Visibility Region Exploitation for PHY Authentication in XL-MIMO Systems

Senanur Demirci, Liza Afeef, and Hüseyin Arslan, *Fellow, IEEE*

***Abstract*—Wireless networks are open to identity spoofing attacks because of their broadcast nature, emphasizing the need for strong security. Physical layer authentication (PLA) is a crucial strategy for securing wireless networks against such threats. Extra-large multiple-input multiple-output (XL-MIMO) technology, with its unique visibility region (VR) concept due to the near-field effect, offers a promising way to enhance network performance. This letter proposes a PLA approach using VR to create unique and robust signatures from the power and beamspace domain of XL-MIMO. Simulation results confirm the effectiveness of the proposed method in detecting attacks with high accuracy and low false alarm rates.**

***Index Terms*—Extra-large MIMO (XL-MIMO), beamspace domain, physical layer authentication (PLA), visibility region (VR), spoofing attack.**

I. Introduction

MASSIVE multiple-input multiple-output (MIMO) is a key technology in fifth-generation (5G) and beyond, especially at high-frequency bands, where it maximizes system gain and enables simultaneous service to many terminals using large antenna arrays [1]. This has led to new deployment strategies that integrate massive arrays into large-scale infrastructures such as city walls, airports, malls, and stadiums [2]. As MIMO evolves into extra-large (XL)-MIMO, the traditional assumption of spatial channel stationarity no longer applies. The extensive size of XL-MIMO arrays leads to non-stationarities in the wireless channel, with each antenna element experiences varying power and phase due to the near-field effect, which result in spherical wavefront (SW) rather than planar ones. Moreover, these near-field effects introduce the concept of visibility region (VR) [3], where different elements of the array experience distinct channel responses. Unlike conventional massive MIMO, in XL-MIMO, each terminal or scatterer interacts with only a portion of the array, further complicating channel behavior. These unique characteristics of XL-MIMO systems pose several practical challenges. As array sizes increase, so too do the demands on hardware complexity, signal processing, and energy efficiency. Moreover, the evolving nature of the channel in such large systems can introduce additional vulnerabilities, particularly with respect to maintaining system security.

Received 21 September 2024; accepted 23 October 2024. Date of publication 28 October 2024; date of current version 10 January 2025. This work was supported in part by Scientific and Technological Research Council of Turkey (TUBITAK) under Grant 123E226. The associate editor coordinating the review of this article and approving it for publication was X. Hu. *(Corresponding author: Liza Afeef.)*

The authors are with the School of Engineering and Natural Science, Istanbul Medipol University, 34810 Istanbul, Türkey (e-mail: senanur.demirci@medipol.edu.tr; liza.shehab@std.medipol.edu.tr; huseyinarslan@medipol.edu.tr).

Digital Object Identifier 10.1109/LWC.2024.3486773

Recent advancements have positioned physical layer security (PLS) as a critical concern in wireless networks, due to the vulnerability of the open wireless medium to impersonation attacks. In particular, authentication plays a crucial role in ensuring secure communications by verifying the identity of all parties involved.

As massive MIMO systems grow more complex, the demand for adaptable and cost-effective authentication methods capable of preventing impersonation attacks while accurately validating legitimate transmitters is increasing. In response to these challenges, physical layer authentication (PLA) techniques have recently gained attention as a promising alternative to traditional cryptography-based methods. By leveraging the inherent properties of the physical layer, PLA offers a more secure and efficient approach to authentication, particularly in the dynamic and complex environments introduced by XL-MIMO. Extensive research has been conducted on PLA techniques for MIMO and massive MIMO systems [4], [5], [6], highlighting their potential to enhance security. In XL-MIMO systems, the PLS concerns have been explored extensively in the literature. For instance, studies such as [7], [8], [9] investigate the impact of SW models in near-field channels, proposing a secure transmission framework where beam focusing at the base station (BS) is used to transmit confidential information to a legitimate user, even in the presence of an eavesdropper positioned between the user and the BS. Furthermore, the work in [10] expands on PLS schemes to secure wideband communications. However, it is important to note that the variations in the channel across the XL array, due to both SW and VR, remains unexplored in the context of PLA.

In this letter, to address the existing gaps in the aforementioned literature, a novel PLA approach for XL-MIMO systems is proposed by investigating the near-field XL-MIMO channel characteristics. The contributions of the work are summarized as:

- The VR-based propagation condition is studied and exploited to provide a novel PLA approach in the XL-MIMO networks. This letter is considered the first in the security field that leverages the VR concept to enhance authentication performance at the physical layer level.
- The VR features utilized in the proposed scheme are extracted from both the power and beamspace domains of the XL-MIMO channel. By identifying the VR characteristics in the system, we formulate VR-based signatures in which the authentication process is robust to spoofing attacks. Two types of signatures are proposed for each identified VR based on birth and death VR points, size of the VR, number of antenna elements within VR that are overlapped with other VRs, and the number of the non-overlapped antenna elements in the given VR.

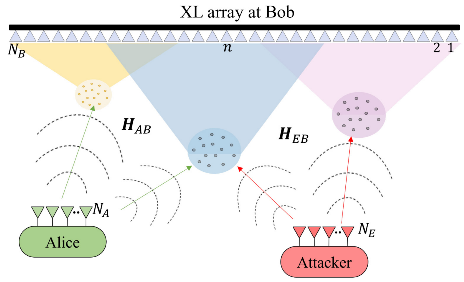

Fig. 1. The illustration of the system model.

- Through simulation analysis, the efficiency of the proposed VR-based signature in the PLA framework is evaluated under various sparsity levels and attacker's positions in terms of probability of detection (PD) and probability of false alarm (PFA).

II. System Model

Consider a 5G new radio (NR) network in uplink scenario comprising three nodes: Alice, a legitimate transmitting node with a MIMO array of N_A antenna elements, Bob, a legitimate receiving node with an XL-MIMO array of N_B antenna elements, and an attacker with N_E antenna elements. All nodes employ a uniform linear array (ULA) configuration, as illustrated in Fig. 1. Within this network, Alice initiates access as the legitimate transmitter, Bob serves as the intended legitimate receiver tasked with authenticating Alice, and the attacker aims to impersonate Alice's signal by transmitting to Bob. PLA process must enable Bob to accept messages from Alice as legitimate while rejecting those from the attacker. To achieve this, a unique signature based on XL-MIMO channel characteristics is developed in this letter for the authentication process.

A. XL-MIMO Channel Model

In the XL-MIMO systems with high frequency bands, most of the signals are propagated within the near-field region of the XL array of Bob node which reflected directly on the steering vector design. Unlike the far-field steering vector, the near-field steering vector design is angle and distance dependent in which it is obtained as

$$\mathbf{a}(\theta, \tilde{r}) = \frac{1}{\sqrt{N}}\left[e^{-j\frac{2\pi}{\lambda}(r_1-\tilde{r})}, \ldots, e^{-j\frac{2\pi}{\lambda}(r_N-\tilde{r})}\right]^T, \quad (1)$$

where λ is the signal wavelength, θ is steering direction, $N \in \{N_A, N_B, N_E\}$, and $r_n = \sqrt{(\tilde{r})^2 + (n-1)^2 d^2 - 2\tilde{r}(n-1)d\sin(\theta)}$ represents the distance between the cluster and the n-th antenna element by taking the distance $\tilde{r}$ (the distance between the first antenna element and the cluster) as a reference point where d represents the inter-element spacing. Besides, the variation of power level over antenna elements at XL array of Bob is observed due to the spatial non-stationary effect in the near-field propagation which introduces the VR concept. Assuming L_X clusters in the environment, the VR of l-th cluster of the XL array can be represented as

$$\boldsymbol{u}_l = \left[u_{l,1}, u_{l,2}, \ldots, u_{l,N_B}\right]^T, \quad (2)$$

where $u_{l,n} = 1$ indicates that the l-th cluster can see antenna n and $u_{l,n} = 0$ indicates the opposite. Based on that, the channel between node X and Bob[1] is modeled as

$$\mathbf{H}_{XB} = \sum_{l=1}^{L_X} \alpha_l \, \mathbf{a}\left(\theta_B^l, \tilde{r}_B^l\right) \odot \boldsymbol{u}_l \, \mathbf{a}^H\left(\theta_X^l, \tilde{r}_X^l\right), \quad (3)$$

where α_l is the complex channel gain of cluster l, θ_B is the angle of arrival (AoA) at Bob node, θ_X is the angle of departure (AoD) at node X, and $\odot$ means the Hadamard product operator.

B. Clusters Evolution

As time progresses, clusters in the non-stationary XL-MIMO channel evolve through a birth-death process, categorizing them into two groups: surviving clusters and newly generated clusters [11]. Surviving clusters undergo evolution, resulting in changes to their corresponding VR positions on the XL array. During this evolution, disappearing clusters are removed from all sets, while newly generated clusters are added to the appropriate cluster sets. The survivability of each cluster at time $t + \Delta t$ is determined by the survival probability P_{sv}, which is calculated as [12]

$$P_{sv} = \exp\left(\frac{-\Lambda_R \partial_{L_x} ||v_{L_x}|| \Delta t}{D_{sp}^S}\right), \quad (4)$$

where Λ_R denotes the recombination rate, and the parameters ∂_{L_x} and v_{L_x} introduce fluctuations of clusters. The moving clusters with mean velocity v_{Lx} comprise a specific percentage ∂_{L_x} of clusters. D_{sp}^S denotes the scenario–dependent coefficient that characterizes the space correlation factor [13]. If a cluster survives, certain parameters such as its mean power and angular parameters are updated according to the first-order Gauss-Markov model given by [14]

$$C_{L_x}(t + \Delta t) = \rho C_{L_x}(t) + \xi(t), \quad (5)$$

where $C_{L_x}(t)$ represents the parameters of the surviving cluster at time t, ρ is a correlation coefficient that determines the degree of correlation between the previous and current cluster parameters states, and $\xi(t)$ is a random variable representing environmental randomness, which follows a Gaussian distribution $\xi(t) \sim \mathbb{CN}(0, \sigma^2)$. The variance σ^2 indicates the degree of cluster parameters variation over time; a low σ value corresponds to a static environment, while a high σ value corresponds to a dynamic environment. Note that the evolution of the clusters over the XL array affects the location and extraction process of the VRs.

III. Proposed Framework Design

A. Power-Based VR Characteristics Extraction

The conventional method for detecting the VRs of a single node (assuming the total number of VRs for the X node is L_X) involves measuring the received power across the XL array from the signal transmitted by the given node. For the l-th VR, its size is defined by the number of array elements it contains, denoted as N_l, where $l = 1, 2, \ldots, L_X$. Adjacent array elements with power above a predefined threshold P_{thr} are considered to constitute a VR, while non-adjacent groups of array elements with received power above the threshold

[1] Here, the X node represents either Alice or the attacker node (i.e., $X \in \{A, E\}$)

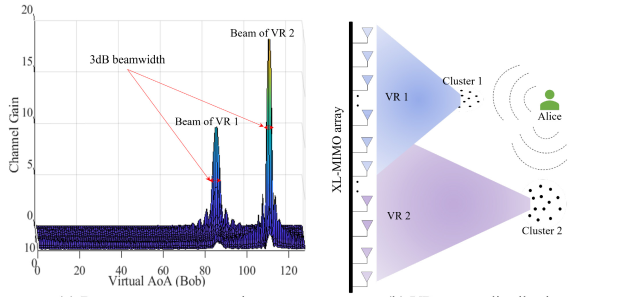

Fig. 2. An example of XL-MIMO system with two overlapped VRs representation in the power and beamspace domains. Here, we assume Alice has 16 antenna elements while Bob (XL array) has 128 antennas operating at 2.5 GHz frequency.

P_{thr} are considered non-overlapping VRs. The number of non-overlapping VRs detected is denoted by L_X^{NOP}, with $L_X^{\text{NOP}} \leq L_X$. For each identified VR, its birth and death points are also determined. The birth point n_b^l of the l-th VR is defined as the antenna index of the array where the VR begins, while the death point n_d^l is the antenna index where the VR ends. However, it is important to note that if the received signal power forms more than one VR, this approach can only identify the presence of multiple VRs when these VRs are non-overlapping. In case where VRs are partially or fully overlapping, detection can be achieved through the beamspace representation of the MIMO channel, as discussed herein.

B. Beamspace-Based VR Characteristics Extraction

The beamspace representation of MIMO channels reduces dimensionality, improves interference management, and simplifies channel estimation, making it robust to channel variability and effective for optimizing MIMO performance. The spatial and beamspace domains are related via the spatial discrete Fourier transform (DFT) represented by the unitary matrix $\mathbf{U}$ [15]. In XL-MIMO networks, the distance- and angle-dependent characteristics of near-field propagation affect the beamspace channel representation. As presented in [16], for a given beam in the beamspace representation, the beamwidth determines the VR size on the XL array since the beamwidth is inversely proportional to the antenna array aperture size. For example, the size of the l-th VR is given by

$$N_l = \frac{0.886\lambda}{\Omega_{3dB}\, d \sin\left(\theta^l\right)}, \tag{6}$$

where $\Omega_{3dB} = 2|\theta^l - \theta_{3dB}^l|$ is the 3 dB beamwidth of the l-th beam with θ_{3dB}^l is the angle at which the gain is 3 dB below the maximum.

According to the estimated channel between the X node and Bob (the XL-MIMO node), the maximum number of VRs equals the number of beams in the beamspace domain. The angular coordinates (virtual AoDs and AoAs) of each beam indicate the angular locations of environmental clusters relative to the X and Bob nodes. It is worth noting that any change in these beams provide insights into VR distribution on the XL array.

C. Proposed VR-Based Signature

By merging VR characteristics from both domains, a unique signature can be formed, which serves as the foundation for a novel PLA scheme. An example illustrating the VRs in these two domains is shown in Fig. 2. Using the following characteristics from the l-th VR: birth point (n_b^l), death point (n_d^l), the total l-th VR size N_l, the overlapped size N_l^{OP}, and the non-overlapped size N_l^{NOP}, the proposed signature can be built as follows:

- Given (n_b^l) and (n_d^l) of the l-th VR, VR size-based signature is derived as
$$s_1^l = \frac{n_b^l}{n_d^l}. \tag{7}$$
This signature captures the spatial extend of a given VR by measuring how far it extends from its beginning to its end. This signature helps in authenticating users by their unique VR footprint, assuming that each legitimate user's VR has a distinct size that can be reliably measured.
- Given N_l^{OP} and N_l^{NOP} of the l-th VR, the VR overlap-based signature is derived as
$$s_2^l = \frac{N_l^{OP}}{N_l}. \tag{8}$$
This signature addresses the interaction between multiple VRs in the environment. It calculates the extent to which other VRs overlap with a specific VR. The overlap-based signature provides additional context comparing to the size-based signature by accounting for environmental interactions, which is useful in complex scenarios with multiple overlapping VRs.
- Arrange these two signatures into one vector as $\mathbf{s}^l = [s_1^l, s_2^l]$.
- Repeat the first three steps for all L_X VRs.
- Sort the $\mathbf{s}^l$ vectors based on based on the value of the non-overlapped size of the VR in decent order.
- Put the sorted vectors into one combined vector as $\mathbf{s} = [\mathbf{s}^1, \mathbf{s}^2, \cdot, \mathbf{s}^{L_X}]^T$ where $\mathbf{s}$ is the proposed VR-based signature.
- Store the proposed VR-based signature vector $\mathbf{s}$ in the Bob node's database as $\mathbf{s}(t_o)$.

D. Detection Model

The creation and storage of the proposed VR-based signature occur at time slot t_o, after rejecting any signal not sent by Alice. Security during this time slot is ensured through upper-layer security mechanisms, such as encryption, allowing Bob to extract only Alice's VR-based features. In the subsequent time slot t_1, Bob detects and extracts VR characteristics from the received signal, whether sent by Alice or other nodes. The proposed signature is then built from these detected characteristics and compared to the stored signature to determine if the signal is from a legitimate or illegitimate node. The decision is made through a binary hypothesis test to verify the signal's identity:

$$\begin{aligned} K_0 &: \eta_L = ||\mathbf{s}(t_1) - \mathbf{s}(t_o)|| \leq \eta_{th}, \\ K_1 &: \eta_L = ||\mathbf{s}(t_1) - \mathbf{s}(t_o)|| > \eta_{th}, \end{aligned} \tag{9}$$

where $\mathbf{s}(t_1)$ is the proposed VR-based signature extracted at timeslot t_1 and η_{th} is a threshold used to separate between K_0 and K_1. Hypothesis K_0 indicates the signal was sent by the legitimate node, Alice, while K_1 suggests it was sent by an illegitimate node (potentially an attacker).

Algorithm 1: The VR-Based Proposed PLA Scheme

⋆ **Timeslot** t_o:
Input: Received signal power, estimated $\mathbf{H}_{AB}$.
1 **Extract** the non-overlapped VRs characteristics from received signal power over the XL array.
2 **Convert** the estimated channel $\mathbf{H}_{AB}$ into beamspace domain.
3 **Extract** the VRs characteristics from the beamspace domain representation.
4 **for** $l = 1, 2, \ldots, L_X$ **do**
5 Calculate the first proposed signature using (7).
6 Calculate the second proposed signature using (6) and (8).
7 Set the l-th VR signature as $\mathbf{s}^l = [s_1^l, s_2^l]$.
8 **Sort** the $\mathbf{s}^l$ signatures based on their non-overlapped size in decent order.
9 **Build** the VR-based proposed signature as $\mathbf{s} = [\mathbf{s}^1, \mathbf{s}^2, \cdots, \mathbf{s}^{L_X}]^T$.
10 **Store** the VR-based proposed signature in the database of Bob as $\mathbf{s}(t_o)$.
⋆ **Timeslot** t_1:
Input: Received signal power, estimated $\mathbf{H}_{XB}$.
11 **Repeat** the steps from 1 to 9 to get the signature vector $\mathbf{s}(t_1)$.
12 **Apply** the binary hypothesis test given in (9).
13 **if** $\eta_L \leq \eta_{th}$ **then**
14 Bob authenticates Alice successfully
15 **else**
16 Bob detects an attacker

The proposed VR-based PLA mechanism is summarized in Algorithm 1. In this letter, within the authentication process (training and verification), we assume that the clusters in the Alice-Bob link have survived and evolved over time. Their parameters are updated as given in (5).

E. PD and PFA Analysis

To analyze the authentication performance, PD and PFA are defined based on the developed binary hypothesis testing given in (9). The PD is defined as the probability of correctly detecting a forged signal when Alice did not transmit, i.e., $P_{pd} = Pr(\eta_L > \eta_{th}|K_1)$. In contrast, PFA is defined as the probability of falsely detecting an attacker when Alice is transmitted, i.e., $P_{fa} = Pr(\eta_L > \eta_{th}|K_0)$. By observing the empirical distribution of η_L, it is noticed that the distribution of K_0 follows log logistic distribution by utilizing the fitting tools introduced in [17], $K_0 \sim$ log logistic(λ, κ), while the distribution of K_1 follows normal distribution, $K_1 \sim \mathcal{N}(\mu, \Sigma^2)$, as shown in Fig. 3. In particular, PFA is mathematically formulated as

$$P_{fa} = Pr(\eta_L > \eta_{th}|K_0), \\ = \int_{\eta_{th}}^{\infty} \frac{\lambda\kappa(\lambda\eta)^{\kappa-1}}{(1+(\lambda\eta)^{\kappa})^2} d\eta = \frac{1}{1+(\lambda\eta_{th})^{\kappa}}. \quad (10)$$

For a given PFA value, η_{th} is obtained as $\eta_{th} = (1/P_{fa} - 1)^{1/\kappa}/\lambda$ to separate hypothesis K_0 and hypothesis K_1, and hence the PD performance of the proposed scheme is captured.

IV. Numerical Results

In this section, the authentication performance of our proposed method is evaluated in terms of PD and PFA. The proposed VR signature is compared with both conventional beamspace channel H_b signature and spatial MIMO channel H signature [18].

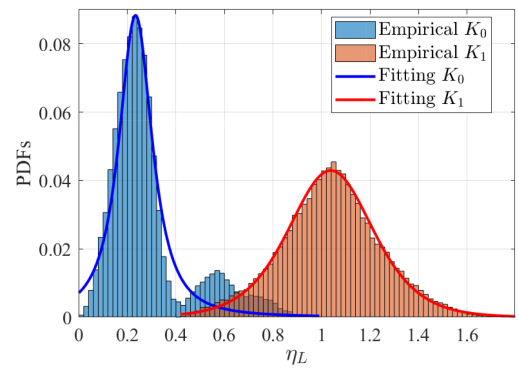

Fig. 3. The distribution of η_L for the normal case K_0 and attacker case K_1 assuming different VRs sizes with $L_X = 3$.

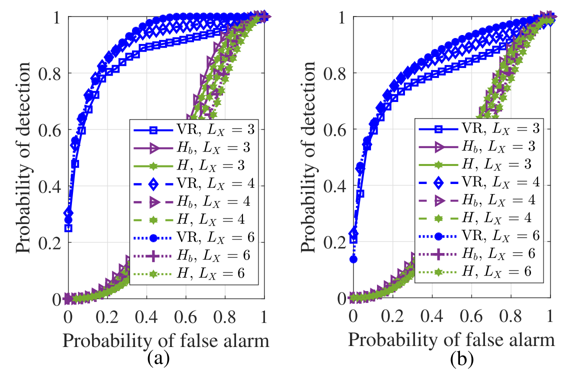

Fig. 4. ROC performance in (a) static and (b) dynamic environments with $N_A = N_E = 16$ and $N_B = 256$.

Figure 4 presents the receiver operating characteristic (ROC) performance of our proposed approach, illustrating the relationship between PD and PFA for authentication under varying channel conditions. In this analysis, we assume equal VR sizes for Alice and the attacker, with each comprising 50 elements. In the static environment depicted in Fig. 4(a), where cluster locations change slowly (angular deviation of $\sigma_\theta^2 = (0.25°)^2$ and a cluster size of 20 antenna elements), authentication performance improves as the number of clusters increases. By contrast, dynamic channels, shown in Fig. 4(b), exhibit more rapid variations with an angular change of $\sigma_\theta^2 = (0.5°)^2$ and a larger cluster size of 30 elements. As shown in Fig. 4, for both static and dynamic scenarios, the proposed VR signature consistently outperforms conventional MIMO channel signatures, H and H_b. For instance, at a PFA of 0.6, the VR signature shows an approximately 87% improvement in PD over the conventional signatures in the static environment, and around 70% improvement in the dynamic environment. While the H and H_b signatures may be adequate for network authorization in sparse MIMO settings, they face challenges in maintaining reliable authentication as the XL-MIMO channel becomes nonstationary. This underscores the significance of the proposed VR signature in ensuring robust PLA, particularly in highly dynamic and nonstationary environments. Compared to the performance in static environments, the proposed approach experiences some degradation in dynamic environments due to rapid VR shifts and changing channel characteristics. These variations widen the gap between the detected and stored signatures, increasing the

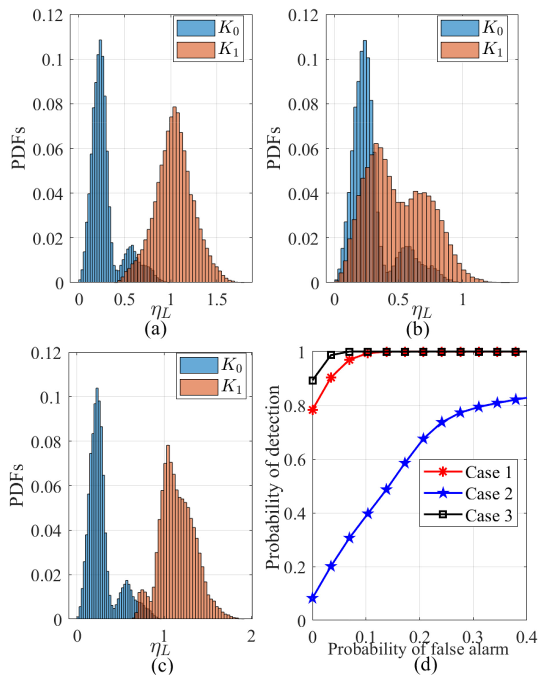

Fig. 5. The PDF performance of (a) case 1, (b) case 2, (c) case 3, and (d) the ROC performance for all cases in a static environment with $L_X = 3$, $N_B = 256$, $N_A = N_E = 16$, and different VR sizes at Bob side where attacker's VRs sizes differ from Bob side.

likelihood of misidentifying the legitimate node. A potential solution, as proposed in our earlier work [19], is to adopt a tracking mechanism that continuously updates the signature database, allowing the system to adapt to the fast-changing XL-MIMO channel. This approach could significantly enhance the system's ability to track rapid VR changes, improving scalability and reliability for real-world deployments in highly dynamic scenarios which is a topic left for future work.

Figure 5 examines the impact of the attacker's location on the proposed PLA performance across three critical locations. In Case 1, the attacker is far from both Alice and Bob, having different clusters from Alice but potentially an equal number of VRs in the worst case. In Case 2, the attacker is close to Alice, with similar VRs visible to both. In Case 3, the attacker is close to Bob, with a limited visible region of the XL array compared to Alice, resulting in fewer VRs for the attacker. The probability density function (PDF) performance of the proposed signature in these scenarios is shown in Figs. 5(a)-(c). We can observe that the legitimate characteristics and illegitimate ones are easily separated in case 3. However, as the attacker gets closer to the Alice channel, the separation capability of the nodes' characteristics declines. The ROC performance is illustrated in Fig. 5(d). As expected, Case 3 performs the best, as the attacker cannot detect or predict the VRs of Alice's channel due to their limited visibility of the XL array.

V. Conclusion

This letter introduces a VR-based PLA method tailored for XL-MIMO systems by leveraging the non-stationarity aspect of the XL array. The proposed approach exploits VR characteristics in both power and beamspace domains, encompassing birth and death VR points, VR size, overlapped size with other VRs, and non-overlapped VR size. A rigorous evaluation of the VR-based PLA approach is conducted, considering performance metrics such as PD and PFA across various attacker locations with respect to the XL array and legitimate node. Leveraging the VR concept in XL-MIMO systems for practical deployment involves addressing challenges of multi-user authentication and adaptability to dynamic environments. Efficient algorithms are needed to manage real-time signal processing and handle the evolving nature of VRs due to user mobility and network changes.

References

[1] X. Gao, F. Tufvesson, and O. Edfors, "Massive MIMO channels—Measurements and models," in *Proc. Asilomar Conf. Signals, Syst. Comput.*, 2013, pp. 280–284.

[2] A. O. Martinez, E. De Carvalho, and J. Ø. Nielsen, "Towards very large aperture massive MIMO: A measurement based study," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, 2014, pp. 281–286.

[3] E. D. Carvalho, A. Ali, A. Amiri, M. Angjelichinoski, and R. W. Heath, "Non-stationarities in extra-large-scale massive MIMO," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 74–80, Aug. 2020.

[4] P. Zhang, T. Taleb, X. Jiang, and B. Wu, "Physical layer authentication for massive MIMO systems with hardware impairments," *IEEE Trans. Wireless Commun.*, vol. 19, no. 3, pp. 1563–1576, Mar. 2020.

[5] W. Li, N. Wang, L. Jiao, and K. Zeng, "Physical layer spoofing attack detection in mmWave massive MIMO 5G networks," *IEEE Access*, vol. 9, pp. 60419–60432, 2021.

[6] L. Afeef, H. M. Furqan, and H. Arslan, "Physical layer authentication scheme in beamspace MIMO systems," *IEEE Commun. Lett.*, vol. 26, no. 7, pp. 1484–1488, Jul. 2022.

[7] 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.

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

[9] 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.

[10] X. Hu 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.

[11] S. Wu, C.-X. Wang, E.-H. M. Aggoune, M. M. Alwakeel, and X. You, "A general 3-D non-stationary 5G wireless channel model," *IEEE Trans. Commun.*, vol. 66, no. 7, pp. 3065–3078, Jul. 2018.

[12] T. Zwick, C. Fischer, D. Didascalou, and W. Wiesbeck, "A stochastic spatial channel model based on wave-propagation modeling," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 1, pp. 6–15, Jan. 2000.

[13] "Study on channel model for frequencies from 0.5 to 100 GHz," 3GPP, Sophia Antipolis, France, Rep. TR 38.901, Sep. 2017.

[14] V. Va, H. Vikalo, and R. W. Heath, "Beam tracking for mobile millimeter wave communication systems," in *Proc. IEEE GlobalSIP*, 2016, pp. 743–747.

[15] A. M. Sayeed and N. Behdad, "Continuous aperture phased MIMO: A new architecture for optimum line-of-sight links," in *Proc. IEEE ISAP*, 2011, pp. 293–296.

[16] A. B. Kihero, L. Afeef, and H. Arslan, "A method for identifying visibility regions in ELAA-based wireless networks," Türk Patent 001 049, May 2024.

[17] J. M. Hamamreh, E. Basar, and H. Arslan, "OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services," *IEEE Access*, vol. 5, pp. 25863–25875, 2017.

[18] J. Tang, A. Xu, Y. Jiang, Y. Zhang, H. Wen, and T. Zhang, "MmWave MIMO physical layer authentication by using channel sparsity," in *Proc. IEEE ICAIIS*, 2020, pp. 221–224.

[19] L. Afeef, H. M. Furqan, and H. Arslan, "Robust tracking-based PHY-authentication in mmWave MIMO systems," *IEEE Trans. Inf. Forensics Security*, to be published, doi: 10.1109/TIFS.2024.3488362.