KEY EXISTING PRIVACY-ENHANCING TECHNIQUES, LIMITATIONS, AND PROSPECTIVE TECHNOLOGIES IN 6G

Privacy-enhancing type	**Target properties**	**Additional data**	**Tested environment**	**Build cost**	**Deployment placement**	**Limitations**	**6G enablers**
► CSI obfuscation	CSI decoding	Yes	WiFi	Medium	► Transmitter device	Affect the transmission performance	AI Empowered
► Beamforming Steering	Signal direction, Broadcasting scope	No	WiFi 5, mmWave	Low	► Base stations, WiFi access points	Used in beamforming antennas only	Holographic beamforming
► Artificial Noise Generation	Downlink signals, CSI collection	Yes	WiFi, mmWave	High	► Base stations	High energy consumption	AI Empowered
► Signal Reflecting Utilization	Signal direction	No	mmWave	Medium	► LIS/IRS, Reflectors	External devices to support	AI Empowered
► Differential privacy	Channel randomization signal perturbation	No	WiFi, mmWave	Medium	► Base stations	Extra computation	AI Empowered
► Laws and regulations	Track actions	–	–	Low	► Apply for every case	Slow development	–

location of the wireless device difficult for an attacker because the signal appears to be originating from various locations (confusing AoA and TDoA values). This technique is similar to K-anonymity in data publishing [5], but it is applied to physical layer data before transmission. For example, we can build "signal-reflecting walls" with reflective materials like intelligent reflecting surfaces (IRS) [4] to reflect wireless signals in multiple directions. However, operating many reflector devices may raise the expense of system maintenance, let alone IRS hardware which is still in its infancy.

Method 5: **Differential privacy techniques for the physical layer**. Unlike differential privacy techniques in data publishing, to prevent linkability, identifiability, and traceability to a specific user via signal-based tracking and personal gazetteer, differential privacy requires the combination of multiple techniques. Integrating identity separation (through SUPI) with artificial noise production (amplitudes/phases/timing perturbation) to transmit signals is one example. Another approach is to use beamforming and antenna pattern diversity. This technology makes use of beamforming weights or antenna designs to spread sent signals over a larger area, making it more difficult for an opponent to pinpoint or track a specific user. Furthermore, offering channel randomization, dynamically varying fading profile parameters, and signal power levels can prevent the tracker from decoding a specific user's CSI. AI-powered models are likely to dramatically improve these differential privacy strategies in 6G.

Method 6: **Privacy laws and data collection regulations at the physical layer**. Laws and regulations, such as the General Data Protection Regulation (GDPR) [14] play an important role in safeguarding users from illicit surveillance. The regulations for data in the physical layer can thoroughly protect individuals' rights to conceal their locations/moving trajectories while allowing wireless technologies to continue advancing. However, there is no function in modern cellphones that disables the potential of radio-based tracking, nor is there a rule that requires it.

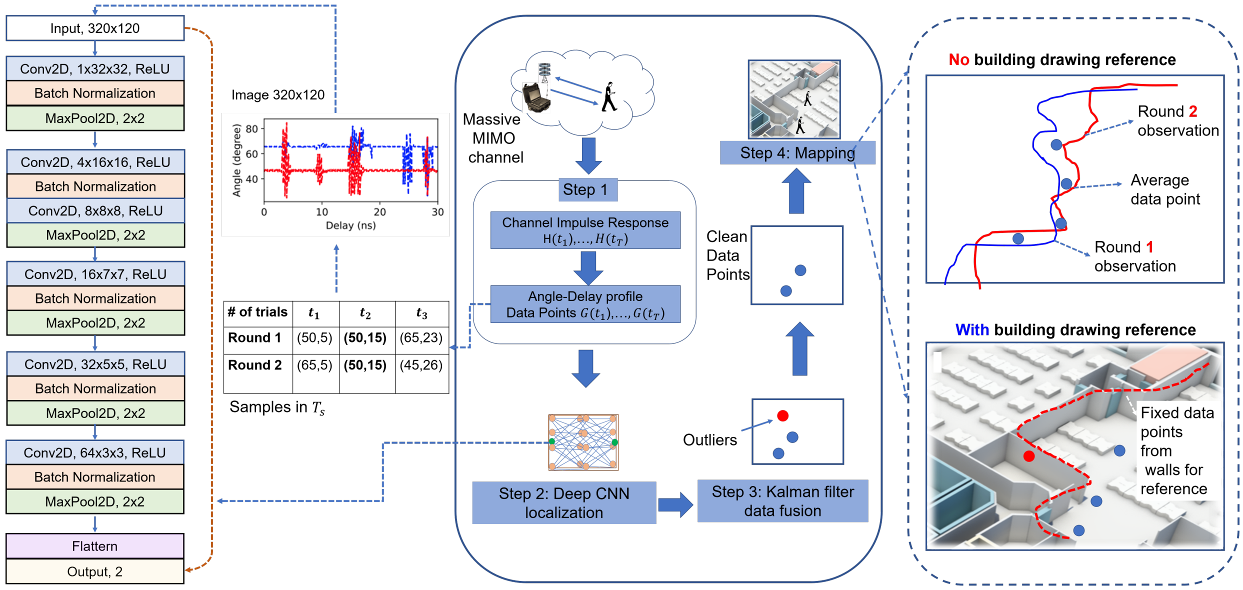
The following section demonstrates the risks of surveillance from high-accuracy radio positioning and highlights our assessment of privacy measurement on common privacy-enhancing techniques.

IV. DEMO OF PRIVACY RISKS VIA AI-EMPOWERED TRACKING IN RESTRICTED ACCESS BUILDINGS

This demonstration aims to monitor a victim user with a smartphone in a limited access building, illustrating the risk of illegal location tracking and evaluating the efficiency of anti-tracking solutions. As illustrated in **Case 1** of **Figure 1**, suppose that the tracking device (aka, anchor or truck tracker) is equipped with N_{rx} antennas. The truck tracker is located outside the building and passively captures the user's main lobe signals. According to [2], the channel impulse response (CIR) for each sub-carrier k at frequency n and the time t is expressed by

$$h[k](t) = \sum_{l=1}^{L} \alpha_l a_l^R(\phi) a_l^T(\theta) e^{-j2\pi n \Delta_f \mu_l} e^{j2\pi k T_s \nu_l}, \quad (1)$$

where T_s denotes the sampling period, Δ_f means the sample gap. τ_l indicates the time-of-arrival, L is the number of propagation paths, α_l (complex channel gain), ϕ (physical angle of arrival), θ (angle of departure), ν_l is Doppler shift. With beamforming techniques, the values of ϕ and θ are limited at the left or right side, i.e., $\phi \sim [-\frac{\pi}{2}, \frac{\pi}{2}], \theta \in [\frac{\pi}{2}, -\frac{\pi}{2}]$.



# of trials	t_1	t_2	t_3
Round 1	(50,5)	**(50,15)**	(65,23)
Round 2	(65,5)	**(50,15)**	(45,26)

Samples in T_s

Fig. 2. The illustration of our proposed tracking method architecture. The left side includes a detail of the DCNN model. The middle side shows the workflow. The right side illustrates the tracking in a private building (without a drawing for reference) and a public complex (with an available drawing for reference).

$a_l^R(\phi)$ is the function of the angle-of-arrival in azimuth and elevation. $a_l^T(\phi)$ is the function of the angle-of-departure [2].

Based on the channel impulse response for each sub-carrier, the CIR vector for all sub-carriers at the time t is given by:

$$H(t) = \left[h[1](t), \ldots, h[k](t), \ldots, h[K](t)\right]^T, \qquad (2)$$

We propose an AI-empowered tracking model as illustrated in **Figure 2**. First, to support deep learning models, we convert the collected CIR matrix in **Equation 2** into linear values of Angle-Delay profile (ADP) through Fourier transformation [2], [11]. In multi-path transmission, ADP reflects the AoA of the received signals in terms of delay with regard to the arrival paths. ADP data from the sample period T_s is fed into a deep convolutional neural network (DCNN) for classification and location determination. The DCNN network configuration is presented at the left side of **Figure 2**.

For privacy preservation testing, we evaluate the top five PET methods presented in **Section III** and **Table II**. We use three privacy measurement metrics: attack success, utility loss, and time cost [5]. The attack success statistic evaluates the possibility of re-identification or the capacity to link data to a specific person correctly. Low attack success implies high anonymity or strong privacy protection. When the privacy-enhancing technique is in use, the utility loss measures the ratio of packet loss/transmitted packets, indicating the negative influence on communication quality. High utility loss means that wireless connectivity suffers significantly. The time cost is the processing time of the privacy-enhancing technique to anonymize transmitting signals. Low time cost contributes to the efficiency of a privacy-enhancing method. Finally, we suggest a new metric, the overall performance effect meter, which is calculated by dividing the attack access ratio by the utility loss ratio minus the time cost. The statistic measures the ability to balance the expense of preserving privacy and ensuring wireless quality. A high impact value indicates good balance capability.

Furthermore, unlike civil tracking techniques in [15], the tracking in this demo must be able to deal with restricted access/private buildings, where ground truth data for DCNN is frequently difficult to obtain. We train the DCNN model using a synthetic dataset generated by Ray Tracing and multi-round averaging data points to overcome the ground truth dilemma. Compared to the prior work [11], DCNN in this demonstration is developed using a few-shot-learning procedure to lessen reliance on large-scale pre-collected datasets. The users randomly walk with a maximum speed of $1.3m/s$.

In the case of *the absence* of privacy-enhancing techniques, **Figure 3** shows that our DCNN-Kalman-filter tracking model can achieve 94% reliability (i.e., high attack success) in determining the location of a given user with precision less than $1m$. As a result, the wireless communication model provides little privacy protection at the physical layer, making it particularly vulnerable to radio-based tracking techniques. When we have no building drawing reference (the top right of **Figure 2**), the attack success drops from 13% to 25% if the target user remains in the innermost room of a complex building structure with many concrete walls, corridors, and rooms within. The performance is worse if there are a group of users moving simultaneously. The attack success is improved by about 10% if we perform averaging the estimation results of multiple observation rounds.

In the case of *the presence* of privacy-enhancing technologies, **Table III** summarizes our evaluation results on the privacy preservation performance of five typical privacy-enhancing techniques and the influence of the parameters. According to our findings, differential privacy and beam steering/reflecting strategies outperform other approaches in effectively minimizing hazards associated with the AI-powered surveillance demo. These strategies are particularly effective

TABLE III
PRIVACY MEASUREMENTS OF 5 TYPICAL PRIVACY-ENHANCING TECHNIQUES AND THE KEY PARAMETERS.

Privacy-enhancing technology	Parameter analysis				Attack success (%)	Utility loss (%)	Time cost (s)	Overall performance impact
	Frequency n (GHz)	Sampling interval (s)	Number of arrays N_{rx}	Number of users				
CSI obfuscation	5	60	16	3	57.34	23.26	0.25	**2.21**
	60	60	16	3	61.17	19.23	0.71	**2.47**
	5	360	32	8	53.45	19.51	0.35	**2.38**
	60	360	32	8	59.73	12.32	0.88	**3.96**
Beamforming steering	5	60	16	3	27.93	6.29	0.09	**4.35**
	60	60	16	3	19.52	3.95	0.17	**4.77**
	5	360	32	8	22.76	4.54	0.11	**4.90**
	60	360	32	8	18.22	3.04	0.19	**5.81**
Artificial noise generation	5	60	16	3	53.27	27.59	0.31	**1.62**
	60	60	16	3	59.86	24.13	0.89	**1.59**
	5	360	32	8	57.38	29.37	0.34	**1.61**
	60	360	32	8	51.05	18.30	0.95	**1.83**
Signal reflecting utilization	5	60	16	3	19.09	3.04	0.08	**6.19**
	60	60	16	3	17.32	2.23	0.12	**7.64**
	5	360	32	8	13.93	2.14	0.09	**6.41**
	60	360	32	8	8.13	0.97	0.13	**8.25**
Differential privacy (channel randomization, beam steering)	5	60	16	3	12.35	1.28	0.19	**9.45**
	60	60	16	3	10.78	1.02	0.23	**10.33**
	5	360	32	8	9.45	0.97	0.21	**9.53**
	60	360	32	8	7.18	0.65	0.23	**10.81**

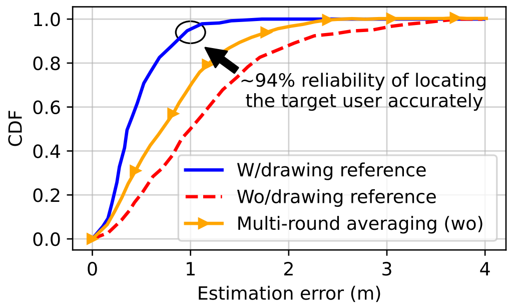


Fig. 3. Tracking performance in the case of the absence of privacy-enhancing techniques with and without building drawing reference.

in achieving a well-balanced approach by minimizing tracking risks (attack success), utility loss, and time expense. The key to success is their ability to keep the tracker from getting any signals. However, beamforming steering and signal-reflecting utilization diminish if the attacker can deploy many track truckers or drones around to collect main lobe signals between the outside base station and the inside users. CSI obfuscation and artificial noise production, on the other hand, are effective for deploying in low-frequency directionless communications ($n = 5GHz$). In this case, the added noise can reduce the attacker's CSI decoding accuracy. It cannot, however, completely prevent the angle (angle-of-arrival) and delay (time-of-flight) resolution.

Furthermore, assuming the number of users in the building remains constant, increasing the number of arrays at the receiver and the sampling period can improve attack success. However, as the number of users grows, the attack access will suffer because of the difficulties in distinguishing overlap signals from neighboring users. The attack success soars up to 85.7% if the attacker combines passive tracking and active sensing to go after the user. Active sensing uses ultra-wideband frequency and helps to detect the area of moving humans [8]. In this instance, a single privacy-enhancing approach is insufficient to protect privacy. Differential privacy is favored as a result of using the strengths of numerous strategies (with the highest overall impact as in the last column of **Table III**). Furthermore, because CSI obfuscation and fake noise production on high frequencies require massive beam-space-based processing, the time cost is substantially higher than in signal reflecting and steering techniques.

V. Open Problems of Privacy Preservation for Further Study in the Era of Wireless Everywhere

The core issue of privacy concerns in radio-based positioning and sensing is the complexity of preventing CSI information leaks from *shared* wireless channels. The other is that there currently exists no perfect unlinkability/untraceability solution for user identities during their communication sessions. In general, accurate CSI estimation is essential in maintaining high-throughput wireless communications since they allow advanced channel equalization and massive MIMO operations. However, to maintain the simplicity of signal modulation in affordable antennas, CSI is rarely encrypted or obfuscated. Every receiver can receive and decode signals. The application layer-based solutions and cryptography methods cannot completely block the CSI collection without degrading channel communications [12]. Because of this, the transmitter has no way of knowing whether the receiver side is in monitoring mode, let alone distinguish between accidentally receiving signals and illegal passive tracking. Besides the above findings, we summarize open problems for privacy preservation in radio positioning and sensing as follows.

Problem 1: **Efficient signal encryption and access control feature in the physical layer**. Neither privacy-enhancing techniques at the application layer, e.g., homomorphic encryption, [4] nor described PET methods can totally prevent signal-based tracking risks at the physical layer. This is because the attacker can easily extract CSI data from *shared* wireless signals or combine that with RF sensing to locate a user.

Enabling signal encryption and access control in the physical layer of 6G networks is thus a promising approach. This can be highly economical as all other methods often require a lot of energy to maintain (noise generation, CSI obfuscation) or additional hardware (signal reflecting, beam steering).

Problem 2: **Scalable privacy-enhancing technologies in the physical layer**. All mentioned anti-tracking techniques require the implementation of low-level firmware. Therefore, large-scale firmware updates or defense implementation to address new tracking strategies will be a huge challenge, particularly with resource-constrained networks/wireless devices. Building an efficient platform for simulating anti-tracking techniques to reflect the diversity of case studies in real environments is also another big deal.

Problem 2: **Efficient learning models for sparse data sources**. Collecting ground truth CSI data is a significant difficulty, especially in developing effective AI-powered privacy-enhancing technologies (PET). These AI-based PET approaches frequently experience severe performance degradation or are circumvented by coordinated attack efforts (passive tracking and active sensing) in the absence of well-collected datasets. Furthermore, due to the high cost of storing CSI data over time, network operators rarely store it. Meta-learners can be used to improve AI-powered PET models with few-shot learning for poorly gathered data.

Problem 4: **Multi-data source data fusion for surveillance and privacy-enhancing efforts**. Rich data sources, including CSI, pictures, radar, and environment structure, can all help to improve tracking capability. These rich sources, on the other hand, can let AI-powered surveillance techniques monitor a user accurately. The idea of reducing privacy threats from several data sources or coordinated attacks is interesting.

Problem 5: **One-centimeter-precision radio positioning is still a challenge**. To provide such a high precision level in 6G, new enabling technologies are necessary. Terahertz communications, directional communications, and wireless radar are among examples. These can provide more detailed CSI data and more exact measurements (greater temporal-spatial resolution, better interference control) to increase radio positioning precision. Privacy for these 6G technologies, however, is still in the research and development stage.

VI. Conclusion

High-accuracy radio positioning and sensing are projected to be important techniques in 6G networks, enabling various precise location-based services such as indoor patient tracking, where GNSS often performs poorly. However, through the survey of the state-of-the-art PET techniques and a demonstration, we have shown that privacy threats in wireless networks are real and difficult to eliminate completely. Given that the capability of AI models might potentially aid attackers, a single privacy-enhancing approach is insufficient to prevent the attacker from exposing user positions and movements. We believe that balancing privacy and innovation, i.e., keeping the freedom to gather rich CSI data for the purpose of improving communication technologies in 6G THz, will be an important future study. Another topic is to provide signal encryption and access control features in wireless chips to mitigate privacy threats from many data sources and coordinated attacks.

Acknowledgement

This work was partly supported by the National Science and Technology Council (NSTC) of Taiwan, under Grant No 111-2222-E-194-007-MY2, Grant No 112-2912-I-194-503, and Grant No 112-2221-E-194-017-MY3.

References

[1] A. Behravan, V. Yajnanarayana, M. F. Keskin, H. Chen, D. Shrestha, T. E. Abrudan, T. Svensson, K. Schindhelm, A. Wolfgang, S. Lindberg, and H. Wymeersch, “Positioning and Sensing in 6G: Gaps, Challenges, and Opportunities,” *https://arxiv.org/abs/2211.01183*, 2022.

[2] H. Wymeersch and G. Seco-Granados, “Radio Localization and Sensing – Part II: State-of-the-art and Challenges,” *IEEE Commun. Lett.*, pp. 1–1, 2022.

[3] O. Kanhere and T. S. Rappaport, “Position Location for Futuristic Cellular Communications: 5G and Beyond,” *IEEE Commun. Mag.”*, vol. 59, no. 1, pp. 70–75, 2021.

[4] V.-L. Nguyen, et al., “Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges,” *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2384–2428, 2021.

[5] F. Jin, et al., “A survey and experimental study on privacy-preserving trajectory data publishing,” *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 6, pp. 5577–5596, 2023.

[6] K. Witrisal et al., “High-Accuracy Localization for Assisted Living: 5G systems will turn multipath channels from foe to friend,” *IEEE Signal Process. Mag.*, vol. 33, no. 2, pp. 59–70, 2016.

[7] A. Shastri, et al., “A Review of Millimeter Wave Device-Based Localization and Device-Free Sensing Technologies and Applications,” *IEEE Commun. Surveys Tuts.*, vol. 24, no. 3, pp. 1708–1749, 2022.

[8] S. M. Hernandez and E. Bulut, “WiFi Sensing on the Edge: Signal Processing Techniques and Challenges for Real-World Systems,” *IEEE Commun. Surveys Tuts.*, pp. 1–1, 2022.

[9] B. Korany, H. Cai, and Y. Mostofi, “Multiple People Identification Through Walls Using Off-the-Shelf WiFi,” *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6963–6974, 2021.

[10] M. Cominelli, F. Gringoli, and R. Lo Cigno, “AntiSense: Standard-compliant CSI obfuscation against unauthorized Wi-Fi sensing,” *Computer Communications*, vol. 185, pp. 92–103, 2022.

[11] V.-L. Nguyen, L.-H. Nguyen, P.-C. Lin, and R.-H. Hwang, “Deep Learning-based Localization and Outlier Removal Integration Model for Indoor Surveillance,” in *IEEE ICC 2023*, Rome, Italy.

[12] R. L. Cigno, F. Gringoli, M. Cominelli, and L. Ghiro, “Integrating CSI Sensing in Wireless Networks: Challenges to Privacy and Countermeasures,” *IEEE Network*, vol. 36, no. 4, pp. 174–180, 2022.

[13] F. Shu, et al., “Beamforming and Transmit Power Design for Intelligent Reconfigurable Surface-Aided Secure Spatial Modulation,” *IEEE J. Sel. Topics Signal Process.*, vol. 16, no. 5, pp. 933–949, 2022.

[14] European-Union, “General data protection regulation,” *European Union - Regulation 2016/679*, 2016.

[15] M. Nabati et al., “Using synthetic data to enhance the accuracy of fingerprint-based localization: A deep learning approach,” *IEEE Sensors Lett.*, vol. 4, no. 4, pp. 1–4, 2020.

Van-Linh Nguyen (Member of IEEE) is an assistant professor at the Department of Computer Science and Information Engineering, National Chung Cheng University, Taiwan.

Ren-Hung Hwang (Senior Member of IEEE) is the dean of the College of Artificial Intelligence, National Yang Ming Chiao Tung University, Taiwan.

Bo-Chao Cheng is a professor at the Department of Electrical Engineering at National Chung Cheng University, Taiwan.

Ying-Dar Lin (Fellow of IEEE) is a chair professor of computer science at National Yang Ming Chiao Tung University, Taiwan.

Trung Q. Duong (Fellow of IEEE) is a professor at Queen’s University Belfast, UK, a Research Chair of the Royal Academy of Engineering, and a visiting professor at Kyung Hee University, South Korea.