IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 17 June 2025, accepted 4 August 2025, date of publication 13 August 2025, date of current version 20 August 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3598502

RESEARCH ARTICLE

Multi-Eavesdropper Detection Through PHY-Aware Cell-Free AP Selection

JOÃO MARTINS[1,2], (Graduate Student Member, IEEE), FILIPE CONCEIÇÃO[1,2], (Graduate Student Member, IEEE), MARCO GOMES[1,2], (Senior Member, IEEE), VITOR SILVA[1,2], AND RUI DINIS[1,3], (Senior Member, IEEE)

[1]Instituto de Telecomunicações, 3810-193 Aveiro, Portugal
[2]Department of Electrical and Computer Engineering, University of Coimbra, 3030-290 Coimbra, Portugal
[3]Faculdade de Ciências e Tecnologia, Universidade Nova de Lisboa, 2829-516 Costa da Caparica, Portugal

Corresponding author: João Martins (jm.martins@co.it.pt)

This work was supported in part by Fundação para a Ciência e a Tecnologia / Ministério da Educação e Ciência (FCT/MEC) through the National Funds co-funded by European Regional Development Fund (FEDER); in part by the Competitiveness and Internationalization Operational Program (COMPETE 2020) of the Portugal 2020 Framework; in part by the Regional Programa Operacional (OP) Centro under Grant POCI-01-0145-FEDER-030588; in part by the Regional Operational Program of Lisbon under Grant Lisboa-01-0145-FEDER-030588; in part by the Financial Support National Public [FCT [Orçamento Estado (OE)]] under Project UIDB/50008/2020 (https://doi.org/10.54499/UIDB/50008/2020), Project UIDP/50008/2020, and Project LA/P/0109/2020, through the Grant B-0109-24 and the Ph.D. Grant SFRH/BD/08221/2021; and in part by European Cooperation in Science and Technology (COST) through the COST Action Physical layer security for trustworthy and resilient 6G systems (6GPHYSEC) under Grant CA22168.

ABSTRACT The ability to provide reliable data rates across several coverage areas establishes massive multiple-input multiple-output (m-MIMO) cell-free (CF) systems as a pivotal technology for future sixth-generation (6G) systems. CF networks do, however, introduce additional security and network integrity vulnerabilities. For that, to complement the traditional cryptographic algorithms, physical layer security (PLS) can be an effective strategy for acquiring essential wireless network information in order to develop authentication methods against impersonation attacks. To prevent these spoofing attacks, we propose leveraging the wireless channel and the access point selection (APS) allocation schemes as authentication mechanisms. Our approach begins with a threshold-based analysis of spectral efficiency (SE) losses across different APS schemes. We then propose an algorithm capable of estimating the number of eavesdroppers executing active attacks while identifying the targeted user equipment (UE). Finally, we test the robustness of our detection scheme by examining how SE loss and achievable secrecy SE change when a single attacker is positioned at various locations relative to the targeted UE. Results demonstrate that monitoring these parameters provides critical insights into network performance and the impact of active eavesdropping. These findings highlight the potential of integrating PLS with upper-layer authentication protocols to significantly enhance wireless network security.

INDEX TERMS Cell-free (CF), physical layer security (PLS), wireless authentication, access point selection (APS), active eavesdropping detection, pilot contamination attacks, spoofing attacks.

I. INTRODUCTION

Cell-free (CF) massive multiple-input multiple-output (MIMO) has emerged as a key technology for future sixth-generation (6G) systems, primarily due to its ability to deliver more consistent data rates throughout the intended coverage area [1], [2], [3], [4]. Unlike traditional massive MIMO (m-MIMO) systems, CF m-MIMO utilizes fewer antennas per access point (AP), resulting in lower cost-effective APs that can be densely deployed [5]. In these architectures, a coordinated set of APs collaboratively handles the payload transmission and reception for each user equipment (UE) and enforces uplink (UL) power control strategies aimed at optimizing a specific network utility function [6].

The associate editor coordinating the review of this manuscript and approving it for publication was Yi Fang.

However, despite the CF mMIMO advantages, this approach introduces its own set of complexities. In particular, managing the distributed cooperation among APs and coordinating signal processing for multiple UEs, whether in the downlink (DL) or UL, can be a complex task for central processing units (CPUs). This can increase fronthaul traffic, and raise computational demands, which lead to higher power consumption, ultimately compromising system scalability.

Therefore, many researchers have been exploring a more efficient strategy known as UE-centric operation within CF m-MIMO networks [7], [8], [9]. This approach involves dynamically assigning a specific subset of APs to serve each UE, rather than requiring every AP to cooperate in serving all UEs. By doing so, the system significantly reduces the processing load on CPUs, minimizes fronthaul traffic, and lowers signaling overhead. This strategy decreases the computational complexity at the APs, resulting in reduced power consumption across the network. However, the CF network topology was designed to support a fully cooperative distributed m-MIMO architecture, where traditional cell boundaries are removed, allowing UEs to be seamlessly served by multiple APs through cooperative transmission and reception.

In addition, CF networks also introduce new security vulnerabilities [10]. The growth in the number of terminal antennas and distributed APs, along with the inherent openness of wireless channels, inevitable increases the risk of malicious attacks, posing not only threats to information security but also to the overall system trustworthiness [11]. Security threats generally fall into two categories: passive and active attacks. Passive attacks primarily involve attempts to access or eavesdrop on someone else's data. In these cases, the attacker aims to observe or gather information from the system without interfering with its resources or operations. On the other hand, active attacks involve transmitting data to disrupt a communication link or impersonate another user to gain unauthorized access and modify system resources or interfere with their operations [12]. Examples of such attacks include man-in-the-middle, spoofing, denial of service (DoS), where jamming is included, replay, and message injection attacks. If successful, these attacks can result in severe consequences for the network quality of service (QoS), integrity and operation [13].

To maintain the network integrity, authentication mechanisms and data confidentiality, traditional security mechanisms are based on the assumption that the time and computational resources required to decode a cryptographic key far exceed the value of the information being protected. Consequently, the use of long keys is considered an effective method to ensure secure communications [14]. However, these traditional encryption mechanisms require significant computational resources resulting in high power consumption [15]. This is challenging for CF m-MIMO wireless networks, since the performance and usability of mobile devices but also small Internet of things (IoT) terminals depend heavily on their battery lifetime, making it crucial to avoid reducing their operational longevity [16].

In this way, physical layer security (PLS) has gained significant attention for next-generation wireless systems [17] due to its potential to develop innovative lower-layer mechanisms that can provide confidentiality and real-time authentication services by leveraging the unique physical layer (PHY) characteristics of the communication channel [18]. With this, physical key generation [19], [20] based on the channel reciprocity and artificial noise [21] techniques have demonstrated their effectiveness in addressing these challenges. On the other hand, several wireless channel features have also gathered significant attention from the scientific community for authentication and security purposes. Important authentication features include the channel state information (CSI) estimations [22], [23] and predictions [24], [25], the signal angle-of-arrival (AoA) direction [26], the received signal strength indicator (RSSI) patterns analysis [27] and the PHY fingerprints, such as the hardware and manufacturers imperfections [28].

A. RELATED WORK

Many studies have explored the incorporation of AP selection (APS) schemes into signal transmission and detection processes within CF m-MIMO networks. In [29], the authors introduce a novel UL APS scheme that includes a new signal detection method aimed at improving UL throughput. It addresses the challenge of reducing the data load exchanged over the fronthaul links between APs and CPUs, which is critical in CF networks where signal processing is distributed. The paper referenced as [30] proposes an APS approach that combines zero-forcing precoding with large-scale fading-based selection for the DL. The goal is to optimize the max-sum rate (MSR), which balances the trade-off between computational complexity and performance. The authors of [5] propose two distinct APS schemes designed for improving power efficiency. One scheme uses power control coefficients, which, though effective, comes with high computational complexity. The other scheme relies on large-scale fading coefficients, which offers a more scalable solution with lower computational overhead. In [31], a sequential APS algorithm is proposed, which evaluates the effective channel gain of UEs to determine the best APs to serve them. This method significantly reduces computational complexity by selecting a subset of APs based on long-term channel statistics. In [32], a deep reinforcement learning-based APS method is presented for DL, dynamically selecting APs to serve UEs based on their locations. The goal is to explore the trade-off between ensuring QoS and minimizing power consumption. The work in [33] introduced a centralized APS scheme for the UL of a radio stripe network. This scheme incorporates a centralized equalization technique based on match filtering, known as MRC. The goal is to concurrently enhance network spectral efficiency (SE) and ensure a balanced distribution of the load among the APs.

TABLE 1. Existing studies on active pilot contamination attacks in m-MIMO CF scenarios.

	Nº Pilots < Nº UEs	Multiple Nº AP Antennas	Nº Attackers	Main Contribution	Security Metric
[34]	No	No	Single	DL power optimization to maximize achievable secrecy SE.	Secrecy SE
[35]	No	No	Single	Trade-off analysis between DL power optimization and the achievable secrecy rate.	
[36]	No	Yes	Single	Provide a Detection method based on AoA. Trade-off analysis between DL power consumption and the UE achievable secrecy rate.	
[37]	No	Yes	Single	Maximize the SINR of the legitimate UE.	
[38]	Yes	Yes	Single	Impact of the RF impairments on the secrecy SE.	
Our Approach	Yes	Yes	Single Multiple	Detection strategy leveraging the wireless channel and the APS performance allocation. We also provide an insight study about the impact of Eve's distance to the target UE and the secrecy SE.	APS SE Losses Secrecy SE

However, only a few studies have addressed security concerns targeting spoofing attacks within the context of mMIMO-CF networks [34], [35], [36], [37], [38].

In [34], the authors propose a power allocation optimization algorithm under a single antenna network environment for all legitimate and non-legitimate agents in order to maximize the achievable secrecy SE (SSE). They also provide an analysis of this approach under co-located and different distanced positions between the targeted UE and the active eavesdropper (Eve). The authors of [35] presents a two problem analysis between maximizing the SSE and a minimization of the DL power optimization while subjected to QoS constraints. In [36], the security of CF m-MIMO systems is studied, focusing on mitigating active pilot attacks by Eves. It proposes a spatial sparsity-based pilot attack detection method and develops a power allocation algorithms for maximizing the SSE of attacked UEs and for fairness among legitimate UEs. Additionally, an AP selection scheme and conjugate beamforming are employed to boost system security. In [37], the authors formulate a maximization signal-to-noise ratio (SINR) optimization problem for the legitimate user, while constrained by a maximum allowable Eve's SINR, a maximum transmit power at each AP and guaranteeing specific SINR requirements on other legitimate UEs. They also propose a greedy APS scheme with the goal to improve the SSE. The paper [38] investigated the performance of secure transmissions impacted by RF impairments and low resolution analog-to-digital (ADC) converters. Based on these factors but also the pilots transmission power, the number of legitimate UEs and total AP antennas, they deduct an achievable ergodic secrecy expression.

B. CONTRIBUTIONS

Our work will address pilot contamination spoofing attacks that if not intercepted can be extremely harmful, as they enable attackers to impersonate legitimate UEs or devices and lead to data theft or even complete DoS disruption. Thus, it is crucial to implement spoofing countermeasures from this physical layer perspective and ensure only the necessary computational load on security upper-layer processing for device authentication [18].

In the domain of PLS countermeasures against spoofing attacks in CF m-MIMO networks, all of the previously mentioned works significantly contribute to advancing the state of the art and provide an important foundation for this paper. However, some of the existing research has limited analyses since they predominantly focus on scenarios involving a single network intrusion and do not account for the possibility of multiple spoofing intruders launching simultaneous attacks on different UEs. Our work aims to fill this literature gap by conducting a comprehensive analysis of the impact of multiple spoofing intruders. Moreover, some of these works operate under the assumption of single antenna APs, which is unrealistic in our modern mobile wireless architectures. Also, apart from [38], all of them assume that during the channel estimation (CE) phase the number of orthogonal pilots is equal to the number of UEs. This simplifies the problem while avoiding additional interference that could degrade the accuracy metrics results. We do agree, however, that in high-mobility situations, this assumption may hold true. However, these are not the cases for the previous works and may not be applicable for all mobile and IoT devices scenarios. Finally, most of these researches focus on developing dedicated security mechanism to protect against eavesdropping attacks. These specialized techniques, while effective, often add computational complexity and require additional resources which can be challenging to implement, especially in decentralized, large-scale CF networks. Hence, the network performance is treated as a constrained rather than being prioritized as the primary objective function (OF). Consequently, most of the security metrics are around the SSE metric.

In contrast, our work introduces an innovative approach to enhance PLS in the UL by leveraging some network performance metrics obtained with APS schemes, typically

employed in a CF m-MIMO context. More specifically, we leverage an APS algorithm that focuses on optimizing the MSR metric, which aims to provide the network's maximum global SE across all the UEs. We also developed a max-min fairness (MMF)-based APS scheme, whose objective is to provide total fairness across the UEs, by maximizing the SE of the UE with the worst channel conditions. Rather than introducing new, dedicated security features, our approach utilizes these existing performance metrics as indirect indicators of potential security vulnerabilities in the system. By analyzing deviations or anomalies in these metrics, we assess the presence of Eves in the network and, in turn, enhance network security through a resource-efficient method that integrates naturally into the CF network framework. This dual-purpose use of performance metrics not only maintains high network efficiency but also achieves security enhancements without the added overhead of specialized security protocols. In order to solve the MSR and MMF APS optimization problems, we adopted a meta-heuristic-based approach based on a genetic algorithm (GA) [39], whose OF directly aligns with the MSR and MMF metrics. This strategy has been widely explored for CF-mMIMO networks and presents the capability to solve non-linear optimization problems with minimal computational effort [6], [33], [40], [41], [42], [43]. Table 1 highlights the significant key differences between our work and the state of the art, outlines the primary focus of these studies and presents a simplified overview of our approach.

Therefore, the main contribution of this paper is:

- Provide a PHY Security framework for multi-eavesdropper detection and toward secure network optimization in Cell-Free (CF) systems. This framework leverages the MSR and MMF derived from the APS algorithm designed to optimize these metrics. An Hybrid (HYB) approach is also considered, which represents a combination of both previous strategies.

This is built upon the following additional contributions, which demonstrate the reliability and relevance of our findings:

- We employed a threshold analysis to understand the SE behavior of the network and to detect anomalies.
- We propose an algorithm based on the MSR and MMF and HYB SE Losses metrics that not only estimates the number of Eves performing active attacks but also detect which are the targeted UEs. To manage the algorithm's stopping criteria, an upper bound was derived based on Chebyshev inequalities.
- We evaluate the detection scheme robustness by analyzing the effect of a single Eve position relative to the targeted UE. Specifically, we conduct a performance gap analysis that compares the observed SE Losses with the achievable SSE.
- We perform a robustness evaluation of the proposed techniques using two different CF scenarios with different AP to UE densities.

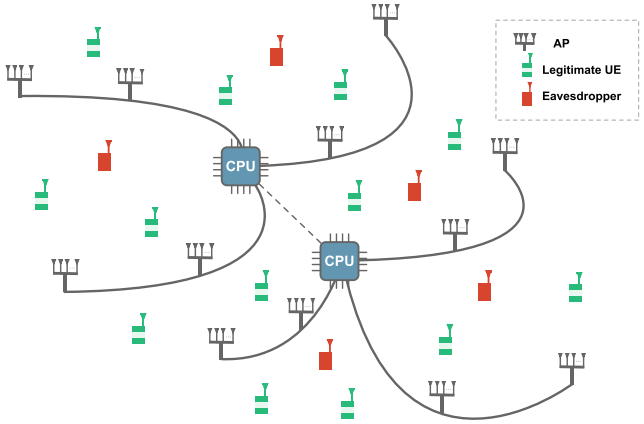


FIGURE 1. Depiction of a CF network with multi-antenna APs and single-antenna UEs and Eves.

C. OUTLINE AND NOTATION

This work is organized as follows. Section II presents the CF system model. Section III introduces our PLS authentication framework and the metrics employed. Our scenario and performance results are presented in Section IV. Section V concludes this paper.

Notation: bold lower-case lettering (e.g. $\mathbf{s}$) denotes a vector, while nonbold lower-case lettering (e.g. s) is used to denote the symbols/samples of each of those block/vectors. Furthermore, the superscripts $\mathbf{A}^T$ and $\mathbf{A}^H$ denote transpose and hermitian of the matrix $\mathbf{A}$, respectively. $\mathbb{C}$ and $\mathbb{B}$ denote the set of complex and Boolean numbers, respectively. Furthermore, $\mathbb{E}\{\}$ is the expected value operation, $\mathcal{N}_{\mathbb{C}}\left(\mu, \sigma_N^2\right)$ denotes a complex Gaussian distribution with mean μ and variance σ_N^2, respectively, $\odot$ symbolizes the Hadamard multiplication, $||\mathbf{s}||$ represents the l^2 norm and $[a]^+ = \max(a, 0)$.

II. CELL-FREE NETWORK MODEL

We consider a CF m-MIMO network consisting of randomly distributed K single-antenna legitimate UEs and L APs, each one equipped with N antennas, as illustrated in Fig. 1. The channel between AP l=1, $\cdots$, L and UE k=1, $\cdots$, K is denoted by $\mathbf{h}_{kl} \in \mathbb{C}^{N\times 1}$. We include the spatial correlation between APs' antennas. Consequently, during each coherent block interval, an independent realization of a spatially correlated channel following a Rayleigh distribution is generated. Each channel can be expressed as

$$\mathbf{h}_{kl} \sim \mathcal{N}_{\mathbb{C}}\left(\mathbf{0}_N, \mathbf{R}_{kl}\right), \tag{1}$$

where $\mathbf{R}_{kl} \in \mathbb{C}^{N\times N}$ is the spatial correlation matrix. The large-scale fading coefficients between AP l and UE k include the path-loss (PL) and shadow fading (SF) and relate to $\mathbf{R}_{kl}$ by [44]

$$\beta_{kl} = \frac{\mathrm{tr}\left(\mathbf{R}_{kl}\right)}{N}. \tag{2}$$

All APs are connected to a dedicated central processing unit (CPU) through fronthaul links and the system will be threatened from one to multiple active Eve(s) that will

attempt to intercept the legitimate wireless link information by performing a pilot spoofing attack.

A. UPLINK PILOT TRANSMISSION AND CHANNEL ESTIMATION

In the initial phase of the UL transmission frame, τ_p mutually orthogonal pilot signals, each consisting of τ_p symbols, are transmitted. Each UE k is allocated a pilot signal from the orthogonal base $\left\{\mathbf{\Phi}_t : \mathbf{\Phi}_t \in \mathbb{C}^{\tau_p \times 1} \wedge t{=}1, \cdots, \tau_p\right\}$, with a power of $||\mathbf{\Phi}_t||^2{=}\tau_p$. These pilot signals are transmitted to each AP [44]. Typically, the number of UEs in the system exceeds the number of mutually orthogonal pilot sequences, i.e., $K{>}\tau_p$, leading to pilot contamination interference in the CE vectors. Following the notation used in [44], the index of the pilot assigned to UE k is denoted as $t_{kp} \in \left\{1, \cdots, \tau_p\right\}$, and $\mathcal{P}_k \subset \{1, \cdots, K\}$ represents the subset of UEs sharing the same pilot as UE k. The received pilot signal at AP l is given by $\mathbf{Z}_l \in \mathbb{C}^{N \times \tau_p}$.

$$\mathbf{Z}_l = \sum_{k=1}^{K} \sqrt{\check{p}_k}\mathbf{h}_{kl}\mathbf{\Phi}_{t_{kp}}^T + \mathbf{N}_l, \tag{3}$$

where $\check{p}_k \geq 0$ represents the power utilized in pilot transmission for UE k, and $\mathbf{N}_l \in \mathbb{C}^{N \times \tau_p}$, follows a complex Gaussian distribution $\mathcal{N}_{\mathbb{C}}(\mathbf{0}, \sigma_N^2)$, denotes the receiver additive white Gaussian noise (AWGN) with power σ_N^2.

Utilizing the received pilot sequence, AP l can estimate the channel to each UE k by projecting $\mathbf{Z}_l$ onto the normalized pilot signal assigned to UE k, denoted as $\mathbf{\Phi}_{t_{kp}}/\sqrt{\tau_p}$, leading to the following

$$\begin{aligned}\mathbf{z}_{t_{kp}l} = \mathbf{Z}_l\mathbf{\Phi}_{t_{kp}}^*/\sqrt{\tau_p} = \sqrt{\check{p}_k\tau_p}\mathbf{h}_{kl} \\ + \sum_{k' \in \mathcal{P}_k, k' \neq k} \sqrt{\check{p}_{k'}\tau_p}\mathbf{h}_{k'l} + \mathbf{n}_{t_{kp},l}.\end{aligned} \tag{4}$$

In Eq. (4), the pilot contamination interference is attributed to the second term, where $\mathbf{n}_{t_{kp},l}$ represents the resulting noise. Assuming that the correlation matrices, $\mathbf{R}_{k'l}$, $k' \in \mathcal{P}_k$, are locally available at AP l, the CE from AP l to UE k can be performed using the MMSE technique [45]. Upon receiving the signal in Eq. (3) and considering the operation in Eq. (4), the resulting CE vector can be denoted as $\hat{\mathbf{h}}_{kl}$ and is given by:

$$\hat{\mathbf{h}}_{kl} = \sqrt{\check{p}_k\tau_p}\mathbf{R}_{kl}\mathbf{\Gamma}_{t_{kp}l}^{-1}\mathbf{z}_{t_{kp}l}, \tag{5}$$

where

$$\begin{aligned}\mathbf{\Gamma}_{t_{kp}l} &= \mathbb{E}\left\{\left(\mathbf{z}_{t_{kp}l}{-}\mathbb{E}\left\{\mathbf{z}_{t_{kp}l}\right\}\right)\left(\mathbf{z}_{t_{kp}l}{-}\mathbb{E}\left\{\mathbf{z}_{t_{kp}l}\right\}\right)^H\right\} \\ &= \sum_{k \in \mathcal{P}_k} \check{p}_k\tau_p\mathbf{R}_{kl} + \mathbf{I}_N,\end{aligned} \tag{6}$$

is the correlation matrix of the signal in Eq. (4), and the CE vector $\hat{\mathbf{h}}_{kl}$ follows a complex Gaussian distribution $\mathcal{N}_{\mathbb{C}}\left(\mathbf{0}, \hat{\mathbf{R}}_{kl}\right)$, with

$$\hat{\mathbf{R}}_{kl} = \check{p}_k\tau_p\mathbf{R}_{kl}\mathbf{\Gamma}_{t_{kp}l}^{-1}\mathbf{R}_{kl}. \tag{7}$$

The CE and its error are statistically independent, following $\hat{\mathbf{h}}_{kl} \sim \mathcal{N}_{\mathbb{C}}\left(\mathbf{0}, \hat{\mathbf{R}}_{kl}\right)$ and $\tilde{\mathbf{h}}_{kl} = \mathbf{h}_{kl} - \hat{\mathbf{h}}_{kl} \sim \mathcal{N}_{\mathbb{C}}\left(\mathbf{0}, \tilde{\mathbf{R}}_{kl}\right)$, respectively, where

$$\tilde{\mathbf{R}}_{kl} = \mathbf{R}_{kl} - \hat{\mathbf{R}}_{kl}. \tag{8}$$

B. UPLINK PAYLOAD TRANSMISSION

An APS scheme can be integrated into the UL channel and collaborate with an equalization algorithm to estimate the original signal. This integration can be represented by a Boolean matrix, $\mathbf{D} \in \mathbb{B}^{K \times LN}$, where each element, D_{km}, indicates whether UE k is intended to be served by antenna element $m{=}1, \cdots, LN$ from the APs, taking the values of 1 or 0 to signify inclusion or exclusion, respectively. The following definitions are derived from [33].

To clarify this definition, the sub-matrix $\mathbf{D}_{\bar{l}} \in \mathbb{B}^{K \times N}$, is introduced. $\mathbf{D}_{\bar{l}}$ is defined as a sub-matrix of $\mathbf{D}$, given by $\mathbf{D}{=}[\mathbf{D}_{\bar{1}}, \cdots, \mathbf{D}_{\bar{L}}]$. Furthermore, $\mathbf{D}_{\bar{l}}$ can be represented as $\mathbf{D}_{\bar{l}}{=}[\mathbf{D}_{\bar{l}\bar{1}}, \cdots, \mathbf{D}_{\bar{k}\bar{l}}, \cdots, \mathbf{D}_{\bar{K}\bar{l}}]^T$, where $\mathbf{D}_{\bar{k}\bar{l}} \in \mathbb{B}^{N \times 1}$.

With this in mind, the received UL signal at AP l, $\mathbf{y}_l \in \mathbb{C}^{N \times 1}$, can be written as

$$\mathbf{y}_l = \left(\mathbf{D}_{\bar{l}}^T \odot \mathbf{H}_l\right)\mathbf{s}_l + \mathbf{n}_l, \tag{9}$$

where $\mathbf{H}_l{=}\left[\mathbf{h}_{1l}^T, \cdots, \mathbf{h}_{Kl}^T\right] \in \mathbb{C}^{N \times K}$ represents the UL channel matrix from AP l to all UEs, and $\mathbf{s}_l{=}[s_{l1}, \cdots, s_{lK}]^T \in \mathbb{C}^{K \times 1}$ is the combined UL signal vector at AP l. The AP's l AWGN is denoted by $\mathbf{n}_l \in \mathbb{C}^{N \times 1}$, where $\mathbf{n}_l \sim \mathcal{N}_{\mathbb{C}}(\mathbf{0}, \sigma_N\mathbf{I}_N)$, and σ_N is its power. Furthermore, the symbol $\odot$ denotes the element-wise product of matrices, also referred to as the Hadamard product. We assume that the power allocated to each UE in the UL is upper-bounded by P_{max}.

Eq. (9) can be rewritten as

$$\mathbf{y}_l = \left(\mathbf{D}_{\bar{l}}^T \odot \hat{\mathbf{H}}_l\right)\mathbf{s}_l + \mathbf{w}_l, \tag{10}$$

where $\hat{\mathbf{H}}_l{=}\mathbf{H}_l{-}\tilde{\mathbf{H}}_l{=}\left[\hat{\mathbf{h}}_{1l}^T, \cdots, \hat{\mathbf{h}}_{Kl}^T\right]$ represent the matrix of MMSE-based CE vectors for AP l and $\tilde{\mathbf{H}}_l$ their corresponding errors. Additionally, $\mathbf{w}_l$ is defined by

$$\mathbf{w}_l = \left(\mathbf{D}_{\bar{l}}^T \odot \tilde{\mathbf{H}}_l\right)\mathbf{s}_l + \mathbf{n}_l, \tag{11}$$

following $\mathbf{w}_l \sim \mathcal{N}_{\mathbb{C}}(\mathbf{0}, \mathbf{\Sigma}_l)$, where

$$\mathbf{\Sigma}_l = \sum_{k=1}^{K} p_k\left(\mathbf{E}_{kl} \odot \tilde{\mathbf{R}}_{kl}\right) + \sigma_N^2\mathbf{I}_N, \tag{12}$$

and $\mathbf{E}_{kl} \in \mathbb{B}^{N \times N}$ determines the channel spatial correlation characteristics to be considered. This determination leverages the antennas from AP l which are included in the equalization of the signal from UE k in the UL. $\mathbf{E}_{kl}$ corresponds to $\mathbf{D}_{\bar{k}\bar{l}}$, with its 1 elements representing the antenna indexes from $\mathbf{D}_{\bar{k}\bar{l}}$ for UE k and AP l.

C. UPLINK PAYLOAD EQUALIZATION

The receiver scheme is based on the second level of receiver cooperation developed in [44]. It involves local CE and combining at the AP, with simplified centralized decoding

at the CPU. Thus, the lth AP preprocesses the received signal in Eq. (9) and calculates the local estimate of the data transmitted by UE k, denoted as $\hat{s}_{kl}$. This is achieved by utilizing a combining vector $\mathbf{v}_{kl} \in \mathbb{C}^{N\times 1}$, where

$$\hat{s}_{kl} = \mathbf{v}_{kl}^H \mathbf{y}_l. \tag{13}$$

In this work, we use the maximum ratio combining (MRC) technique [2], where

$$\mathbf{v}_{kl} = \hat{\mathbf{h}}_{kl}. \tag{14}$$

Subsequently, each signal in Eq. (13), is transmitted to the supporting CPU to generate a final estimation of the UE data signal, $\hat{s}_k$. This is accomplished by averaging the local estimates [2], i.e.

$$\hat{s}_k = \frac{1}{L}\sum_{l=1}^{L} \hat{s}_{kl}, \quad k = 1, \cdots, K. \tag{15}$$

The SE of UE k can be expressed by Eq. (16), as shown at the bottom of the next page, as per [44]:

where τ_c is the total number of samples in a coherence block and SINR_k represents the SINR ratio for UE k.

D. ACCESS POINT SELECTION OPTIMIZATION

The UL APS schemes developed in this paper are formalized as two optimization problems that incorporate the MSR and the MMF SE metrics. These functions are quantified in the CPU. The former aims to enhance system performance and maximize overall system capacity, while the latter has a goal of providing complete fairness towards all the UEs. The decision variables of the optimization problem are the elements of $\mathbf{D}$. This determination also governs the consideration of channel spatial correlation characteristics for matrices $\mathbf{E}_{kl}$ $\forall k, l$. All possible AP-UE association solutions are considered. Therefore, the MSR optimization problem can be formulated by

$$\begin{aligned} \mathbb{P}_{\text{MSR}}: \quad & \max_{\mathbf{D}} \quad f_1(\mathbf{D}), \\ & \overline{\text{SE}}_k > 0, \forall k, \end{aligned} \tag{17}$$

where

$$f_1(\mathbf{D}) = \sum_{k=1}^{K} \overline{\text{SE}}_k, \tag{18}$$

and the MMF optimization problem can be formulated by

$$\begin{aligned} \mathbb{P}_{\text{MMF}}: \quad & \max_{\mathbf{D}} \quad f_2(\mathbf{D}), \\ & \overline{\text{SE}}_k > 0, \forall k, \end{aligned} \tag{19}$$

where

$$f_2(\mathbf{D}) = \min_{k=1,\cdots,K} \overline{\text{SE}}_k. \tag{20}$$

In both cases, the solutions for the APS schemes were obtained by running N_a independent runs of a GA similar to the one described in [33]. The GA include a population of size N_{pop}, a parent selection with a tournament of size t_k, a crossover probability or p_r, a mutation probability of p_m, with an increasing rate of p_{mr}, a nominal value of p_{mn} and a maximum value of p_{mm}. Furthermore, the stopping criteria include a maximum number of iterations of N_m, or a maximum number of iterations without any improvement on the objective function of N_i.

III. PHY SECURITY FRAMEWORK

As mentioned earlier, CF networks have emerged as a promising paradigm for enhancing connectivity, SE, and UE experience. Despite their benefits, these systems are not immune to security threats, particularly from sophisticated Eves. One such security concern arises from an Eve equipped with advanced signal processing capabilities. Eve's attack strategy involves exploiting the key mechanisms of the network, such as pilot signal-based CE and resource allocation procedures. Specifically, we consider that an Eve can perform a spoofing attack on any UE in the network by:

- **Copying Pilot Signals**: During the UL training phase, Eve intercepts the pilot signals, with the objective of replicate and retransmit the same sequence in order to effectively pretend to be a legitimate UE.
- **Mimicking Resource Allocation**: Eve further escalates the attack by replicating the resource allocation pattern of the legitimate UE. This means that the Eves imitates the intended UE's row in the APS matrix $\mathbf{D}$.

This dual copying attack allows Eve to intercept confidential data, through Eq. (10), but also degrades the network's performance by introducing interference and disrupting legitimate UE operations, as can be analyzed by Eq. (16). Moreover, the distributed and cooperative nature of CF networks makes them particularly vulnerable to such attacks, as APs must coordinate their responses based on potentially compromised CE.

Therefore, in the presence of an Eve, the attacked UE k has its CE compromised because AP l estimates their channel with an additional interference term, following

$$\begin{aligned} \mathbf{z}_{t_{kp}l} = \mathbf{Z}_l \boldsymbol{\Phi}^*_{t_{kp}}/\sqrt{\tau_p} = \sqrt{\check{p}_k \tau_p}\mathbf{h}_{kl} + \sum_{k_e=1}^{k_E} \sqrt{\check{p}_{k_e}\tau_p}\mathbf{h}_{k_e l} \\ + \sum_{k'\in\mathcal{P}_k, k'\neq k} \sqrt{\check{p}_{k'}\tau_p}\mathbf{h}_{k'l} + \mathbf{n}_{t_{kp}l}, \end{aligned} \tag{21}$$

where k_E is the total number of Eves targeting UE k.

A. HOW THE AUTHENTICATION WORKS?

To deal with these attacks, it is essential to design a robust detection mechanism that can identify an Eve's presence on the network. In this paper, this is done at the Physical Layer illustrated in Fig. 2.

To analyze the impact of an Eve and assess the robustness of the network, we begin by considering a baseline for the CF network, without Eves, during a large number of channel coherence blocks. Therefore, we consider a large number of channel realizations, N_c, and calculate their corresponding baseline SE as a reference for system performance.

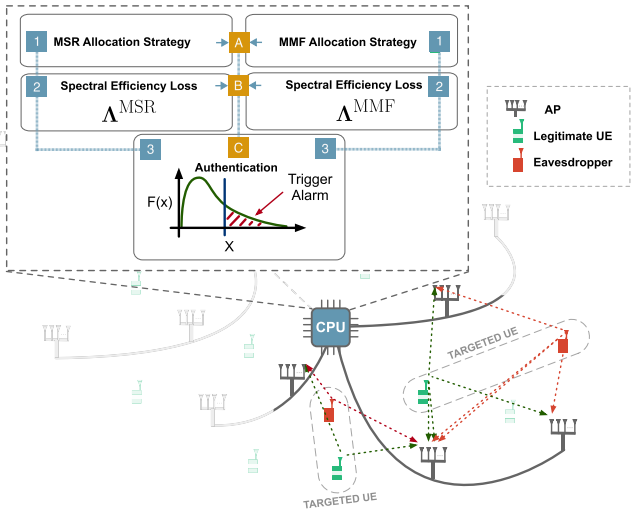


FIGURE 2. Depiction of the Eves' attacks on legitimate UEs in the CF network. The diagram shows how the SE losses are calculated for all UEs.

Then, when Eve(s) is(are) present, we define a time-domain channel window memory length (CWML), T_c, which represents the number of channel realizations of the baseline network included in the calculation of the SE in Eq. (16), according to

$$\overline{\mathrm{SE}}^{x}_{k,\mathrm{Eve}} = \frac{1}{T_c+1}\left(\mathrm{SE}^{x}_{k,\mathrm{Eve}}(t) + \sum_{i=1}^{T_c}\mathrm{SE}^{x}_{k}(t-i)\right), \quad (22)$$

with $x \in \{\mathrm{MSR}, \mathrm{MMF}\}$. With this, a new SE is calculated to capture the effects of Eve(s)' interference(s), $\overline{\mathrm{SE}}_{k,\mathrm{Eve}}$.[1] Based on this updated SE, we compute the performance loss(es) for two optimization approaches: the MMF and the MSR strategy. These loss(es), derived from Eqs. (18) and (20), respectively, provide critical insights into the system's vulnerability under Eve(s)' presence. Then, we leverage Eves' interference by quantifying and analyzing the SE(s)' loss(es) induced by them in the attacked UE(s)', allowing the network to effectively detect their presence, along with indicating the attacked UEs. We can consider the SE losses for each allocation strategy individually, according to

$$\lambda^{x}_{k} = \frac{\left|\overline{\mathrm{SE}}^{x}_{k} - \overline{\mathrm{SE}}^{x}_{k,\mathrm{Eve}}\right|}{\overline{\mathrm{SE}}^{x}_{k}}, \quad (23)$$

[1]The instantaneous SEs in Eq. (22) are calculated through Eq. (16), without the expected value operation.

or combine them into the total loss,

$$\lambda_k = \frac{\lambda^{\mathrm{MMF}}_{k} + \lambda^{\mathrm{MSR}}_{k}}{2}. \quad (24)$$

This will result in a vector of losses for each k UE as $\Lambda^{\mathrm{MMF}} = \left[\lambda^{\mathrm{MMF}}_{1}, \lambda^{\mathrm{MMF}}_{2}, \cdots, \lambda^{\mathrm{MMF}}_{K}\right]$, $\Lambda^{\mathrm{MSR}} = \left[\lambda^{\mathrm{MSR}}_{1}, \lambda^{\mathrm{MSR}}_{2}, \cdots, \lambda^{\mathrm{MSR}}_{K}\right]$, and $\Lambda = [\lambda_1, \lambda_2, \cdots, \lambda_K]$.

B. EVALUATION METRICS

Since we are addressing an open set identification problem, the system's decision-making task involves either binary classification or threshold-based analysis, denoted by ψ. Specifically, the algorithm identifies one of two possible class events: κ representing a spoofing attack, or $\widetilde{\kappa}$, representing a non-spoofing event.

Depending on the identification a detection trigger function can defined as,

$$\begin{cases} \text{flag alarm} & \kappa \quad if \quad \lambda_k > \psi \\ \text{no alarm} & \widetilde{\kappa} \quad if \quad \lambda_k < \psi, \end{cases} \quad (25)$$

Here λ_k can represent either SE losses from Eqs. (23) and (24). Therefore, under these assumptions two types of errors can emerge:

- a false alarm, or false positive (FP), indicating that there is no attack from Eve but an alarm is activated, i.e., $\mathrm{FP}_{(\psi)} = Pr(\lambda_k \geq \psi | \widetilde{\kappa})$;
- a miss detection, or false negative (FN), representing a non-detected Eve's attack, i.e., $\mathrm{FN}_{(\psi)} = Pr(\lambda_k < \psi | \kappa)$.

In turn, two classes of successful hits can appear:

- a detection, or true positive (TP), which represents a detected Eve's attack, i.e., $\mathrm{TP}_{(\psi)} = Pr(\lambda_k \geq \psi | \kappa)$.
- and finally a true negative (TN) denoting that there is no attack from Eve and the system did not trigger an alarm, i.e., $\mathrm{TN}_{(\psi)} = Pr(\lambda_k < \psi | \widetilde{\kappa})$.

The objective is to reduce the chance of triggering a false alarm while maintaining a high level of detection accuracy (ACC).

$$\mathrm{ACC} = \frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP}+\mathrm{TN}+\mathrm{FP}+\mathrm{FN}}. \quad (26)$$

Although providing a high level of accuracy to detect an Eves is necessary, this metric can be misleading since it provides equal weight to TP and TN. Therefore, as it is in our scenario, it will provide a biased analysis since the number of Eves, M, is not proportional to the number of UEs in the

$$\overline{\mathrm{SE}}_{k} = \left(1-\frac{\tau_p}{\tau_c}\right)\mathbb{E}\left\{\log_2\left(1+\mathrm{SINR}_k\right)\right\} =$$
$$= \left(1-\frac{\tau_p}{\tau_c}\right)\log_2\left(1+\frac{p_k\left|\sum_{l=1}^{L}\mathbb{E}\left\{\mathbf{v}^{H}_{kl}\left(\mathbf{D}^{T}_{\bar{l}l}\odot\hat{\mathbf{h}}_{kl}\right)\right\}\right|^2}{\sum_{k'=1,k'\neq k}^{K}p_{k'}\mathbb{E}\left\{\left|\sum_{l=1}^{L}\mathbf{v}^{H}_{kl}\left(\mathbf{D}^{T}_{\bar{k}'l}\odot\hat{\mathbf{h}}_{k'l}\right)\right|^2\right\}+\sigma^2_N\sum_{l=1}^{L}\mathbb{E}\left\{\left|\left|\mathbf{D}^{T}_{\bar{k}l}\odot\mathbf{v}_{kl}\right|\right|^2\right\}}\right), \quad (16)$$

network. So in other words, the system can achieve a high accuracy by simply predicting "no attack" for most UEs.

Therefore the precision (PREC), recall (REC), and F1-score (F1) metrics are more meaningful. The precision tells us you how many of the detected attacks are actual attacks (important to avoid false alarms) while the recall reflects how many of the actual attacks were detected (important to detect attacks). They can be expressed as follows:

$$\text{PREC} = \frac{\text{TP}}{\text{TP} + \text{FP}}, \tag{27}$$

and

$$\text{REC} = \frac{\text{TP}}{\text{TP} + \text{FN}}. \tag{28}$$

Finally, the F1-score can be a harmonic mean quantification of both these two metrics, balancing both FPs and FNs.

$$\text{F1} = 2 \times \frac{\text{PREC} \times \text{REC}}{\text{PREC} + \text{REC}}. \tag{29}$$

IV. PERFORMANCE RESULTS

In this section, the performance results obtained for each employed CF scenario will be presented.

A. SCENARIO DESCRIPTION

The large-scale fading model follows the Urban Microcell propagation model proposed by 3rd Generation Partnership Project (3GPP) in [46, Table B.1.2.1-1]. All of the parameters' values used throughout the simulations for two distinct scenarios (**P1** and **P2**) are summarized in table 2. Additionally, we consider 1000 different instances of Eve(s)' attacks for both scenarios. The pilot assignment algorithm for UEs employs a greedy strategy as described in [2], and the multipath signal components of UEs arrive at the AP based on a Gaussian distribution with a standard deviation of σ_ϕ degrees around the angle between each AP and UE [45]. We assume that each Eve targets a random UE within the CF network. The positions of the Eve(s) are considered to be close to their respective target UEs, with a random displacement of up to 1 m in each direction.

In our simulations, we considered that the total number of L APs and K UEs are uniformly distributed in a squared D total area. We also consider a multi-Eve scenario depending on the K and L dimensions. Therefore $M \in \{1, 2, \ldots, \lfloor 0.3 \times K \rfloor\}$ and the network based on the following strategies needs to ensure it detects each one of them with success.

Furthermore, the GA parameters' values are summarized in table 3.

B. SPECTRAL EFFICIENCY LOSSES DISTRIBUTION

We conducted a Monte Carlo simulation study to evaluate SE losses in the presence of Eves. The scenario mirrored the setup described in **P1**, with SE losses recorded under various conditions: no attack, a single Eve attacking one UE, two Eves targeting two different UEs, and four Eves attacking four separate UEs. The results of this analysis are depicted

TABLE 2. List of parameters for the simulated scenarios.

		P1	P2
Parameter	**Variable**	**Value**	
Carrier frequency	f_c	3.5 GHz	
AP antenna height	h_{AP}	15 m	10 m
UE antenna height	h_{UE}	1.5 m	
SF variance	σ_{sf}	2 dB	
AP/UE SF contributions	Δ	0.7	
Distance for SF model	d_{sf}	13 m	
Decorrelation distance from the SF model	d_c	9 m	
Multipath angular standard deviation	σ_ϕ	5 °	
Total number of APs	L	10	10
Number of antennas per AP	N	4	2
Number of channel realizations	N_c	100	
Maximum UE transmission power	P_{max}	100 mW	30 mW
Number of orthogonal pilots	τ_p	11	6
Number of legitimate UEs	K	15	8
Number of Eves	M	$\{1, ..., 4\}$	$\{1, 2\}$
Total area	D	100 m × 100 m	20 m × 20 m
Bandwidth	B	500 MHz	250 MHz
Channel coherence	τ_c	1000	
Noise power	N_0	−84.99 dBm	−88 dBm
CWML	T_c	$\{0, 1, 5, 10, 25, 50, 100\}$	

TABLE 3. List of GA parameters.

Parameter	**Variable**	**Value**
Maximum number of iterations	N_m	10000
Maximum iterations without improvement	N_i	100
Size of the population	N_{pop}	100
Independent attempts	N_a	10
Size of the tournament	t_k	2
Crossover probability	p_r	1
Mutation probability	p_m	0.02
Increase rate of p_m	p_{mr}	0.01
Nominal value of p_m	p_{mn}	0.02
Maximum value of p_m	p_{mm}	0.1

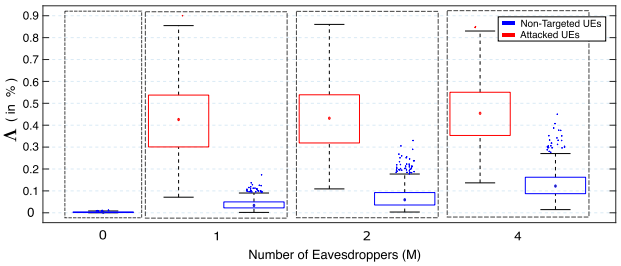


FIGURE 3. UEs' SEs losses distributions for the cases of no attack, one Eve, two Eves and four Eves in scenario $\mathbf{P_1}$.

in Fig. 3, which presents the error distribution across these cases. To contextualize the choice of SE losses as a metric in this figure, we assume a coherence time $T_c = 100$ and leverage the vector of losses $\mathbf{\Lambda}$ in Eq. (24) metric to support our analysis.

The results depicted in the figure showcase the potential of SE losses as a reliable indicator of pilot contamination attacks. The error spread for the attacked UEs is significant and remains nearly constant despite the increase in M. Notably, a key observation is that increasing M within the network results in higher individual $\mathbf{\Lambda}$ values for the non-targeted UE, thereby broadening the SE loss distribution

among these UEs. Interestingly, even the presence of a single Eve introduces a substantial degradation in SE across the network, highlighting the vulnerability of the system to such intrusions. This finding emphasizes the importance of detecting and mitigating pilot contamination attacks, as the resulting SE losses not only affect the targeted UEs but can also propagate disruptions across non-targeted UEs, leading to instability in the CF network.

C. THRESHOLD ANALYSIS

The results in Fig. 3 offered valuable insights for our decision-making analysis, motivating the adoption of a threshold-based methodology. This approach relies on defining a critical threshold value, ψ, derived from statistical knowledge or system-specific requirements, based on the metrics ACC, PREC, REC and F1, defined by (26)-(29). By doing so, it not only enhances the results interpretability but also establishes a systematic framework to guide decisions across diverse scenarios.

Fig. 4 illustrates an example of how the results for these metrics are presented and interpreted. This serves as a reference for the results shown later in Figs. 5 and 6, which correspond to scenarios **P1** and **P2** under different APS strategies (i.e., MSR, MMF, or a combined approach) and CWMLs. The performance results are primarily visualized through areas of interest, determined by the given metrics the employed CWML. The optimal operating region corresponds to the point of highest ACC or its adjacent curve points. A threshold, ψ, set below this region leads to low ACC performance, while significantly above it results in undesirable outcomes, as discussed in detail in the previous section. Additionally, the green-shaded region represents a trade-off zone, which can be considered if the security network deployer prioritizes either PREC and REC performance. The intersection of these metrics serves as an equilibrium point, where neither metric is favored over the other.

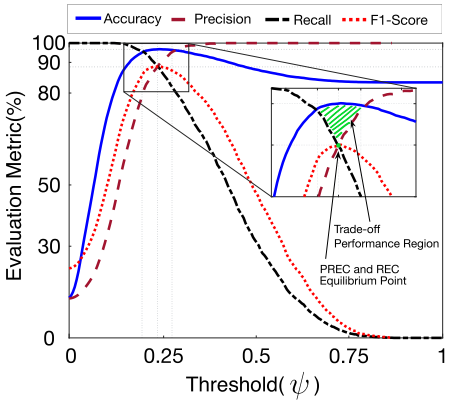


FIGURE 4. Threshold performance results layout, showing the areas of interest.

The subsequent Figs. in 5 (a)-(d) illustrate the performance metrics across different scenarios for **P1**. The analysis covers the cases with one, two, three, and four instances of Eve(s). Similarly, for scenario **P2**, the performance metrics are evaluated in Figs. 6 (a)-(b) for cases with one and two instances of Eve(s). It is important to note that the eavesdroppers are randomly selected to attack a given UE across multiple simulation runs, ensuring a diverse set of conditions.

The first key insight is that we must consider as much from the earlier channel measurements to compute Eqs. (23) and (24) as possible, i.e. a moderate-high value fo the CWML (T_c), particularly in terms of precision, recall, and F1-score. A reasonable detection performance begins to emerge only when $T_c > 10$. On the other hand, it is evident that increasing to much the CWML memory does not provide significant benefits. The difference for $T_c \in \{50, 100\}$ is minimal, making a higher memory allocation unnecessary.

Secondly, relying solely Λ^{MMF} is insufficient for a good detection performance across all metrics, which show, in this case, modest results. Therefore Λ^{MSR} serves as a better performance indicator, while a slightly more optimized performance in all evaluation parameters is achieved by considering Λ.

Lastly, as expected, increasing the number of Eves in the network leads to a notable decline in accuracy. For instance, focusing on the Λ trade-off performance region, defined in Fig. 4, the maximum achieved accuracy drops from 98.92% to 89.36% across both scenarios, with PREC ranging from $[94.47\% - 82.47\%]$ and REC from $[97.2\% - 89\%]$.

In essence, this approach is particularly valuable due to its efficiency and straightforward implementation, making it a suitable option for practical applications. However, the main issue is that as the number of Eves in the CF network increases, the percentage loss in the evaluation metrics becomes significantly more pronounced. Therefore, its effectiveness is highly dependent on how well the threshold is defined. A poorly chosen threshold can lead to increased sensitivity or reduced accuracy in detecting the Eve(s) presence, highlighting the need for a careful balance between precision and robustness. On the other hand, establishing an optimal threshold range that accommodates all possible Eves' situations would be insufficient to detect all attackers with precision. This is because the dynamic range of thresholds that yields the best detection performance heavily depends on the number of attackers present in the network. Consequently, it is crucial to first accurately identify the number of Eves before considering applying this analysis.

D. ITERATIVE MULTI-EVE DETECTION

Once again, establishing the previous threshold techniques would be challenging, as it requires careful consideration based on the precise number of attackers in the network. A poorly chosen threshold could result in incorrect decisions and significantly increase the error percentages of the evaluation metrics. Moreover, accurate prior knowledge of the number of eavesdroppers inside the network is essential to minimize such errors. Given these constraints, we will propose, in this sub-section, an iterative multi-eve detection technique/algorithm, focusing on the SE losses derived from

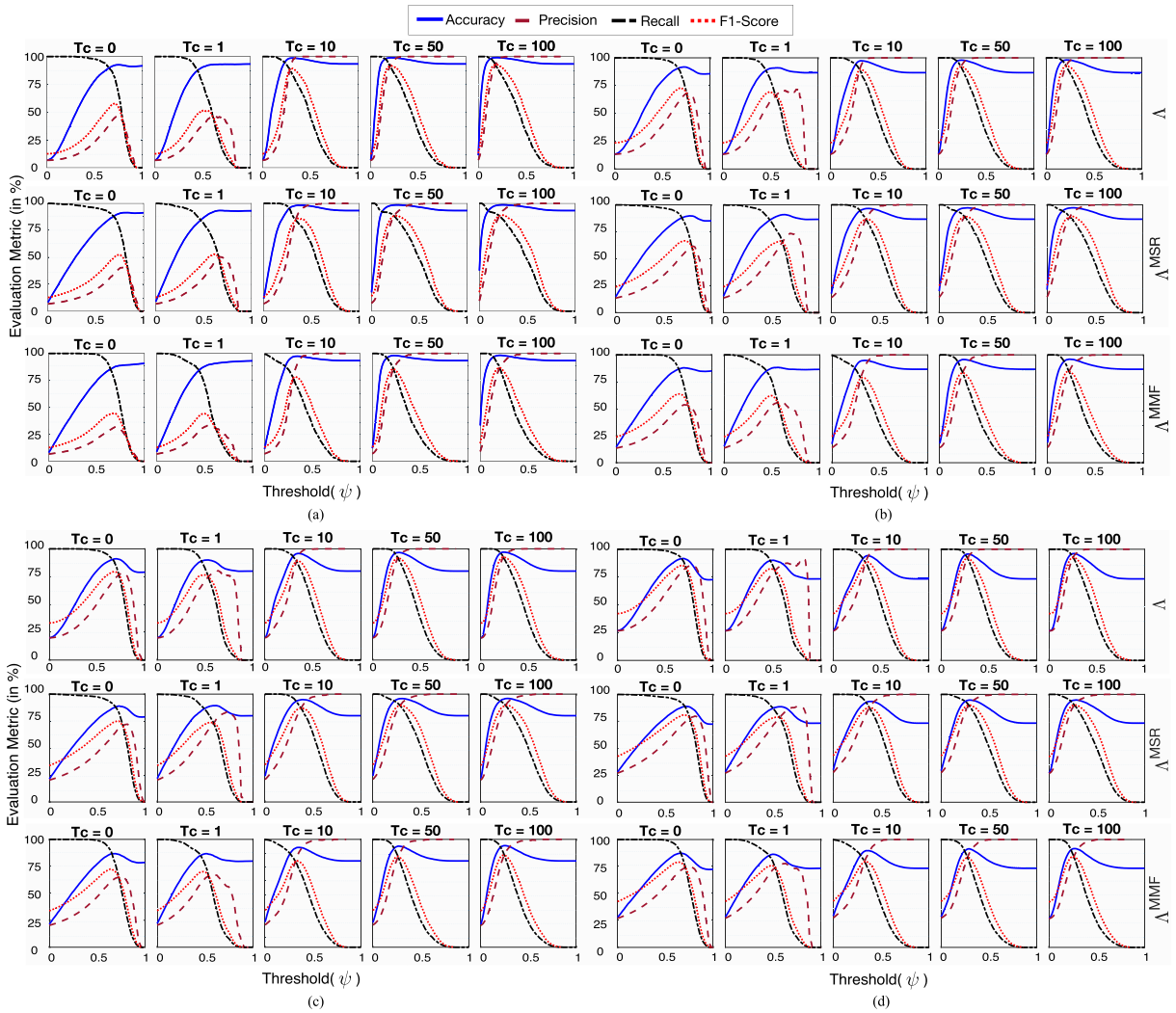


FIGURE 5. Scenario $\mathbf{P_1}$ threshold analysis performance for (a) 1 Eve, (b) 2 Eve, (c) 3 Eves and (d) 4 Eves: here we showcase the trade-off detection capabilities (ACC, PREC, REC and F1 in %) using different CWMLs in Λ, $\Lambda^{\mathbf{MSR}}$, and $\Lambda^{\mathbf{MMF}}$.

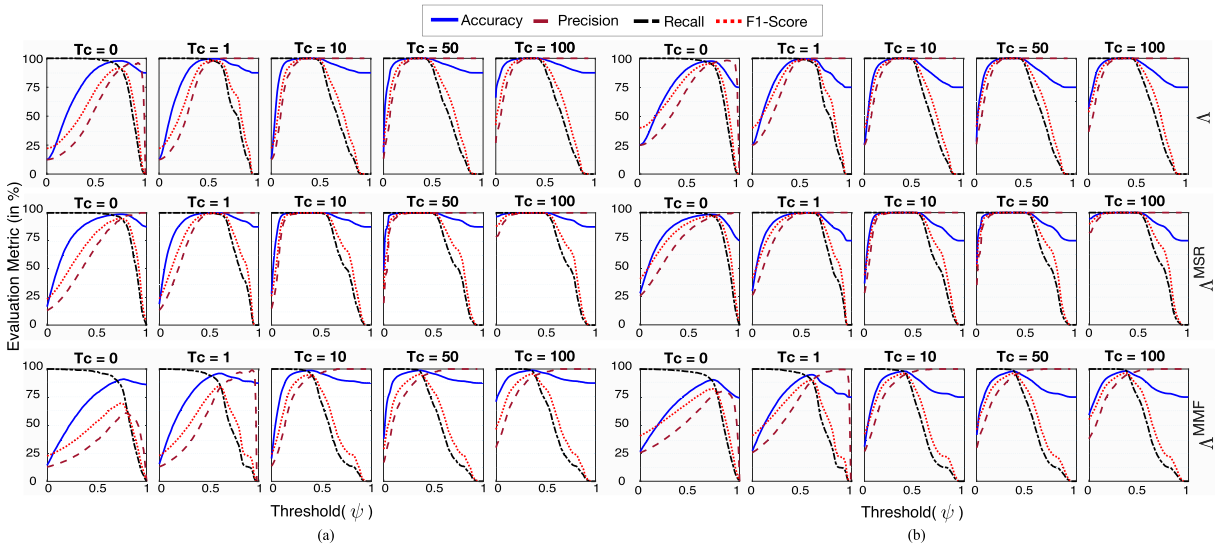


FIGURE 6. Scenario P2 threshold analysis performance for (a) 1 Eve and (b) 2 Eves: here we showcase the trade-off detection capabilities (ACC, PREC, REC and F1 in %) using CWMLs in Λ, $\Lambda^{\mathbf{MSR}}$, and $\Lambda^{\mathbf{MMF}}$.

TABLE 4. Chebyshev inequalities and upper bounds for every observation window.

T_c	$P(\lambda_k >= \text{UB}_k)$	UB_k
0	0.4	$\mu_k^{\text{NE}} + \sqrt{\frac{5}{3}}\zeta_k^{\text{NE}}$
1	0.8	$\mu_k^{\text{NE}} + \sqrt{5}\zeta_k^{\text{NE}}$
5	0.96	$\mu_k^{\text{NE}} + \sqrt{40}\zeta_k^{\text{NE}}$
10	0.98	$\mu_k^{\text{NE}} + \sqrt{50}\zeta_k^{\text{NE}}$
25	0.98	$\mu_k^{\text{NE}} + \sqrt{50}\zeta_k^{\text{NE}}$
50	0.99	$\mu_k^{\text{NE}} + 10\zeta_k^{\text{NE}}$
100	0.99	$\mu_k^{\text{NE}} + 10\zeta_k^{\text{NE}}$

$\mathbf{\Lambda}$, as defined in (24), since this metric has consistently provided the best results in our previous analysis.

To address this challenge, we propose Alg. 1, which presents an iterative procedure to identify UEs associated with high SE loss values in the $\mathbf{\Lambda}$ vector serving as an indicator of a potential Eve's presence and attack, based on the analysis of results from Fig. 3. Specifically, in an offline mode, we iteratively remove a UE k from the network, thus concurrently removing the interference generated by the Eve sharing the same row of the APS matrix in $\mathbf{D}$, i.e., $\mathbf{D}_{k\bar{1}}$ to $\mathbf{D}_{k\bar{L}}$. This removal occurs when λ_k exceeds a predefined upper bound for UE k. In each iteration, the SE of the reduced system and its corresponding APS matrix are recalculated. This process is repeated until $\mathbf{\Lambda}$ exhibits low values across all UEs, at which point we assume that no Eves remain in the network.

To define the upper bounds of the SE losses for each UE as stopping criteria, we leverage the vector of SE losses associated with the case where there are no Eves in the CF network., i.e., $\mathbf{\Lambda}^{\text{NE}}$, similar to the one used to generate the first column of Fig. 3. The bounds are derived using Chebyshev's inequality, which enable us to quantify the probability that a random variable deviates from its mean by a certain number of standard deviations, as shown in Eq. (30). In other words, this allows us to establish a conservative upper bound, based on SE losses, that any UE should not exceed under normal conditions, i.e., attack free conditions.

$$P(\lambda_k \geq \text{UB}_k) \geq 1 - \frac{\left(\zeta_k^{\text{NE}}\right)^2}{\left(\text{UB}_k - \mu_k^{\text{NE}}\right)^2}, \tag{30}$$

where, in this case, the probability operation includes the values of $\mathbf{\Lambda}$ for UE k when the CF network is attacked by an arbitrary value of M, μ_k^{NE} is the mean of $\mathbf{\Lambda}^{\text{NE}}$ for UE k. Furthermore, ζ_k^{NE} is its standard deviation, and $\mathbf{UB} \in \mathbb{C}^{K\times 1}$ is the upper bound vector for all UEs. The values are adjusted accordingly to ensure robust decision-making. Furthermore, the inequality can be relaxed based on the value of T_c applied in the analysis. This relaxation provides additional flexibility. Therefore, the values of UB_k can be obtained by

$$\text{UB}_k \geq \mu_k^{\text{NE}} + \sqrt{\frac{1}{1 - P(\lambda_k \geq \text{UB}_k)}}\zeta_k^{\text{NE}}. \tag{31}$$

The values of Eqs. (30) and (31) for the different CWMLs, T_c, are represented in table 4.

The pseudocode for the algorithm described in this section is provided in the following Alg. 1.

Algorithm 1 Number of Eve(s) Estimation and Corresponding Detection

Require: $\mathbf{\Lambda}^{\text{NE}}, K, L, N, \mathbf{UB}, T_c, \mathbf{D}, \hat{\mathbf{H}}$

$\mu_k^{\text{NE}} = \mathbb{E}\left\{\Lambda^{\text{NE}}\right\}, k = 1, \cdots, K$
$\zeta_k^{\text{NE}} = \text{std}\left\{\Lambda^{\text{NE}}\right\}, k = 1, \cdots, K$
Obtain UB_k according to Eq. (31) and table 4
$m \leftarrow 0$
$\mathcal{K} \leftarrow \{1, \cdots, K\}$
while there is any $k \in \mathcal{K}$ that $\lambda_k > \text{UB}_k \wedge m \leq K$ **do**
  Calculate $k_{max} = \max\{\lambda_k\}$, for $k \in \mathcal{K}$ and consider this UE as being attacked
  Determine f as the corresponding Eve by matching the same row of the APS matrix $\mathbf{D}$
  Remove k_{max} from $\mathcal{K}$
  Compute $\bar{\text{SE}}_k^{\text{MSR}}$ and $\bar{\text{SE}}_k^{\text{MMF}}$ from the stored values obtained for baseline network without any Eve, based on Eqs. (18) and (20) for the indexes in $\mathcal{K}$.
  Compute $\bar{\text{SE}}_{k,\text{Eve}}^{\text{MSR}}$ and $\bar{\text{SE}}_{k,\text{Eve}}^{\text{MMF}}$ based on Eqs. (18) and (20) for the indexes in $\mathcal{K}$ considering that f is removed from the network.
  Compute $\mathbf{\Lambda}$ based on Eqs. (23) and (24).
  $m \leftarrow m + 1$
end while
$M \leftarrow m$

TABLE 5. Scenario P1: algorithm accuracy (in %) for the estimated number of Eves.

NºEves	CWML (Tc) 0	1	5	10	25	50	100	NºEves Estimated
0	41.2	93.8	100	100	100	100	100	0
	6.7	1.4	0	0	0	0	0	1
	22.2	2.7	0	0	0	0	0	2
	15.9	1.6	0	0	0	0	0	3
	6.4	0.5	0	0	0	0	0	4
1	3.9	6.3	21.1	16.5	4.4	0.5	0	0
	31.9	43	62	80.1	95.1	99.5	100	1
	38.3	34.1	16.1	2.6	0.4	0	0	2
	16.2	13.1	0.8	0.5	0.1	0	0	3
	7.5	2.9	0	0	0	0	0	4
2	0.3	1.3	4.4	1.7	0.3	0	0	0
	8.2	17.8	21.3	21.8	5.7	0.4	0	1
	35.3	40.5	60.9	72.4	93.5	98.5	99.9	2
	31.6	28.1	12.1	2.9	0.5	1.1	0.1	3
	15.9	9.8	1.3	0.9	0	0	0	4
3	0	0.5	0.4	0	0	0	0	0
	1.4	4.4	4.7	2.5	0	0	0	1
	13.8	17.2	26.3	24	8.6	6.4	0	2
	37.9	44.4	58.3	66.7	91	98.5	99.9	3
	28.7	24.8	9.6	5.3	0.4	1.1	0.1	4
4	0	0.1	0.2	0	0	0	0	0
	0	0.6	1.1	0.1	0	0	0	1
	1.9	5.1	7.4	3.9	0.1	0	0	2
	15	22.7	28.4	26.4	10.5	0.5	0	3
	42.4	47.7	51.9	61.5	89.3	97.6	99.9	4

1) PERFORMANCE IN ESTIMATING THE NUMBER OF EVES

The previously described iterative multi-Eve detection algorithm allows us to estimate the presence of M

TABLE 6. Scenario P2: algorithm accuracy (in %) for the estimated number of Eves.

NºEves	CWML (Tc) 0	1	5	10	25	50	100	NºEves Estimated
0	53,3	90.3	100	100	100	100	100	0
	3.9	1.1	0	0	0	0	0	1
	26.3	6.8	0	0	0	0	0	2
	12.4	1.8	0	0	0	0	0	3
1	0.1	0	0	0	0	0	0	0
	54	81.2	100	100	99.9	100	100	1
	31.8	16.8	0	0	0.1	0	0	2
	10.5	2	0	0	0	0	0	3
2	0	0	0	0	0	0	0	0
	0.2	0	0	0	0	0	0	1
	60	83.7	100	100	100	100	100	2
	29.3	15.6	0	0	0	0	0	3

eavesdroppers in the CF network. The accuracy results are presented in tables 5 and 6 for scenarios **P1** and **P2**, respectively, with the simulation assumptions remaining the same as in the previous analysis. However, we also explored the scenario where no eavesdroppers are present in the network, representing its normal operation without any attacks on legitimate users. Thus, the number of Eves in the network is displayed in the left column while the right column shows the algorithm's estimation.

The previous results provide an even more evident and deterministic conclusion that increasing the CWML, T_c; enhances the algorithm's capability to achieve high performance. Overall, around $T_c = 25$ may be considered the minimum value required to start achieving good results, while $T_c = 100$ appears excessive compared to the gains achieved with a smaller window of 50. Interestingly, the smaller and less populated **P2** scenario can achieve the perfect accuracy score starting from $T_c = 5$.

2) PERFORMANCE IN DETECTING USERS UNDER EVES' ATTACKS

The last section showcased the algorithm's accuracy in estimating the number of Eves inside the network. The same algorithm outlined can also be used by the CPU to identify which UE(s) is(are) being targeted by an attacker. This is done in instruction (9) where the algorithm iteratively removes the target user from the set $\mathcal{K}$. We can apply a similar statistical analysis to identify the attacked UEs, using not only the accuracy evaluation metric but also considering the precision, recall, and F1-score. However, since the PREC and REC metrics are often close, we only present the F1 alongside the ACC in figures 7 and 8 for scenarios **P1** and **P2**, respectively.

The results are similar. However, the key takeaway from this finding is that it is possible to correctly identify with high precision and recall which specific UEs are under a spoofing attack. Finally, we show that this strategy also adds value in situations where the system is operating under normal conditions, without triggering high-accuracy false alarms. This is essential for maintaining network stability and ensuring reliable detection performance.

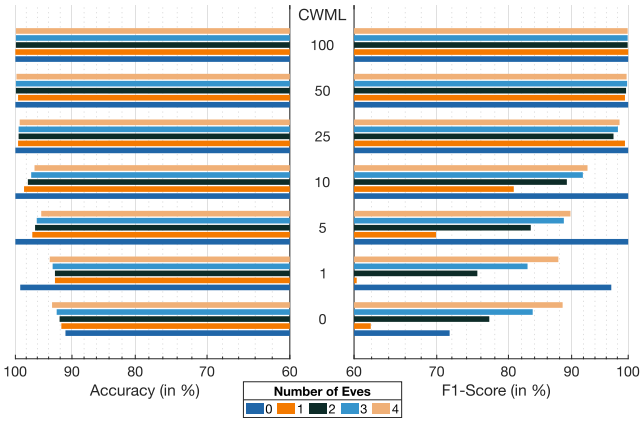


FIGURE 7. Scenario P1: algorithm's F1 vs ACC (in %) for detecting the targeted attacked UEs.

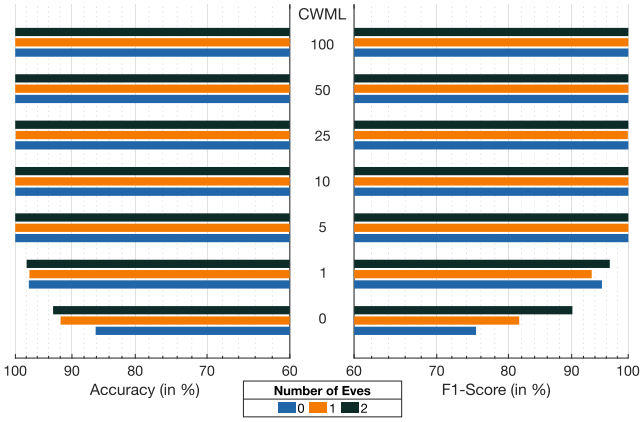


FIGURE 8. Scenario P2: algorithm's F1 vs ACC (in %) for detecting the targeted attacked UEs.

E. IMPACT OF EVE'S DISTANCE ON USER SPECTRAL EFFICIENCY AND SECRECY

In this section, we evaluate how the Eavesdropper relative distance to its target UE affects the attack detection scheme. Specifically, we assume that Eve is randomly positioned above a circumference centered on the UE's position, with a radius r (in meters). Taking into account the total area, D, of the CF network, we define the radius vectors as $r_{\mathbf{P1}} = [0, 1, 2, 3, 5, 10, 15, 20, 30, 40, 50]$ and $r_{\mathbf{P2}} = [0, 1, 2, 3, 5, 8, 9, 10, 13, 15, 18]$ for **P1** and **P2**, respectively. When $r_{\mathbf{P1}}{=}r_{\mathbf{P2}} = 0$, we assume that Eve is positioned at the exact location of the UE, separated by a distance equal to half of the wavelength.

We analyze the trade-off between the SE losses of a UE under attack and the secrecy SE (SSE) towards Eve, as a function of their distance. For that, we present the average SSE for the attacked UEs. Assuming that, in one instance, k' is the UE attacked by the Eve denoted as ε, the instantaneous SSE of UE k' can be calculated through

$$\mathrm{SSE}_{k'}(t) = \frac{1}{2} \sum_{x \in \{\mathrm{MSR,MMF}\}} [\mathrm{SE}^{x}_{k',\mathrm{Eve}}(t) - \mathrm{SE}^{x}_{\varepsilon}(t)]^{+}, \quad (32)$$

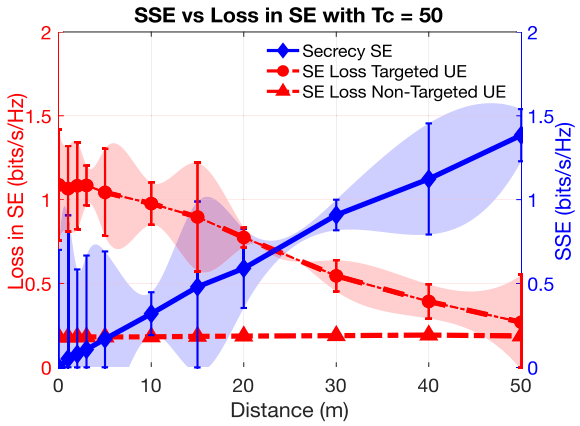


FIGURE 9. SE loss and SSE as a function of the distance for scenario P1.

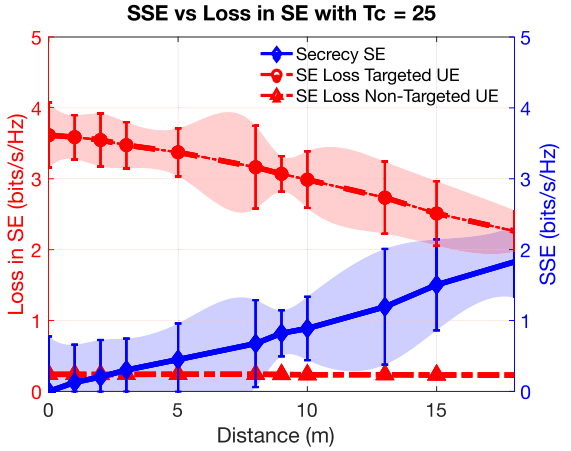


FIGURE 10. SE loss and SSE as a function of the distance for scenario P2.

and the average linear SE losses measured at the attacked UEs can be obtained with

$$\lambda^{x}_{k',\text{Eve}} = \frac{1}{2} \sum_{x \in \{\text{MSR},\text{MMF}\}} \left| \overline{\text{SE}}^{x}_{k'} - \overline{\text{SE}}^{x}_{k',\text{Eve}} \right|, \tag{33}$$

while for the non-attacked UEs the same Eq. (33) can be used for $k \neq k'$. Figs. 9 and 10 show these metrics as a function of the distance, for $T_c = 50$ and $T_c = 25$ in scenarios **P1** and **P2**, respectively, since these CWML values have proven effective in the previous analysis. For scenario **P1**, we conclude that the Eve detection scheme based on SE losses is effective at smaller distances. Furthermore, as the distance increases, Eve's interference on the SE of the targeted UE decreases significantly, resulting in SE loss values similar to those observed for non-attacked UEs. Interestingly, the SSE has the opposite effect, as it increases rapidly with distance. However, higher SSE values indicate that Eve's ability to intercept information intended for the targeted UE is significantly reduced, ensuring undisturbed communication. This occurs because the optimized APS scheme considers the position of the targeted UE, making resource allocation less favorable for more distant Eves. A similar conclusion applies to scenario **P2**. However, since the area in this case is smaller, the Eve detection method proves effective across nearly all distances. We did not extend the results to include more Eves, as this would lead to a more significant increase in SE losses for the attacked UE compared to the non-attacked ones.

V. CONCLUSION

In conclusion, this work introduces a new approach to strengthen PLS in CF m-MIMO networks by leveraging MSR and MMF metrics as indirect indicators of spoofing eavesdropping vulnerabilities. Unlike traditional methods, our approach boosts security and SE without adding extra computational overhead.

We use a threshold analysis to detect unusual changes in SE that may indicate an attacker. To improve this scheme, we apply an iterative method to identify possible eavesdroppers and their targeted UEs, stopping when the SE loss values show no attacker is present. We also study the effect of the attacker's distance and find that our method successfully detects eavesdroppers in most cases. At greater distances, the SSE stays high enough to ensure secure communications.

Future work could integrate the APS strategy with a secrecy metric to proactively enhance security by allowing the network to ensure secure communications from the start, minimizing potential vulnerabilities before an attack occurs.

REFERENCES

[1] J. Zhang, S. Chen, Y. Lin, J. Zheng, B. Ai, and L. Hanzo, "Cell-free massive MIMO: A new next-generation paradigm," *IEEE Access*, vol. 7, pp. 99878–99888, 2019.
[2] H. Q. Ngo, A. Ashikhmin, H. Yang, E. G. Larsson, and T. L. Marzetta, "Cell-free massive MIMO versus small cells," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1834–1850, Mar. 2017.
[3] E. Björnson and L. Sanguinetti, "Scalable cell-free massive MIMO systems," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4247–4261, Jul. 2020.
[4] H. Q. Ngo, G. Interdonato, E. G. Larsson, G. Caire, and J. G. Andrews, "Ultradense cell-free massive MIMO for 6G: Technical overview and open questions," *Proc. IEEE*, vol. 112, no. 7, pp. 805–831, Jul. 2024.
[5] H. Q. Ngo, L.-N. Tran, T. Q. Duong, M. Matthaiou, and E. G. Larsson, "On the total energy efficiency of cell-free massive MIMO," *IEEE Trans. Green Commun. Netw.*, vol. 2, no. 1, pp. 25–39, Mar. 2018.
[6] F. Conceição, C. H. Antunes, M. Gomes, V. Silva, and R. Dinis, "Max-min fairness optimization in uplink cell-free massive MIMO using meta-heuristics," *IEEE Trans. Commun.*, vol. 70, no. 3, pp. 1792–1807, Mar. 2022.
[7] Ö. T. Demir, E. Bjrnson, and L. Sanguinetti, *Foundations of User-Centric Cell-Free Massive MIMO*. Boston, MA, USA: Now, 2021.
[8] S. Buzzi and C. D'Andrea, "Cell-free massive MIMO: User-centric approach," *IEEE Wireless Commun. Lett.*, vol. 6, no. 6, pp. 706–709, Dec. 2017.
[9] H. A. Ammar, R. Adve, S. Shahbazpanahi, G. Boudreau, and K. V. Srinivas, "User-centric cell-free massive MIMO networks: A survey of opportunities, challenges and solutions," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 611–652, 1st Quart., 2022.
[10] S. Elhoushy, M. Ibrahim, and W. Hamouda, "Cell-free massive MIMO: A survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 492–523, 1st Quart., 2022.
[11] J. Karoliny, B. Etzlinger, R. Khanzadeh, A. Springer, and H.-P. Bernhard, "Network support layers trustworthiness computation for wireless networks," *IEEE Trans. Commun.*, vol. 73, no. 3, pp. 1879–1894, Mar. 2025.
[12] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.

[13] W. Stallings, *Cryptography and Network Security: Principles and Practice*. London, U.K.: Pearson, 2022.

[14] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[15] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory To Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[16] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2702–2733, 3rd Quart., 2019.

[17] M. Mitev, T. M. Pham, A. Chorti, A. N. Barreto, and G. Fettweis, "Physical layer security—From theory to practice," *IEEE BITS Inf. Theory Mag.*, vol. 3, no. 2, pp. 67–79, Jun. 2023.

[18] J. Zhang, G. Shen, W. Saad, and K. Chowdhury, "Radio frequency fingerprint identification for device authentication in the Internet of Things," *IEEE Commun. Mag.*, vol. 61, no. 10, pp. 110–115, Oct. 2023.

[19] M. A. Aygtil, H. A. Cirpan, and H. Arslan, "A novel physical layer secret key generation method for wireless sensor networks," in *Proc. IEEE Int. Black Sea Conf. Commun. Netw. (BlackSeaCom)*, Jun. 2024, pp. 231–235.

[20] E. Dehmollaian, B. Etzlinger, and A. Springer, "A lightweight CIR-based physical layer key generation scheme for UWB," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2024, pp. 1–6.

[21] D. A. Tubail, M. Alsmadi, and S. Ikki, "Physical layer security in downlink of cell-free massive MIMO with imperfect CSI," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 2945–2960, 2023.

[22] F. Pan, H. Wen, R. Liao, Y. Jiang, A. Xu, K. Ouyang, and X. Zhu, "Physical layer authentication based on channel information and machine learning," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2017, pp. 364–365.

[23] G. Li, H. Yang, J. Zhang, H. Liu, and A. Hu, "Fast and secure key generation with channel obfuscation in slowly varying environments," in *Proc. IEEE Conf. Comput. Commun.*, May 2022, pp. 1–10.

[24] K. S. Germain and F. Kragh, "Channel prediction and transmitter authentication with adversarially-trained recurrent neural networks," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 964–974, 2021.

[25] J. Martins, M. Gomes, V. Silva, and R. Dinis, "Deep learning-based channel prediction for wireless physical layer security," in *Proc. IEEE Int. Medit. Conf. Commun. Netw. (MeditCom)*, Jul. 2024, pp. 114–118.

[26] T. M. Pham, L. Senigagliesi, M. Baldi, G. P. Fettweis, and A. Chorti, "Machine learning-based robust physical layer authentication using angle of arrival estimation," in *Proc. GLOBECOM*, Dec. 2023, pp. 1–7.

[27] Z. Yang, Z. Zhou, and Y. Liu, "From RSSI to CSI: Indoor localization via channel response," *ACM Comput. Surveys*, vol. 46, no. 2, pp. 1–32, Nov. 2013.

[28] Y. Li, K. Xu, J. Zhang, C. Gu, Y. Ding, G. Goussetis, and S. K. Podilchak, "PUF-assisted radio frequency fingerprinting exploiting power amplifier active load-pulling," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 5015–5029, 2024.

[29] T. Doan and L. Nguyen, "Uplink performance of cell-free massive MIMO with access point selections," *EAI Endorsed Trans. Ind. Netw. Intell. Syst.*, vol. 5, no. 16, Nov. 2018, Art. no. 155998.

[30] Q. Peng, H. Ren, C. Pan, N. Liu, and M. Elkashlan, "Resource allocation for cell-free massive MIMO enabled URLLC downlink systems," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Aug. 2022, pp. 838–843.

[31] H. T. Dao and S. Kim, "Effective channel gain-based access point selection in cell-free massive MIMO systems," *IEEE Access*, vol. 8, pp. 108127–108132, 2020.

[32] C. F. Mendoza, S. Schwarz, and M. Rupp, "Deep reinforcement learning for dynamic access point activation in cell-free MIMO networks," in *Proc. WSA; 25th Int. ITG Workshop Smart Antennas*, Nov. 2021, pp. 1–6.

[33] F. Conceição, L. Martins, M. Gomes, V. Silva, and R. Dinis, "Access point selection for spectral efficiency and load balancing optimization in radio stripes," *IEEE Commun. Lett.*, vol. 27, no. 9, pp. 2383–2387, Sep. 2023.

[34] S. Timilsina, D. Kudathanthirige, and G. Amarasuriya, "Physical layer security in cell- free massive MIMO," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–7.

[35] T. M. Hoang, H. Q. Ngo, T. Q. Duong, H. D. Tuan, and A. Marshall, "Cell-free massive MIMO networks: Optimal power control against active eavesdropping," *IEEE Trans. Commun.*, vol. 66, no. 10, pp. 4724–4737, Oct. 2018.

[36] N. Li, Y. Gao, K. Xu, M. Guo, N. Sha, X. Wang, and G. Wang, "Spatial sparsity-based pilot attack detection and transmission countermeasure for cell-free massive MIMO system," *IEEE Syst. J.*, vol. 17, no. 2, pp. 2065–2076, Jun. 2023.

[37] Y. S. Atiya, Z. Mobini, H. Q. Ngo, and M. Matthaiou, "Secure transmission in cell-free massive MIMO under active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 23, no. 12, pp. 18036–18052, Dec. 2024.

[38] X. Zhang, T. Liang, K. An, G. Zheng, and S. Chatzinotas, "Secure transmission in cell-free massive MIMO with RF impairments and low-resolution ADCs/DACs," *IEEE Trans. Veh. Technol.*, vol. 70, no. 9, pp. 8937–8949, Sep. 2021.

[39] L. Davis, *Handbook of Genetic Algorithms*. New York, NY, USA: Van Nostrand Reinhold, 1991.

[40] F. Conceição, C. H. Antunes, M. Gomes, V. Silva, and R. Dinis, "User fairness in radio stripes networks using meta-heuristics optimization," in *Proc. IEEE 95th Veh. Technol. Conference: (VTC-Spring)*, Jun. 2022, pp. 1–6.

[41] F. Conceição, M. Gomes, V. Silva, R. Dinis, and C. Henggeler Antunes, "Bi-objective power optimization of radio stripe uplink communications," *Electronics*, vol. 11, no. 6, p. 876, Mar. 2022.

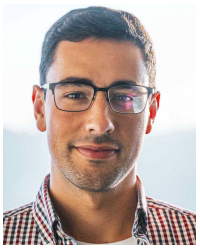
[42] F. Conceição, M. Gomes, V. Silva, R. Dinis, and C. H. Antunes, "Joint spectral and power efficiency optimization in uplink radio stripes," *IEEE Trans. Commun.*, vol. 72, no. 8, pp. 5209–5225, Aug. 2024.

[43] P. Bento, C. H. Antunes, M. Gomes, R. Dinis, and V. Silva, "Beamforming optimization for multiuser wireless systems using meta-heuristics," in *Proc. IEEE 84th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2016, pp. 1–5.

[44] E. Björnson and L. Sanguinetti, "Making cell-free massive MIMO competitive with MMSE processing and centralized implementation," *IEEE Trans. Wireless Commun.*, vol. 19, no. 1, pp. 77–90, Jan. 2020.

[45] E. Björnson, J. Hoydis, and L. Sanguinetti, "Massive MIMO networks: Spectral, energy, and hardware efficiency," *Found. Trends Signal Process.*, vol. 11, nos. 3–4, pp. 154–655, 2017.

[46] *Study on Scenarios and Requirements for Next Generation Access Technologies*, 3GPP, Sophia Antipolis, France, 2017.



JOÃO MARTINS (Graduate Student Member, IEEE) received the M.Sc. degree in electrical and computer engineering specialty in telecommunications from the University of Coimbra, in 2020. He is currently pursuing the Ph.D. degree in electrical and computer engineering with the Faculty of Science and Technology, University of Coimbra, in collaboration with the Instituto de Telecomunicações (IT). His research interests include physical layer security and authentication techniques for distributed massive MIMO systems, with a particular emphasis on spoofing attack detection and mitigation in 6G communication networks. His current research interests include physical layer security, wireless authentication, spoofing attacks, 6G networks, distributed massive MIMO, cell-free systems, and radio stripe-based communications.

FILIPE CONCEIÇÃO (Graduate Student Member, IEEE) was born in Coimbra, Portugal, in 1996. He received the M.Sc. degree in electrical and computer engineering specialty in telecommunications from the University of Coimbra, in 2019, and the Ph.D. degree from the Department of Electrical and Computer Engineering, Faculty of Science and Technology, University of Coimbra, in collaboration with the Instituto de Telecomunicações (IT), in 2025. His research interests include the development of transmission, detection, and resource allocation techniques for radio stripe systems. His current research interests include cooperative communications 6G networks, including distributed massive MIMO, cell-free, radio stripe, resource allocation, and pre-coding/equalization techniques.

MARCO GOMES (Senior Member, IEEE) was born in Coimbra, Portugal, in 1977. He received the M.Sc. and Ph.D. degrees in electrical and computer engineering specialty in telecommunications from the University of Coimbra, in 2004 and 2011, respectively. He is currently a Tenure Assistant Professor with the University of Coimbra. He is also a Senior Researcher with IT. His research interests include signal processing for wireless communications, massive MIMO, LIS, software-defined radio, and physical layer security. He is a member of the IEEE Communications Society and the IEEE Vehicular Technology Society. He is an Editor of IEEE COMMUNICATIONS LETTERS, IEEE OPEN JOURNAL OF THE COMMUNICATIONS SOCIETY, the IEEE ComSoc On-Line Content, and *Physical Communication* (Elsevier).

VITOR SILVA received the Graduate Diploma degree in electrical engineering and the Ph.D. degree from the University of Coimbra, Portugal, in 1984 and 1996, respectively. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, University of Coimbra, where he lectures on signal processing and information and coding theory. He has published more than 200 articles. He is currently the Coordinator of IT, Coimbra site, University of Coimbra. His research interests include signal processing, parallel computing, and coding theory.

RUI DINIS (Senior Member, IEEE) received the Ph.D. degree from the Technical University of Lisbon (IST), Portugal, in 2001, and the Habilitation degree in telecommunications from the Universidade Nova de Lisboa (UNL), in 2010. From 2001 to 2008, he was a Professor at IST. In 2003, he was an Invited Professor at Carleton University, Ottawa, Canada. Currently, he is a Professor with FCT-UNL. He is also a Senior Researcher at IT. He has been actively involved in several national and international research projects in the broadband wireless communications area. His research interests include transmission, estimation, and detection techniques. He is a VTS Distinguished Lecturer and is or was an Editor of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE OPEN JOURNAL ON COMMUNICATIONS, and *Physical Communication* (Elsevier). He was also a guest editor of several special issues.