University of Essex

Research Repository

An Intelligent RIS-Assisted Hybrid Communication-Localization Framework for Physical-Layer Authentication in Wireless Networks

Accepted for publication in Internet of Things

Research Repository link: https://repository.essex.ac.uk/43921/

Please note:

Changes made as a result of publishing processes such as copy-editing, formatting and page numbers may not be reflected in this version. For the definitive version of this publication, please refer to the published source. You are advised to consult the published version if you wish to cite this paper.
https://doi.org/10.1016/j.iot.2026.102112

www.essex.ac.uk

University of Essex

An Intelligent RIS-Assisted Hybrid Communication-Localization Framework for Physical-Layer Authentication in Wireless Networks

Mahmoud A. Shawky[a], Walid M. Saad[b], Ahmed G. Abdellatif[c], Insaf Ullah[a], Danish Mehmood Mughald[d], Ahmad Almogren[e,*] and Syed Tariq Shah[a,*]

[a]School of Computer Science and Electronic Engineering, University of Essex, Colchester, UK
[b]The Egyptian Technical Research and Development Centre, Cairo, 11618, Egypt
[c]Faculty of Computers and Information Systems, Egyptian Chinese University, Cairo, 11765, Egypt
[d] Department of Electrical and Computer Engineering, Sungkyunkwan University, 16419, Suwon-si, Republic of Korea
[e]Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh, 11633, Saudi Arabia

ARTICLE INFO

Keywords:
Reconfigurable Intelligent Surface (RIS)
Physical-Layer Security
Industrial IoT
Machine Learning
Device Authentication
Signal Processing

ABSTRACT

As industrial internet-of-things (IIoT) networks grow, the need for reliable communication, accurate positioning, and strong security is essential. Traditional security methods, like public key infrastructure (PKI), are effective but can be vulnerable to denial-of-service (DoS) attacks due to their heavy computational and communication loads. This paper introduces a dual-mode reconfigurable intelligent surface (RIS) system that combines secure communication with physical position verification. The system uses two modes: a communication mode that uses a 64×64 RIS elements to improve signal strength, and a localization mode that divides the surface into four sections to create unique location fingerprints. By combining signal strength and phase responses with a simple machine learning model, we create a reliable map for verifying device locations. The proposed protocol links digital identities to these physical fingerprints, allowing the system to track moving devices securely without constant re-authentication. Experimental tests on a real hardware setup show that dividing the RIS into sections significantly improves tracking accuracy compared to standard methods. The system achieves over 99% accuracy in complex indoor settings, offering a practical and secure solution for industrial applications without needing extra expensive infrastructure.

1. Introduction

Industrial internet-of-things (IIoT) applications, such as autonomous guided vehicles, robot navigation, asset tracking, and safety zoning, demand wireless infrastructure that delivers both reliable connectivity and precise, timely device localization. Indoor industrial settings pose significant challenges for these requirements due to building penetration losses, metallic structures, dense machinery, and frequent reconfiguration, leading to severe multipath, persistent shadowing, and dynamic propagation conditions. These factors make dense anchor deployment, frequent site re-surveys, or dedicated sensing infrastructure costly or impractical, while simultaneously motivating solutions that enhance link quality and enable location awareness using the existing wireless infrastructure [1], [2].

Traditionally, communication and localization have been developed and optimized as separate problems. Classical positioning approaches, including time-based ranging, angle-of-arrival estimation, and radio fingerprinting, usually assume a static propagation environment or abundant anchors and synchronized reference signals [3], [4], [5]. Communication-centric designs instead prioritize metrics such as signal-to-noise ratio (SNR), throughput, and latency, and do not shape the propagation environment for localization observability. In practice, the competing objectives and constraints of industrial deployments, such as limited infrastructure budget, device mobility, and frequent layout changes, make a single-purpose strategy insufficient. Many IIoT scenarios need a practical, integrative approach that can enhance communication performance where needed and produce location-dependent observables for trustworthy position verification, without large additional hardware or operational overhead.

Reconfigurable intelligent surfaces (RIS) have emerged as a promising enabler for integrated designs. By reflecting and phase-shifting incident signals, RIS panels provide a low-power, low-profile way to modify the local propagation field, offering gains in coverage, interference management, and received SNR [6]. For positioning, programmable surfaces can structure multipath and produce controllable, location-dependent channel signatures that augment conventional sensing and fingerprinting [7, 8]. These features make RIS attractive for IIoT deployments where retrofitting active radios is costly, but placing passive, reconfigurable elements is feasible. However, the RIS design space is multidimensional. Unit-cell quantization, surface partitioning strategies, and control protocols all influence trade-offs among coverage, power gain, and the informativeness of received channel observations for localization. Careful system design is needed to navigate these trade-offs, particularly because the physical mechanisms that maximize SNR for communication can reduce the spatial diversity required for accurate localization.

*Corresponding authors.
mahmoud.a.shawky-ahmed@essex.ac.uk (M.A. Shawky); walid@sce.carleton.ca (W.M. Saad); Ahmed.Gamal@ecu.edu.eg (A.G. Abdellatif); insaf.ullah@essex.ac.uk (I. Ullah); danish@skku.edu (D.M. Mughald); ahalmogren@ksu.edu.sa (A. Almogren); syed.shah@essex.ac.uk (S.T. Shah)
ORCID(s): 0000-0003-3393-8460 (M.A. Shawky)

Beyond positioning accuracy and communication reliability, industrial IIoT systems have strict identity and trust requirements. Safety-critical or access-controlled operations often require not only device authentication, but also proof that the device is physically where it claims [9]. While conventional cryptographic frameworks, such as public key infrastructure (PKI) utilizing elliptic curve cryptography (ECC), offer robust guarantees for identity and message integrity, their high computational and communication overhead can introduce vulnerabilities to denial-of-service (DoS) attacks [10]. To address this issue, transmitter localization serves as a complementary security layer, enabling the system to identify and filter malicious requests originating from suspicious or redundant physical locations. Furthermore, by analyzing the spatial consistency of moving nodes, the system can implement a "delegation of trustworthiness," maintaining a node's verified status as it transitions between adjacent positions. This motivates architectures that combine cryptographic identity proofs with physical-layer information, such as channel measurements or engineered propagation patterns, to provide a location-dependent fingerprint that is hard to replicate remotely [6]. This integrating raises new design questions: how to generate robust, discriminative physical fingerprints under realistic indoor multipath, how to bind those fingerprints to cryptographic identities, and how to verify them without degrading communication performance.

Despite progress in RIS-aided communications, RIS-enabled sensing, physical-layer authentication, and classical fingerprinting, there is limited prior work integrating these components into an end-to-end, experimentally validated architecture for industrial constraints [11, 12, 13]. Communication-focused RIS studies often optimize for link quality without considering localization observability or identity verification. Physical-layer authentication research usually assumes passive channel observations without active control of the propagation environment. Many localization studies remain theoretical or rely on dense infrastructure that is impractical for IIoT retrofits. As a result, an integrated system that addresses communication reliability, location verification, and cryptographic identity binding, while being feasible on realistic hardware, remains an open challenge.

In this paper, we address that challenge by proposing a practical dual-purpose RIS architecture and an end-to-end protocol that combines controlled RIS probing, lightweight machine learning, and cryptographic binding to support both communication and location-based identity verification. The architecture operates in two modes: a communication mode that configures the full RIS surface to enhance link SNR when high throughput or robustness is needed, and a localization mode that partitions the surface into four quadrants and reconfigures each independently to produce location-dependent channel observations for training and running a classifier for position verification. These modes are managed within a protocol that couples a standard cryptographic handshake (PKI/ECC) with a physical-layer verification step, so that an asserted identity is accepted only when the device's cryptographic claim and the verified physical fingerprint match. A key feature of the protocol is the smooth transition phase, which tracks device mobility between verified positions without requiring full re-authentication at every step, reducing computational overhead during continuous operation. In general, the main contributions of this paper are summarized as follows:

1. We present a dual-mode RIS system design that alternates between global RIS configurations for communication and quadrant-partitioned RIS probing for localization, together with practical optimization algorithms for both modes based on Hadamard codebook search (see Algorithm 1 and Algorithm 2).
2. We develop an offline manifold construction and lightweight ML pipeline that fuses received signal strength (RSS) and channel phase response (CPR) features from RIS quadrants to form robust spatial fingerprints, and we train a classifier for coordinate verification that achieves near-perfect accuracy in experimental evaluation.
3. We design an integrated authentication protocol that binds PKI/ECC identity assertions to physical-layer verification through RIS-probed channel estimates, augmenting cryptographic identity with location-dependent evidence; we detail the verifier's decision rule and analyze resistance to impersonation, modification, and replay attacks under an explicit threat model.
4. We implement the complete system on a laboratory testbed with a 64×64 element RIS panel and software-defined radio front-ends, and we provide an experimental evaluation that quantifies the fundamental tradeoff between communication gain and localization observability, demonstrating that quadrant-based partitioning substantially outperforms global optimization for localization tasks.

The experimental validation reported here uses dedicated RIS hardware and software-defined radios in a controlled indoor environment with four reference positions (see Section 4 for hardware and measurement details). The results demonstrate the practicality of the proposed approach under the tested scenarios. Extending the evaluations to denser spatial grids, multiple simultaneous mobile devices, and longer-term environmental variability are important directions for future work and are discussed in Section 5.

The remainder of this paper is organized as follows. Section 2 reviews related literature to highlight existing design gaps, followed by the formulation of the system model and a detailed breakdown of the dual-mode RIS control and authentication protocol. Section 3 presents the experimental setup, including testbed configuration, dataset construction, and an analysis of the ML-driven empirical results. Finally, Section 4 addresses current limitations and suggests avenues for future research, with concluding remarks provided in Section 5.

2. Background and Preliminaries

This section reviews the current state-of-the-art and discusses the preliminary functions used in this study.

2.1. Overview of the current state-of-the-art

In [14], the authors proposed a rigorous theoretical analysis, as they derived fundamental position and orientation error bounds for RIS-assisted localization using the Fisher information matrix (FIM), providing algorithm-independent insights into the best achievable accuracy. That analysis uniquely addresses both position and orientation estimation and highlights the critical role of near-field RIS operation, offering clear design guidelines regarding RIS size, placement, and geometry for future 6G localization systems. However, the work is limited by its idealized assumptions, as it does not consider practical hardware impairments, control quantization, mobility, or multi-user scenarios, nor does it propose concrete estimation algorithms to approach the derived bounds. In [15], the authors combined the RIS technology with orthogonal frequency-division multiplexing (OFDM) to develop an improved resource allocation strategy for multiple users in a far-field scenario. Although this method allows RIS-enhanced networks to operate efficiently while avoiding complex and costly channel-estimation procedures, the authors acknowledged that the performance of the proposed technique can be influenced by mobility, multi-path propagation, and localization precision, thereby highlighting the need for further research. The authors in [16] provide a RIS-assisted time difference of arrival (TDOA) localization approach that can significantly improve positioning accuracy in non-line-of-sight (NLOS) scenario and challenging propagation environments by introducing controllable reflected paths, while remaining compatible with existing 5G infrastructure and avoiding the need for major hardware changes at user end.

Building on these foundational works, recent research has moved toward integrating security and localization through data-driven and cross-layer frameworks. In [8], a "coded environment" concept is introduced where RIS panels are used to create unique spatial signatures for data-driven indoor localization, demonstrating that passive surfaces can effectively replace complex active hardware for spatial awareness. This shift toward advanced modeling is further refined in [17], where the authors utilize Kolmogorov-Arnold Networks (KAN) to extract intricate spatial features from RIS-enhanced channels, achieving superior localization accuracy with fewer parameters than traditional neural networks. Beyond positioning, the security potential of RIS has been explored in [18], which demonstrates how RIS can facilitate physical-layer secret key generation to maintain secure vehicular communication even under DoS attacks. This security paradigm is extended to mobility management in [19], where a lightweight handover authentication protocol is proposed to ensure seamless and secure transitions in RIS-aided vehicular networks. Finally, [20] integrates these concepts into a comprehensive cross-layer authentication framework that combines physical-layer channel characteristics with upper-layer protocols, offering a robust defense against identity-based threats.

The use of RIS enhances geometric diversity and strengthens TDOA measurements, making the system more robust than conventional 5G TDOA methods. However, the approach relies on precise time synchronization between base stations and accurate RIS phase control, which can be challenging in practical deployments. Additionally, the algorithm may suffer from increased system complexity, sensitivity to channel estimation errors, and limited scalability in dense multi-user scenarios. In [21], the authors propose using RIS not only as a passive reflector but as an active sensing tool. The RIS can adaptively change its reflection patterns over multiple stages. This enables the system to sense multipath propagation more effectively and extract useful localization information. Instead of fixing the RIS pattern, the authors train a machine-learning controller long short-term memory (LSTM) neural network which is used to generate RIS reflection patterns over time. The LSTM learns from past pilot signals to choose the next RIS configuration. It is very suitable for indoor and dense environments. The main drawbacks of this paper are that it depends extensively on a data-driven learning approach, which requires training an LSTM network and may suffer from generalization issues when the environment changes or differs from the training data. The method increases system complexity because it needs adaptive RIS control and real-time inference, which can be challenging for low-power or large-scale RIS deployments. In addition, the paper provides limited theoretical analysis making rigorous comparison with classical localization methods difficult. Finally, the results are mainly based on simulations, with no experimental or hardware validation, which leaves the practical feasibility of the proposed approach insufficiently demonstrated.

In intelligent radio systems, programmable metasurfaces play an important role in enhancing physical-layer security through defensive and adversarial operations. In addition, reconfigurable metasurfaces can be manipulated by intelligent attackers to conduct covert passive eavesdropping or active deception attacks [22]. On the other hand, metasurfaces employing chaotic modulation enable simple and secure encryption at the physical layer without requiring complex digital decryption [23]. Accordingly, the proposed model employs RIS technology not only to improve the channel conditions but also as a spatial verifier. By dynamically configuring the RIS sub-surface quadrants, the system creates a spatially unclonable multipath fingerprinting vector. Since it is infeasible for an adversary to physically occupy the precise location of the legitimate receiver, the spoofed/replayed message would exhibit a non-correlated physical signature, thereby enabling early rejection of such attacks at the physical layer itself. This is the key idea behind the study. For simplicity and clarity, the notations used in the proposed method are presented in Table 1.

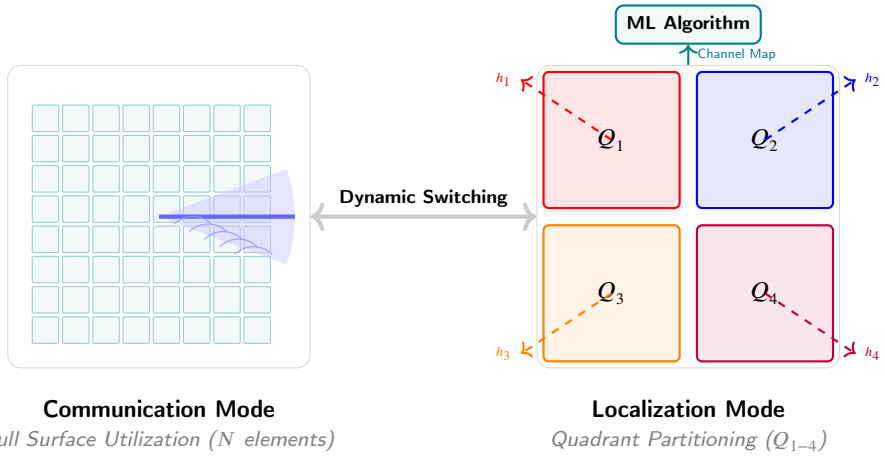


Figure 1: Graphical Dual-mode RIS operation. The left panel shows full surface configuration for constructive interference, while the right panel illustrates quadrant partitioning for independent probing and ML-based localization.

Table 1
Summary of key notations and symbols.

Symbol	Description
Network & Architectural Parameters	
J	Total APs, AP_j, $\forall j \in \{1, \ldots, J\}$
I	Total IoT devices, D_i, $\forall i \in \{1, \ldots, I\}$
L	Total grid positions, P_l, $\forall l \in \{1, \ldots, L\}$
N	Total RIS elements, $N = N_x \times N_y$
N_x, N_y	RIS elements along horizontal/vertical axes
Q_r	RIS quadrant, $r \in \{1, 2, 3, 4\}$
x	Grid resolution/inter-spacing (m)
Channel & Signal Metrics	
SNR	Signal-to-noise ratio
$\mathbf{h}_1, \mathbf{h}_2$	AP–RIS/RIS–device channel vectors
RSS	Received signal strength
CPR	Channel phase response
RIS_l^{opt}	Optimal RIS configuration for P_l
Positioning & Security Terms	
P_l	Ground-truth physical position
$\hat{P}_l$	Estimated position from ML_{Loc}
P'_l	Device-claimed position
ML_{Loc}	ML-based position verification model
PPs	TA-generated public parameters
PKI/ECC	Public key infrastructure/ECC

2.2. System modelling

This section presents the system architecture and provides a detailed description of the proposed method.

2.2.1. System architecture

The system architecture of the proposed method consists of four entities defined as the administrator (Trusted authority; TA), number of J access points $\left(AP_j, \forall j = \{1, \cdots, J\}\right)$, number of I mobile IoT sensors $(D_i, \forall i = \{1, \cdots, I\})$, reconfigurable intelligent surface. The following describes the role of each entity in the network.

1. *Administrator*: The TA oversees all network terminals and has sufficient computational capabilities to enroll and register different entities, ensuring that only authenticated and authorized entities can participate in the network. The TA is responsible for managing, authenticating, and securing the communication link between AP_j and D_i. Additionally, it generates and disseminates the system's public parameters PPs. In the event of suspicious activity or security threats such as a DoS attack, the TA is the only entity authorized to revoke a user's access to the network.
2. *Access points (AP_j)*: AP_j is working as a secure and reliable communication bridge between D_i and the TA, using OFDM communication system. Also, it contains phased array antenna, which is a beam formed towards the RIS. In addition, it may also send probing packets to D_i passing through the RIS for channel estimation and creating a channel map for the working area "area under test". The area under test is divided into a grid of L positions $\left(P_l, \forall l = \{1, \cdots, L\}\right)$ with an inter-spacing distance x per meter. The estimated channel map is used for efficient localization for D_i located in each position P_l. Moreover, it may act as an intermediary relay during the handshake process, relaying authentication messages or credentials between the D_i and the trusted authority. Furthermore, each AP_j maintains a reliable connection with the smart controller of the RIS located within its communication region, enabling AP_j to dynamically manage and adjust the RIS configuration.
3. *IoT sensors D_i*: physical devices that collect and generate data from the industrial environment e.g. (robot, vacuum cleaner). It also responsible for detecting physical changes and generate data that drives monitoring, control, and decision-making and directly communicate with the AP_j in its communication region. Besides it has on-board bidirectional wireless communication device, which allows D_i to securely communicate with AP_j. Additionally, this OBU is equipped with an indoor localization chip to estimate its position $\hat{P}_l$.

4. *Reconfigurable intelligent surface*: The RIS comprises N $\left(N = N_x \times N_y\right.$, where N_x and N_y are the number of reflectors in the x and y directions) metasurface reflectors strategically deployed to establish robust communication and localization links between AP_j and D_i located in $P_l, \forall l \in \{1, \ldots, L\}$. Accordingly, the RIS operates in two distinct modes: In the communication mode, all N RIS elements are configured to constructively interfere in the direction of the designated device D_i. In the localization mode, the RIS elements are divided into four quadrants $\left(Q_r, \forall r \in \{1, \ldots, 4\}\right)$, with each quadrant independently configured to target D_i located at position P_l. This configuration generates distinct channel estimates for each P_l across the quadrants. The collection of these channel estimates, referred to as the dataset, forms a channel map that facilitates efficient localization through a machine learning algorithm. The system determines the optimal configuration of each quadrant Q_r corresponding to each specific location P_l. This approach significantly enhances the localization accuracy of mobile IoT sensors, particularly in complex industrial environments characterized by low SNRs.

The interaction between these entities and the tiered functional separation of the proposed method is illustrated in Figure 2. The architecture is partitioned into four main operations: administration by the TA, Control by the AP_j, propagation and RIS configuration, and sensor, to facilitate a secure communication pipeline where the TA manages global security parameters, the AP_j executes ML_{Loc} position verification logic, and the RIS dynamically reconfigures the physical environment to optimize either signal strength or localization precision for the mobile IoT sensors.

3. Scheme Modelling

Generally, the scheme consists of two stages: the offline mode and the online mode.

3.0.1. Stage 1: Offline mode

This mode of operation comprises two phases, the communication and localization phases. In each phase, the RIS is configured in different ways defined as follows.

1. *Communication phase*: In this phase, the whole RIS of N elements are configured in away that maximises the SNR of the reflected signal towards the designated user D_i, located in different locations $P_l, \forall l = \{1, \cdots, L\}$ in the area under test, constituting the optimum RIS configuration $RIS_l^{opt}, \forall l = \{1, \cdots, L\}$.
2. *Localization phase*: In this phase, each RIS quadrant Q_r, $\forall r \in \{1, \ldots, 4\}$ is configured in away that maximises the SNR of the reflected signal towards the designated user D_i, located in different locations $P_l, \forall l = \{1, \cdots, L\}$ in the area under test, constituting the optimum configuration of each quadrant $RIS_l^{opt,Q_r}, \forall l = \{1, \cdots, L\}, r = \{1, \cdots, 4\}$.

Subsequently, the channel is probed using M OFDM probing packets transmitted from AP_i to each destination D_l located at position P_l, $\forall l \in \{1, \cdots, L\}$, via the RIS under two settings.

1. *Communication settings*: In this step, the optimum RIS configuration RIS_l^{opt} associated with a specific position P_l is obtained by maximizing the SNR value towards the device D_l, located at position P_l. This process is performed for all the positions P_l , $\forall l \in \{1, \cdots, L\}$, constituting a list $List_{RIS}^{Com} = \{\langle RIS_1^{opt} : P_1\rangle, \cdots, \langle RIS_L^{opt} : P_L\rangle\}$.
2. *Localization settings*: In this step, the optimized RIS configuration of each quadrant RIS_l^{opt,Q_r}, $\forall r = \{1, \cdots, 4\}$ is employed for channel estimation $\hat{Ch}_l^{Q_r}$ at the receiver D_l, located at position P_l, $\forall l \in \{1, \cdots, L\}$. This process yields the channel chart or dataset of the localization mode, denoted as $Dataset_{RIS}^{loc} = \{\{Dataset_{Q_1,1}^{loc}, \cdots Dataset_{Q_4,1}^{loc}\}, \cdots, \{Dataset_{Q_1,L}^{loc}, \cdots Dataset_{Q_4,L}^{loc}\}\}$, where $Dataset_{Q_r,l}^{loc} = \{\hat{Ch}_{1,l}^{Q_r}, \cdots, \hat{Ch}_{M,l}^{Q_r}\}$, $\forall\, l = \{1, \cdots, L\}, r = \{1, \cdots, 4\}$. Subsequently, the obtained dataset $Dataset_{RIS}^{loc}$ is split into 80% for training and 20% for testing the machine learning model ML_{Loc}. The trained ML_{Loc} model is then employed for accurate localization, as demonstrated in the online mode.

3.0.2. Stage 2: Online mode

In this mode, an initial cryptographic handshaking process is initiated to verify the legitimacy of the newly added device D_i, which is initially located at position P_l. This is accompanied by precise channel-based localization. Subsequently, the location of D_i is periodically monitored to ensure smooth transitions between adjacent positions as it moves from P_l. Any anomalous or irrational transitions between locations may indicate suspicious activity, thereby triggering a re-execution of the initial handshaking procedure for D_i. This mode generally consists of two main phases: the initial handshaking and localization phase, and the smooth transition phase. The following outlines the steps involved in each phase.

1. *Initial handshaking and localization phase*: This phase employs a traditional public key infrastructure (PKI)-based authentication mechanism utilizing the elliptic curve cryptosystem (ECC). Generally, this phase consists of two main steps: the initialization and registration step, and the handshaking and localization step.
   - *Initialization and registration step*:
     (a) An elliptic curve E of the form $y^2 = x^3 + ax + b$, defined over a finite field, is constructed by TA with order q, ensuring the non-singularity condition $4a^3+27b^2 \neq 0$. A base point P is chosen to generate a cyclic subgroup of order q, forming the basis for elliptic curve cryptographic operations.

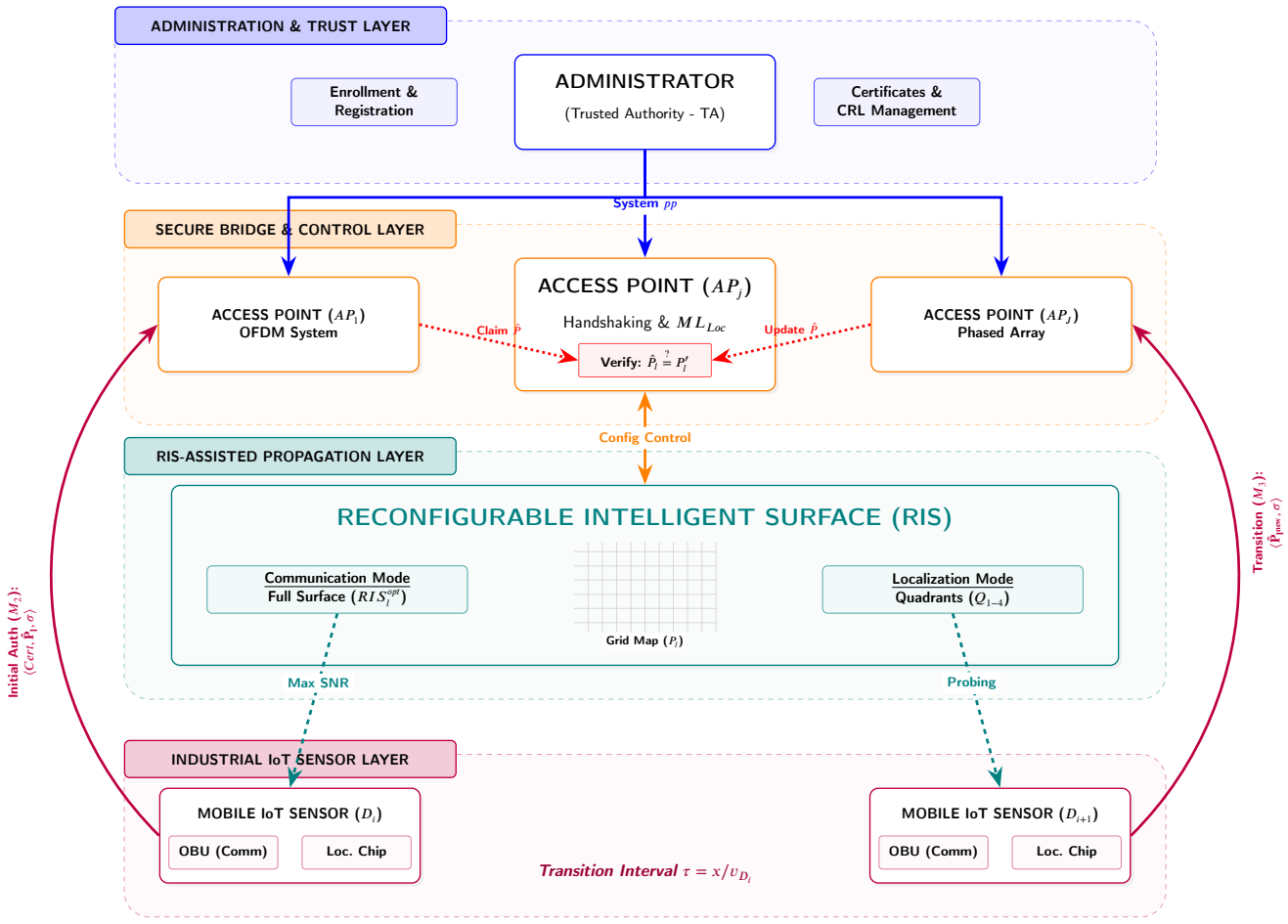


Figure 2: Final system architecture with vertical flow labels and optimized layer spacing.

(b) The TA generates its master secret key $mk_{TA} \in \mathbb{Z}_q^*$ and computes the corresponding public parameter $pk_{TA} = mk_{TA} \cdot P$. The system public parameters are then defined as $pp = \{a, b, p, q, P, pk_{TA}\}$. Accordingly, the TA generates secret keys $sk_{D_i}, sk_{AP_j} \in \mathbb{Z}_q^*$ for each entity D_i and AP_j, respectively, and computes their associated public parameters as $pk_{D_i} = sk_{D_i} \cdot P$ and $pk_{AP_j} = sk_{AP_j} \cdot P$.

(c) Then, the TA issues long-term digital certificates for D_i and AP_j, denoted as $Cert_{D_i} = \langle pk_{D_i}, T_R, \sigma_{TA} \rangle$ and $Cert_{AP_j} = \langle pk_{AP_j}, T_R, \sigma_{TA} \rangle$, where T_R represents the expiration date, and σ_{TA} is the TA's signature on the certificate contents, generated using the master secret key mk_{TA}.

(d) Finally, the TA creates a certificate revocation list (CRL) containing revoked vehicle certificates and distributes the tuple $\langle CRL, pp, Cert_{D_i/AP_j} \rangle$ to each terminal D_i and AP_j within the network.

- *Handshaking and localization step*:

(a) In this step, AP_j broadcasts the message $M_1 = \langle Cert_{AP_j}, T_1, \sigma_{AP_j} \rangle$, where σ_{AP_j} is the signature on the tuple, generated using the secret key sk_{AP_j} at timestamp T_1.

(b) D_i, in turn, replies by $M_2 = \langle Cert_{D_i}, PPs, \hat{P}_l, T_2, \sigma_{D_i} \rangle$, where σ_{D_i} is the signature on the tuple, generated using the secret key sk_{D_i} at timestamp T_2, $\hat{P}_l$ is the estimated location of D_i using its OBU, and PPs is a number of probing packets used for channel estimation.

(c) During the receiving of M_2, AP_j dynamically changes the RIS configuration of each quadrant RIS_l^{opt,Q_r}, $\forall r = \{1, \cdots, 4\}$ associated with the revived position $\hat{P}_l \in M_2$, constituting $\hat{Ch} : \{\hat{Ch}_l^{Q_1}, \cdots, \hat{Ch}_l^{Q_4}\}$.

(d) Finally, AP_j classifies the position of D_i using $\hat{Ch}$ as an input to the trained model ML_{Loc} to obtain P'_l and verifies whether the estimated position P'_l matches $\hat{P}_l$. If yes, AP_j check the freshness of T_2, finds out if $Cert_{D_i} \in CRL$, and finally, verifies $\sigma_{D_i} \in M_2$.

2. *Smooth transition phase*: This phase focuses on the real-time tracking of the incremental movements exhibited by D_i as it transitions between its current position P_l and neighboring positions within the working area. The primary objective is to ensure high-precision localization and seamless communication while maintaining low computational overhead. In this context, the RIS dynamically reconfigures its surface elements to enhance the SNR and improve channel estimation accuracy for each position update. This approach enables the delegation of D_i's trustworthiness across various $P_l, \forall l = 1, \cdots, L$, situated along its trajectory between distinct end-point locations. In general, this phase comprises the following steps.

   - *RIS configuration adjustment step*: In this step, the RIS is optimized based on D_i's communication or localization requirements. For instance, if AP_j is directly communicating with D_i by sending or receiving messages or control commands, the entire RIS surface is configured towards D_i's location. This is because configuring the full RIS yields higher SNR and throughput compared to configuring only a single quadrant. Consequently, the RIS is optimized to its optimal configuration, RIS_l^{opt}, for the position P_l. Simultaneously, AP_j manages the localization process by optimizing the RIS configuration for each quadrant, denoted as $RIS_{l^{new}}^{opt,Q_r}$, $\forall r = \{1,2,3,4\}$, corresponding to P_l's neighboring positions $P_{l^{new}}$. In this scenario, AP_j requests localization data from D_i, and in response, D_i sends the tuple $M_3 = \langle Cert_{D_i}, PPs, \hat{P}_{l^{new}}, T_3, \sigma_{D_i} \rangle$. Subsequently, AP_j estimates the channel state information, $\hat{Ch} = \{\hat{Ch}_{l^{new}}^{Q_1}, \cdots, \hat{Ch}_{l^{new}}^{Q_4}\}$, for each quadrant, and classifies it using the localization machine learning model ML_{Loc} to obtain the estimated position $P'_{l^{new}}$. It then verifies whether $P'_{l^{new}}$ matches the claimed position $\hat{P}_{l^{new}}$. If the positions match and $P_{l^{new}}$ is a neighboring position to P_l, then AP_j continues to trust D_i; otherwise, the system flags the transition as suspicious, triggering the subsequent re-authentication step.

   - *Crypto-based re-authentication step*: In this step, AP_j check the freshness of T_3, finds out if $Cert_{D_i} \in CRL$, and finally, verifies $\sigma_{D_i} \in M_3$. Then updates $P'_{l^{new}}$ to be the current position.

   Note that the localization step is performed at fixed time intervals τ, where τ represents the transition time from position P_l to $P_{l^{new}}$. This interval is determined based on the average speed of D_i (v_{D_i}) and the interspacing distance x between adjacent positions, such that $\tau = x/v_{D_i}$ seconds. Figure 3 illustrates the RIS-assisted localization workflow, highlighting the interaction between offline dataset construction and online real-time authentication.

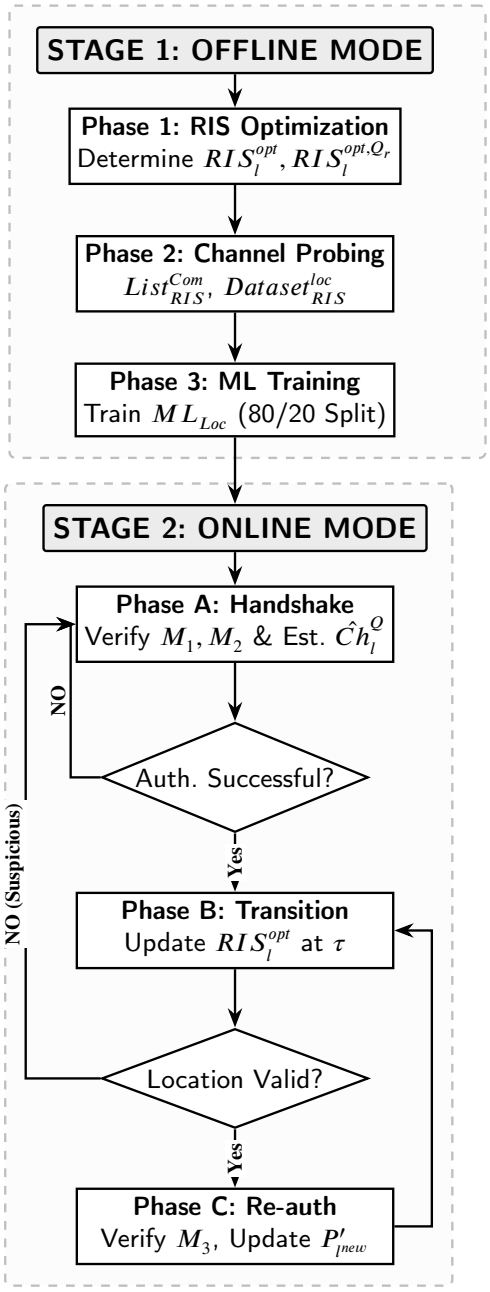


Figure 3: Operational framework illustrating the transition between the offline manifold learning phase and the online real-time authentication phase.

4. Performance Evaluation

This section presents the experimental validation and performance evaluation of the proposed RIS-assisted localization and authentication framework. It is organized to first describe the experimental setup and RIS configuration optimization, followed by dataset construction, results analysis, and a comprehensive security assessment.

4.1. Experimental setup

The experimental validation was conducted in a controlled indoor environment, as illustrated in Fig. 4. The hardware testbed centers around a RIS comprising 64×64

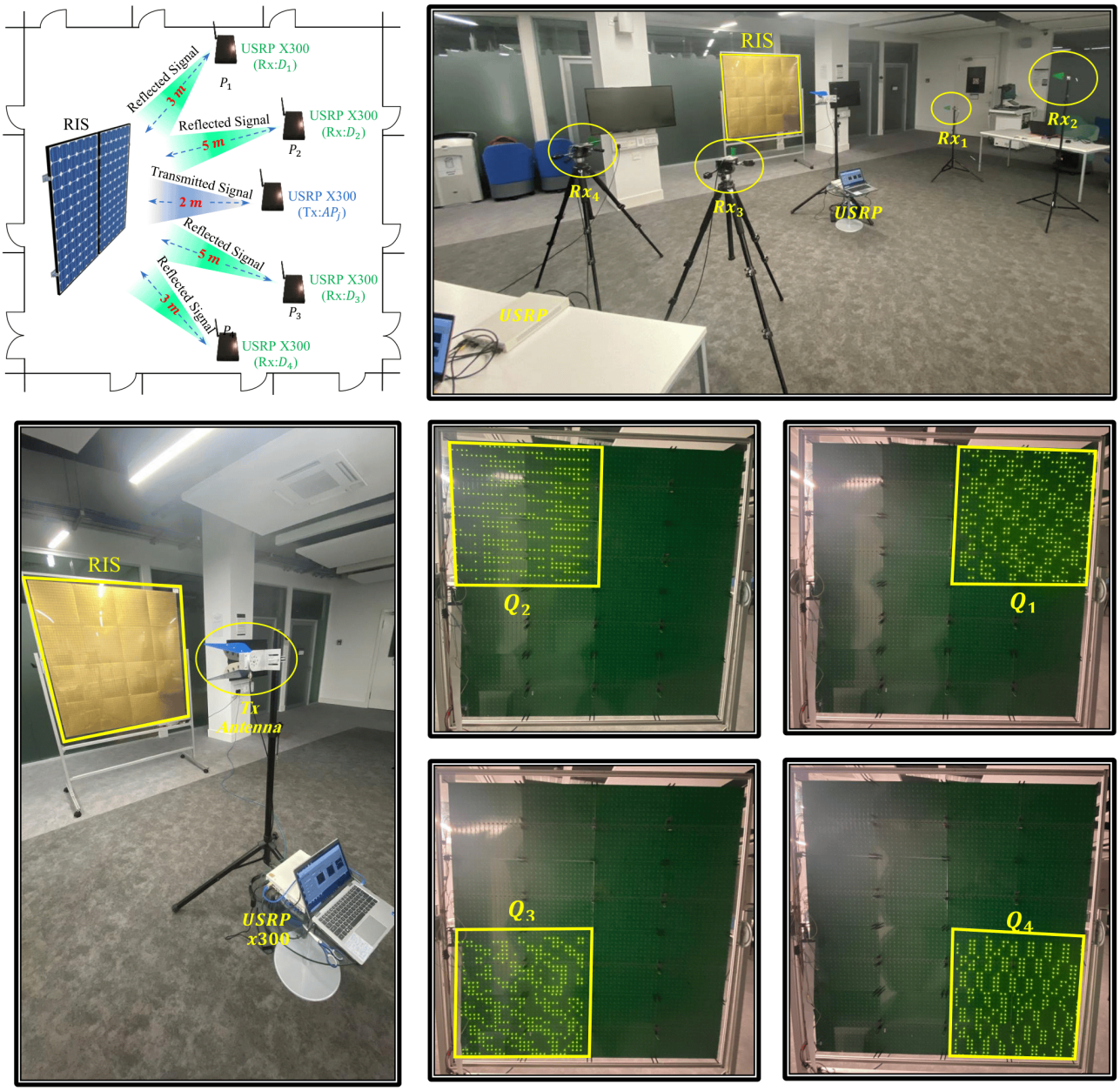


Figure 4: Experimental setup and RIS configuration. (Top-left) Floor plan of the Laboratory showing the spatial distribution of the USRP X300 transceivers and the RIS. (Top-right) Real-world laboratory environment featuring the RIS, Rx nodes, and USRP controllers. (Bottom-left) Detailed view of the Tx antenna and the RIS interface controlled via USRP X300. (Bottom-right) Visualization of the four distinct RIS phase-shift configurations (Q_1 through Q_4) utilized for spatial multiplexing and signal orientation.

unit elements. The system operates at a carrier frequency of $f_c = 3.75$ GHz with an OFDM waveform configuration utilizing 256 subcarriers and a sampling rate of 200 kHz. Signal transmission and reception are managed by Ettus USRP X300 software defined radios (SDRs). The Tx is equipped with a high-gain horn antenna positioned $d_{Tx} = 2$ m from the center of the RIS, while the Rx nodes employ directive antennas. Both Tx and Rx antennas provide a gain of 20 dBi. To characterize the spatial propagation environment and facilitate manifold learning, the Rx nodes are strategically positioned at angles of 30° and 60° relative to the boresight of the RIS. During the channel probing phase, four distinct RIS phase-shift configurations are optimized to generate the necessary spatial diversity for the localization dataset. Table 2 provides a comprehensive summary of the system parameters and hardware specifications employed in the experimental setup.

Table 2
System and Experimental Setup Parameters

Parameter	Value
RIS Element Grid	64×64 elements
Carrier Frequency	3.75 GHz
Waveform Type	OFDM (256 subcarriers)
Sampling Rate	200 kHz
Antenna Gain (Tx/Rx)	20 dBi
Tx–RIS Distance	2 m
Rx Angular Positions	30° and 60°
Tx Antenna Type	Horn Antenna
Rx Antenna Type	Directive Antenna
USRP Model	Ettus X300

4.2. RIS configuration optimization

To establish a robust communication link and generate the spatial diversity required for localization, the proposed framework employs a two-tier optimization strategy. This section details the identification of the global optimal RIS state and the quadrant-specific configurations used to characterize localized channel manifolds. The following subsections detail the optimization methodologies developed for the global surface and the quadrant-specific RIS configurations.

4.2.1. Global surface optimization

As outlined in Algorithm 1, the goal of the global phase is to maximize the SNR at the target receiver by treating the 64×64 RIS as a unified reflecting surface. Utilizing a Hadamard codebook $\mathcal{H}$ of size $64 \times 64 = 4096$, the surface is iteratively configured to test orthogonal phase-shift patterns. For each configuration H_i, the average SNR, $\overline{\gamma}_i$, is measured across the $K = 256$ subcarriers of the OFDM signal. The resulting optimal configuration, RIS_l^{opt}, ensures the maximum power transfer for the legitimate link between the Tx and the Rx positions (located at 30° or 60° relative to the RIS boresight).

Algorithm 1 Optimization of Global RIS Configuration (RIS_l^{opt})

Initialization
Construct Hadamard codebook $\mathcal{H} = \{H_1, H_2, \ldots, H_L\}$ for 64×64 units
Define target position P_l and initialize $\Gamma = \emptyset$
Full-Surface Channel Characterization
for $i = 1$ to L **do**
    Apply Hadamard matrix H_i to the entire RIS surface
    Measure average SNR: $\overline{\gamma}_i = \frac{1}{K} \sum_{k=1}^{K} \mathrm{SNR}_k$
    $\Gamma \leftarrow \Gamma \cup \{\overline{\gamma}_i\}$
end for
Optimal Selection
Find optimal index: $i^* = \arg\max_i(\Gamma)$
return $RIS_l^{opt} = H_{i^*}$

4.2.2. Quadrant-wise manifold probing

To facilitate the offline training phase (*Stage 1*) described in the operational flowchart, the RIS is subdivided into four 32×32 quadrants $Q_r, \forall r = \{1, 2, 3, 4\}$. Algorithm 2 details the process of optimizing each quadrant independently. During this phase, elements outside the active quadrant Q_r are set to a deactivation state (e.g., phase-shift $\phi = \pi$) to minimize interference. By applying localized Hadamard configurations $H_j \in \mathcal{H}_{sub}$, the system identifies the quadrant-specific optimal states RIS_l^{opt,Q_r}. These configurations are pivotal for constructing $Dataset_{RIS}^{loc}$, as they provide the unique spatial fingerprints necessary for manifold learning and position verification.

Algorithm 2 Optimization of Quadrant-Based Configurations (RIS_l^{opt,Q_r})

Initialization
Define quadrants $Q_r \in \{Q_1, Q_2, Q_3, Q_4\}$
Construct Hadamard codebook $\mathcal{H}_{sub}$ for 32×32 units
Initialize $Set_{opt} = \emptyset$
Localized Manifold Probing
for each quadrant $r = 1$ to 4 **do**
    Deactivate elements in RIS $\setminus Q_r$
    for $j = 1$ to L_{sub} **do**
        Apply $H_j \in \mathcal{H}_{sub}$ to quadrant Q_r
        Measure $\overline{\gamma}_{r,j}$ at Rx positions
    end for
    Find local optimal: $j^* = \arg\max_j(\overline{\gamma}_{r,j})$
    $Set_{opt} \leftarrow Set_{opt} \cup \{RIS_l^{opt,Q_r} = H_{j^*}\}$
end for
return Set_{opt}

While the continuous phase-shift optimization technique offers theoretical limits, its non-convex nature makes it difficult to process in a timely manner. By utilizing an orthogonal Hadamard-based discrete search over a spatial grid L, Algorithms 1 and 2 pre-learn and map the optimal surface patterns RIS_l^{opt} associated with each position P_l offline. During online operation, the RIS controller executes an instantaneous lookup of the pre-configured pattern matching the receiver's claimed position $\hat{P}_l$, enabling seamless physical-layer verification for dynamic mobile nodes. Furthermore, because indoor multipath channels possess bounded spatial rank and RIS panels operate under discrete B-bit phase quantization, a finite number of spatial points and feasible RIS configurations is sufficient for the considered environment/deployment area.

4.3. Dataset collection and visualization

Upon identifying the optimal global configuration RIS_l^{opt} and the quadrant-specific configurations RIS_l^{opt,Q_r} ($\forall r \in \{1, \ldots, 4\}$) for each reference position P_l ($\forall l \in \{1, \ldots, 4\}$) as depicted in Figure 4, the dataset construction phase was initiated. The channel state information (CSI), specifically the RSS and the CPR, was extracted for all four reference positions by probing the environment with $M = 1000$ OFDM packets. Each packet consists of $K = 256$ subcarriers with a cyclic prefix (CP) length of 64. These signals were transmitted from an Ettus USRP X300 (Tx) to each destination D_l located at P_l via the RIS under two distinct operational modes:

1. *Communication Mode:* Utilizing the full-surface optimal configuration RIS_l^{opt}.
2. *Localization Mode:* Employing the quadrant-wise configurations RIS_l^{opt,Q_r} for all $r \in \{1, \dots, 4\}$.

This process yielded a comprehensive dataset of received OFDM symbols, examples of which are illustrated in Figure 5. As illustrated in Fig. 5(a-e), the RIS significantly enhances the RSS at the designated receiver, D_1. Notably, the SNR achieved when the full RIS aperture is activated (Fig. 5(e)) exceeds that of the individual quadrant configurations (Fig. 5(a-d)). This gain is attributed to the constructive superposition of reflections from the entire 64 × 64 element array, all optimized toward D_1. Consequently, the full RIS mode is ideal for long-range communication where high SNR is critical. In contrast, the individual quadrant configurations provide the localized spatial diversity required for high-precision localization, even though the operational range is reduced due to the smaller effective aperture. This observation highlights the fundamental trade-off between localization resolution and communication range in RIS-assisted systems. Note that, during the localization mode, the acquisition of the CSI is controlled by a time-division multiplexing (TDM) frame structure that consists of four probing slots, where each slot corresponds to the separate reconfiguration of RIS quadrants Q_1 to Q_4. For each TDM frame, OFDM pilot subcarriers (Block-type) are used to estimate the channel via least square (LS) channel estimation technique.

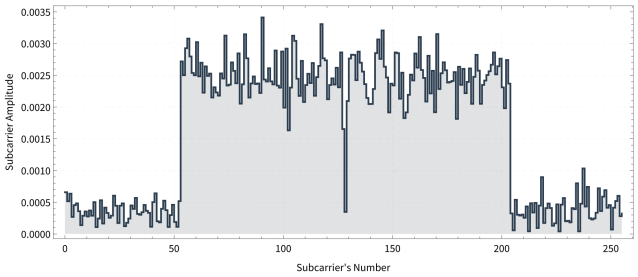
4.4. Results and discussion

Following the dataset acquisition, the data was partitioned into an 80% training set and a 20% testing set to ensure robust model evaluation. A comparative analysis of the evaluated ML models was conducted to assess the accuracy of localized position estimation for each destination D_l at its respective coordinate $P_l, \forall l \in \{1, 2, 3, 4\}$. The comparative performance of the evaluated ML models is summarized in Table 3. Among the nine candidate algorithms, the support vector machine (SVM) demonstrates the highest efficiency, achieving a near-perfect accuracy of 99.50% and leading across all primary metrics, including average recall, precision, and F1-score. This superior performance is closely followed by gradient boosted trees (99.00%) and neural networks (97.75%), suggesting that the high-dimensional channel state information features extracted from the RIS configurations are highly separable when mapped through non-linear kernels. A more comprehensive analysis of the top-performing models is provided in Table 4, which details the F1-scores across the four reference positions (P_1-P_4). The SVM model achieves perfect classification scores for positions P_3 and P_4, indicating that the quadrant-wise RIS configurations (RIS_l^{opt,Q_r}) at these coordinates produce unique and highly distinct spatial fingerprints, see Figure 6d. Even for the more challenging positions (P_1 and P_2), the SVM maintains a robust F1-score of 0.9900.

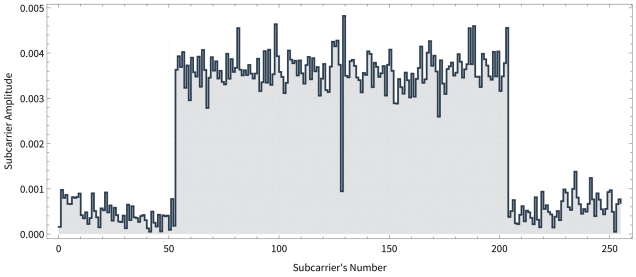
In contrast, simpler distance-based models such as nearest neighbors (k-NN) exhibit significantly lower performance, with an accuracy of only 40.63%. The failure of k-NN to characterize the environment suggests that the relationship between the CSI manifold, comprising RSS and CPR, and the physical location is not a simple Euclidean proximity problem. Instead, the success of the SVM indicates that the optimized RIS reflections create complex, localized signal patterns. These patterns require the high-dimensional feature mapping provided by the SVM's kernel functions to effectively distinguish between legitimate coordinates and potential authentication threats, thereby validating the proposed dual-tier optimization framework.

To investigate the impact of spatial granularity, we analyze the performance degradation of the Logistic Regression model as the number of active RIS quadrants is reduced, as summarized in Table 5. The results reveal a direct correlation between the spatial degrees of freedom and the fidelity of the localized channel manifold, where the transition from four quadrants (97.13% accuracy) to three (96.25%) shows marginal loss, indicating that the system remains sufficiently over-determined to maintain high-precision authentication. However, a significant performance collapse is observed when moving to a single quadrant, where accuracy drops to 74.50%, suggesting that a restricted subarray provides insufficient spatial entropy to uniquely fingerprint the environment. This decline is particularly evident at position P_2, which exhibits the highest sensitivity to aperture reduction. Ultimately, these findings validate the proposed quadrant-wise optimization strategy, proving that while the full 64×64 aperture is necessary for maximizing communication gain, the subdivision into multiple spatial quadrants is essential for generating the unique phase responses and signal strength variations required for robust, coordinate-based localization.

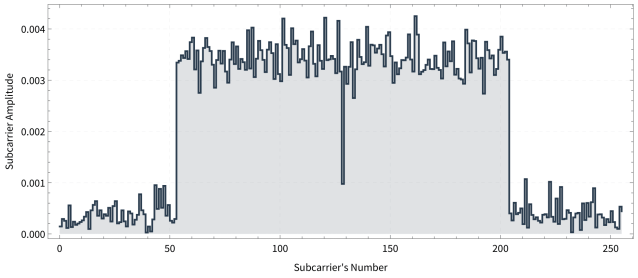
The evaluation of the "Whole RIS" configuration reveals a critical performance bottleneck when global optimization is applied to a localization-centric task. Despite utilizing the full 64 × 64 aperture, the model achieves a localization accuracy of only 74.38%, which is statistically comparable to the performance of a single isolated quadrant (74.50%). This phenomenon occurs because global beamforming focuses the RIS reflections into a single, high-gain dominant path toward the receiver, effectively smoothing out the fine-grained spatial variations in the CSI. While this maximizes the SNR for communication, it simultaneously reduces the entropy of the spatial manifold, making it significantly more difficult for the ML model to distinguish between the unique coordinates P_1 through P_4. These results provide empirical evidence that high-gain beamforming and high-resolution localization are inherently at odds; the very process that optimizes the link for data transfer suppresses the multipath diversity required for precise fingerprinting. Consequently, the transition from a unified "Whole RIS" mode to the proposed "Four Quadrants" strategy is essential to restore the spatial degrees of freedom required for robust coordinate-based authentication.



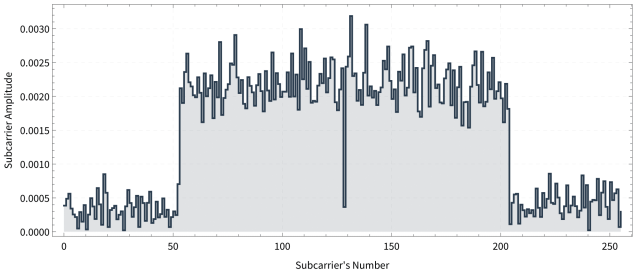
(a) Received OFDM symbol utilizing quadrant Q_1 (32×32 elements) configured at RIS_l^{opt,Q_1} towards D_1.



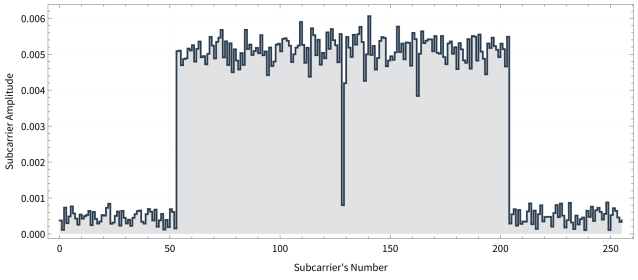
(b) Received OFDM symbol utilizing quadrant Q_2 (32×32 elements) configured at RIS_l^{opt,Q_2} towards D_1.



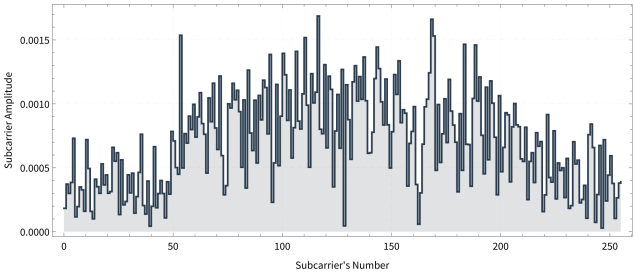
(c) Received OFDM symbol utilizing quadrant Q_3 (32×32 elements) configured at RIS_l^{opt,Q_3} towards D_1.



(d) Received OFDM symbol utilizing quadrant Q_4 (32×32 elements) configured at RIS_l^{opt,Q_4} towards D_1.



(e) Received OFDM symbol utilizing the full RIS (64×64 elements) configured at RIS_l^{opt} towards D_1.



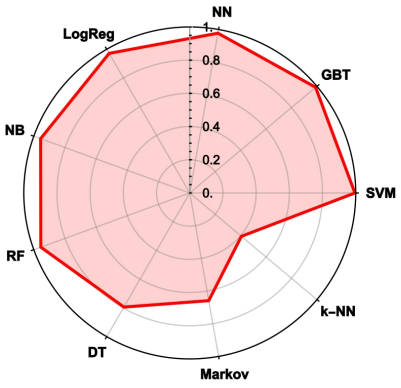
(f) Received OFDM symbol with the RIS in the deactivated (OFF) state towards D_1.

Figure 5: Characterization of received OFDM symbols under various RIS configurations: (a-d) quadrant-specific localization settings, (e) baseline deactivated state, and (f) global communication optimization (RIS_l^{opt}).

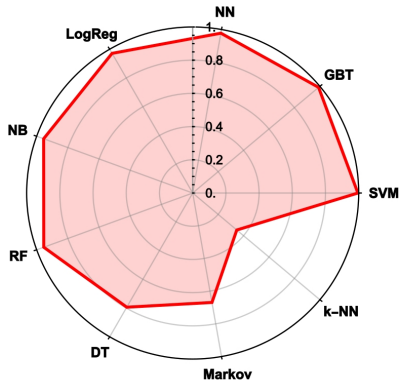
Table 3
Performance Comparison of Machine Learning Models for RIS-Assisted Localization and Authentication

ML Model	Accuracy	Avg. Recall	Avg. Precision	Avg. F1-Score
Support Vector Machine (SVM)	**0.9950**	**0.9950**	**0.9950**	**0.9950**
Gradient Boosted Trees	0.9900	0.9900	0.9901	0.9900
Neural Network	0.9775	0.9775	0.9781	0.9776
Logistic Regression	0.9712	0.9712	0.9712	0.9713
Naive Bayes	0.9563	0.9563	0.9593	0.9554
Random Forest	0.9550	0.9550	0.9579	0.9546
Decision Tree	0.7938	0.7938	0.7966	0.7940
Markov	0.6588	0.6588	0.7006	0.6693
Nearest Neighbors (k-NN)	0.4063	0.4063	0.8214	0.3466

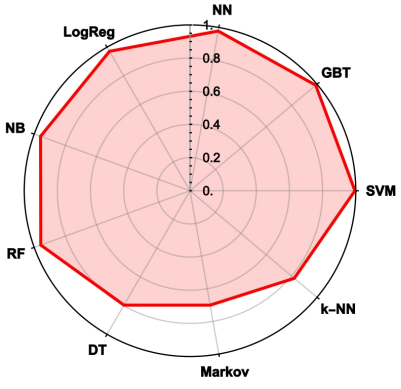
In the "RIS OFF" scenario, the system's performance serves as a baseline for the ambient multipath environment, yielding a limited accuracy of "68.14%". As shown in Table 5, the lack of reconfigurable reflections leads to a significant degradation in spatial separability, particularly at position P_1, where the recall drops to a minimum of 0.5000. This suggests that without the active phase modulation provided by the RIS, the natural CSI is insufficiently distinct to overcome the spatial correlation between the different destination coordinates. The baseline results demonstrate that relying solely



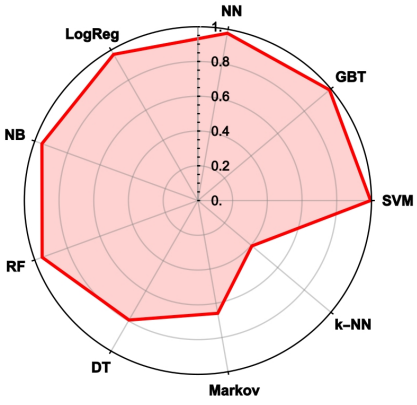
(a) Comparison of overall classification Accuracy across all evaluated machine learning models.



(b) Model performance profile based on the F1-Score, illustrating harmonic balance between precision and recall.



(c) Geometric distribution of Precision scores, highlighting the models' ability to minimize false positives.



(d) Sensitivity analysis via Recall manifolds, depicting the models' success in detecting authenticated signals.

Figure 6: Radar chart performance profiles of various machine learning models for RIS-assisted localization and authentication: (a) Accuracy, (b) F1-Score, (c) Precision, and (d) Recall. The radial axes represent evaluated model architectures, highlighting the performance dominance of the SVM and GBT configurations.

Table 4
Detailed Per-Position F1-Scores for Top-Performing Models

Model	P_1	P_2	P_3	P_4
SVM	0.9900	0.9900	1.0000	1.0000
GBT	0.9826	0.9900	0.9874	1.0000
Neural Network	0.9796	0.9559	0.9774	0.9975

on static environmental reflections is inadequate for reliable authentication, thereby highlighting the necessity of the RIS in shaping the wireless environment to create a robust and high-entropy spatial manifold.

The results presented in Table 6 illustrate the significant performance gains achieved through multi-modal feature fusion, establishing that the integration of RSS and CPR is vital for high-precision spatial authentication. While the RSS-only configuration provides a robust baseline accuracy of 93.38% by capturing coarse distance-dependent power gradients, the CPR-only mode achieves 91.50%, reflecting the fine-grained spatial phase shifts induced by the RIS quadrants. However, the fusion of both metrics in the "Both (RSS + CPR)" configuration yields a superior accuracy of 97.13%. This improvement suggests that RSS acts as a stable anchor for the signal manifold, while CPR provides the high-resolution angular sensitivity required to resolve spatial ambiguities. Notably, position P_4 maintains a nearly perfect recall of 0.9950 across all feature sets, indicating a highly distinct spatial signature that is resilient to feature subsetting. Ultimately, this ablation study confirms that leveraging the full complex-valued channel information, rather than power

Table 5
Impact of RIS Spatial Granularity and Activation State on Logistic Regression Performance

Configuration	Metric	P_1	P_2	P_3	P_4
Four Quadrants	Recall	0.9650	0.9550	0.9700	0.9950
(Accuracy: 0.9713)	Precision	0.9797	0.9455	0.9700	0.9901
	F1-Score	0.9723	0.9502	0.9700	0.9925
Three Quadrants	Recall	0.9000	0.9250	1.0000	0.9950
(Accuracy: 0.9625)	Precision	1.0000	0.9250	0.9390	0.9901
	F1-Score	0.9637	0.9250	0.9685	0.9925
Two Quadrants	Recall	0.9850	0.8050	0.9800	0.9950
(Accuracy: 0.9413)	Precision	0.9801	0.9527	0.8673	0.9755
	F1-Score	0.9825	0.8726	0.9202	0.9851
One Quadrant	Recall	0.6950	0.6100	0.9000	0.7750
(Accuracy: 0.7450)	Precision	0.8176	0.6740	0.7004	0.8073
	F1-Score	0.7514	0.6404	0.7877	0.7908
Whole RIS	Recall	0.7250	0.9500	0.5150	0.7850
(Accuracy: 0.7438)	Precision	0.6532	0.9845	0.5568	0.7850
	F1-Score	0.6872	0.9669	0.5351	0.7850
RIS OFF	Recall	0.5000	0.7200	0.9250	0.8150
(Accuracy: 0.6814)	Precision	0.7353	0.7701	0.8810	0.6105
(Baseline)	F1-Score	0.5952	0.7442	0.9024	0.6981

Table 6
Impact of Feature Selection (RSS vs. CPR) on Logistic Regression Performance (Four Quadrants)

Feature Set	Metric	P_1	P_2	P_3	P_4
RSS Only	Recall	0.8950	0.9200	0.9250	0.9950
(Accuracy: 0.9338)	Precision	0.9227	0.8720	0.9585	0.9851
	F1-Score	0.9086	0.8954	0.9415	0.9901
CPR Only	Recall	0.9000	0.8750	0.8900	0.9950
(Accuracy: 0.9150)	Precision	0.8911	0.8537	0.9418	0.9755
	F1-Score	0.8955	0.8642	0.9152	0.9851
Both (RSS + CPR)	Recall	0.9650	0.9550	0.9700	0.9950
(Accuracy: 0.9713)	Precision	0.9797	0.9455	0.9700	0.9901
	F1-Score	0.9723	0.9502	0.9700	0.9925

or phase in isolation, is the optimal approach for minimizing localization error and ensuring secure coordinate-based authentication.

The division of the $N_x \times N_y$ RIS array into $|r| = 4$ equal quadrants (2×2) is chosen by evaluating the fundamental trade-off between spatial localization resolution, effective coverage range, and reflected SNR. Partitioning an RIS into a higher number of sub-surfaces ($|r| > 4$) increases spatial path diversity, which enhances localized positioning accuracy close to the array. However, reducing the physical aperture diameter D of each sub-surface scales down the Rayleigh distance ($d_R = 2D^2/\lambda$) and decreases the reflected power. This significantly reduces the effective operational distance over which accurate localization can be maintained. The proposed 2×2 partitioning balances this trade-off by preserving 1024 elements per quadrant on our 64×64 panel, maintaining robust signal coverage across extended indoor distances, while creating symmetric horizontal and vertical spatial diversity. Furthermore, $|r| = 4$ produces an 8-dimensional feature vector (4 RSS + 4 CPR metrics) that enables ML_{Loc} to achieve $> 99\%$ verification accuracy with minimal probing latency.

Table 7
Comparison of the proposed RIS-assisted localization framework with representative state-of-the-art approaches.

Method	Distance	Antenna	RIS	Accuracy
GBT [8]	1 m	Directive	On	82.40 %
RHL-Net [17]	1 m	Directive	On	85.58 %
Proposed Method (SVM)	**1 m**	**Directive**	**On**	**99.50 %**

Note: For a fair comparison, all experiments were conducted by the same research group in the same laboratory on Ettus Research USRP X300 hardware with the same 64×64-element RIS, horn/directive antenna pair, and OFDM settings.

From Table 7, the proposed framework provides higher accuracy in localization than some representative state-of-the-art RIS-assisted algorithms under similar conditions of 1-meter distance, directive antenna, and RIS-assisted scenario. Specifically, the framework using the SVM classifier is able to reach 99.50% of accuracy, which is higher than GBT [8] and RHL-Net [17], achieving 82.40% and 85.58%, respectively. In other words, there is a performance gain of 17.10% and 13.92%, compared to GBT [8] and RHL-Net [17], respectively.

4.5. Security analysis

This part discusses the security strength of the proposed method against impersonation, modification, and replaying attacks through formal (i.e., random oracle modeling (ROM)) and informal security analyses.

4.5.1. Formal security analysis under ROM

In this section, a formal security analysis of the cryptographic handshake protocol and physical layer verification process is provided using the ROM.

Hardness assumptions and threat model The security strength of the ECC computations is based on the problem of solving the elliptic curve discrete logarithm problem (ECDLP) for the curve $E : y^2 = x^3 + ax + b \pmod p$ where P is a point of order q. In addition, the assumptions made for the physical-layer re-authentication part depend on the multipath channel fingerprint vector $\hat{Ch} = \{\hat{Ch}_l^{Q_1}, \ldots, \hat{Ch}_l^{Q_4}\}$ evaluated by ML_{Loc}. Accordingly, an active attacker $\mathcal{E}$ is modeled that has the capability to intercept, replay, and spoof network communications, while not having the physical ability to be at the same spatial location P_l as D_i ($\mathcal{E}_{\text{loc}} \neq P_l$).

Formal adversarial advantage bound By considering hash functions as random oracles, we can see that the advantage of any polynomial time probabilistic algorithm $\mathcal{E}$

in forging a valid signature for a handshake or tricking the ML_{Loc} cross layer verification scheme is bounded by:

$$\Pr[\text{Succ}_{\mathcal{E}}] \leq \frac{Q_S(Q_H + Q_S)}{q} + \left(1 - P_{\text{detection}}^{ML_{Loc}}\right) + \text{negl}(\lambda), \tag{1}$$

where Q_H is the number of queries made to the random hash oracle $H()$, while Q_S is the number of queries to the signing oracle $\mathcal{O}_{\text{sign}}$. q denotes the order of the cyclic subgroup, $P_{\text{detection}}^{ML_{Loc}}$ is the probability of detection of the ML_{Loc} classifier, which is trained in the presence of a physical-layer mismatch, and $\text{negl}(\lambda)$ is a negligible function w.r.t. security parameter λ.

Quantifying $P_{detection}^{ML_{Loc}}$ The adversarial advantage bound in (1) includes the term $P_{\text{detection}}^{ML_{\text{Loc}}}$, which requires explicit characterization to complete the security argument. Let $\mathcal{D}_l$ denote the distribution of the channel fingerprint vector $\hat{Ch} = \{\hat{Ch}_l^{Q_1}, \ldots, \hat{Ch}_l^{Q_4}\}$ produced when a device occupies position P_l. An adversary $\mathcal{E}$ at location $\mathcal{E}_{\text{loc}} \neq P_l$ generates measurements drawn from $\mathcal{D}_{\mathcal{E}_{\text{loc}}}$, a distinct distribution. For $\mathcal{E}$ to bypass physical-layer verification while claiming position P_l, the classifier must output $ML_{\text{Loc}}(\hat{Ch}^*) = P_l$ on a sample that did not originate from $\mathcal{D}_l$. This event is the inter-class false positive: a fingerprint from the wrong spatial distribution accepted as belonging to the claimed position. We therefore define

$$P_{\text{detection}}^{ML_{\text{Loc}}} = 1 - \max_{j \neq l} \Pr\left[ML_{\text{Loc}}(\hat{Ch}) = P_l \;\middle|\; \hat{Ch} \sim \mathcal{D}_j\right]. \tag{2}$$

This quantity is distinct from standard test-set accuracy, which measures performance on samples drawn from the same distribution as training. The empirical precision of the SVM classifier, 0.9950 averaged across positions and 0.9900 at the worst-case positions (P_1 and P_2, Table 4), provides a direct lower bound: of all channel vectors the classifier accepts as P_l, at most 1% originated from a different position. This bounds the inter-class confusion probability at ≤ 0.01, giving $P_{\text{detection}}^{ML_{\text{Loc}}} \geq 0.99$. Substituting into (1), and noting that $Q_S(Q_H + Q_S)/q$ is negligible for 256-bit ECC parameters ($q \approx 2^{256}$), the total adversarial advantage satisfies

$$\Pr[\text{Succ}_{\mathcal{E}}] \leq 0.01 + \text{negl}(\lambda). \tag{3}$$

We note that this bound is empirically supported over four reference positions; a denser spatial grid would tighten the estimate. The physical-layer and cryptographic checks are also independent security layers: an adversary who forged a valid certificate (infeasible by ECDLP hardness) would still fail the fingerprint check, since channel measurements cannot be replicated from a different physical location without occupying it.

Game-based reduction and security proof The security reduction process occurs through a series of games where both the challenger $\mathcal{C}$ and the adversary $\mathcal{E}$ are involved.

1. *Setup phase*: Entity $\mathcal{C}$ is responsible for initializing an elliptic curve E and calculating $mk_{TA} \in \mathbb{Z}_q^*$ such that the system public parameters $pp = \{a, b, p, q, P, pk_{TA}\}$ are derived, where $pk_{TA} = mk_{TA} \cdot P$. Entity $\mathcal{C}$ generates certificates for entities D_i and AP_j as follows: $Cert_{D_i} = \langle pk_{D_i}, T_R, \sigma_{TA}\rangle$ and $Cert_{AP_j} = \langle pk_{AP_j}, T_R, \sigma_{TA}\rangle$, respectively.
2. *Query Phase*: $\mathcal{E}$ makes adaptive queries to the simulated oracles:
   - *Hash Oracle (H)*: $\mathcal{C}$ maintains an initially empty tracking list L_H. Upon receiving a hash query on message tuple $\mathbf{m}_k$, $\mathcal{C}$ returns the cached value if present; otherwise, it samples $h_k \xleftarrow{\$} \mathbb{Z}_q^*$, stores $\langle \mathbf{m}_k, h_k\rangle$ in L_H, and outputs h_k.
   - *Signing Oracle ($\mathcal{O}_{sign}$)*: For a signing query on message $M_2 = \langle Cert_{D_i}, PPs, \hat{P}_l, T_2\rangle$ or $M_3 = \langle Cert_{D_i}, PPs, \hat{P}_{l^{new}}, T_3\rangle$, $\mathcal{C}$ checks L_{sign}. If unqueried, $\mathcal{C}$ samples $k_i \xleftarrow{\$} \mathbb{Z}_q^*$, computes valid signature parameters $\sigma_{D_i} = (R_i, s_i)$ adhering to standard ECDSA verification rules, updates L_{sign}, and returns the generated signature.
3. *Forgery and cross-layer decision*: $\mathcal{E}$ outputs a forged tuple $M_2^* = \langle Cert_{D_i}^*, PPs^*, \hat{P}_l^*, T_2^*, \sigma_{D_i}^*\rangle$. To succeed, $\mathcal{E}$ must satisfy two independent verification conditions simultaneously at AP_j:
   (a) *Cryptographic Verification*: $\mathcal{E}$ must forge $\sigma_{D_i}^*$ such that $s_i^* \cdot P = R_i^* + H(M_2^*) \cdot pk_{D_i}$. By the Forking Lemma, extracting two valid forgeries for distinct hash outputs allows $\mathcal{C}$ to solve the ECDLP instance $\alpha = \log_P(pk_{D_i})$ in polynomial time with probability $\epsilon_{\text{ECDLP}} \geq \Pr[\text{Succ}_{\mathcal{E}}] - Q_S(Q_H + Q_S)/q$.
   (b) *Physical-Layer Verification*: Even if $\mathcal{E}$ replays a valid tuple $\langle Cert_{D_i}, PPs, \hat{P}_l, T_2, \sigma_{D_i}\rangle$ intercepted from D_i, AP_j reconfigures the RIS quadrants RIS_l^{opt,Q_r} ($\forall r \in \{1, \ldots, 4\}$) according to claimed position $\hat{P}_l^*$. Because $\mathcal{E}_{\text{loc}} \neq P_l$, the resulting channel estimate vector $\hat{\mathbf{Ch}}^*$ yields an uncorrelated spatial signature. The classifier $ML_{Loc}(\hat{\mathbf{Ch}}^*)$ evaluates to position $P_l' \neq \hat{P}_l^*$, causing immediate rejection at the initial verification step before certificate/CRL checking.

Consequently, the advantage $\Pr[\text{Succ}_{\mathcal{E}}]$ of forging a valid authentication message or bypassing physical-layer binding is computationally negligible, confirming that the proposed scheme is provably secure under the ROM.

4.5.2. Informal security analysis

The proposed mechanism resists various types of active attacks such as impersonation, modification, and replay. The resistance mechanisms are detailed as follows.

1. *Resistance to impersonation*: The proposed scheme demonstrates robust resistance to impersonation by multi-factorially binding a device's digital identity to its physical location. During the handshaking phase, the AP_j requires the IoT sensor D_i to provide a valid digital certificate $Cert_{D_i}$ signed by the TA, which is cryptographically verified using ECC. Accordingly, this digital claim is cross-validated against the device's physical location $\hat{P}_l$ using the ML_{Loc} classifier. An adversary attempting to impersonate D_i must not only steal the private key sk_{D_i} but also perfectly replicate the unique RIS-modulated CSI fingerprint associated with that specific spatial quadrant. Since the RIS quadrant configurations $RIS_l^{opt,Q_r}, \forall r = \{1,2,3,4\}$ generate location-specific scattering signatures that are nearly impossible to spoof from a different physical coordinate, the AP_j can immediately detect and revoke any illegitimate access requests, ensuring only authenticated entities at verified locations gain network entry. In addition, the spatial resolution of the physical-layer verifier is fundamentally bounded by the spatial coherence distance of the channel, $\rho_c \approx \lambda/2$. While the discretization grid spacing x is selected for computational efficiency during map construction, the feature vector exhibits high phase sensitivity to sub-wavelength displacements ($\Delta d > \lambda/4$). Furthermore, because the four RIS quadrants ($Q_1 \dots Q_4$) probe the grid cell from distinct spatial angles, an adversary positioned within the same grid cell x but displaced by $\Delta d > \rho_c$ fails to match the combined amplitude and phase responses across all four quadrants simultaneously, preventing localized channel spoofing.
2. *Resistance to modification*: The proposed scheme ensures resistance to modification by employing elliptic curve digital signature algorithm (ECDSA) to guarantee the integrity of all transmitted messages (M_1, M_2, M_3). Every critical data packet, including the timestamps and claimed position $\hat{P}_l$, is hashed and signed using the sender's private key sk_{D_i}. Upon reception, the AP_j verifies the signature using the corresponding public key pk_{D_i}. Any unauthorized alteration of the bitstream by an active attacker would result in a cryptographic mismatch, leading to immediate packet rejection. Furthermore, because the localization process relies on sensitive RIS-modulated CSI, any physical-layer tampering with the RIS phase shifts would distort the quadrant-specific fingerprints. This ensures that the ML_{Loc} model would yield an inconsistent position estimate P_l', thereby exposing the modification attempt during the spatial verification stage.
3. *Resistance to replay*: The proposed scheme achieves resistance to replay attacks by incorporating timestamps within the handshaking and transition phases. Each message (M_1, M_2, M_3) includes a current timestamp T_n, which is protected under the digital signature σ_{D_i}. Upon receiving a message, the AP_j calculates the transmission delay and compares it against a predefined maximum threshold to ensure the freshness of the packet. If an adversary captures a legitimate authentication sequence and attempts to retransmit it at a later time, the AP_j will immediately detect the expired timestamp and reject the request. Furthermore, the dynamic reconfiguration of the RIS quadrants ensures that localization probes are time-dependent; a replayed channel estimate would fail to align with the real-time, randomized probing schedule managed by the AP_j, thereby preventing attackers from bypassing security using previously recorded valid sessions.

5. Conclusions

This paper proposes a novel hybrid framework for RIS-aided industrial networks that integrates high-precision localization with robust cryptographic authentication. By employing a dual-mode operational strategy that uses the full RIS surface for communication gain and quadrant partitioning for spatial probing, the system achieves a superior balance between spectral efficiency and positioning accuracy. The implementation of machine learning classifiers, particularly SVMs and gradient-boosted trees, on quadrant-based channel maps yielded localization accuracies exceeding 99%, even in complex scattering environments. Extensive simulations further reveal that the proposed RIS-optimized configuration provides a significant SNR improvement compared to baseline deactivated states, ensuring reliable connectivity in signal-attenuated zones. Furthermore, integrating the elliptic curve cryptosystem within a PKI-based framework ensures that position verification is inherently linked to device identity, thereby mitigating impersonation and spoofing attacks. The proposed "smooth transition" phase significantly reduces computational latency by delegating trust across trajectories, making it highly suitable for real-time industrial IoT applications such as robotic navigation. This work validates that RIS technology is not merely a passive relay but a dynamic tool for enhancing physical-layer security and spatial awareness. Future work will extend validation to multiple environments, higher position densities, and NLOS configurations, address multi-user interference scenarios, and evaluate the impact of hardware impairments on the reliability of the ML-based channel fingerprints.

Acknowledgement

This work was supported by King Saud University, Riyadh, Saudi Arabia, through the Ongoing Research Funding program (ORF-2025-184). The authors would also like

to sincerely acknowledge Dr. Muhammad Ali Jamshed for his valuable support and contributions to this work.

Declaration

Declaration of generative AI and AI-assisted technologies in the writing process: During the preparation of this work, the author(s) used Grammarly in order to improve the language and readability. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.

References

[1] Taofeek A.O. Yusuf, et al. AI-Assisted NLOS Sensing for RIS-Based Indoor Localization in Smart Factories. *arXiv preprint arXiv:2505.15989*, 2025. https://doi.org/10.48550/arXiv.2505.15989

[2] Sefa Kayraklik, Ibrahim Yildirim, Ibrahim Hokelek, et al. Indoor Measurements for RIS-Aided Communication: Practical Phase Shift Optimization, Coverage Enhancement, and Physical Layer Security. *IEEE Open Journal of the Communications Society*, 5, 1243–1255, 2024. https://doi.org/10.1109/OJCOMS.2024.3363423

[3] F. Jiang, A. Abrardo, K. Keykhosravi, H. Wymeersch, D. Dardari, and M. Di Renzo. Two-Timescale Transmission Design and RIS Optimization for Integrated Localization and Communications. *IEEE Transactions on Wireless Communications*, 22(12), 2023. https://doi.org/10.1109/TWC.2023.3264559

[4] Thuy M. Pham, Linda Senigagliesi, Marco Baldi, et al. Machine Learning-Based Robust Physical Layer Authentication Using Angle of Arrival Estimation. In *IEEE Global Communications Conference (GLOBECOM)*, pp. 13–18, 2023. https://doi.org/10.1109/GLOBECOM54140.2023.10437915

[5] Adnan Umer, Ivar Müürsepp, Muhammad Mahtab Alam, and Henk Wymeersch. Reconfigurable Intelligent Surfaces in 6G Radio Localization: A Survey of Recent Developments, Opportunities, and Challenges. *IEEE Communications Surveys & Tutorials*, 27(6), 3526–3560, 2025. https://doi.org/10.1109/COMST.2025.3536517

[6] Runhui Zhao, Houbing Song, Hong Wen, et al. Wireless Security Enhancement Framework Based on AI and RIS in Industrial IoT Networks. *IEEE Network*, 39(4), 29–36, 2025. https://doi.org/10.1109/MNET.2025.3543829

[7] Ozkan Yildiz. Toward Intelligent and Sustainable Wireless Environments with Hybrid and AI-Enhanced RIS Strategies. *MDPI Electronics*, 14(22), 4421, 2025. https://doi.org/10.3390/electronics14224421

[8] Syed Tariq Shah, Mahmoud A. Shawky, Junaid ur Rehman Kazim, et al. Coded Environments: Data-Driven Indoor Localisation with Reconfigurable Intelligent Surfaces. *Communications Engineering*, 3, 66, 2024. https://doi.org/10.1038/s44172-024-00209-0

[9] Rong Ye, Yan Peng, Meng Yue, and Ju Lee. Physical Layer Security for IoT Application With Assistance of Active STAR-RIS. *IEEE Internet of Things Journal*, 12(24), 55949–55952, 2025. https://doi.org/10.1109/JIOT.2025.3619527

[10] Kim Son Lim, Shih Yin Ooi, Muhammad Salman Sayeed, et al. Securing the Internet of Things: Systematic Insights into Architectures, Threats, and Defenses. *MDPI Electronics*, 14(20), 3972, 2025. https://doi.org/10.3390/electronics14203972

[11] Rajni Kaur, Bhawna Bansal, Sudip Majhi, et al. A Survey on Reconfigurable Intelligent Surface for Physical Layer Security of Next-Generation Wireless Communications. *IEEE Open Journal of Vehicular Technology*, 5, 172–199, 2024. https://doi.org/10.1109/OJVT.2023.3348658

[12] Rang Liu, Ming Li, Hongyu Luo, Qian Liu, and A. Lee Swindlehurst. Integrated Sensing and Communication with Reconfigurable Intelligent Surfaces: Opportunities, Applications, and Future Directions. *IEEE Wireless Communications*, 30(1), 50–57, 2023. https://doi.org/10.1109/MWC.002.2200206

[13] Minghao Wang, Tianqing Zhu, Tao Zhang, et al. Security and Privacy in 6G Networks: New Areas and New Challenges. *Digital Communications and Networks*, 6(3), 281–291, 2020. https://doi.org/10.1016/j.dcan.2020.07.003

[14] Ahmed Elzanaty, Anna Guerra, Francesco Guidi, and Mohamed-Slim Alouini. Reconfigurable Intelligent Surfaces for Localization: Position and Orientation Error Bounds. *IEEE Transactions on Signal Processing*, 2021. https://doi.org/10.1109/TSP.2021.3101644

[15] Fabio Saggese, Kimmo Kansanen, and Petar Popovski. Localization-Based OFDM Framework for RIS-Aided Systems. In *IEEE International Conference on Communications Workshops*, Italy, 2023. https://doi.org/10.1109/ICCWorkshops57953.2023.10283593

[16] Changbao Liu and Yuexia Zhang. 5G Reconfigurable Intelligent Surface TDOA Localization Algorithm. *Electronics*, 13(12), 2409, 2024. https://doi.org/10.3390/electronics13122409

[17] Abdelghani Dahou, Syed Tariq Shah, Insaf Ullah, et al. Reconfigurable Intelligent Surfaces for Enhanced Localisation: Advancing Performance with KAN-Based Deep Learning Models. *Internet of Things*, 34, 101813, 2025. https://doi.org/10.1016/j.iot.2025.101813

[18] Mahmoud A. Shawky, Syed Tariq Shah, Qammer H. Abbasi, et al. RIS-Enabled Secret Key Generation for Secured Vehicular Communication in the Presence of Denial-of-Service Attacks. *Sensors*, 23(8), 4104, 2023. https://doi.org/10.3390/s23084104

[19] Mahmoud A. Shawky, et al. Revolutionising Vehicular Security: Lightweight Handover Authentication in RIS-Aided VANETs. In *IEEE 36th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 1–6, 2025. https://doi.org/10.1109/PIMRC62392.2025.11275330

[20] Mahmoud A. Shawky, Syed Tariq Shah, et al. Reconfigurable Intelligent Surface-Assisted Cross-Layer Authentication for Secure and Efficient Vehicular Communications. *IEEE Internet of Things Journal*, 12(24), 54450–54467, 2025. https://doi.org/10.1109/JIOT.2025.3623733

[21] Yinghan Li and Wei Yu. Localization in Multipath Environments via Active Sensing With Reconfigurable Intelligent Surfaces. *IEEE Communications Letters*, 2024. https://doi.org/10.1109/LCOMM.2024.3421370

[22] Jia Wen Xu, Menglin Wei, Lei Zhang, Vincenzo Galdi, Lianlin Li, and Tie Jun Cui. Chaotic Information Metasurface for Direct Physical-Layer Secure Communication. *Nature Communications*, 16, 5853, 2025. https://doi.org/10.1038/s41467-025-60725-1

[23] Menglin Wei, Hanting Zhao, Vincenzo Galdi, Lianlin Li, and Tie Jun Cui. Metasurface-Enabled Smart Wireless Attacks at the Physical Layer. *Nature Electronics*, 6, 610–618, 2023. https://doi.org/10.1038/s41928-023-01011-0