Physical Layer Security in Near-Field Communications for 6G: A Survey

Milton Kumar Kundu
Electrical and Computer Engineering
Colorado State University
Colorado, USA
Email: *mkkeee002@gmail.com*

***Abstract*—Extremely large-scale antenna arrays (ELAAs) and terahertz-band operation are pushing the boundary of the electromagnetic near field outward to tens or even hundreds of meters, bringing spherical-wavefront propagation into the operating regime of everyday sixth-generation (6G) links. This shift introduces a new spatial degree of freedom – range, alongside angle – that fundamentally changes how confidentiality can be enforced at the physical layer. Where far-field physical layer security (PLS) can only discriminate users by direction, near-field PLS can additionally discriminate by distance, enabling secrecy even when a legitimate receiver and an eavesdropper share the same line of sight. This survey consolidates the fast-growing literature on near-field PLS, organizing it around five thrusts: (i) beamfocusing-based secure transmission, which exploits range-dependent energy concentration; (ii) artificial-noise, directional-modulation, and wavefront-domain techniques; (iii) reconfigurable-intelligent-surface (RIS/STAR-RIS)-assisted near-field security; (iv) convergence with non-orthogonal multiple access (NOMA), rate-splitting multiple access (RSMA), and integrated sensing and communication (ISAC); and (v) emerging enablers, namely movable/fluid antennas and learning-based optimization. We also summarize fundamental secrecy-performance-limit results that quantify exactly how much the near-field range dimension improves on far-field secrecy capacity. A companion Chinese-language survey published in the *Journal of Electronics & Information Technology* in late 2025 covers similar ground; this article is intended as a complementary, English-language synthesis that additionally incorporates results published through early 2026, and it is organized around a threat-model-first taxonomy rather than a scenario-first one. We close by identifying open problems in channel modeling, security-performance-energy tradeoffs, hybrid near/far-field coexistence, and the near-total absence of experimental (as opposed to simulation-only) validation in this literature.**

***Index Terms*—Physical layer security, near-field communications, extremely large-scale antenna arrays, beamfocusing, reconfigurable intelligent surfaces, 6G.**

I. Introduction

A. Motivation

Sixth-generation (6G) wireless systems are expected to rely on extremely large-scale antenna arrays (ELAAs), holographic surfaces, and terahertz (THz)-band carriers to meet aggressive throughput, latency, and localization targets [1], [2]. A direct consequence of enlarging the array aperture and raising the carrier frequency is that the Rayleigh (Fraunhofer) distance – the conventional boundary between near-field and far-field propagation – scales with the square of the aperture and linearly with frequency. For arrays envisioned in 6G deployments, this boundary can extend to tens or hundreds of meters [3], [4], meaning that near-field, spherical-wavefront propagation is no longer a short-range curiosity confined to reactive antenna zones; it is the operating regime for a meaningful fraction of practical links.

This matters for security because far-field physical layer security (PLS), which has been studied for decades following Wyner's original wiretap-channel formulation [7], fundamentally discriminates users only by *angle*: a legitimate receiver and an eavesdropper sharing the same direction from the transmitter are, from a plane-wave standpoint, indistinguishable, and secrecy collapses. Near-field propagation breaks this constraint. Because the array can synthesize a spherical wavefront that concentrates energy at a specific *point* in space – a technique commonly called beamfocusing – rather than merely along a specific *direction* (beamsteering) [3], secrecy becomes achievable even between co-located-in-angle users, as long as they differ in range from the transmitter [8]. This additional range-domain degree of freedom is the central enabler that near-field PLS research exploits, and it is also the source of new vulnerabilities – joint angle-range eavesdropping, frequency-dependent beam-split leakage in wideband systems, and security-performance conflicts at the near/far-field boundary – that this literature must address.

B. Relation to Existing Surveys

PLS itself is one of the most heavily surveyed areas of wireless communications, with comprehensive treatments of multi-antenna PLS [9], [10], optimization-based PLS [11], and PLS for 5G [12], [13]. Near-field communications (NFC) more broadly has also been surveyed extensively, most comprehensively in [14] and [15], both of which identify PLS as one of several emerging integration opportunities for NFC but treat it only briefly, as one subsection among many (alongside RIS, NOMA, wireless power transfer, and ISAC integration).

A dedicated survey of PLS specifically *within* near-field communications was published in late 2025 in the *Journal of Electronics & Information Technology* [16], organizing the literature around beamfocusing, artificial-noise injection, and multi-technology integration (RIS, THz, ISAC), and around line-of-sight (LoS), non-LoS, and hybrid near/far-field transmission scenarios. That survey is thorough and, to our knowledge, is the first dedicated treatment of this topic; however,

it is published in Chinese, which limits its reach to the broader international research community reading in English. A separate tutorial, [17], surveys PLS techniques for next-generation multiple access broadly, of which near-field access is one instance among several (alongside RSMA and NOMA in conventional far-field settings), rather than a focused near-field treatment.

This survey's coverage of the literature in Sections IV–VII was assembled starting from the corpus of papers catalogued in [16], and we state this plainly rather than presenting the bibliography as independently discovered from scratch. Every citation drawn from that starting point was, however, independently re-verified against its primary source rather than accepted on [16]'s characterization of it – a process that surfaced and corrected at least one classification error of our own, where a general STAR-RIS secrecy paper using a purely statistical channel model had initially been grouped with the near-field-specific results in Section VI (a correction reflected in that section's discussion).

Three aspects of this survey are not derived from [16]. First, the two results anchoring its technical core – the foundational near-field secrecy-capacity result [8] (Section IV) and the closed-form performance-limit analysis [46] (Section IX) – were located independently, before [16] was known to us. Second, this survey covers near-field PLS results published from October 2025 through early 2026, entirely after [16]'s own literature search: the first hardware-validated near-field RIS-PLS system [37], movable-antenna-based secrecy [43], and the mixed near/far-field secrecy analysis [47] postdate it and could not have been included. Third, and most substantively, this survey organizes its taxonomy around the *security mechanism* employed – beamfocusing, artificial noise, RIS, multiple-access integration, learning-based methods – rather than around the propagation scenario. This reorganization surfaces a pattern that scenario-first organization obscures: considered as a mechanism rather than a scenario feature, artificial noise turns out to shift from merely beneficial to structurally necessary once multiple legitimate users share the near field (Section V), a finding that recurs across otherwise unrelated beamfocusing and NOMA results (Sections IV, VII) but is easy to miss when those results are instead grouped by LoS/NLoS scenario, as in [16]. The closed-form depth-of-insecurity result in Section IX is further illustrated here with an original numerical evaluation (Fig. 4), computed directly from its published closed-form expression, which does not appear in [16] or, to our knowledge, elsewhere in this literature.

C. Contributions and Organization

The remainder of this survey is organized as follows. Section II reviews the necessary background on PLS fundamentals and near-field propagation. Section III presents the taxonomy used throughout the survey. Sections IV–VIII review, respectively, beamfocusing-based secure transmission, artificial-noise and wavefront-domain techniques, RIS/STAR-RIS-assisted near-field PLS, convergence with NOMA/RSMA/ISAC, and emerging enablers (movable antennas and learning-based optimization). Section IX reviews fundamental secrecy-performance-limit results. Section X discusses open challenges and future directions, and Section XI concludes.

II. Background and Preliminaries

A. Physical Layer Security Fundamentals

PLS exploits the physical properties of the wireless channel – rather than computational hardness assumptions, as in cryptographic security – to guarantee confidentiality. In Wyner's original wiretap-channel model [7], a transmitter (Alice) sends confidential information to a legitimate receiver (Bob) over a channel that is also observed, in degraded form, by an eavesdropper (Eve). The secrecy capacity is the supremum of rates at which Alice can communicate to Bob while keeping Eve's information about the message arbitrarily small; in the Gaussian case, for a beamforming vector $\mathbf{w}$ transmitted over channels $\mathbf{h}_b$ and $\mathbf{h}_e$ to Bob and Eve respectively, it reduces to the positive difference between Bob's and Eve's channel capacities [46]:

$$C_w = \max\left\{\log_2\left(\frac{1+\gamma_b}{1+\gamma_e}\right), 0\right\}, \qquad \gamma_k = \frac{|\mathbf{h}_k^H \mathbf{w}|^2}{\sigma_k^2}, \quad (1)$$

where γ_k is the receive SNR at node $k \in \{b, e\}$ and σ_k^2 its noise power. Equation (1) makes explicit why angle-only far-field discrimination fails when Bob and Eve share a direction: under a far-field planar-wave model, $\mathbf{h}_b$ and $\mathbf{h}_e$ become near-parallel whenever the two nodes are angularly co-located, driving $\gamma_b \approx \gamma_e$ and hence $C_w \to 0$ regardless of $\mathbf{w}$ – the beamformer simply has no way to favor one node's channel over the other's. Section II-B and Section IX make precise how the near-field, spherical-wave case breaks this degeneracy.

In multi-antenna systems, secrecy capacity can be actively engineered rather than left to channel statistics alone, via secure beamforming (directing signal energy toward Bob and away from Eve), artificial-noise (AN) injection (transmitting deliberate interference in the null space of Bob's channel, degrading only Eve's reception), and physical-layer key generation (extracting shared secret keys from reciprocal channel randomness) [9]–[11]. These techniques were developed and analyzed almost exclusively under far-field, plane-wave channel models, in which the array response depends only on the angle of departure/arrival. This is the assumption that near-field propagation invalidates.

B. Near-Field Communications Fundamentals

Under far-field propagation, the wavefront impinging on (or emitted by) an antenna array is well-approximated as planar, and the array steering vector depends only on angle. This approximation is valid at distances beyond the Rayleigh distance, $d_R = 2D^2/\lambda$, where D is the array aperture and λ is the wavelength [14]. As D grows to the scale of ELAAs (potentially several meters) and λ shrinks in mmWave and THz bands, d_R grows sharply, extending the near-field region well beyond conventional cell-edge distances [4]. It is worth noting that d_R is itself a somewhat conservative boundary: it is derived from a phase-error criterion that has no direct bearing

on achievable rate, and [5] shows that a beamforming-gain-based "effective Rayleigh distance"

$$R_{\text{eff}} \approx C_\Delta \cos^2\theta \, \frac{2D^2}{\lambda}, \qquad C_\Delta = \frac{1}{4\beta_\Delta^2}, \tag{2}$$

– the range within which far-field beamforming's gain loss exceeds a chosen threshold Δ, with β_Δ the solution of a Fresnel-integral equation fixed by that threshold – is generally smaller than d_R for a receiver at angle θ. For example, at $\Delta = 5\%$, $C_\Delta \approx 0.367$, so R_{eff} is already only about 37% of d_R at boresight ($\theta = 0$) and shrinks further off-boresight via the $\cos^2\theta$ factor. None of the near-field PLS works surveyed below adopt this refined boundary in their own analysis, but it is a relevant caveat when interpreting any secrecy result that treats d_R as a hard near/far-field cutoff.

Within the near field, the wavefront is spherical rather than planar, and the array response depends jointly on both angle *and* range. This is the basis of *beamfocusing*: by appropriately phasing (and, in wideband systems, time-delaying) each antenna element, the array can constructively combine energy at a specific point in three-dimensional space rather than along an entire ray [3], [5]. Beamfocusing has been studied primarily for its multiplexing benefits – serving multiple users at the same angle but different ranges without inter-user interference [1] – but the same range-selectivity is precisely what near-field PLS techniques exploit for secrecy.

Fig. 1 illustrates schematically why this range-domain freedom matters for secrecy. Under far-field beamsteering, energy is directed along a ray defined solely by angle; a legitimate receiver (Bob) and an eavesdropper (Eve) sharing that angle both fall within the beam regardless of how their distances from the array differ, so secrecy is impossible to enforce spatially. Under near-field beamfocusing, the array instead concentrates energy within a bounded region surrounding a specific *point* in space. Eve, sharing Bob's angle but positioned at a sufficiently different range, falls outside this focal region and receives a substantially degraded signal. The size of this region – shrinking as array aperture grows – is precisely what [46] formalizes as the "depth of insecurity" introduced in Section IX.

Two practical complications recur throughout the near-field PLS literature. First, near-field *wideband* systems suffer from the beam-split effect: because the phase shifters in a hybrid beamforming architecture are frequency-independent, a beam designed to focus at (θ^B, r^B) using the center-frequency array response instead focuses, at subcarrier frequency f_m, on the point (θ^m, r^m) given by [6]

$$\theta^m = \arcsin\left(\frac{\lambda_m}{\lambda_c}\sin\theta^B\right), \qquad r^m = r^B \, \frac{\lambda_c\left(1-\sin^2\theta^m\right)}{\lambda_m\left(1-\sin^2\theta^B\right)}, \tag{3}$$

where λ_c and λ_m are the wavelengths at the center frequency and at f_m, respectively. This degrades focusing accuracy at off-center subcarriers and, for security purposes, can leak energy toward unintended range-angle locations unless compensated via true-time-delay elements or specialized precoding [18], [19]. Fig. 2 evaluates (3) directly across a representative 3 GHz band at 30 GHz center frequency (parameters matching [5], [19]'s own simulation setups) and shows that this range-domain drift is not a fixed-percentage nuisance: for a user near boresight it stays within about $\pm 6\%$ of r^B, but for a user at $\theta^B = 60^\circ$ it swings from -36% to $+34\%$ across the band. This matters directly for security, since the range-domain resolution that beamfocusing-based PLS schemes rely on (Section IV) degrades precisely where this drift is largest – off-boresight users and eavesdroppers are the ones a wideband, phase-shifter-only implementation protects least reliably. Second, realistic deployments frequently contain a mix of near-field and far-field users simultaneously (a *hybrid* near/far-field scenario), which complicates both channel estimation and secure resource allocation [42], [47].

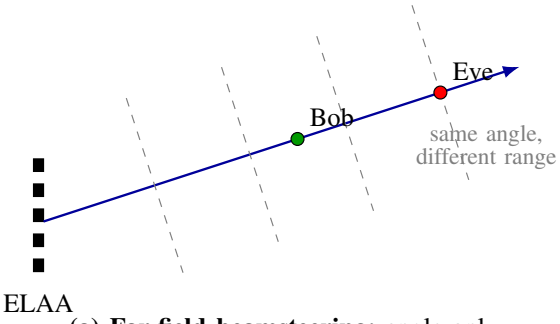
III. Taxonomy

We organize the near-field PLS literature into five thrusts, summarized in Table I. This structuring choice is threat-model- and mechanism-first: each thrust corresponds to a distinct signal-processing lever available at the transmitter (and, in the RIS case, at a passive/active reconfigurable element in the environment) for achieving range- and/or angle-domain secrecy. Fig. 3 gives a visual overview of the five thrusts before Table I details their representative works.

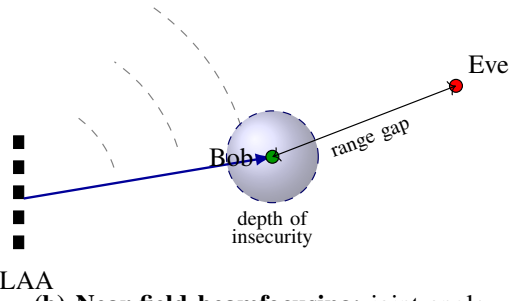
IV. Beamfocusing-Based Secure Transmission

The foundational result establishing beamfocusing as a secrecy mechanism is due to Zhang *et al.* [8], who showed that in near-field systems a positive secrecy rate remains achievable even when Bob and Eve are perfectly aligned in angle, provided their ranges differ – a scenario in which any far-field beamforming scheme yields zero secrecy capacity. This single result motivates essentially the entire subsequent literature reviewed in this section.

Building on this, [18] developed an analog beamfocusing approach for near-field *wideband* secure communication, addressing the beam-split problem directly in the security context; [19] proposed a true-time-delayer-based hybrid digital-TTD-analog beamfocusing architecture to secure wideband near-field MIMO links against the same wideband distortion, formulating a sum secrecy-capacity maximization problem solved via alternating optimization over the digital beamformer, TTD delays, and phase shifters. Against a piecewise-far-field low-complexity benchmark that focuses only on maximizing Bob's channel capacity without actively minimizing Eve's, [19] reports that this cheaper scheme still recovers around 70% of the full scheme's sum secrecy capacity in a general deployment with Bob, Eve, and scatterers spread across a sector, rising to about 80% specifically when Bob and Eve are not in the same direction from the BS – a useful practical data point on the cost of the low-complexity fallback when Eve's CSI is unavailable. [20] and its follow-up uplink treatment [21] analyzed near-field beamforming for PLS in both downlink and uplink directions, while [22] formulated a max-min secrecy-rate optimization across multiple legitimate users via beamfocusing, and [23] evaluated beamfocusing's secrecy enhancement in a system-level near-field setting. [24]



(a) Far-field beamsteering: angle-only discrimination – Eve intercepts the full beam



(b) Near-field beamfocusing: joint angle-range discrimination – Eve falls outside the focal spot

Fig. 1. Schematic (not to scale) comparison of far-field and near-field spatial secrecy. In (a), Bob and Eve share the same angular direction and both lie inside the beam, so no angle-only scheme can separate them. In (b), the array focuses energy on Bob's specific range-angle location; Eve, at the same angle but a different range, falls outside the focal region (the "depth of insecurity") and receives a degraded signal.

TABLE I
TAXONOMY OF NEAR-FIELD PHYSICAL LAYER SECURITY TECHNIQUES

Thrust	Core Mechanism	Representative Works
Beamfocusing-based	Exploit range-dependent energy concentration to confine signal quality degradation to Eve's location	[8], [18]–[27]
AN / directional modulation / wavefront-domain	Inject deliberate interference or exploit frequency/wavefront diversity so only the intended range-angle bin decodes correctly	[28]–[32]
RIS/STAR-RIS-assisted	Use passive or active reconfigurable surfaces to reshape the near-field propagation environment for secrecy	[33]–[39]
Multiple-access & ISAC convergence	Extend near-field secrecy to NOMA, RSMA, and joint sensing-communication settings	[39]–[42]
Emerging enablers	Movable/fluid antennas and learning-based (DRL/ML) optimization as new secrecy degrees of freedom	[43], [44]

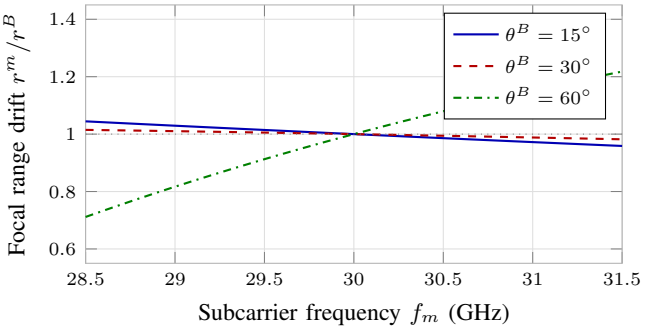


Fig. 2. Focal-range drift r^m/r^B across a 3 GHz band at 30 GHz center frequency, computed directly from the closed-form beam-split relation (3) (angles in the plot legend use TikZ's native degree trigonometry). The drift is mild near boresight but grows sharply off-boresight, meaning the wideband beam-split-induced information leakage that Sections II and IV discuss qualitatively is itself angle-dependent – exactly the users a narrowband analysis would treat as safest are the most exposed once bandwidth is taken into account.

specifically studied the effect of *imperfect* beamfocusing resolution – a practically important consideration, since real arrays cannot focus with arbitrary precision – on NOMA-aided near-field secrecy performance. [25] showed that, once multiple legitimate users are present, artificial noise is not merely helpful but *necessary* for near-field beamfocusing security – their single-user/single-eavesdropper analysis demonstrates AN can transform an otherwise insecure configuration into a secure one – and proposed a low-complexity multi-user beamforming-plus-AN design (built around an "interference domain" that captures inter-user interference levels) that matches conventional optimization-based performance at substantially lower computational cost; [26] introduced the concept of a receiver-centered "protected zone" – a physical or virtual region around Bob within which beamfocusing plus AN jointly guarantee secrecy without requiring Eve's channel state information (CSI), addressing a major practical limitation of most prior beamfocusing-based schemes, which assume Eve's CSI is known. Earlier exploratory work in [27] had already demonstrated PLS gains from spherical-wave massive MIMO channels using conventional (non-time-delay) architectures, predating the beam-split-aware designs above.

A consistent theme across this thrust is the tradeoff between focusing accuracy (which improves with array aperture and reduces with bandwidth-induced beam-split) and the achievable secrecy rate: several of the works above explicitly quantify how larger apertures shrink the spatial region in which an eavesdropper can achieve non-negligible information leakage.

V. ARTIFICIAL NOISE, DIRECTIONAL MODULATION, AND WAVEFRONT-DOMAIN TECHNIQUES

A second family of techniques does not rely solely on spatial energy confinement but actively distorts the signal seen outside the intended range-angle bin. [28] applied directional modulation – scrambling the constellation for any receiver

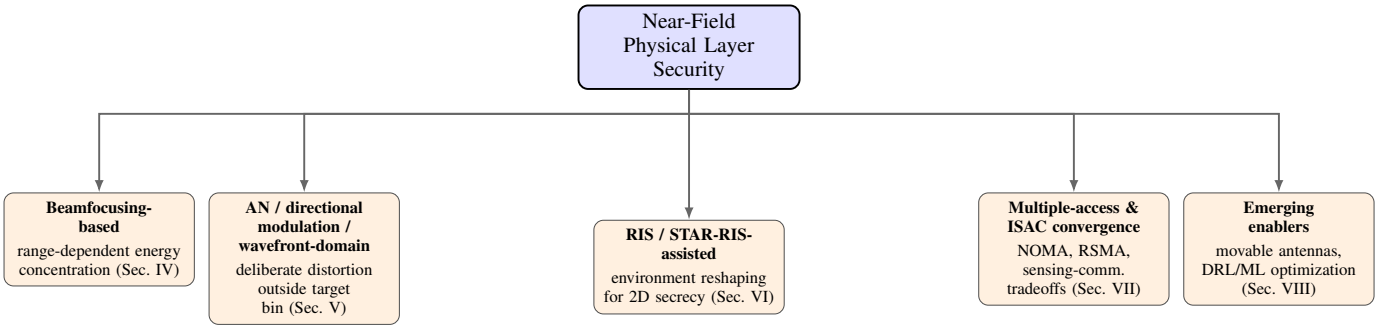


Fig. 3. Visual overview of the five-thrust taxonomy used to organize this survey. Each thrust corresponds to a distinct security-enabling mechanism, detailed with representative works in Table I.

outside a designed spatial region – to the near-field setting, exploiting the joint angle-range dependence of the near-field array response to achieve a two-dimensional (rather than angle-only) security region. [29] proposed a low-complexity AN-aided beamfocusing design specifically for near-field THz systems, where computational complexity is a first-order practical constraint given the very large arrays involved.

At THz frequencies specifically, [30] examined multi-antenna techniques for *range*-domain security (as distinct from angle-domain security, which dominates the lower-frequency literature), directly analyzing the security implications of the THz band's naturally short Rayleigh-to-near-field transition distances. [31] and its extended journal version [32] introduced *wavefront hopping*, a technique that rapidly and pseudorandomly varies the near-field wavefront shape (e.g., via reconfigurable lens or metasurface elements) so that only a receiver with precise, time-synchronized knowledge of the hopping pattern can coherently combine the signal; an eavesdropper without this knowledge experiences the equivalent of AN even without any dedicated jamming signal being transmitted. This is conceptually distinct from beamfocusing-based approaches in that security derives from a shared secret (the hopping sequence) rather than purely from geometry, blurring the line between physical layer security and physical-layer-assisted key-based security.

VI. RIS- and STAR-RIS-Assisted Near-Field PLS

Reconfigurable intelligent surfaces (RIS) add a further degree of design freedom by allowing the propagation environment itself, not just the transmitter's beamforming, to be shaped for security. [33] addressed a particularly practical concern – robust full-space secrecy design for simultaneously transmitting and reflecting (STAR-)RIS-aided networks when the eavesdropper's location and channel are only imperfectly known, using a large-system analytical technique to derive a closed-form asymptotic average secrecy rate under this uncertainty. We note that [33] models the BS-RIS and RIS-user links via standard statistical (Rayleigh) fading rather than a deterministic near-field array response, so it is not itself a near-field result; we include it here because the robust-CSI technique it develops – designing against location *and* channel uncertainty jointly, rather than assuming perfect Eve CSI – addresses a gap (identified in Section X-A) that near-field-specific RIS designs largely have not yet closed, and could plausibly transfer to a near-field array-response setting. [34] extended RIS-assisted security to the covert-communication setting in the near field, where the goal is not merely confidentiality but concealing the very existence of the transmission from a watchful adversary (a warden). [35] combined near-field secure transmission with orbital-angular-momentum (OAM) multiplexing using a double-RIS architecture, adding a further (mode-domain) degree of freedom to the range/angle security picture. [36] optimized secure energy efficiency – rather than raw secrecy rate – for STAR-RIS-assisted near-field wideband THz links, explicitly foregrounding the energy cost of maintaining security, a concern largely absent from the beamfocusing-only literature in Section IV.

The most recent and, to our knowledge, first *experimentally validated* RIS-based near-field PLS system is NF-SecRIS [37], which uses an ultra-large-scale RIS to implement secure location modulation: legitimate users at the correct range-and-angle location receive clean constellations, while eavesdroppers at any other range or angle receive obfuscated ones, achieving what the authors term genuinely two-dimensional (range-angle) PLS rather than the angle-only security of conventional far-field RIS schemes. This is validated on a physical 14×56-element (2-bit) RIS prototype operating at 5.8 GHz with a $39\,\text{cm} \times 156\,\text{cm}$ aperture: the reported bit-error-rate (BER) at Bob's location is 7.83×10^{-5}, while eavesdroppers outside the measured secure zone ($r \in [1.6, 1.7]\,\text{m}$, $\theta \in [-5^\circ, 5^\circ]$) experience BERs exceeding 40% across ASK, FSK, PSK, and QAM modulation schemes, making it one of the only hardware-validated results in the entire near-field PLS literature (see Section X-D). An ablation reported in the same work confirms that the artificial-noise (beam-nulling) component is essential: with it disabled, eavesdroppers achieve low BER and successfully intercept the signal, despite beamfocusing alone already suppressing their received power. Complementary work in [38] tackles a passive eavesdropper of *unknown* location – a harder and more realistic setting than most near-field PLS designs, which assume Eve's location or CSI is known – by combining frequency diverse arrays (FDA) with RIS via random inverted transmit beamforming and reflective-element subset selection; the authors derive a closed-form worst-case secrecy rate over all possible eavesdropper positions and show the largest secrecy gains occur precisely

when Eve is close to the RIS or the legitimate user, the regime where conventional angle-only RIS security is weakest. RIS-assisted near-field NOMA schemes explicitly trading off secrecy against user fairness [39] round out this thrust.

VII. Convergence with Multiple Access and ISAC

As near-field systems are expected to serve multiple users simultaneously and, increasingly, to jointly sense their environment, a growing body of work studies near-field PLS under NOMA, RSMA, and ISAC. [39] addresses a specifically NOMA-flavored threat – *internal* eavesdropping, where the untrusted party is not an external Eve but the near NOMA user itself, who must decode and cancel the far user's signal via successive interference cancellation (SIC) and can therefore also intercept it. In the far field, securing the far user against this near, stronger-channel internal eavesdropper is provably impossible, since SIC ordering requires the near user's channel to dominate; [39] shows that near-field beamfocusing breaks this constraint by adding range as an independent degree of freedom, making the far user's security achievable precisely in the regime (near-field) where the far-field result rules it out. [24] (already discussed in Section IV in its beamfocusing-resolution aspect) similarly addresses near-field NOMA security, showing that the near-field range dimension can be used to separate legitimate NOMA users from an eavesdropper in ways that are simply unavailable in far-field NOMA secrecy analysis.

For ISAC, [40] analyzed physical-layer security for NOMA-assisted ISAC systems explicitly under near-field propagation, characterizing how the sensing functionality's probing signals – which by design illuminate a wide spatial region, including any potential eavesdropper – interact with the secrecy of the communication functionality's data signal. [41] extended near-field ISAC security to UAV networks, where node mobility adds a further time-varying dimension to the range-angle secrecy problem. Finally, [42] addressed the important *hybrid* near/far-field case directly, proposing multi-beam symbol-level precoding to secure transmission simultaneously to near-field and far-field legitimate users, a scenario that neither purely near-field nor purely far-field PLS techniques handle well in isolation.

VIII. Emerging Enablers: Movable Antennas and Learning-Based Optimization

Two more recent threads depart from the fixed-position-antenna, model-based-optimization paradigm common to Sections IV–VII. [43] introduced movable-antenna (MA)-empowered secure near-field MIMO, in which the physical positions of a modest number of antenna elements – not merely their phase weights – are jointly optimized alongside hybrid beamforming to maximize secrecy rate. This is motivated by a genuine practical concern: conventional fixed-position-antenna ELAAs require on the order of 4×10^4 antennas to cover a $100\lambda \times 100\lambda$ aperture at half-wavelength spacing, which the authors note as a serious hardware, energy, and signal-processing burden; allowing a much smaller number of antennas to physically relocate offers comparable secrecy gains at substantially lower hardware cost.

Separately, [44] applied deep reinforcement learning (DRL) directly to near-field MIMO PLS optimization, motivated by the fact that the joint angle-range beamforming and (where applicable) AN-design optimization problems in Sections IV–VI are typically non-convex and solved via iterative, model-based algorithms (alternating optimization, successive convex approximation, semidefinite relaxation) that can be slow to adapt to fast-changing channel and eavesdropper conditions; a trained DRL agent can, in principle, output near-optimal beamforming decisions with far lower online computational latency. Physical-layer key generation exploiting near-field channel decorrelation properties has also been explored in a learning-assisted setting, discussed as one component of a broader near-field ML survey [45], though this specific direction remains comparatively less developed than the beamforming-centric approaches above.

IX. Fundamental Secrecy Performance Limits

Alongside scheme-specific designs, a smaller body of work has sought to characterize fundamental secrecy-performance limits of near-field systems in closed form. [46] derived closed-form secrecy-capacity expressions for a uniform planar-wave (UPW, far-field), uniform spherical-wave (USW, near-field), and non-uniform spherical-wave (NUSW, reactive near-field) channel model under a common framework, and proved that when Bob and Eve share a direction, the far-field secrecy capacity is exactly zero whenever $r_b \geq r_e$ (Bob no closer than Eve), whereas both near-field models retain strictly positive secrecy capacity for any $r_b \neq r_e$ – formally confirming, rather than merely observing empirically as much of the literature in Sections IV–VIII does, that near-field beamfocusing provides a genuine range-domain security mechanism unavailable in the far field.

Table II summarizes the resulting comparison across the three models as the number of transmit antennas $M \to \infty$, reproducing the qualitative pattern established in [46]. The UPW column's zero high-SNR slope confirms Eq. (1)'s implication from Section II-A directly – in the co-directional worst case, adding transmit power buys nothing under a far-field model, since C_w is capacity-limited by angular correlation alone, not SNR. More strikingly, the table shows that even the near-field USW model – despite correctly capturing the range-domain discrimination that makes co-directional secrecy possible at all – allows secrecy capacity to grow without bound as $M \to \infty$, which is physically impossible under any fixed transmit power constraint; only the NUSW model, which retains the full non-uniform channel-power variation across antenna elements omitted by USW's uniform-power approximation, respects energy conservation. This is a caution for any near-field PLS scheme (including several beamfocusing designs in Section IV) that adopts the simpler USW model for tractability: its qualitative conclusion that near-field beamfocusing outperforms far-field secrecy is correct, but its quantitative secrecy-rate predictions at very large M should be treated as optimistic.

TABLE II
COMPARISON OF FAR-FIELD AND NEAR-FIELD CHANNEL MODELS AS $M \to \infty$, WHEN BOB AND EVE SHARE A DIRECTION [46]

Model	Energy conserved?	Secrecy capacity	High-SNR slope
UPW (far-field)	No	0 if $r_b \geq r_e$	0
USW (near-field)	No	> 0, unbounded	1
NUSW (reactive NF)	**Yes**	> 0, bounded	1

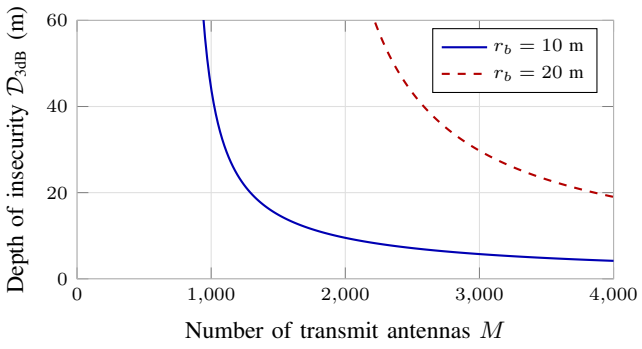


Fig. 4. The closed-form 3 dB depth of insecurity, Eq. (4), computed for $\lambda = 0.125$ m, $d = \lambda/2$, $\Upsilon_{3\text{dB}} = 0.79$ (parameters as used in [46]'s own numerical validation), plotted directly from the closed-form expression rather than digitized from the source. Each curve begins just above its own critical antenna count ($M \approx 799$ for $r_b = 10$ m, $M \approx 1598$ for $r_b = 20$ m) – below this count the depth is formally infinite – and both decay toward zero as M grows further, confirming that larger apertures monotonically tighten the near-field secrecy guarantee.

To quantify this benefit, the same work introduces the *depth of insecurity*: given Bob at range r_b and boresight alignment with Eve, it is the length of the range interval $[r_{\min}, r_{\max}]$ within which Eve's channel remains correlated enough with Bob's ($\cos\psi \leq \Gamma$, for a -3 dB threshold $\Gamma = 1/2$) to leak non-negligible information via the high-SNR-optimal beamformer. Under the USW model with a square array ($M_x = M_z = \sqrt{M}$) at boresight, this admits the closed form

$$\mathcal{D}_{3\text{dB}} = \begin{cases} \dfrac{2r_b^2 r_s}{r_s^2 - r_b^2}, & r_b < r_s \\ \infty, & r_b \geq r_s \end{cases}, \qquad r_s = \frac{Md^2}{4\lambda\,\Upsilon_{3\text{dB}}^2}, \tag{4}$$

where d is the antenna pitch, λ the wavelength, M the number of transmit antennas, and $\Upsilon_{3\text{dB}} \approx 0.79$ a constant fixed by the -3 dB threshold. Fig. 4 plots (4) directly, illustrating the central quantitative claim of this thrust: below a critical antenna count ($r_b \geq r_s$), the depth of insecurity is formally infinite – an eavesdropper anywhere along Bob's direction leaks non-negligible information, the far-field-like worst case. Once the array grows large enough to push r_s past r_b, the depth becomes finite and then shrinks further, monotonically, as M continues to grow – the closed-form, analytical counterpart to the empirical beam-focusing-improves-secrecy claims made throughout Sections IV and VI.

[47] extended this line of analysis to the practically important *mixed* setting – far-field legitimate users served by an XL-array in the presence of eavesdroppers located in its near field – and derived a genuinely counter-intuitive result: because a far-field steering vector correlates with a near-field eavesdropper's channel over a wider angular range than it would with another far-field user's channel (an *energy-spread*, rather than energy-focusing, effect), the insecure-transmission region for a far-field Bob is *larger* against a near-field Eve than the classical far-field-only result would predict, even when Bob and Eve sit at different angles. With only one legitimate user, this makes the mixed scenario strictly worse for security than the pure far-field case. The paper's second finding recovers the loss: with two or more legitimate users, one Bob's signal acts as unintentional interference at the near-field Eve, and optimizing the power split across Bobs can shrink or eliminate the enlarged insecure region altogether – so multi-user scheduling, not just beamforming, becomes a security lever specific to the mixed-field regime that neither pure-near-field nor pure-far-field analyses surface. This is the most direct evidence in the surveyed literature that treating a mixed deployment with either idealized model alone (as most works in Sections IV–VIII implicitly do) can be actively misleading, not merely imprecise.

X. OPEN CHALLENGES AND FUTURE DIRECTIONS

A. Channel Modeling and Estimation Complexity

Nearly all works reviewed above assume perfect, or near-perfect, CSI for both the legitimate receiver and, in many cases, the eavesdropper – an assumption increasingly relaxed for near-field geometries specifically by [26] (and, in a non-near-field STAR-RIS setting whose robust-CSI technique is a natural candidate for adaptation, by [33]) but still far from resolved for realistic near-field channels, which exhibit spatial non-stationarity across a large aperture and frequently mix LoS and non-LoS (NLoS) paths in ways that are still under active study even outside the security context [4]. Secure beamforming and AN designs that are robust to *both* range and angle estimation error, jointly, remain comparatively underexplored relative to angle-only robustness results inherited from the far-field literature.

B. Security-Performance-Energy Tradeoffs

Most schemes in Sections IV–VI optimize secrecy rate or secrecy energy efficiency in isolation; comparatively few works (an exception being [36]) jointly characterize the three-way tradeoff between secrecy performance, communication throughput, and energy consumption that a real ELAA/RIS deployment would need to navigate, particularly given the hardware power draw of ultra-large-scale RIS or MA arrays.

C. Hybrid Near/Far-Field Coexistence

As Section VII and the JEIT survey [16] both emphasize, realistic multi-user deployments will rarely be purely near-field. The handful of hybrid-scenario works to date [42], [47] suggest this is analytically and algorithmically harder than either pure regime, and represents, in our assessment, the single largest open gap in the current literature.

D. Experimental and Hardware Validation

With the notable exception of NF-SecRIS's physical RIS prototype [37], essentially every result surveyed in Sections IV–IX is validated by numerical simulation alone. Real ELAA hardware exhibits mutual coupling, phase-shifter quantization, and calibration errors that are not captured in idealized array-response models, and it remains an open question how much of the secrecy improvement predicted analytically survives contact with real RF front-ends.

E. AI-Native and Standardization Directions

Beyond the model-based DRL application in [44], both this survey and [16] identify AI-assisted, adaptive near-field security – potentially incorporating foundation-model-style channel representations now emerging in the broader wireless AI literature – as a promising but largely unrealized direction, alongside the broader observation, echoed in [16], that no unified standard or systematic security framework yet exists for near-field 6G deployments.

XI. Conclusion

The near-field regime introduces a genuinely new degree of freedom – range – into physical layer security design, enabling secrecy in configurations (angularly co-located legitimate and eavesdropping receivers) where far-field PLS provably fails. This survey organized the resulting literature into beamfocusing-based transmission, artificial-noise and wavefront-domain techniques, RIS/STAR-RIS-assisted designs, multiple-access and ISAC convergence, and emerging movable-antenna and learning-based enablers, alongside the fundamental secrecy-performance-limit results that formally justify why larger apertures yield stronger near-field secrecy. The field is young: a dedicated survey did not exist in English prior to this work, its Chinese-language counterpart [16] was published only months ago, and the most advanced result to date with physical hardware validation [37] appeared within the final weeks of the period this survey covers. Channel-modeling robustness, security-performance-energy tradeoffs, hybrid near/far-field coexistence, and experimental validation stand out as the most consequential open problems for the next several years of work in this area.

References

[1] M. Cui, Z. Wu, Y. Lu, X. Wei, and L. Dai, "Near-field MIMO communications for 6G: Fundamentals, challenges, potentials, and future directions," *IEEE Commun. Mag.*, vol. 61, no. 1, pp. 40–46, Jan. 2023.

[2] Z. Wang *et al.*, "A tutorial on extremely large-scale MIMO for 6G: Fundamentals, signal processing, and applications," *IEEE Commun. Surv. Tut.*, vol. 26, no. 3, pp. 1560–1605, 3rd Quart. 2024.

[3] H. Zhang, N. Shlezinger, F. Guidi, D. Dardari, and Y. C. Eldar, "6G wireless communications: From far-field beam steering to near-field beam focusing," *IEEE Commun. Mag.*, vol. 61, no. 4, pp. 72–77, Apr. 2023.

[4] M. Cui and L. Dai, "Channel estimation for extremely large-scale MIMO: Far-field or near-field?" *IEEE Trans. Commun.*, vol. 70, no. 4, pp. 2663–2677, Apr. 2022.

[5] M. Cui and L. Dai, "Near-field wideband beamforming for extremely large antenna arrays," *IEEE Trans. Wireless Commun.*, vol. 23, no. 10, pp. 13110–13124, Oct. 2024.

[6] M. Cui, L. Dai, Z. Wang, S. Zhou, and N. Ge, "Near-field rainbow: Wideband beam training for XL-MIMO," *IEEE Trans. Wireless Commun.*, vol. 22, no. 6, pp. 3899–3912, Jun. 2023.

[7] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[8] Z. Zhang, Y. Liu, Z. Wang, X. Mu, and J. Chen, "Physical layer security in near-field communications," *IEEE Trans. Veh. Technol.*, vol. 73, no. 7, pp. 10761–10766, Jul. 2024.

[9] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 2014.

[10] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surv. Tut.*, vol. 19, no. 2, pp. 1027–1053, 2nd Quart. 2017.

[11] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1878–1911, 2nd Quart. 2019.

[12] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[13] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[14] Y. Liu, Z. Wang, J. Xu, C. Ouyang, X. Mu, and R. Schober, "Near-field communications: A tutorial review," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 1999–2049, 2023.

[15] Y. Liu, C. Ouyang, Z. Wang, J. Xu, X. Mu, and A. L. Swindlehurst, "Near-field communications: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 27, no. 3, pp. 1687–1728, 2025.

[16] Y. Xu, J. Li, D. Luo, J. Wang, X. Li, L. Yang, and L. Chen, "A survey on physical layer security in near-field communication" (in Chinese), *J. Electron. Inf. Technol.*, vol. 47, no. 11, pp. 4129–4143, Nov. 2025.

[17] L. Lv, D. Xu, R. Q. Hu, Y. Ye, L. Yang, X. Lei, X. Wang, D. I. Kim, and A. Nallanathan, "Safeguarding next-generation multiple access using physical layer security techniques: A tutorial," *Proc. IEEE*, vol. 112, no. 9, pp. 1421–1466, Sep. 2024.

[18] Y. Zhang, H. Zhang, S. Xiao, W. Tang, and Y. C. Eldar, "Near-field wideband secure communications: An analog beamfocusing approach," *IEEE Trans. Signal Process.*, vol. 72, pp. 2173–2187, Apr. 2024.

[19] X. Hu, Y. Zhang, L. Yang *et al.*, "Securing near-field wideband MIMO communications via true-time delayer-based hybrid beamfocusing," *IEEE Trans. Wireless Commun.*, vol. 23, no. 10, pp. 13562–13578, Oct. 2024.

[20] J. Ferreira, J. Guerreiro, and R. Dinis, "Physical layer security with near-field beamforming," *IEEE Access*, vol. 12, pp. 4801–4811, Jan. 2024.

[21] J. Ferreira, D. Macedo, J. Guerreiro, and R. Dinis, "Optimized beamforming design for PLS in near-field uplink communications," in *Proc. IEEE 99th Veh. Technol. Conf. (VTC2024-Spring)*, Singapore, 2024, pp. 116–120.

[22] A. A. Nasir, "Max-min secrecy rate optimization through beam focusing in near-field communications," *IEEE Commun. Lett.*, vol. 28, no. 7, pp. 1594–1598, Jul. 2024.

[23] S. Droulias, G. Stratidakis, and A. Alexiou, "Beam-focusing in near-field communications: Enhancing the physical layer security," in *Proc. IEEE 25th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Lucca, Italy, 2024, pp. 216–220.

[24] B. Zhuo, J. Gu, G. Zhang, and W. Duan, "Imperfect resolution of near-field beamfocusing for NOMA-aided physical-layer security," *IEEE Internet Things J.*, vol. 12, no. 12, pp. 18147–18160, Jun. 2025.

[25] Y. Zhang, Y. Fang, C. You, Y.-J. A. Zhang, and H. C. So, "Performance analysis and low-complexity beamforming design for near-field physical layer security," *IEEE Trans. Commun.*, vol. 74, pp. 781–796, 2026, doi: 10.1109/TCOMM.2025.3626021. Also available as arXiv preprint arXiv:2407.13491.

[26] C. Liu, X. Zhou, N. Yang, S. Durrani, and A. L. Swindlehurst, "Near-field secure beamfocusing with receiver-centered protected zone," *arXiv preprint arXiv:2505.19523*, 2025, to appear in *IEEE Trans. Wireless Commun.*

[27] D. Yu, L. Yang, X. Gao *et al.*, "Physical layer security in spherical-wave channel using massive MIMO," in *Proc. IEEE 33rd Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Kyoto, Japan, 2022, pp. 288–293.

[28] J. Chen, Y. Xiao, K. Liu, Y. Zhong, X. Lei, and M. Xiao, "Physical layer security for near-field communications via directional modulation," *IEEE Trans. Veh. Technol.*, vol. 73, no. 8, pp. 12242–12246, Aug. 2024.

[29] Z. Tang, N. Yang, X. Zhou, S. Durrani, M. Juntti, and J. M. Jornet, "Low complexity artificial noise aided beam focusing design in near-field terahertz communications," *IEEE Trans. Veh. Technol.*, early access, 2025, doi: 10.1109/TVT.2025.3625557. Also available as arXiv preprint arXiv:2502.08967.

[30] W. Gao, C. Han, X. Lu *et al.*, "On multiple-antenna techniques for physical-layer range security in the terahertz band," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 3089–3103, 2024.

[31] V. Petrov, H. Guerboukha, D. M. Mittleman *et al.*, "Wavefront hopping: An enabler for reliable and secure near field terahertz communications in 6G and beyond," *IEEE Wireless Commun.*, vol. 31, no. 1, pp. 48–55, Feb. 2024.

[32] V. Petrov, H. Guerboukha, A. Singh *et al.*, "Wavefront hopping for physical layer security in 6G and beyond near-field THz communications," *IEEE Trans. Commun.*, vol. 73, no. 5, pp. 2996–3012, May 2025.

[33] H. Xiao, X. Hu, A. Li *et al.*, "Robust full-space physical layer security for STAR-RIS-aided wireless networks: Eavesdropper with uncertain location and channel," *IEEE Trans. Wireless Commun.*, vol. 24, no. 9, pp. 7206–7220, Sep. 2025.

[34] J. Liu, G. Yang, Y. Liu *et al.*, "RIS empowered near-field covert communications," *IEEE Trans. Wireless Commun.*, vol. 23, no. 10, pp. 15477–15492, Oct. 2024.

[35] L. Liang, M. Wang, W. Cheng *et al.*, "Double-RIS-assisted orbital angular momentum near-field secure communications," *IEEE Trans. Wireless Commun.*, vol. 24, no. 6, pp. 4952–4965, Jun. 2025.

[36] A. A. Nasir, "Max-min secure energy efficiency optimization for STAR-RIS-assisted near-field wideband THz communication," *IEEE Trans. Green Commun. Netw.*, early access, 2025.

[37] Z. Wang, C. Meng, J. Yang, J. Wang, Y. Li, L. Jiang, and J. Zhang, "NF-SecRIS: RIS-assisted near-field physical layer security via secure location modulation," *arXiv preprint arXiv:2511.02949*, Nov. 2025.

[38] C. Li, S. Roth, and A. Sezgin, "Enhancing the secrecy rate with direction-range focusing with FDA and RIS," *IEEE Trans. Veh. Technol.*, vol. 74, no. 5, pp. 7835–7849, May 2025.

[39] J. Lei, X. Mu, T. Zhang, and Y. Liu, "RIS assisted near-field NOMA communications: A security-fairness trade-off," *IEEE Trans. Veh. Technol.*, vol. 74, no. 7, pp. 11656–11661, Jul. 2025.

[40] L. Zhang, Y. Wang, H. Chen, and Y. Cao, "Physical-layer security of the NOMA-assisted ISAC systems under near-field scenario," *IEEE Internet Things J.*, vol. 12, no. 12, pp. 18546–18553, Jun. 2025.

[41] J. Zhao, S. Xue, K. Cai, X. Mu, Y. Liu, and Y. Zhu, "Near-field integrated sensing and communications for secure UAV networks," *IEEE J. Sel. Areas Commun.*, early access, 2025, doi: 10.1109/JSAC.2025.3608737. Also available as arXiv preprint arXiv:2502.01003.

[42] W. Deng, B. Qiu, and W. Cheng, "Multi-beam symbol-level secure communication for hybrid near- and far-field communications," in *Proc. Int. Conf. Ubiquitous Commun. (Ucom)*, Xi'an, China, 2024, pp. 16–20.

[43] Y. Ma, K. Liu, Y. Liu, and L. Zhu, "Movable antenna empowered secure near-field MIMO communications," *arXiv preprint arXiv:2509.00901*, 2025.

[44] M. M. Razaq and L. Peng, "DRL-based physical-layer security optimization in near-field MIMO systems," *IEEE Internet Things J.*, vol. 12, no. 12, pp. 18606–18615, Jun. 2025.

[45] A. Iqbal, A. Al-Habashna, G. Wainer, and G. Boudreau, "Machine learning in near-field communication for 6G: A survey," *arXiv preprint arXiv:2509.16723*, 2025.

[46] B. Zhao, C. Ouyang, X. Zhang, and Y. Liu, "Performance analysis of physical layer security: From far-field to near-field," *IEEE Trans. Wireless Commun.*, vol. 24, no. 9, pp. 7392–7408, Sep. 2025.

[47] T. Liu, C. You, C. Zhou, Y. Zhang, S. Gong, H. Liu, and G. Zhang, "Physical-layer security in mixed near-field and far-field communication systems," *IEEE Trans. Cogn. Commun. Netw.*, early access, 2025, doi: 10.1109/TCCN.2025.3613539. Also available as arXiv preprint arXiv:2504.19555.