University of Baghdad
College of Engineering
JE
JOURNAL OF ENGINEERING

Journal of Engineering

journal homepage: www.jcoeng.edu.iq

Volume 32 Number 7 July 2026

Joint AP Selection and Power Allocation for Secure Cell-Free Massive MIMO Under Active Eavesdropping

Ghaydaa Alaa Hussain *, Aqiel Niama Almamori

Department of Electronics and Communications Engineering, College of Engineering, University of Baghdad, Baghdad, Iraq

ABSTRACT

Cell-Free Massive MIMO is believed to be one of the most promising designs of future wireless networks due to its ability to provide more coverage, high reliability and improved spectral efficiency, while also supporting secure communication through distributed access point (AP) cooperation. However, secure downlink transmission in cell-free massive Multiple-Input Multiple-Output (CF-mMIMO) systems becomes challenging when an active eavesdropper (Eve) is located near the targeted user. To achieve high secrecy spectral efficiency (SSE) with a limited number of active APs and a restricted power budget under Nakagami-m fading and imperfect channel state information (CSI), a secrecy-oriented AP selection algorithm is proposed with maximum-ratio transmission (MRT) precoding. Two power allocation schemes are considered: equal power allocation (EPA) and water-filling (WF). Simulation results indicate that the proposed joint-optimization AP activation method enhances the secrecy rate for the targeted user compared with non-optimized selection strategies. For CSI estimation error $\eta_k = 0.1$, the proposed method achieves SSE improvements of 149% with WF and 317% with EPA. At a higher CSI estimation error $\eta_k = 0.4$, the improvements are 144.5% with WF and 280.6% with EPA.

Keywords: Cell-free MIMO, Secrecy rate, Multi-User MIMO, Nakagami-m fading, Physical Layer Security (PLS).

1. INTRODUCTION

Cell-free massive multiple-input multiple-output (CF-mMIMO) has attracted considerable attention as a candidate architecture for beyond fifth-generation (5G) and sixth-generation (6G) wireless networks **(Kassam et al., 2023)**. In CF-mMIMO, many distributed access points (APs) jointly serve user equipment (UEs) through a central processing unit (CPU), which eliminates conventional cell boundaries and delivers uniform spectral efficiency, high energy efficiency, and macro-diversity gains that surpass those of co-located massive MIMO and small-cell deployments **(Nayebi et al., 2017; Ngo et al., 2017; Bjornson and**

*Corresponding author
Peer review under the responsibility of University of Baghdad.
https://doi.org/10.31026/j.eng.2026.07.03

Article received: 19/03/2026
Article revised: 07/06/2026
Article accepted: 22/06/2026
Article published: 01/07/2026

Sanguinetti, 2020). However, this distribution of APs shortens the distances to both legitimate users and potential eavesdroppers, thereby increasing the risk of confidential information leakage. Therefore, securing the physical layer of CF-mMIMO against eavesdropping has emerged as an important research topic **(Hoang et al., 2018)**. Physical-layer security (PLS) provides a complementary line of defence to conventional cryptographic methods by exploiting the dynamic characteristics of the wireless environment **(Solaija et al., 2022)**. Secrecy spectral efficiency (SSE) is commonly used to measure the rate difference between the legitimate user and the eavesdropper links. Within CF-mMIMO, eavesdropping threats are broadly categorized into active and passive paradigms **(Kapetanovic et al., 2015)**. Active eavesdroppers transmit spoofing pilot sequences during the uplink training phase **(Li et al., 2023)** to contaminate channel estimates, thereby steering the downlink beams toward themselves and amplifying information leakage **(Hoang et al., 2018; Zhang et al., 2019)**. Passive eavesdroppers, on the other hand, silently intercept the downlink signal without interfering with the training process **(Hasan and Almamori, 2025)**, making their presence harder to detect and their threat model relevant in scenarios where proactive pilot attacks are infeasible **(Wu et al., 2018)** or countermeasures such as pilot authentication have been deployed **(Ma et al., 2023; Tubail et al., 2023)**. The security of CF-mMIMO was first examined in the context of active eavesdropping and pilot spoofing attacks. **(Hoang et al., 2018)** proposed detection mechanisms for pilot spoofing and formulated power-control optimization problems including secrecy-rate maximization and power-consumption minimization solved via path-following algorithms for a network of single-antenna APs with conjugate beamforming. **(Zhang et al., 2019)** extended the analysis to a multigroup multicasting scenario and derived closed-form secrecy rate expression, while also proposing a minimum description length criterion for spoofing-attack detection. These studies established the serious impact of active attacks in CF-mMIMO. They assumed that every AP in the network participates in the transmission to every user, which may limit scalability and energy efficiency.

Subsequent research has sought to improve secrecy performance by moving beyond single-antenna APs and simple maximum-ratio transmission (MRT). **(Wang et al., 2022)** studied the deployment of multi-antenna APs under active eavesdropping and showed that additional antenna elements strengthen channel hardening and secrecy performance when paired with a channel-quality-aware power allocation scheme. More recently, **(Atiya et al., 2023)** developed CF-mMIMO framework with multi-antenna APs and protective partial zero-forcing (PPZF) precoding under active eavesdropping, demonstrating that PPZF can enhance SSE relative to MRT by suppressing inter-user interference. The same authors subsequently proposed a joint power-optimization and AP-selection approach based on accelerated projected gradient methods **(Atiya et al., 2024)**, and later combined PPZF, greedy large-scale-based AP selection, and path-following power control, reporting SSE gains of up to 220% from AP selection alone and an additional 55% from optimized power allocation under active eavesdropping conditions **(Atiya et al., 2024)**. A parallel line of research has addressed passive eavesdropping in CF-mMIMO **(Park et al., 2024)**, where the eavesdropper does not intervene in the channel estimation process. **(Tubail et al., 2023)** considered a hidden passive eavesdropper and proposed cooperative and independent power-allocation schemes that inject artificial noise (AN) to jam the eavesdropper's reception while maintaining quality-of-service guarantees for legitimate users under imperfect CSI. **(Nguyen et al., 2018)** considered a passive multi-antenna eavesdropper in massive MIMO systems and proposed AN-aided downlink training and transmission to

degrade the eavesdropper's channel estimation also to improve the total achievable secrecy rate. **(Ma et al., 2023)** investigated scalable CF-mMIMO with multiple passive eavesdroppers using stochastic geometry and showed that null-space AN can improve secrecy while revealing a trade-off between AP density and the number of antennas per AP. These studies highlight the importance of addressing passive threats, and primarily rely on AN injection as the secrecy mechanism and do not explore AP-selection under active eavesdropping. Beyond passive eavesdropping, **(Nasir, 2024)** showed that in cell-free integrated sensing and communication (ISAC) systems, directed sensing beams can increase leakage to eavesdroppers, reinforcing that secrecy-aware AP selection and power allocation remain essential in CF-mMIMO deployments. Despite the growing body of work, several important gaps remain. First, existing AP-selection methods for secure CF-mMIMO are combined with advanced precoding schemes such as PPZF, while their performance with the simpler and more scalable MRT precoder under imperfect CSI remains less explored. Second, existing power allocation strategies in prior secure CF-mMIMO studies have either been limited to equal power allocation (EPA) or have been optimized in isolation from the AP-selection process; the potential benefit of water-filling (WF) within AP-selection framework has not been investigated. Third, the effect of heterogeneous CSI imperfection, where the targeted user experiences a larger estimation error than other users, has not been explicitly modelled in the AP-selection and power-allocation design.

Table 1 summarises the key differences between this work and recent studies of secure CF-mMIMO under active eavesdropping. The proposed framework is distinguished from prior work by its use of low-complexity MRT precoding suitable for scalable distributed deployments, its explicit treatment of heterogeneous per-user CSI imperfection where the targeted user experiences a larger estimation error than other users, its use of generalized Nakagami-m fading that captures Rayleigh, Rician, and near-line-of-sight propagation within a unified model, and the provision of a closed-form ergodic secrecy-rate lower bound that supports analytical design.

Table 1. Comparison of representative secure CF-mMIMO frameworks under active eavesdropping

Reference	Precoder	AP Selection	Power Allocation	Fading	Heterog. CSI	Theoretical Guarantee
(Hoang et al., 2018)	Conjugate BF	All APs serve	Path-following	Rayleigh	No	None
(Wang et al., 2022)	MRT (multi-antenna)	All APs serve	Channel-quality-aware	Rayleigh	No	None
(Atiya et al., 2023)	PPZF	All APs serve	EPA	Rayleigh	No	None
(Atiya et al., 2024)	PPZF	Joint (projected gradient)	Optimized (projected gradient)	Rayleigh	No	Convergence only
(Atiya et al., 2024)	PPZF	Greedy (large-scale)	Path-following	Rayleigh	No	None
This work	MRT	Two-stage greedy regularised	EPA + WF + secrecy-ratio	Nakagami-m	Yes	Closed-form ergodic bound; heuristic (1 − 1/e)

Motivated by these observations, this paper investigates the downlink secrecy performance of a user-centric CF-mMIMO system in the presence of an active eavesdropper located near a targeted legitimate user, under imperfect CSI conditions. Unlike recent PPZF-based secure CF-mMIMO studies, this work focuses on the use of MRT precoding and develops a joint AP-selection algorithm that iteratively adds the AP yielding the largest improvement in a regularized secrecy objective function, thereby balancing the sum secrecy rate against the overhead of activating additional APs. We further integrate a water-filling power allocation policy that distributes the available transmit power according to the effective legitimate-channel gains. The main contributions of this work are summarized as follows:

1- A secrecy AP-selection framework based on MRT precoding is introduced for CF-mMIMO systems under active eavesdropping, offering lower complexity than PPZF-based approaches and greater suitability for large-scale deployments.
2- A WF power-allocation scheme is integrated with the proposed MRT-based AP-selection framework and compared with EPA. WF distributes transmit power according to the legitimate-channel conditions, allowing the impact of adaptive power allocation on the targeted user's SSE to be evaluated.
3- The framework considers imperfect CSI, where the targeted user suffers an equal or higher estimation error than others, reflecting a challenging and practically relevant secrecy scenario.
4- A tractable ergodic secrecy-rate lower bound is derived under MRT precoding, Nakagami-m fading, and imperfect CSI, capturing the effects of AP subset selection, CSI quality, and fading severity.
5- Monte Carlo experiments are used to compare the proposed joint AP selection to several baselines, such as distance-based and max-rate greedy selection and show significant improvement in the SSE across Nakagami-m fading, which models Rayleigh fading, Rician fading, and near-LOS fading conditions.

2. SYSTEM MODEL

Consider a cell-free massive MIMO (CF-mMIMO) downlink network, as illustrated in **Fig. 1,** comprising L access points (APs), each equipped with M antennas, K single-antenna legitimate users, and a single-antenna active eavesdropper (Eve).

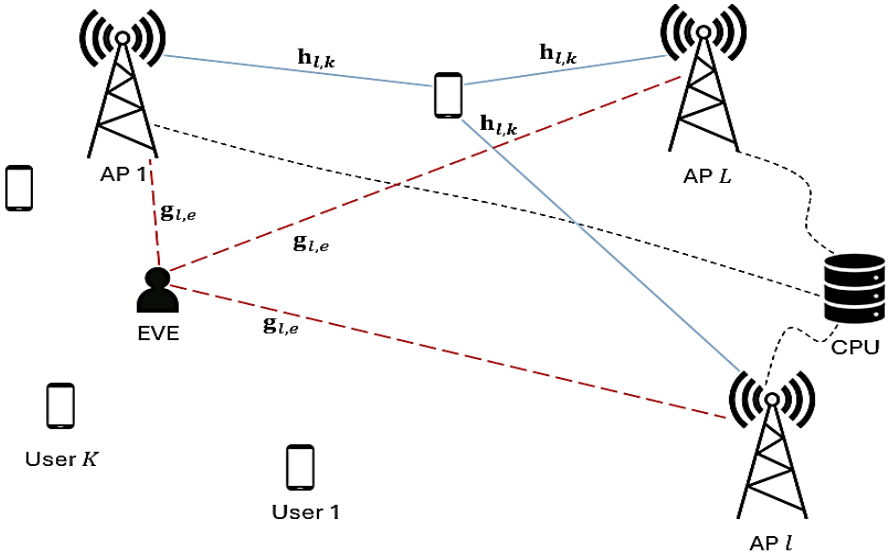


Figure 1. Network topology of system model

The eavesdropper is located near the targeted user, specifically at a random location within a radius r centered at the targeted user position. The system operates under time-division duplexing (TDD) **(Chen et al., 2022)**. Downlink data transmission is carried out using maximum-ratio transmission (MRT) precoding based on imperfect channel state information (CSI) **(Wang et al., 2022)**. Two power allocation strategies are considered for the downlink transmission. In the first, equal power allocation (EPA) is applied across all served users; in the second, water-filling (WF) policy is adopted. Under both strategies, only a selected subset of APs is activated **(Chen et al., 2020)**. The corresponding AP-selection procedure is described in a later section. The active eavesdropper attempts to intercept the downlink signal intended for one of k legitimate users. Because CSI estimation is imperfect, a portion of the transmitted signal may leak toward Eve, thereby degrading the achievable secrecy performance. It is assumed that the system is aware of the eavesdropper's presence and knows which user is being targeted.

2.1 Channel Model

Let $\mathrm{h}_{l,k} \in \mathbb{C}^{M\times 1}$denote the downlink channel from AP l to user k, which can be expressed as:

$$h_{l,k} = \sqrt{\beta_{l,k}}\ \tilde{h}_{l,k}\ , \quad l \in L, k \in K \tag{1}$$

Where $\beta_{l,k}$ denotes large-scale fading coefficient, which accounts for both path loss and shadow fading, and $\tilde{\mathrm{h}}_{l,k}$ denotes small-scale fading coefficient, modeled as Nakagami-m fading **(Wang et al., 2022)** which is widely used due to its ability to capture different channel conditions within a unified framework. Specifically, setting $\mathrm{m} = 1$ yields Rayleigh fading, moderate m values approach Rician fading, and the limit $\mathrm{m} \to \infty$ corresponds to an almost deterministic (non-fading) free-space channel. This makes it a standard choice for evaluating secrecy performance under multiple propagation scenarios, follow **(Gómez-Déniz and Gómez-Déniz, 2024)**

$$f_R(r) = \frac{2m^m}{\Gamma(m)\,\Omega^m}\ r^{2m-1}\ \exp\Big(-\frac{m}{\Omega}r^2\Big), r \geq 0 \tag{2}$$

Where $f_R(r)$ is the probability density function (PDF) of the Nakagami-m fading, r is a non-negative realization, m is the Nakagami-m fading parameter, which controls the severity of fading, Ω is the average fading power and $\Gamma(m)$ is gamma function.
Similar to the standard assumption that the small-scale coefficient is modelled as i.i.d. and remains constant within a coherence interval while varying independently across successive intervals **(Tubail et al., 2023)**.
Also let $\mathrm{g}_{l,e} \in \mathbb{C}^{M\times 1}$denote the channel from AP l to Eve, which can be expressed as:

$$\mathrm{g}_{l,\mathrm{e}} = \sqrt{\beta_{l,e}}\ \tilde{h}_{l,e} \tag{3}$$

Where $\beta_{l,e}$ denotes large-scale fading coefficient including shadow fading and path loss, and $\tilde{h}_{l,e}$ is small-scale fading coefficient, also modeled as Nakagami-m fading **(Wang et al., 2022)**. The uplink training phase is not explicitly simulated; instead, an imperfect channel state information (CSI) model is adopted. Specifically, the standard additive estimation-error decomposition is used, where the downlink channel is decomposed into an estimated component and an estimation error $h_{l,k} = \hat{h}_{l,k} + \tilde{h}_{l,k}^{err}$ where $\tilde{h}_{l,k}^{err} \triangleq h_{l,k} - \hat{h}_{l,k}$ **(Bjornson**

and Sanguinetti, 2020) where $h_{l,k} \in \mathbb{C}^{M\times 1}$denotes the actual channel vector from AP l to user k, $\hat{h}_{l,k}$ is the estimated channel vector and $\tilde{h}_{l,k}^{err}$ is the channel estimation error vector. The channel estimation quality is characterized by the normalized mean-square error (NMSE) level η_k as in **(Guo et al., 2026)**:

$$\eta_k \triangleq \frac{\mathbb{E}\{\| \tilde{h}_{l,k}^{err} \|^2\}}{\mathbb{E}\{\| h_{l,k} \|^2\}} = \frac{\mathbb{E}\{\| h_{l,k} - \hat{h}_{l,k} \|^2\}}{\mathbb{E}\{\| h_{l,k} \|^2\}} \in [0,1 \tag{4}$$

$\mathbb{E}\{\cdot\}$ is the expectation operator, and $\|\cdot\|$ denotes the Euclidean norm. Here $\eta_k = 0$ corresponds to perfect CSI, while larger η_k indicates more severe estimation uncertainty.

2.2 Precoding Design

Maximum-ratio transmission (MRT) is adopted as the downlink precoding strategy for the CF-mMIMO system. MRT is a matched filter precoder that aligns each beamforming vector with the corresponding estimated channel, thereby maximizing the desired signal power and exploiting the distributed array gain **(Atiya et al., 2024)**.

MRT offers a scalable, low-complexity approach that is particularly well suited to large-scale CF-mMIMO deployments. In particular, MRT can be implemented using local channel state information (CSI) at each AP, which reduces both the computational burden and the fronthaul signalling requirements; a critical advantage in a practical CF-mMIMO systems with a large number of distributed APs. MRT thus offers a favorable trade-off between implementation complexity and performance and also serves as a reliable baseline for evaluating the proposed AP-selection and power allocation mechanisms under realistic CSI imperfections. Accordingly, MRT is employed throughout this work: the precoding vectors are constructed from the estimated channels and normalized to satisfy the per-AP transmit power constraints, while the achieved SINR and secrecy rates are evaluated using the corresponding channels.

Following the standard CF-mMIMO downlink model, the composite transmitted signals for k users is given by:

$$s_l = \sum_{k=1}^{K} \sqrt{p_{l,k}}\ \omega_{l,k}\ s_{d,k} \tag{5}$$

where $s_{d,k}$ denotes the normalized data symbol for the user k, such that $\mathbb{E}\{|\ s_{dk}\ |^2\} = 1$. The coefficient $p_{l,k} \geq 0$ denotes the downlink power allocated by AP l to the user k, and $\omega_{l,k} \in \mathbb{C}^{L\times 1}$ is the corresponding precoding vector with M antennas per AP. This formulation reflects that each AP simultaneously serves all legitimate users by linearly combining their data streams **(Wang et al., 2022)**. A normalized MRT precoder is defined as:

$$\boldsymbol{\omega_{l,k}} = \frac{h_{l,k}^*}{\sqrt{\mathbb{E}\{\|h_{l,k}^*\|^2\}}} \tag{6}$$

where $(\cdot)^*$denotes the Hermitian transpose and $\|.\|$ is Euclidean norm. This normalization ensures that each beamforming vector has controlled average energy. Under this convention, the average transmit power at AP L satisfies:

$$\mathbb{E}\{\| s_l \|^2\} = \sum_{k=1}^{K} p_{l,k} \tag{7}$$

so that $p_{l,k}$ directly controls the average power allocated to the k-th stream at AP L. The received downlink signal at user k is superposition of contributions from all APs through the channels $h_{l,k}$ and adding the noise and define as:

$$x_k = \sum_{l=1}^{L} h_{l,k}^H s_l + w_{d,k} \tag{8}$$

where $w_{d,k} \sim \mathcal{CN}(0, \sigma^2)$ is complex additive white Gaussian noise AWGN. Expanding Eq. (8), the received signal can be decomposed into a desired component and multiuser interference as follows:

$$x_k = \underbrace{a_{kk} s_{d,k}}_{desired\ information} + \underbrace{\sum_{k' \neq k}^{K} a_{kk'} s_{d,k'}}_{multiuser\ interference} + \underbrace{w_{d,k}}_{noise} \tag{9}$$

where the first term represents the desired signal intended for user k, the second term represents the interference caused by all other users $k' \neq k$, and the third term is the additive noise. The effective combined channel gain is defined as:

$$a_{k,k'} \triangleq \sum_{l=1}^{L} \sqrt{p_{l,k'}}\ h_{l,k}^* \omega_{l,k'} \tag{10}$$

Here, $a_{k,k}$ represents the aggregate beamformed gain of the stream intended for user k, while $a_{k,k'}$ for $k' \neq k$ is the residual interference leaked from user k''s stream to user k **(Wang et al., 2022)**. This reflects a fundamental characteristic of MRT: it enhances the desired signal through channel-matched beamforming but does not explicitly cancel inter-user interference **(Atiya et al., 2023)**.

Similarly, Eve intercepts the superposition of all transmitted streams through its channels $g_{l,e}$ from the APs:

$$z_e = \sum_{l=1}^{L} g_{l,e}^* s_l + w_{d,e} \tag{11}$$

where $w_{d,e} \sim \mathcal{CN}(0, \sigma^2)$. After substitution, Eve's received signal can be written as

$$z_e = a_{e,k} s_{d,k} + \sum_{k' \neq k}^{K} a_{e,k'} s_{d,k'} + w_{d,e} \tag{12}$$

with

$$a_{e,k'} \triangleq \sum_{l=1}^{L} \sqrt{p_{l,k'}}\ g_{l,e}^* \omega_{l,k'} \tag{13}$$

$$a_{e,k} \triangleq \sum_{l=1}^{L} \sqrt{p_{l,k}}\ g_{l,e}^* \omega_{l,k} \tag{14}$$

In this expression, $a_{e,k}$ represents the effective channel gain of the targeted user's stream as received by Eve, while the remaining terms constitute interference **(Wang et al., 2022)**. This signal model forms the basis for computing Eve's SINR and, in turn, the secrecy rate, which is obtained by comparing the achievable rates of the legitimate user and the eavesdropper.

2.3 Downlink Data Transmission

As described in the precoding design, MRT is employed for downlink transmission toward the intended legitimate users. Given the aggregated channel from the selected AP set $\mathcal{S}$ to user kThe received signal consists of the desired component, multiuser interference, and additive noise. The instantaneous downlink SINR at the legitimate user k is given by the ratio between the desired signal power to the multiuser interference plus noise power, following **(Atiya et al., 2025)**, the power-weighted aggregated MRT precoding vector for the user i is defined as $\mathbf{v}_i(\mathcal{S}) = \left[\sqrt{p_{l_1,i}}\mathbf{w}_{l_1,i}^T, \sqrt{p_{l_2,i}}\mathbf{w}_{l_2,i}^T, \dots, \sqrt{p_{l_{|\mathcal{S}|},i}}\mathbf{w}_{l_{|\mathcal{S}|},i}^T\right]^T \in \mathbb{C}^{|\mathcal{S}|M\times 1}$, where $p_{l,i}$ is the transmit power allocated by AP l to user i, and $\mathbf{w}_{l,i}$is the normalize MRT precoding vector $\boldsymbol{w}_i(S) = \left[\boldsymbol{w}_{l_1 i}^T, \boldsymbol{w}_{l_2 i}^T, \dots, \boldsymbol{w}_{l_{|S|} i}^T\right]^T \in \mathbb{C}^{SM\times 1}$, $\boldsymbol{w}_k(S)$ represents the desired precoding vector for user k, while when $i = j, j \neq k$, $\mathbf{w}_j(\mathcal{S})$ represents the interfering precoding vector, and is expressed by:

$$SINR_k^{user}(\mathcal{S}) = \frac{|\boldsymbol{h}_k^H(\mathcal{S})\boldsymbol{v}_k(\mathcal{S})|^2}{\sum_{j\neq k}|\boldsymbol{h}_k^H(\mathcal{S})\,\boldsymbol{v}_j(\mathcal{S})|^2 + \sigma^2} \quad (15)$$

Where $(.)^H$ denotes the conjugate transpose and the selected AP set denoted by $S = \{l_1, l_2, \dots, l_{|S|}\}$. Here, $\boldsymbol{h}_k(S) = \left[\boldsymbol{h}_{l_1 k}^T, \boldsymbol{h}_{l_2 k}^T, \dots, \boldsymbol{h}_{l_{|S|} k}^T\right]^T \in \mathbb{C}^{SM\times 1}$ denotes the aggregated downlink vector from the selected AP set $\mathcal{S}$ to user k, and $\sigma^2$is the noise power.

Eve is assumed to decode user k 's message while treating other users' signals as interference. The corresponding eavesdropper SINR is defined as the ratio of Eve's desired signal power to the sum of multiuser interference plus noise **(Atiya et al., 2024)** and is given by:

$$\mathrm{SINR}_k^{\mathrm{eve}}(\mathcal{S}) = \frac{|\,\mathrm{g}_e^H(\mathcal{S})\,\boldsymbol{v}_k(\mathcal{S})\,|^2}{\sum_{j\neq k}|\,\mathrm{g}_e^H(\mathcal{S})\,\boldsymbol{v}_j(\mathcal{S})\,|^2 + \sigma^2} \quad (16)$$

where $\mathrm{g}_e(S) = \left[\mathrm{g}_{l_1 e}^T, \mathrm{g}_{l_2 e}^T, \dots, \mathrm{g}_{l_{|S|} e}^T\right]^T \in \mathbb{C}^{SM\times 1}$ is the aggregated channel vector from the selected AP cluster to Eve.

2.4 Secrecy Spectral Efficiency

The achievable downlink rates at user k and at the eavesdropper are computed as **(Wang et al., 2022)**:

$$R_k^{\mathrm{user}} = \log_2(1+\mathrm{SINR}_k^{\mathrm{user}}) \quad (17)$$

$$R_k^{\mathrm{eve}} = \log_2(1+\mathrm{SINR}_k^{\mathrm{eve}}) \quad (18)$$

SSE of user k is defined as the non-negative difference between the legitimate user's achievable rate and that of the eavesdropper **(Atiya et al., 2024)** and expressed as:

$$R_k^{\mathrm{sec}}(\mathcal{S}) = [\ R_k^{\mathrm{user}} - R_k^{\mathrm{eve}}\ ]^+ \quad (\mathrm{bits/s/Hz}) \quad (19)$$

Where $[x]^+ \triangleq \max(0, x)$.

To characterize secrecy at the network level under a given AP activation and power allocation policy, defining the sum secrecy spectral efficiency as:

$$R_{\text{sum}}^{\text{sec}}(\mathcal{S}) = \sum_{k=1}^{K} R_k^{\text{sec}}(\mathcal{S}) \tag{20}$$

and the mean secrecy spectral efficiency as:

$$R_{\text{mean}}^{\text{sec}}(\mathcal{S}) = \frac{1}{K}\sum_{k=1}^{K} R_k^{\text{sec}}(\mathcal{S}) \tag{21}$$

Here, $R_{\text{sum}}^{\text{sec}}(\mathcal{S})$ and $R_{\text{mean}}^{\text{sec}}(\mathcal{S})$ provide the overall secrecy performance of the network for a given AP cluster $\mathcal{S}$.

2.5 Ergodic Secrecy Rate Lower Bound

To complement the simulation-based evaluation, we derive a tractable lower bound on the ergodic secrecy rate of the targeted user under MRT precoding and imperfect CSI. This bound enables analytical insight into the interplay between AP selection, power allocation, and secrecy performance without requiring extensive Monte Carlo averaging.

Under MRT precoding with the estimated channel, the effective desired signal at user k from the selected AP set S can be decomposed using the use-and-then-forget (UatF) bound **(Zhang et al., 2022)**. Specifically, the received signal at user k is rewritten by taking the expectation of the desired channel gain and treating the residual as uncorrelated effective noise:

$$x_k = \mathbb{E}\{a_{kk}\}s_{d,k} + (a_{kk} - \mathbb{E}\{a_{kk}\})s_{d,k} + \sum_{k' \neq k} a_{kk'}\, s_{d,k'} + w_{d,k} \tag{22}$$

For consistency with (5) and (8), $s_{d,k}$ denotes the normalized data symbol of user k, while x_k denotes the received downlink signal at user k. The first term is the deterministic desired signal component and the remaining terms constitute uncorrelated effective noise. Applying the UatF bound, a lower bound on the achievable rate at user k **(Alageli et al., 2019)** is:

$$R_k^{\text{user,lb}} = \log_2\left(1+\text{SINR}_k^{\text{lb}}\right) \tag{23}$$

where the lower-bound SINR is:

$$\text{SINR}_k^{\text{lb}} = \frac{|\,\mathbb{E}\{a_{kk}\}\,|^2}{\text{Var}\{a_{kk}\} + \sum_{k' \neq k}\mathbb{E}\{|\,a_{kk'}\,|^2\} + \sigma^2} \tag{24}$$

Moment Derivations Under Nakagami-m Fading and Imperfect CSI:

Under the imperfect CSI model with NMSE level η_k, the channel between AP l and user k is decomposed as:

$$h_{l,k} = \hat{h}_{l,k} + \tilde{h}_{l,k}^{err} \tag{25}$$

where $\hat{h}_{l,k}$ is the estimated channel and $\tilde{h}_{l,k}^{err}$ the channel estimation error. The estimated channel can be expressed as:

$$\hat{h}_{l,k} = \sqrt{\beta_{l,k}(1-\eta_k)}\,\tilde{\hat{h}}_{l,k} \tag{26}$$

where $\tilde{\hat{h}}_{l,k}$ denotes the normalized small-scale fading vector. The normalized MRT precoder is $\boldsymbol{\omega_{l,k}} = \frac{h_{l,k}^*}{\sqrt{\mathbb{E}\{\|h_{l,k}^*\|^2\}}}$, for the effective channel gain a_{kk} and $k' = k$,

$$\mathbb{E}\{a_{k,k}\} = \sum_{l\in\mathcal{S}} \sqrt{p_{l,k}} \frac{\mathbb{E}\{\| \hat{\boldsymbol{h}}_{l,k} \|^2\}}{\mathbb{E}\{\| \hat{\boldsymbol{h}}_{\boldsymbol{l,k}} \|\}} \tag{27}$$

Under Nakagami-m fading with imperfect CSI:

$$\| \hat{\boldsymbol{h}}_{l,k} \|^2 \sim \Gamma\left(mM, \frac{\beta_{l,k}(1-\eta_k)}{m}\right) \tag{28}$$

where m is the Nakagami fading parameter, M is the number of antennas per AP, $\beta_{l,k}$ is the large-scale fading coefficient, and η_k is the CSI estimation error level of user k. Hence,

$$\mathbb{E}\{\| \hat{\boldsymbol{h}}_{l,k} \|^2\} = M\beta_{l,k}(1-\eta_k) \tag{29}$$

And

$$\mathbb{E}\{\| \hat{\boldsymbol{h}}_{l,k} \|\} = \sqrt{\frac{\beta_{l,k}(1-\eta_k)}{m}} \frac{\Gamma\left(mM+\frac{1}{2}\right)}{\Gamma(mM)} \tag{30}$$

After Substituting (29) and (30) in (27)

$$\mathbb{E}\{a_{k,k}\} = \sum_{l\in\mathcal{S}} \sqrt{p_{l,k}}\, M\sqrt{m\beta_{l,k}(1-\eta_k)} \frac{\Gamma(mM)}{\Gamma(mM+\frac{1}{2})} \tag{31}$$

where $\Gamma(\cdot)$ denotes the Gamma function. The Gamma-ratio terms appear from the moment identities of the Nakagami-m fading distribution and are used to evaluate the first- and second-order moments of the estimated channel gain. The variance and interference moments are:

$$\mathrm{Var}\{a_{kk}\} = \sum_{l\in S} p_{l,k}\ M\,\beta_{l,k}^2 \left[1 - (1-\eta_k)\frac{\left(\Gamma\left(m+\frac{1}{2}\right)\right)^2}{m(\Gamma(m))^2}\right] \tag{32}$$

$$\mathbb{E}\{|\ a_{k,k'}\ |^2\} \approx \sum_{l\in\mathcal{S}} p_{l,k'}\,\beta_{l,k} \tag{33}$$

Similarly, for the eavesdropper's channel, an upper bound on Eve's achievable rate is obtained by assuming the worst-case scenario where Eve can cancel all multiuser interference:

$$R_k^{\mathrm{eve,ub}} = \log_2\left(1+\frac{\sum_{l\in S} p_{l,k}\ |\ \mathrm{g}_{l,e}^H w_{l,k}\ |^2}{\sigma^2}\right) \tag{34}$$

The resulting ergodic secrecy rate lower bound as in **(Zhang et al., 2021)** is:

$$R_k^{\mathrm{sec,lb}}(S) = \left[R_k^{\mathrm{user,lb}} - R_k^{\mathrm{eve,ub}}\right]^+ \tag{35}$$

This bound is tight in the large-M regime due to channel hardening, and provides a computationally efficient alternative to full Monte Carlo evaluation for AP-selection optimization. Importantly, the bound separates the contributions of the AP set S, the CSI quality η_k, and the Nakagami-m parameter, enabling analytical insight into design trade-offs.

3. POWER ALLOCATION

Power allocation distributes the available downlink transmit power across users from each AP in order to improve system performance in the presence of multiuser interference and imperfect CSI **(Zaher et al., 2023)**. Let $p_{l,k}$ denotes the power coefficient assigned to user k from AP l, subject to a per-AP power constraint, such that the total power transmitted by each AP is limited by $P_{\max}$:

$$\sum_{k=1}^{K} p_{l,k} \leq P_{\max}, \quad \forall l = 1, \dots, L \tag{36}$$

where $P_{\max}$ denotes the maximum transmit power per AP. Two power allocation strategies are considered. First, equal power allocation (EPA) **(Choi et al., 2025)** serves as a baseline, distributing power uniformly among the served legitimate users, where $p_{l,k} = \frac{P_{\max}}{K}$ $\forall l, k$ follow **(Atiya et al., 2024)**. Second, a water-filling (WF) policy is adopted, which adapts the power distribution according to the effective channel conditions under a total power constraint. In this structure, the allocated powers are nonnegative, and weak channels may receive zero power depends on the water level μ_l **(Xing et al., 2020)**. For each AP l, the vector $\mathbf{p}_l = [p_{l,1}, \dots, p_{l,K}]$ is computed using a standard water-filling form:

$$p_{l,k} = [\mu_l - \frac{1}{g_{l,k}}]^+, k = 1, \dots, K \tag{37}$$

where $[x]^+ = \max(x, 0)$ **(Xing et al., 2020)**, Specifically, for each active AP l, the effective gains for power allocation $g_{l,k} \triangleq \| \hat{\mathbf{h}}_{l,k} \|^2$, toward all users is first computed, and the AP power budget $P_{\max}$ was then distributed across the K users according to the WF rule to obtain $\{p_{l,k}\}$ satisfying the Eq. (36). This allocation was repeated sequentially for all APs in the selected cluster until the power coefficients $p_{l,k}$ were obtained for every AP–user pair.

To enable a meaningful comparison against secrecy-aware power allocation strategies, a secrecy-ratio heuristic is further considered. For each AP $l \in S$, the power coefficients are defined as

$$p_{l,k} = P_{\max} \frac{\frac{\beta_{l,k}}{\beta_{l,e}+\epsilon}}{\sum_{k'=1}^{K} \frac{\beta_{l,k'}}{\beta_{l,e}+\epsilon}}, \forall\, k \tag{38}$$

where $\epsilon > 0$ is a small regularization constant introduced to avoid division by zero and $\beta_{l,k'}$ denotes the large-scale fading coefficient between AP l and user k'**.** The normalization ensures that the per-AP power constraint $\sum_{k=1}^{K} p_{l,k} \leq P_{\max}$ is satisfied with equality. This heuristic requires knowledge of the legitimate large-scale fading coefficients $\beta_{l,k}$, which are already available at the CPU for AP selection, together with the eavesdropper large-scale fading coefficient $\beta_{l,e}$. It is emphasized that the secrecy-ratio heuristic is introduced solely as a comparison benchmark to evaluate the role of secrecy-aware power allocation within

the proposed framework. It is not considered as one of the main contributions of this work, which are focused on the two-stage AP-selection algorithm and its analytical characterization. The heuristic is used in Section 5 to demonstrate that the proposed AP-selection framework remains compatible with power-allocation policies having different CSI requirements, computational costs, and secrecy-performance levels

4. PROPOSED ALGORITHM

This section presents the proposed two-stage AP-cluster selection algorithm for secrecy enhancement in the CF-mMIMO downlink under imperfect CSI and MRT precoding. The objective is to select an active AP set $\mathcal{S} \subseteq \{1, \dots, L\}$ that improves the secrecy performance while avoiding the activation of an excessive number of APs. A penalized secrecy objective $J(\mathcal{S})$ is adopted, where the secrecy term is evaluated from the users' and eavesdropper's achievable rates. The algorithm consists of an initialization stage based on a large-scale secrecy metric, followed by a joint enhancement stage that iteratively appends APs providing positive marginal gains.

Stage 1: For each user k, compute a secrecy-motivated large-scale metric for every AP l

$$\mathrm{SM}[l,k] = \frac{\beta_{l,k}}{\beta_{l,E} + \epsilon} \tag{39}$$

For user k, the AP index $l* = \arg\max_{l \in \{1,\dots,L\}} \mathrm{SM}[l,k]$ is selected to maximize the secrecy metric $\mathrm{SM}[l,k]$ over all APs l then add it to the initial set $\mathcal{S}$, ϵ is a small positive constant to avoid division by zero.

Stage 2: To balance secrecy enhancement against activating an excessive number of APs, the following penalized objective is considered:

$$J(\mathcal{S}) \triangleq \sum_{k=1}^{K} R_k^{sec}(\mathcal{S}) - \lambda \mid \mathcal{S} \mid \tag{40}$$

Where $\mid \mathcal{S} \mid$ is the cluster size, $R_k^{\mathrm{sec}}(\mathcal{S})$ is the secrecy rate of user k achieved when using the AP set $\mathcal{S}$, and $\lambda \geq 0$ is the regularization penalty factor. In this work, λ = 0.1 was adopted to provide a trade-off between secrecy improvement and the cost of activating additional APs. Although the absolute SSE values may vary slightly with different λ values, the main performance trend remains unchanged, where the proposed secrecy-oriented AP-selection method outperforms the non-optimized selection strategies. Smaller values of λ give higher priority to secrecy maximization and therefore tend to activate a larger number of APs, while larger values of λ impose a stronger penalty on AP activation and may reduce the selected AP subset.

Iteratively check each candidate AP $l \notin \mathcal{S}$ by computing the marginal objective gain:

$$\Delta_l = J(\mathcal{S} \cup \{l\}) - J(\mathcal{S}) \tag{41}$$

select $l_{\mathrm{best}} = \arg\max_l \Delta_l$, and update $\mathcal{S} \leftarrow \mathcal{S} \cup \{l_{\mathrm{best}}\}$ as long as $\Delta_{\max} > 0$. As follow:

Algorithm: Joint Greedy AP Selection
// Stage 1: Core Initialization
S ← ∅
for k = 1 to K do
  for each AP l do

```
      SM[l,k] ← β[l,k] / (β[l,E] + ε)
    end for
    l* ← argmax_l SM[l,k]
    S ← S ∪ {l*}
  end for
  // Stage 2: Joint Enhancement
  repeat
    Δ_max ← 0
    l_best ← null
    for each AP l such that l ∉ S do
      Δ_l ← J(S ∪ {l}) - J(S)
      if Δ_l > Δ_max then
        Δ_max ← Δ_l
        l_best ← l
      end if
    end for
    if l_best ≠ null then
      S ← S ∪ {l_best}
    end if
  until Δ_max ≤ 0
  return S
```

4.1 Performance Guarantee of the AP Selection

The proposed AP-selection algorithm is greedy in nature: it iteratively appends to the active set S the AP that maximizes the marginal gain of a regularized secrecy objective. The use of a greedy procedure is motivated by the performance guarantee for greedy maximization of submodular set functions **(Krause and Golovin, 2014)**.
Let the sum secrecy-rate function be defined as:

$$f(S) = \sum_{k} R_k^{\text{sec}}(S) \tag{42}$$

To avoid activating an unnecessarily large number of APs, a regularized objective function is considered as:

$$J(S) = f(S) - \lambda \mid \mathcal{S} \mid \tag{43}$$

For each candidate AP $l \notin \mathcal{S}$, the marginal objective gain is defined as:

$$\Delta J(l \mid \mathcal{S}) = J(\mathcal{S} \cup \{l\}) - J(\mathcal{S}) \tag{44}$$

By substituting (43) into (44), the marginal gain becomes:

$$\Delta J(l \mid \mathcal{S}) = [f(\mathcal{S} \cup \{l\}) - f(\mathcal{S})] - \lambda \tag{45}$$

A set function f: 2^V → R is submodular if for all A ⊆ B ⊆ V and l ∉ B:

$$f(A \cup \{l\}) - f(A) \geq f(B \cup \{l\}) - f(B) \tag{46}$$

This is called the diminishing-returns property. **(Nemhauser et al., 1978)** proved that the greedy algorithm achieves at least (1 − 1/e) ≈ 0.63 of the optimum, and **(Krause and Golovin, 2014)** showed that this guarantee degrades gracefully to (1 − 1/e) − O(ε) for ε-approximately diminishing-return behavior functions satisfying. No formal approximation ratio is claimed for the proposed secrecy objective.

$$f(A \cup \{l\}) - f(A) \geq f(B \cup \{l\}) - f(B) - \varepsilon \tag{47}$$

The sum secrecy-rate function $f(S) = \sum_k R_k^{\text{sec}}(S)$ is not strictly submodular under MRT precoding and imperfect CSI. However, three structural observations indicate that it exhibits approximate diminishing returns of the form in (47). First, the legitimate user rate R_k^{user} is a concave function of the received desired signal power, which grows with each added AP through coherent MRT combining. The concavity of $\log_2(1+x)$ translates this growth into diminishing returns as $|S|$ increases. Second, the eavesdropper rate R_k^{eve} grows more slowly than R_k^{user} as $|S|$ increases, because the MRT precoders $\omega_{l,k}$ are matched to the legitimate user channels rather than to the eavesdropper channel $g_{l,e}$. Therefore, additional APs contribute strongly to the legitimate user rate but only weakly to the eavesdropper rate. Third, the non-negative truncation preserves the monotonicity of $R_k^{\text{sec}}(S)$ and bounds the deviation from strict sub modularity within the inter-user interference cross-coupling term. These observations suggest that a residual term ε, capturing the inter-user interference coupling bounded but not yet computed in closed form is sufficient to place $f(S)$ within the scope of the **(Krause and Golovin, 2014)** analysis. Under this heuristic, the greedy procedure used in our algorithm is motivated by

$$f(S_{\text{greedy}}) \geq \left(1-\frac{1}{e}\right) f(S^*) - O(\varepsilon\,|S^*|) - \lambda\,|S^*| \tag{48}$$

where S^* denotes the optimum AP set under the regularized objective. It is emphasized that Eq. (48) is presented here as the standard guarantee that motivates the choice of a greedy procedure in the presence of the structural properties discussed above, rather than as a theorem established for the specific secrecy setting. A rigorous derivation of an explicit bound on ε for the imperfect CSI Nakagami-m MRT regime requires a separate analytical study and is identified as a direction for future work. The empirical validation provided by the Monte-Carlo experiments in Section 5, where the achieved SSE saturates well before $|S|$ approaches L across all CSI levels and fading conditions, supports the practical relevance of the greedy procedure in the present setting.

4.2 Complexity Analysis

The computational complexity of the algorithm is dominated by the greedy enhancement stage (Stage 2). At the t-th iteration, the algorithm evaluates (L − t) candidate APs, each evaluation requires constructing MRT precoding vectors over the trial cluster and computing the SINR of all K users and the eavesdropper, amounting to $O(K^2tM)$ operations. Summing over all iterations, the worst-case complexity of Stage 2 is $O(K^2ML^3)$. Stage 1 requires only O(KL) operations for computing the secrecy metric across all user–AP pairs and is therefore negligible relative to Stage 2. In practice, the regularization term $\lambda|S|$ in the objective function causes early termination at an optimal cluster size $|S^*| \ll L$, which reduces the effective complexity to approximately $O(K^2ML^2|S^*|)$. For the simulation parameters adopted in this work (L = 70, K = 10, M = 4), this results in a manageable computational load suitable for centralized processing at the CPU. The water-filling variant includes an additional O(K log K) term for the sorting step, which does not affect the overall complexity order. **Table 2.** summarizes the per-component complexity.

Table 2. Computational Complexity of the algorithm

Component	**Complexity**
Stage 1: Core initialization	$O(KL)$
Single cluster evaluation (MRT + SINR)	$O(K^2 \cdot \|S\| \cdot M)$
Stage 2: Greedy enhancement (worst case)	$O(K^2ML^3)$
Stage 2: With early stopping at |S*|	$O(K^2ML^2\|S^*\|)$
Water-filling overhead (per evaluation)	$+O(K \log K)$

5. SIMULATION RESULT AND DISCUSSION

This section describes the proposed procedure for evaluating the secrecy performance of the CF-mMIMO downlink system under AP selection, MRT precoding and power allocation. The workflow includes:

(i) Constructing effective channels for the selected AP set.
(ii) Forming the MRT precoders using imperfect CSI and applying power loading (EPA or WF).
(iii) Computing the users' and eavesdropper's SINRs and achievable rates by treating multiuser interference as noise.
(iv) Evaluating the secrecy rate via the non-negative rate difference.

The simulation environment follows **(Atiya et al., 2024)**. To ensure a fair comparison when evaluating the secrecy performance of the CF-mMIMO downlink under MRT precoding with EPA and WF power allocation. Unless otherwise, all results are obtained over a large number of independent Monte-Carlo simulations by averaging over a sufficiently large number of independent channel realizations under Nakagami-m fading to represent different propagation conditions. Specifically, Rayleigh fading is obtained by setting $m = 1$. A Rician channel is approximated using an intermediate $m > 1$ which is mapped from the Rician K-factor, while a near-deterministic line-of-sight (LOS) channel is modeled by using a very large m ($m \to \infty$). The service area is modelled as a square region which L distributed APs and K users are randomly deployed according to a uniform spatial distribution, and to mitigate boundary effects, a wrap-around topology is adopted in the simulations **(Jiang et al., 2023)**. Following the wrap-around principle, the effective distance between two nodes is computed by selecting the minimum distance among periodic images as follows:

$$\Delta x = \min\left(\left| x_u - x_v \right|, D - \left| x_u - x_v \right| \right), \Delta y = min(\left| y_u - y_v \right|, D - \left| y_u - y_v \right|)$$
$$d_{\text{wrap}} = \sqrt{\Delta x^2 + \Delta y^2} \quad (49)$$

where $D = 1000$ m in the simulations, this wrap-around setting is widely adopted in recent cell-free massive MIMO studies to avoid border bias. An active eavesdropper (Eve) is placed in the same area, typically near the attacked user, to represent a worst-case scenario. The active APs subset is determined by the AP-selection mechanism, yielding an active subset $\mathcal{S} \subseteq \{1, \dots, L\}$. The large-scale fading coefficient between the AP l and user k is modelled as the product of a distance-dependent path-loss term and log-normal shadowing. In linear scale, it is given by:

$$\beta_{l,k} = 10^{\frac{PL_{l,k}^{d}}{10}} \cdot 10^{\frac{F_{l,k}}{10}} \quad (50)$$

where $F_{l,k} \sim \mathcal{N}(0, 4^2)$(in dB) models shadow fading. The path-loss term (in dB) follows:

$$PL_{l,k}^{d} = -30.5 - 36.7\log_{10}\left(\frac{d_{l,k}}{1\,\mathrm{m}}\right) \tag{51}$$

Here, $d_{l,k}$ represent the distance between AP l and user k **(Atiya et al., 2024)**.In addition to secrecy performance, we evaluate the energy efficiency (EE) of the downlink transmission as the ratio between the sum secrecy spectral efficiency and the total power consumption of the active AP subset $\mathcal{S}$ following the standard definition of energy efficiency **(Ngo et al., 2018)**. The total consumed power is modelled as the sum of the transmit-related power and circuit power of the active APs, yielding:

$$\mathrm{E} = \frac{\mathrm{SSE}_{\mathrm{sum}}}{P_{\mathrm{cons}}} = \frac{\mathrm{SSE}_{\mathrm{sum}}}{|\,\mathcal{S}\,|\;P_{AP} + |\,\mathcal{S}\,|\;P_{\mathrm{circuit},AP}} = \frac{\mathrm{SSE}_{\mathrm{sum}}}{|\,\mathcal{S}\,|\left(P_{AP} + P_{\mathrm{circuit},AP}\right)} \tag{52}$$

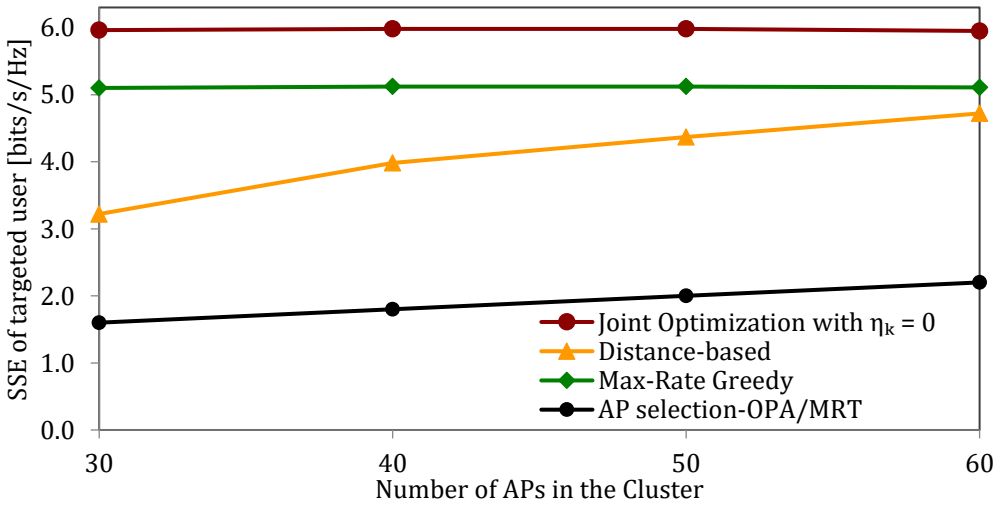
Here, $\mathrm{SSE}_{\mathrm{sum}}$ denotes the sum secrecy spectral efficiency, $|\,\mathcal{S}\,|$is the number of active APs selected by the AP-selection scheme, P_{AP} represents the per-AP transmit-related power (bounded by $P_{AP,\max}$), and $P_{\mathrm{circuit},AP}$ is the circuit power per active AP. Also, in the simulations, we consider $\eta_k \in \{0, 0.1, 0.2, 0.4\}$ to represent perfect, mildly-imperfect, and moderately imperfect CSI conditions, respectively, which is a common approach in the cell-free massive MIMO literature for assessing robustness under imperfect CSI. All the parameters used in the simulation are listed in **Table 3**.

Table 3. Simulation Parameters

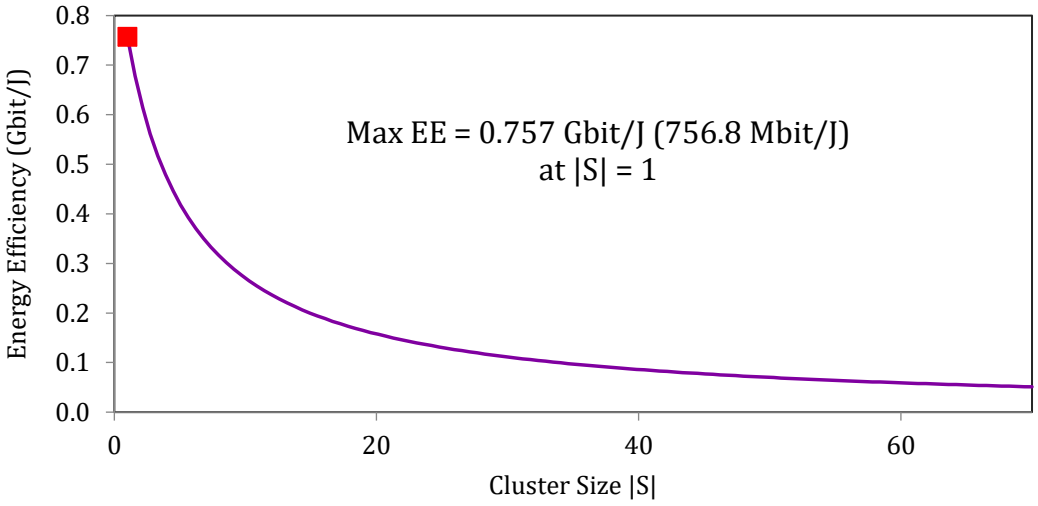
Parameter	**Value**
Number of Aps, L	70
Number of antennas per AP, M	4
Number of users, K	10
Bandwidth	20×10^6 Hz
Noise power, σ^2	$10^{\frac{-92-30}{10}}\mathrm{W} \approx 6.31 \times 10^{-13}$ Watt
Shadowing distribution, $F_{l,k} \sim$	$\mathcal{N}(0, 4^2)\ dB$
Path-loss model, $PL_{l,k}^{d}$	$-30.5 - 36.7\log_{10}\left(\frac{d_{l,k}}{1\,\mathrm{m}}\right)$
Distance from EVE to user K, $d_{k,e}$	$\sim$ 100 m1
Max transmit power per AP, P_{max}	.2 Watt0
Max transmit power per UE, P_{UE}	0.1 Watt
Circuit power per active AP, $P_{circuit,AP}$	0.2 Watt
Regularization parameter, λ	0.1
CSI error level η_k of targeted user	$0, 0.1, 0.2, 0.4$
CSI error level η_k of other users	0, 0.1
Simulation area size	1 km × 1 km
Eve radius (around user 1), r_{eve}	100 m
Attacked user index, k_{attack}	1
Number of Monte Carlo realizations	1000
Nakagami-m parameter	$m = 1,\ \frac{(RiceFactor+1)^2}{2 * RiceFactor + 1},$ and $\sim \infty$

Power-related parameters $(P_{AP,\max}, P_{UE,\max}, P_{circuit,AP})$ are adopted from **(Atiya et al., 2024)**. Downlink transmission employs MRT precoding with normalized per-user beamforming vectors and power loading according to EPA or WF. WF consistently outperforms EPA in terms of secrecy because it allocates more power to links with favorable effective legitimate-channel conditions, while reducing power on weaker links. This advantage is more important when Eve is located close to the targeted user, as the secrecy metric becomes highly sensitive to the power balance between the legitimate and eavesdropper channels. Different values of the CSI error level η_k are considered to investigate the impact on the secrecy performance. **Figs. 2 to 5** present the secrecy performance of the proposed AP-selection method with WF power allocation under different CSI estimation error levels. In these figures, the same simulation setup and AP-selection strategies are used, while only the CSI estimation error level is varied to evaluate the impact on the SSE, EE, and CDF performance. For the moderately imperfect CSI case where the targeted user has η_k = 0.4 and under water filling power allocation, SSE improves monotonically with the cluster size $|S|$ for all AP-selection strategies, but with clear diminishing returns as $|S|$ grows, since additional APs with weak large-scale fading contribute marginally to the useful signal and secrecy balance. In particular, the proposed joint optimization achieves an SSE of approximately 5.38 bit/s/Hz at $|S| = 30$ and 5.39 bit/s/Hz at $|S| = 60$, these values are significantly higher than the benchmark baseline, which is about 1.59 bit/s/Hz at $|S| = 30$ since the benchmark curve starts from this cluster size**,** and 2.19 bit/s/Hz at $|S| = 60$ as illustrated in **Fig. 5**.

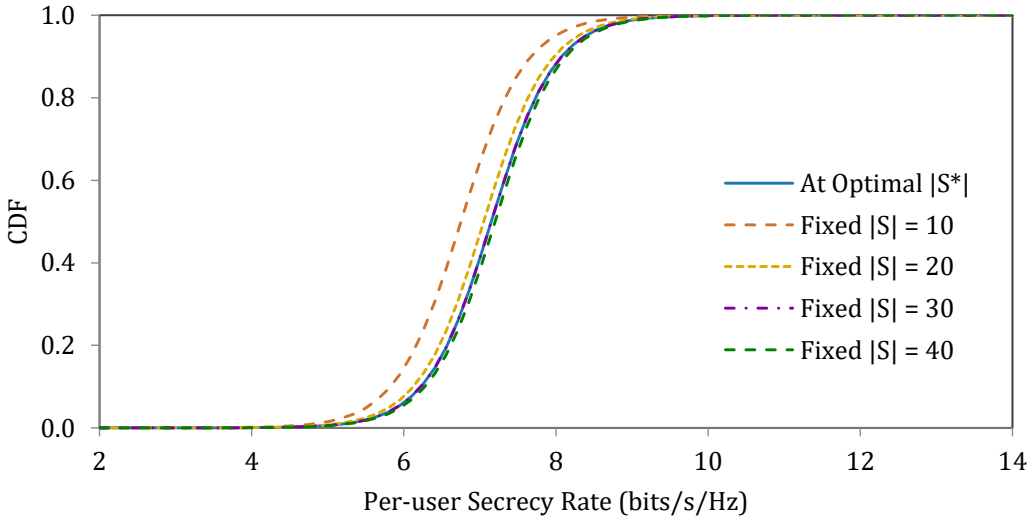
These results validate the ability of the proposed framework to achieve superior secrecy performance relative to the benchmark schemes under equivalent operating conditions. In addition to secrecy, the energy efficiency results indicate a fundamental trade-off: increasing $|S|$ typically raises secrecy but also increases total consumed power due to the larger active-AP subset and associated circuit power. The accompanying CDF curves further corroborate improved secrecy reliability, as the optimized design shifts the secrecy distribution toward higher values across realizations.



(a) SSE

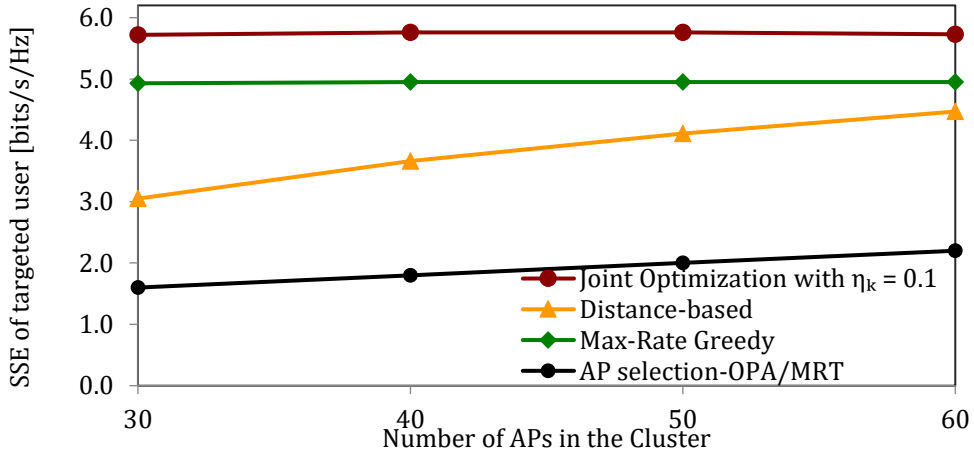


(b) Energy Efficiency

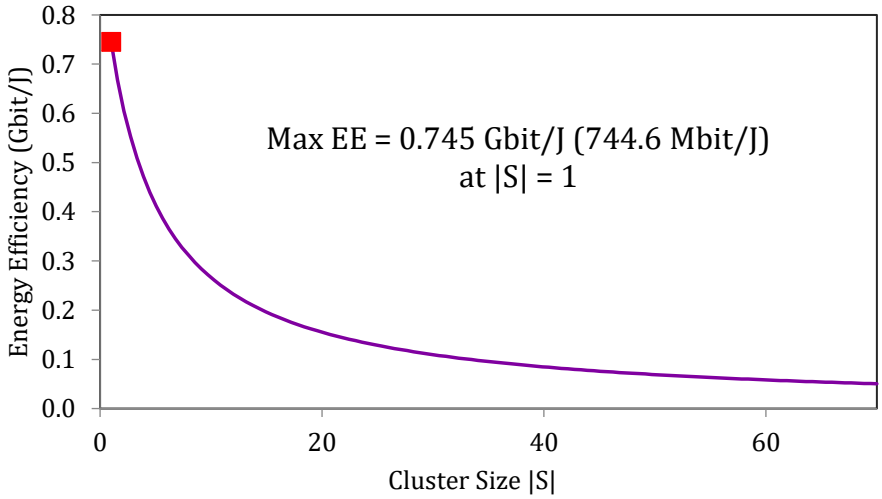


(c) CDF

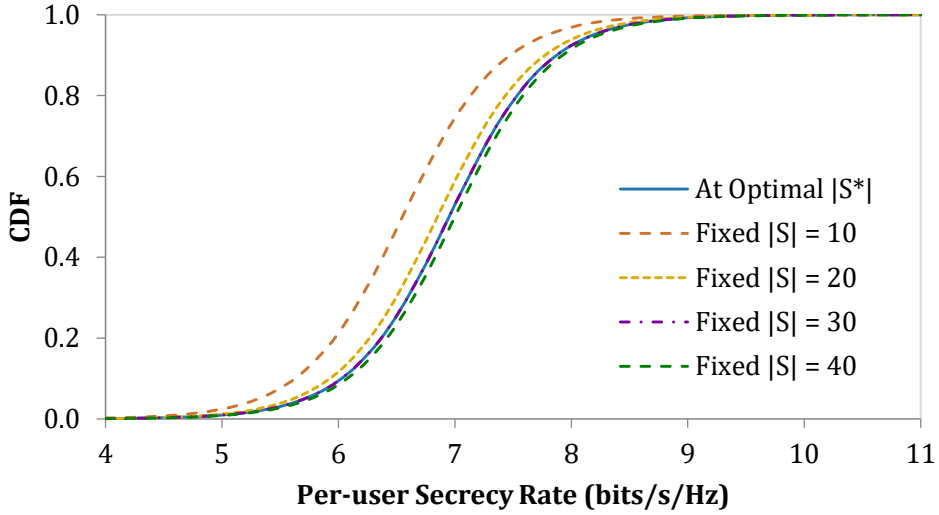
Figure 2. SSE, EE, and CDF with AP selection and WF power allocation when $\eta_k = 0$ for both the targeted user and other users.



(a) SSE

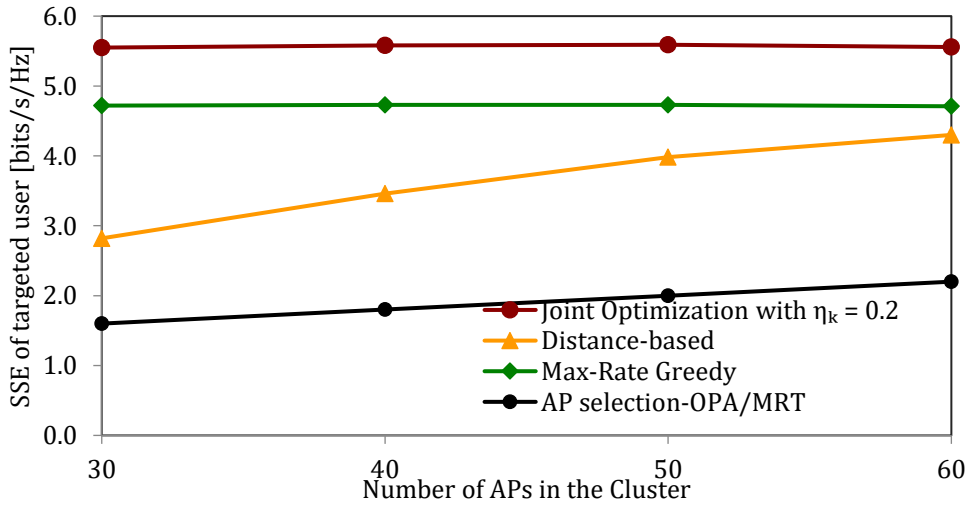


(b) Energy Efficiency

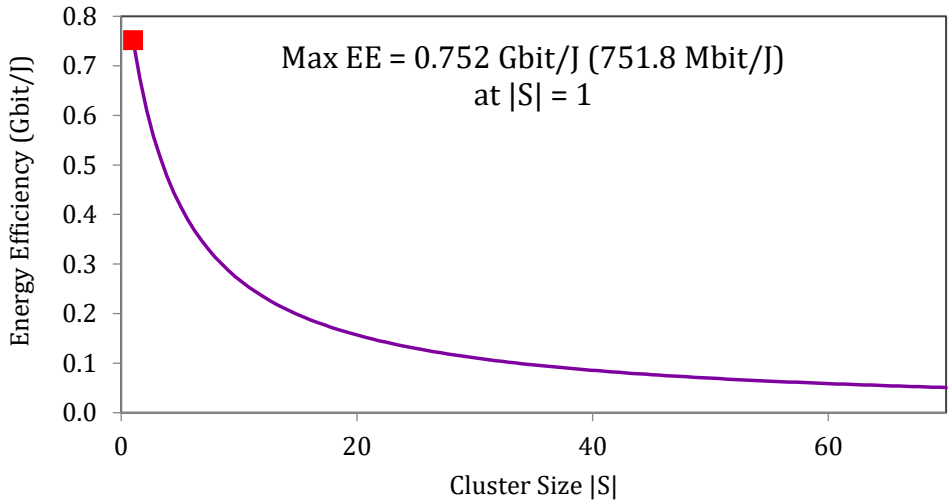


(c) CDF

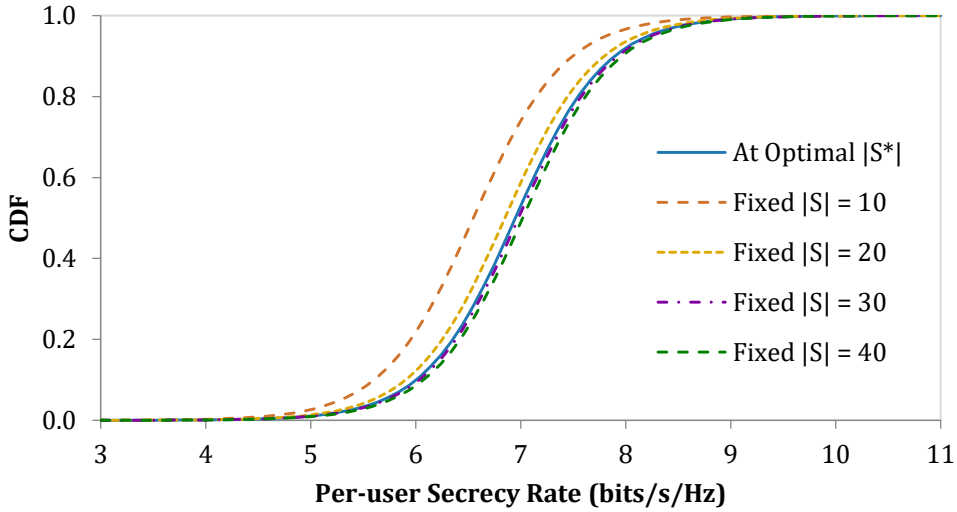
Figure 3. SSE, EE and CDF with AP selection and WF power allocation when $\eta_k = 0.1$ for both the targeted user and other users.



(a) SSE

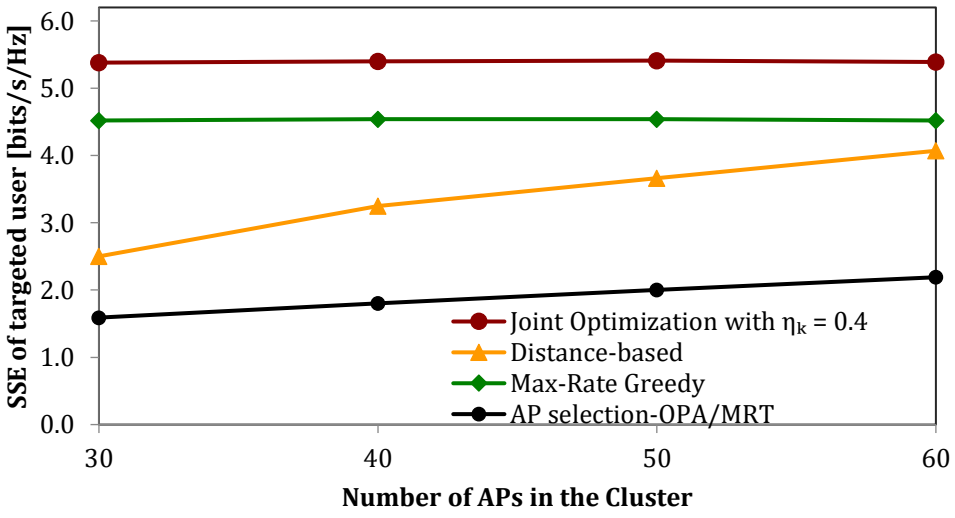


(b) Energy Efficiency

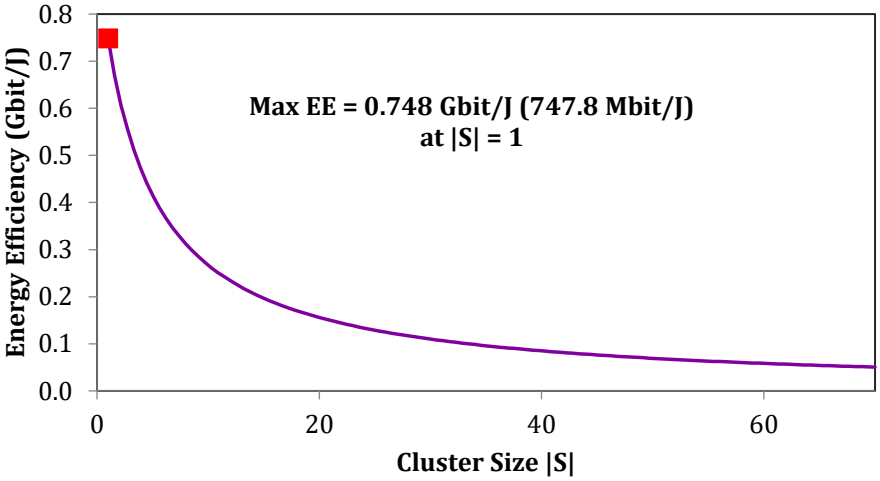


(c) CDF

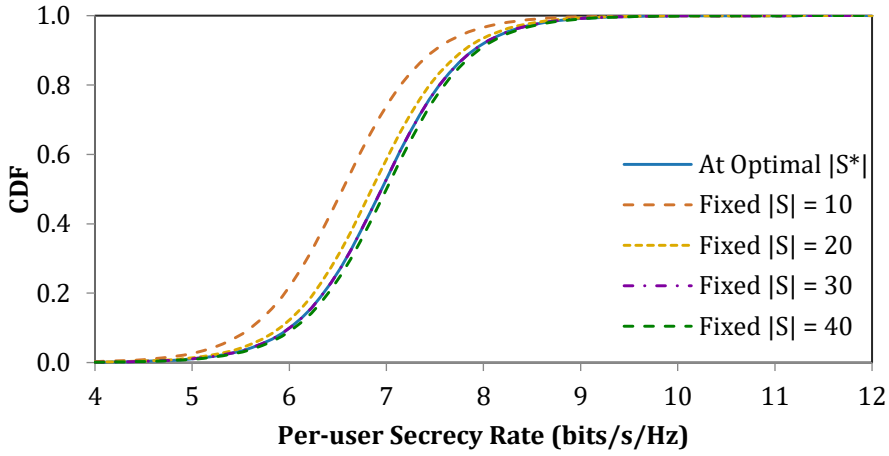
Figure 4. SSE, EE and CDF with AP selection and WF power allocation when $\eta_k = 0.2$ of targeted users and $\eta_k = 0.1$ for other users



(a) SSE



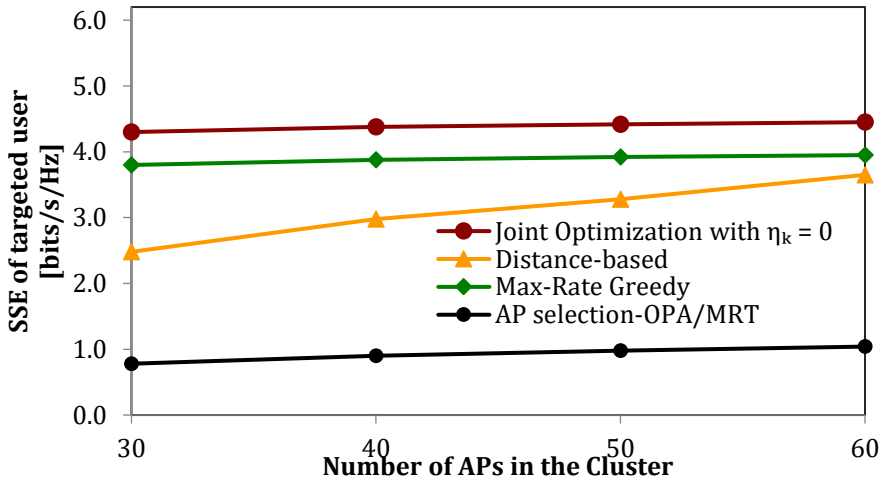
(b) Energy Efficiency



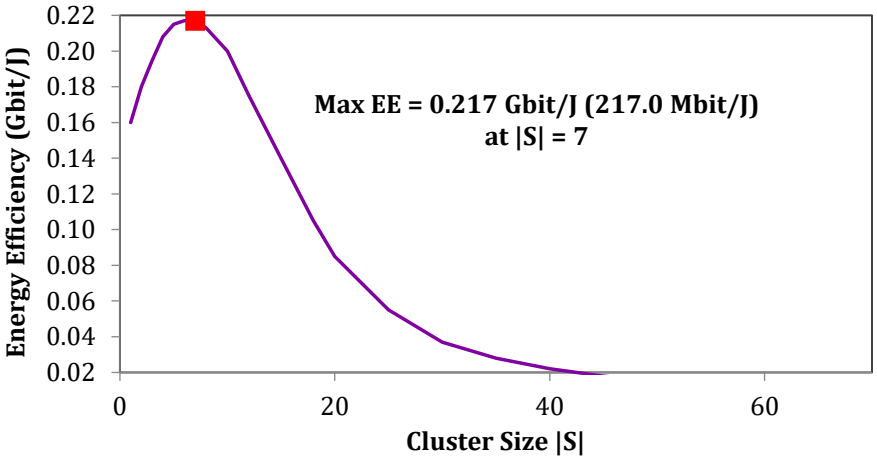
(c) CDF

Figure 5. SSE, EE and CDF with AP selection and WF power allocation when $\eta_k = 0.4$ of targeted users and $\eta_k = 0.1$ for other users

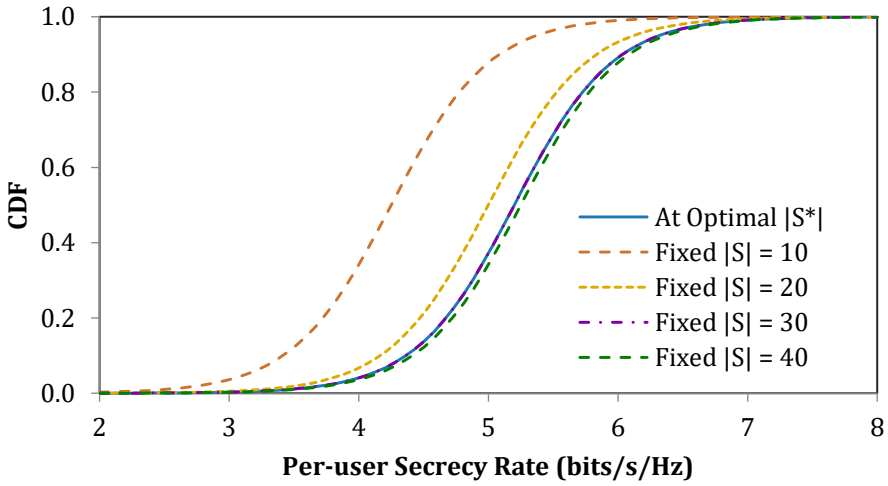
On **Figs. 6 to 9** show the results obtained with EPA under different CSI estimation error levels. The simulation parameters and AP-selection schemes are kept unchanged, while only the CSI estimation error level is varied. For the targeted user with $\eta_k = 0.4$, SSE also increases with $|S|$ but at a lower envelope than WF, since EPA cannot exploit link diversity by reallocating power toward stronger effective channels. The proposed joint optimization achieves approximately 3.78 bit/s/Hz at $|S| = 30$ and 3.92 bit/s/Hz at $|S| = 60$, again showing a clear saturation behaviour for large $|S|$. Compared with the benchmark baseline, this corresponds to a significant improvement, as illustrated in **Fig. 9**.



(a) SSE

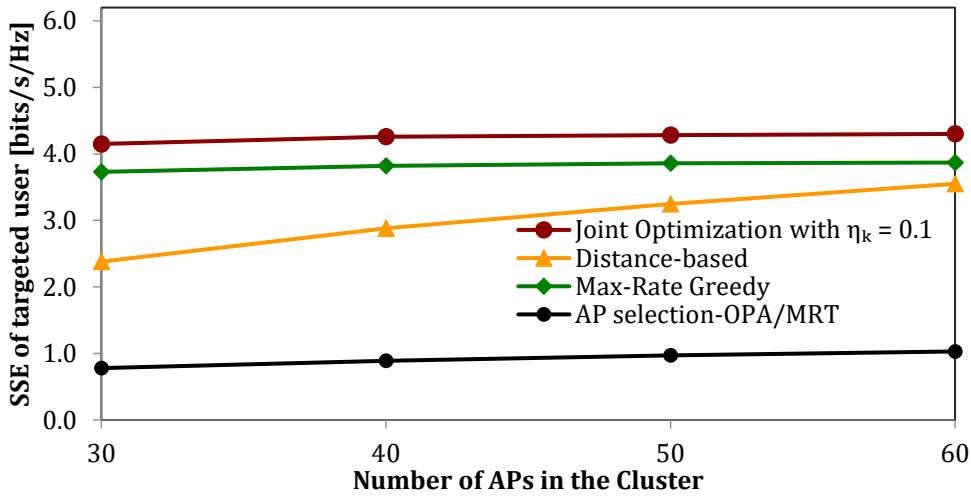


(b) Energy Efficiency

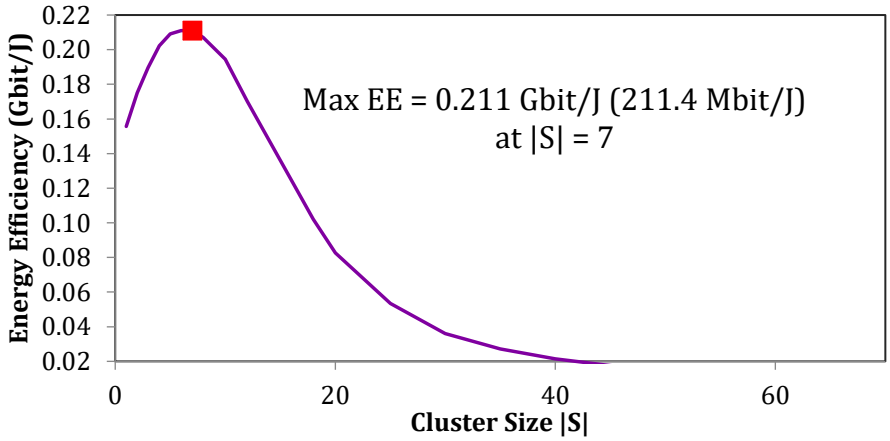


(c) CDF

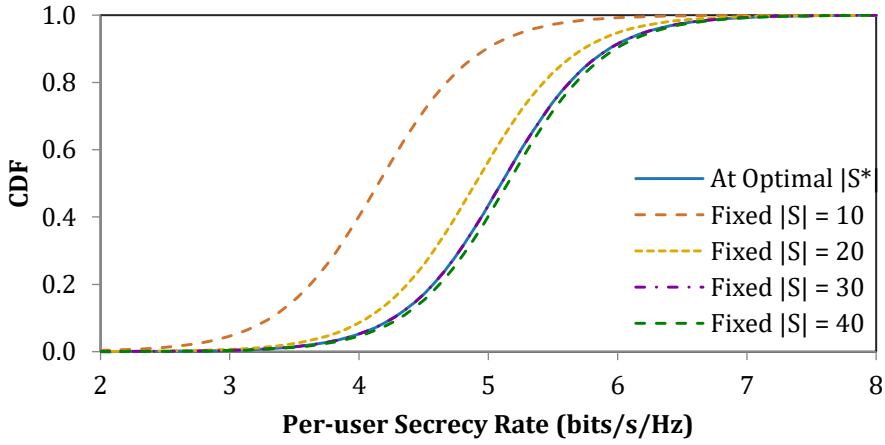
Figure 6. SSE, EE and CDF with AP selection and EPA when $\eta_k = 0$ for both the targeted user and other users.



(a) SSE

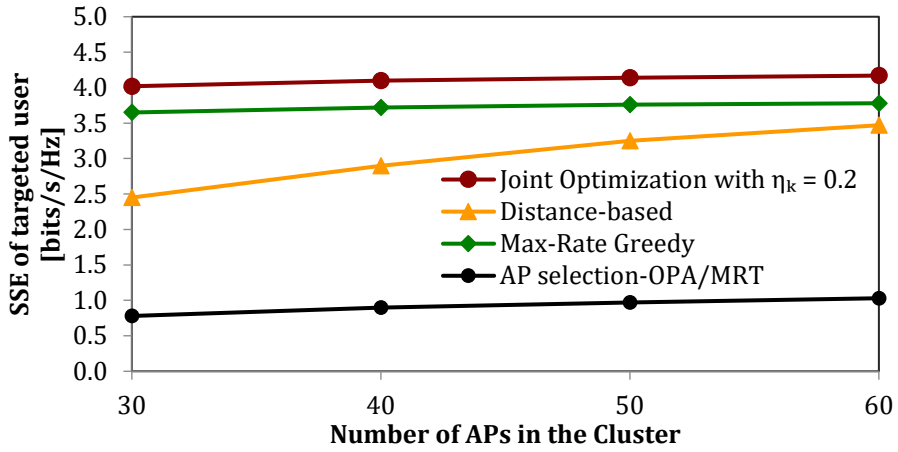


(b) Energy Efficiency

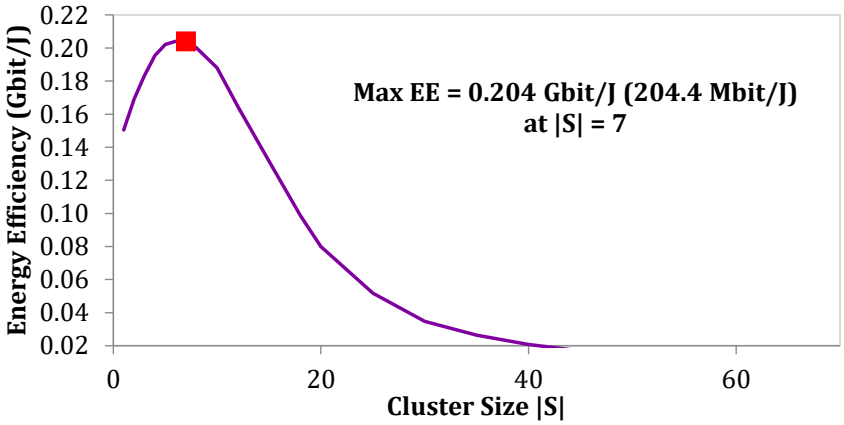


(c) CDF

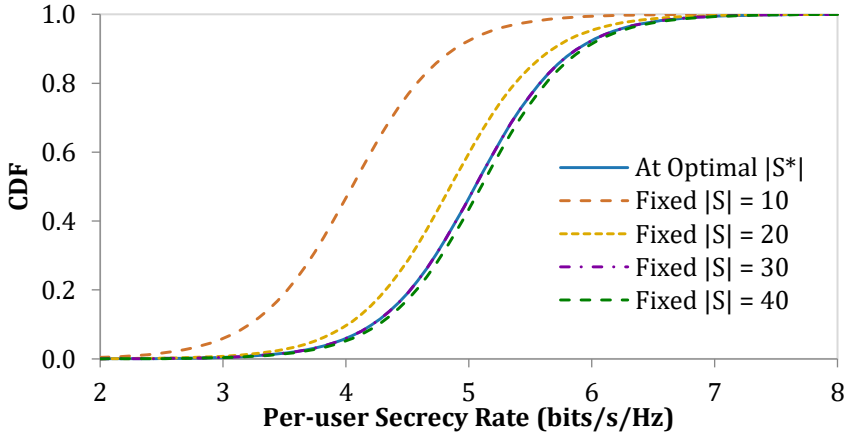
Figure 7. SSE, EE and CDF with AP selection and EPA when $\eta_k = 0.1$ for both the targeted user and other users.



(a) SSE

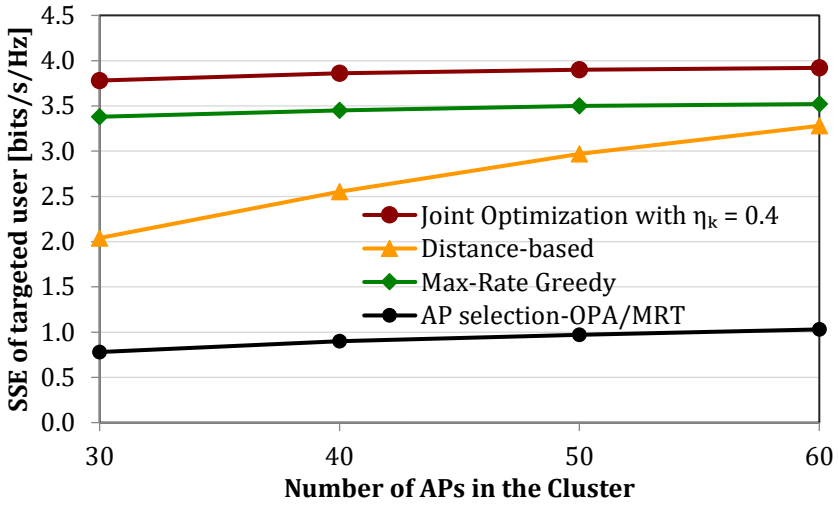


(b) Energy Efficiency

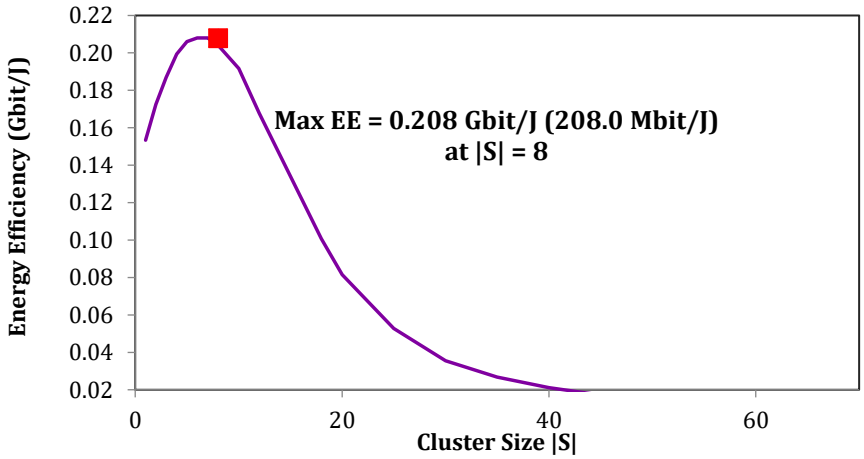


(c) CDF

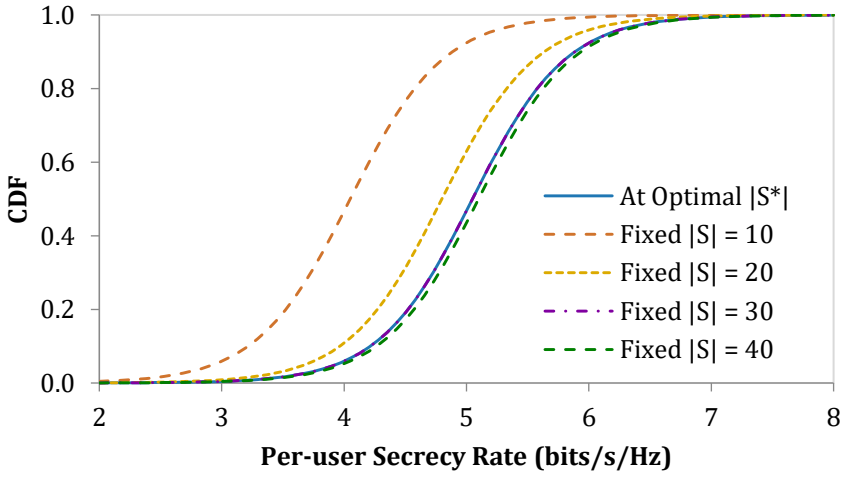
Figure 8. SSE, EE and CDF with AP selection and EPA when $\eta_k = 0.2$ of targeted users and $\eta_k = 0.1$ for other users.



(a) SSE



(b) Energy Efficiency



(c) CDF

Figure 9. SSE, EE and CDF with AP selection and EPA when $\eta_k = 0.4$ of targeted users and $\eta_k = 0.1$ for other users.

About the Rician channel that modelled via Nakagami-m with $m > 1$ in **Figs. 10** and **12,** which is applied for both the legitimate and eavesdropper channels, the secrecy spectral efficiency increases with the cluster size for all AP-selection strategies and then gradually saturates for large $|S|$. This behavior is expected since the presence of a dominant component improves the effective channel quality. However, secrecy depends on the difference between the legitimate and eavesdropper channels. When Eve benefits similarly from the dominant component, the secrecy can be reduced, so this explains why Rayleigh may yield higher SSE in the considered setup.

Finally, under Nakagami-m approximate no fading (LOS) when $\eta = 0.1$, WF continues to outperform EPA by giving more power to the most beneficial AP–user links. In this scenario, the Nakagami-m setting was applied to the small-scale fading of both the legitimate and eavesdropper channels. Although the channel becomes more deterministic, the effective channel strengths across the selected APs remain non-uniform due to large-scale fading, which allows WF to exploit link heterogeneity and avoid wasting power on weak AP links. As shown in **Fig. 13**, the proposed joint optimization with WF achieves an SSE of approximately 5.50 bit/s/Hz at $|S| = 30$ and 5.48 bit/s/Hz at $|S| = 60$. In contrast, under EPA as shown in **Fig. 11**, the proposed method give about 4.30 bit/s/Hz at $|S| = 30$ and 4.45 bit/s/Hz at $|S| = 60$. These results confirm that WF remains beneficial even in near-no-fading channels, particularly when combined with secrecy-aware AP selection.

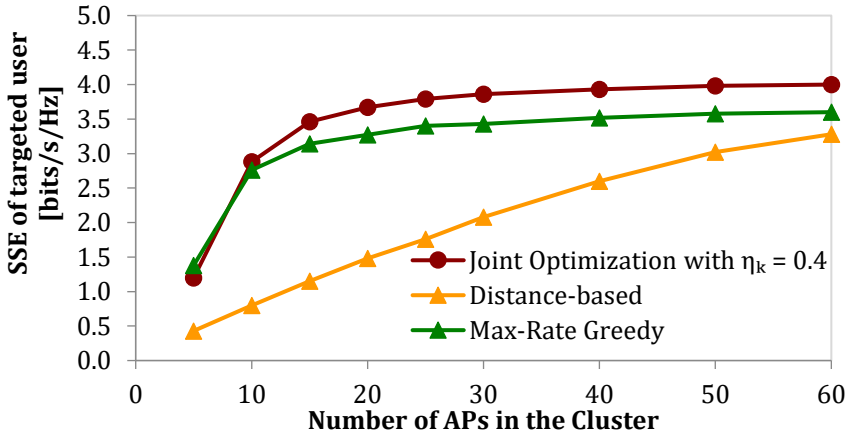


Figure 10. SSE with AP selection and EPA when $\eta_k = 0.4$ of the targeted user and $\eta_k = 0.1$ for other users, under Nakagami-m fading, which approximates Rician fading.

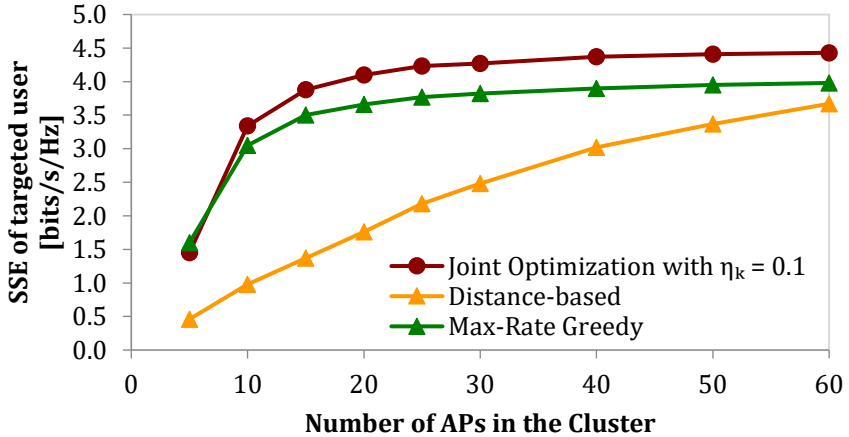


Figure 11. SSE with AP selection and EPA when $\eta_k = 0.1$ for both the targeted user and other users., under Nakagami-m fading which approximates no fading

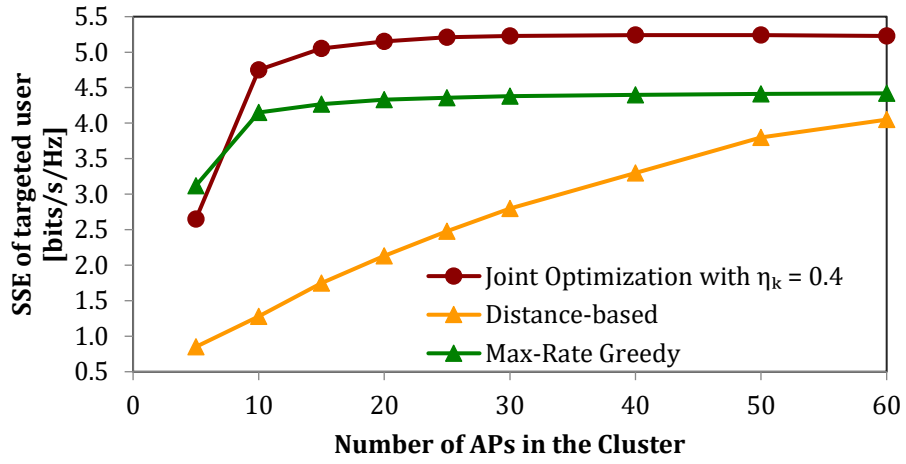


Figure 12. SSE with AP selection and WF power allocation when $\eta_k = 0.4$ of targeted user and $\eta_k = 0.1$ for other users, under Nakagami-m fading which approximates Rician fading

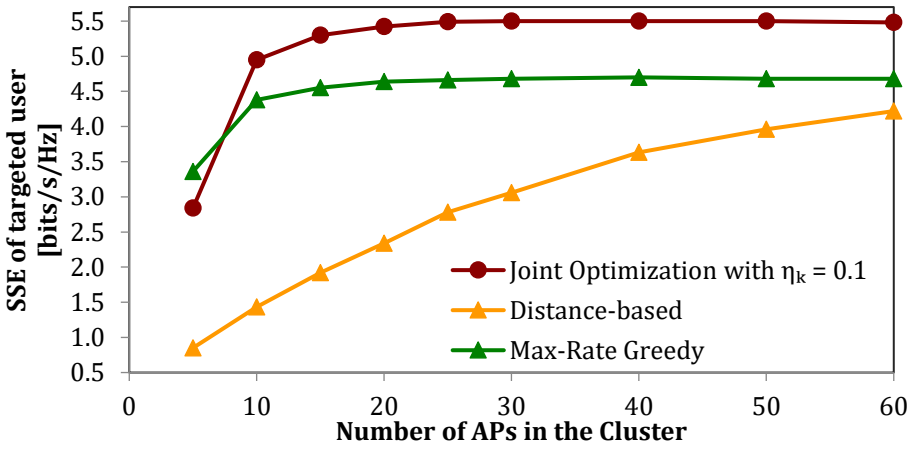


Figure 13. SSE with AP selection and WF power allocation when $\eta_k = 0.1$ for both the targeted user and other users, under Nakagami-m fading which approximates no fading

5.1 Sensitivity Analysis of the Regularization Parameter λ

To validate the robustness of the proposed algorithm with respect to the choice of regularization parameter, the impact of λ on both the selected cluster size |S*| and the achieved secrecy spectral efficiency (SSE) is evaluated. As λ increases, the regularization penalty more strongly discourages the activation of additional APs, leading to a monotonic decrease in the selected cluster size. When EPA is applied, the selected cluster size decreases from approximately 58 APs at λ = 0.01 to approximately 12 APs at λ = 1.0. A similar behavior is observed under WF power allocation, where the selected cluster size decreases from approximately 37 APs at λ = 0.01 to approximately 9 APs at λ = 1.0. This confirms that increasing λ consistently reduces the number of active APs under both power-allocation policies. The corresponding SSE exhibits a more gradual behavior. Under EPA, the SSE remains nearly constant in the intermediate range λ ∈ [0.05, 0.2], where it decreases by

approximately 4% from 4.29 to 4.11 bit/s/Hz, while the selected cluster size is reduced by nearly half, from 38 to 22 APs. Under WF, the SSE is also relatively stable in the same range, decreasing only from 5.847 to 5.708 bit/s/Hz, corresponding to approximately 2.4% reduction, while the selected cluster size decreases from about 26.5 to 16.6 APs as shown in **Fig. 14**. The gradual rather than abrupt nature of the SSE response confirms that the proposed framework is robust to the choice of λ within a reasonable range, and that λ = 0.1 represents a stable operating point rather than a fine-tuned setting.

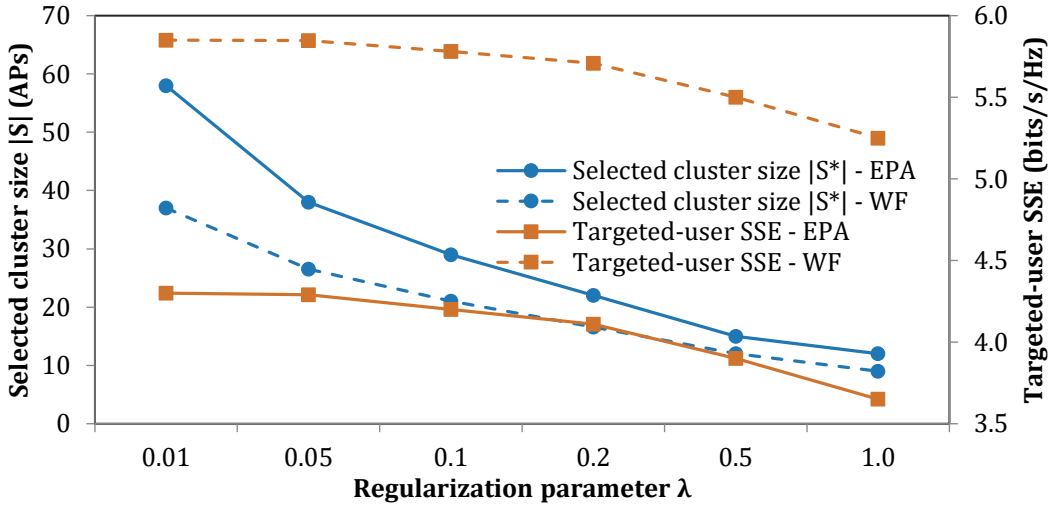


Figure 14. Sensitivity of the proposed AP-selection algorithm to the regularization parameter λ for both EPA and WF for η_k = 0.1 and Nakagami-m fading with m = 1.

Fig. 15 compares the targeted-user SSE under EPA, WF, and the secrecy-ratio heuristic using the same proposed AP-selection order for $\eta_k = 0.4$ and Nakagami-m fading with $m = 1$. The results show that WF clearly improves over EPA because it allocates power according to the effective legitimate-channel quality instead of distributing it uniformly. The secrecy-ratio heuristic achieves a slightly higher SSE than WF; however, this result represents an idealized benchmark, since it assumes that the large-scale Eve channel gain $\beta_{l,e}$ is known at the CPU.

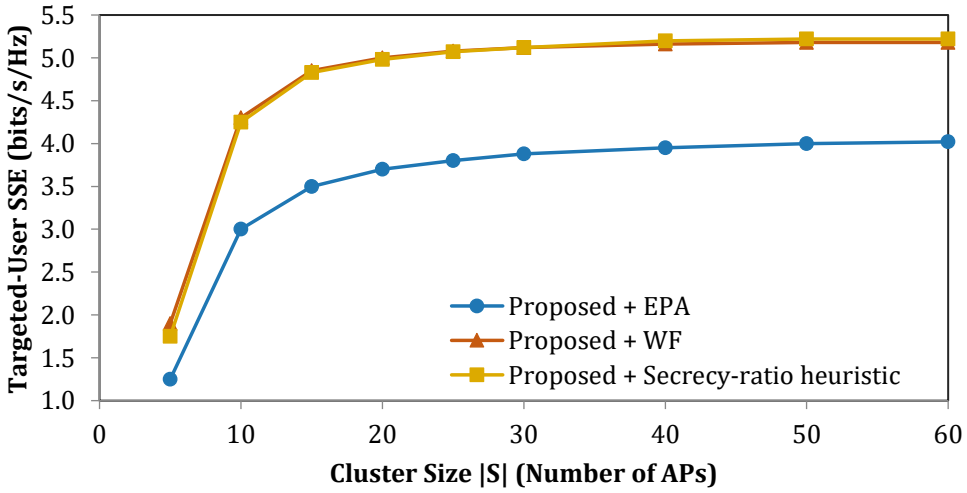


Figure 15. Targeted-user SSE comparison for EPA, WF, and the secrecy-ratio heuristic using the same proposed AP-selection order under $\eta_k = 0.4$ and Nakagami-m fading with $m = 1$.

6. CONCLUSIONS

This work investigated physical-layer security in the downlink of cell-free massive MIMO systems in the presence of an active eavesdropper, with emphasis on the secrecy performance of a targeted user. A scalable MRT-based transmission framework was considered under imperfect CSI, and secrecy performance was quantified through SINR-based achievable rates and the corresponding secrecy rate metric. To enhance secrecy under practical power and infrastructure constraints, two power allocation strategies were examined: equal power allocation (EPA) as a baseline and water-filling (WF), together with an optimized AP-selection mechanism that activates a limited subset of APs according to a secrecy-oriented objective. The simulation results demonstrate that WF consistently achieves higher secrecy than EPA, with the largest gains observed when Eve is close to the targeted user. Furthermore, secrecy-oriented AP selection outperforms non-optimized strategies by prioritizing APs that best contribute to the secrecy objective. Under matched benchmark settings, the proposed framework achieves higher secrecy performance than the reference baseline. In addition, the energy efficiency results highlight a fundamental trade-off in which increasing the cluster size can improve secrecy, but it may also increase total power consumption due to the larger active AP subset and circuit power, suggesting an operating point that balances secrecy and energy efficiency. Finally, to capture diverse propagation conditions, Nakagami-m fading was employed with different parameter settings, $m = 1$ corresponds to Rayleigh fading, intermediate $m > 1$ values approximate Rician channels, and very large values of m model near no-fading propagation. Overall, the results show that the proposed joint optimization framework provides improved secrecy performance gains over the benchmark baseline. For an estimation error of 0.1, the SSE improvement reaches 149% under WF and 317% under EPA. At an estimation error of 0.4, the proposed algorithm achieves 144.5% under WF and 280.6% under EPA.

NOMENCLATURE

Symbol	Description	Symbol	Description
$a_{i,k}$	effective aggregate beamformed gain from the stream of user i observed at user k, dimensionless	n_k	additive white Gaussian noise at user k
$a_{k,k}$	effective aggregate beamformed gain of the stream intended for user k, dimensionless	$p_{l,k}$	downlink power allocated by AP l to user k, W
B	system bandwidth, Hz	P_c	circuit power consumed by each active AP, W
$d_{l,E}$	distance between AP l and Eve, m	P_{max}	maximum transmit power per AP, W
$d_{l,k}$	distance between AP l and user k, m	P_{tot}	total consumed power of the active AP subset, W
E[·]	expectation operator	$R_{E,k}$	achievable rate at Eve for decoding user k, bit/s/Hz
EE	energy efficiency, Gbit/J	R_k	achievable downlink rate of user k, bit/s/Hz
f(S)	sum secrecy-rate function for selected AP set S, bit/s/Hz	R_k^{sec}	secrecy spectral efficiency of user k, bit/s/Hz
$g_{l,E}$	downlink channel from AP l to Eve, dimensionless	R_{mean}^{sec}	mean secrecy spectral efficiency, bit/s/Hz

Symbol	Description	Symbol	Description
$h_{l,k}$	downlink channel from AP l to user k, dimensionless	R_{sum}^{sec}	sum secrecy spectral efficiency of all users, bit/s/Hz
$\hat{h}_{l,k}$	estimated downlink channel from AP l to user k, dimensionless	S	selected AP subset, dimensionless
$\tilde{h}_{l,k}$	channel-estimation error from AP l to user k, dimensionless	S*	optimal selected AP subset, dimensionless
J(S)	regularized secrecy objective function for AP set S, bit/s/Hz	s_k	normalized data symbol intended for user k, dimensionless
K	number of legitimate users, dimensionless	$SM_{l,k}$	large-scale secrecy metric for AP l and user k, dimensionless
k	legitimate-user index, dimensionless	V	ground set of all candidate APs, dimensionless
L	number of access points, dimensionless	$w_{l,k}$	normalized MRT precoding vector from AP l to user k, dimensionless
l	access-point index, dimensionless	x_l	transmitted downlink signal from AP l, dimensionless
M	number of antennas per access point, dimensionless	y_E	received signal at Eve, dimensionless
m	Nakagami-m fading parameter, dimensionless	y_k	received signal at user k, dimensionless
n_E	additive white Gaussian noise at Eve	|S|	cardinality of the selected AP subset, dimensionless
α	path-loss exponent, dimensionless	ε	small positive constant used to avoid division by zero, dimensionless
$\beta_{l,E}$	large-scale fading coefficient between AP l and Eve, dimensionless	η_k	CSI estimation error level or NMSE level of user k, dimensionless
$\beta_{l,k}$	large-scale fading coefficient between AP l and user k, dimensionless	λ	regularization parameter for penalizing AP activation, dimensionless
$\gamma_{E,k}$	SINR at Eve when decoding user k, dimensionless	μ_l	water level used for water-filling power allocation at AP l, W
γ_k	downlink SINR at user k, dimensionless	σ^2	noise power, W
Γ(·)	gamma function	Ω	average fading power of the Nakagami-m distribution, dimensionless
Δ_l	marginal objective gain obtained by adding AP l, bit/s/Hz		

Acknowledgements

The authors would like to thank the Department of Electronics and Communications Engineering, College of Engineering, University of Baghdad, for providing academic support.

Credit Authorship Contribution Statement

Ghaydaa Alaa Hussain: Methodology, Software, Validation, Formal analysis, Investigation, Visualization, Writing – original draft. Aqiel Niama Almamori: Supervision, Methodology, Project administration, Writing – review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

Alageli, M., Ikhlef, A., Alsifiany, F., Abdullah, M.A.M., Chen, G. and Chambers, J., 2020. Optimal downlink transmission for cell free SWIPT massive MIMO Systems with active eavesdropping. In: *IEEE Transactions on Information Forensics and Security*, 15, pp. 1983-1998. https://doi.org/10.1109/TIFS.2019.2954748.

Atiya, Y.S., Mobini, Z., Ngo, H.Q. and Matthaiou, M., 2023. Cell-free massive MIMO with protective partial zero-forcing and active eavesdropping. In: *IEEE Vehicular Technology Conference*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/VTC2023-Spring57618.2023.10201104.

Atiya, Y.S., Mobini, Z., Ngo, H.Q. and Matthaiou, M., 2024. Joint power optimization and AP selection for secure cell-free massive MIMO. In: *2024 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE. pp. 1–6. https://doi.org/10.1109/WCNC57260.2024.10570555.

Atiya, Y.S., Mobini, Z., Ngo, H.Q. and Matthaiou, M., 2024. Secure transmission in cell-free massive MIMO under active eavesdropping. *IEEE Transactions on Wireless Communications*, 23(12), pp. 18036-18052. https://doi.org/10.1109/TWC.2024.3459628.

Atiya, Y.S., Mobini, Z., Ngo, H.Q. and Matthaiou, M., 2025. Cell-free massive MIMO with multiple active eavesdroppers. *IEEE Open Journal of the Communications Society*, 6, pp. 1859–1872. https://doi.org/10.1109/OJCOMS.2025.3534640.

Bjornson, E. and Sanguinetti, L., 2020. Making cell-free massive MIMO Competitive with MMSE processing and centralized implementation. *IEEE Transactions on Wireless Communications*, 19(1), pp. 77–90. https://doi.org/10.1109/TWC.2019.2941478.

Chen, S., Zhang, J., Björnson, E., Zhang, J. and Ai, B., 2021. Structured massive access for scalable cell-free massive MIMO systems. In: *IEEE Journal on Selected Areas in Communications*, 39(4), pp. 1086-1100. https://doi.org/10.1109/JSAC.2020.3018836.

Chen, S., Zhang, J., Zhang, J., Björnson, E. and Ai, B., 2022. *A survey on user-centric cell-free massive MIMO systems*. *Digital Communications and Networks*, 24(1), pp. 611-652. https://doi.org/10.1016/j.dcan.2021.12.005.

Choi, Y.J., Yu, J.H., Seo, S.H., Choi, S.G., Jeong, H.Y., Kim, J.-E., Baek, M.-S., You, Y.-H. and Song, H.-K., 2025. CNN-based end-to-end CPU-AP-UE power allocation for spectral efficiency enhancement in cell-free massive MIMO networks. *Mathematics*, 13(9), P. 1442. https://doi: 10.3390/math13091442.

Gómez-Déniz, E. and Gómez-Déniz, L., 2024. A new derivation of the Nakagami-m distribution as a composite of the Rayleigh distribution. *Wireless Networks*, 30(5), pp. 3051–3060. https://doi.org/10.1007/s11276-024-03713-5.

Guo, Z., Sen, V. and Deng, H., 2026. Robust low-complexity WMMSE precoding under imperfect CSI with Per-antenna power constraints. *Sensors*, 26(1). https://doi.org/10.3390/s26010159.

Hasan, M.F. and Almamori, A.N., 2025. Secrecy Rate in BD-RIS-Assisted uplink multi-user MIMO systems under nakagami-m fading with passive eavesdropping. *Journal of Engineering*, 31(11), pp. 73–89. https://doi.org/10.31026/j.eng.2025.11.05.

Hoang, T.M., Ngo, H.Q., Duong, T.Q., Tuan, H.D. and Marshall, A., 2018. Cell-free massive MIMO networks: Optimal power control against active eavesdropping. *IEEE Transactions on Communications*, 66(10), pp. 4724–4737. https://doi.org/10.1109/TCOMM.2018.2837132.

Jiang, H., Kong, L. and Du, S., 2023. Compute-and-forward transmission scheme in cell-free massive MIMO systems. *ICT Express*, 9(6), pp. 1138–1143. https://doi.org/10.1016/j.icte.2023.02.008.

Kapetanovic, D., Zheng, G. and Rusek, F., 2015. Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks. *IEEE Communications Magazine*, *53*(6), pp. 21-27. https://doi.org/10.1109/MCOM.2015.7120012.

Kassam, J., Castanheira, D., Silva, A., Dinis, R. and Gameiro, A., 2023. A review on cell-free massive MIMO systems. *Electronics (Switzerland)*. https://doi.org/10.3390/electronics12041001.

Krause, A. and Golovin, D., 2014. Submodular function maximization. In *Tractability: Practical Approaches to Hard Problems*, pp. 71–104. https://doi.org/10.1017/CBO9781139177801.004.

Li, N., Gao, Y., Xu, K., Guo, M., Sha, N., Wang, X. and Wang, G., 2023. Spatial sparsity-based pilot attack detection and transmission countermeasure for cell-free massive MIMO system. *IEEE Systems Journal*, 17(2), pp. 2065–2076. https://doi.org/10.1109/JSYST.2022.3188279.

Ma, X., Lei, X., Zhou, X. and Tang, X., 2023. Secrecy performance evaluation of scalable cell-free massive MIMO systems: A stochastic geometry approach. *IEEE Transactions on Information Forensics and Security*, 18, pp. 2826–2841. https://doi.org/10.1109/TIFS.2023.3268443.

Nasir, A.A., 2024. joint users' secrecy rate and target's sensing SNR maximization for a secure cell-free ISAC system. *IEEE Communications Letters*, 28(7), pp. 1549–1553. https://doi.org/10.1109/LCOMM.2024.3406398.

Nayebi, E., Ashikhmin, A., Marzetta, T.L., Yang, H. and Rao, B.D., 2017. Precoding and power optimization in cell-free massive MIMO systems. *IEEE Transactions on Wireless Communications*, 16(7), pp. 4445–4459. https://doi.org/10.1109/TWC.2017.2698449.

Nemhauser, G.L., Wolsey, L.A. and Fisher, M.L., 1978. An analysis of approximations for maximizing submodular set functions — I, *Mathematical Programming*, 14(1), pp. 265–294. https://doi.org/10.1007/BF01588971

Ngo, H.Q., Ashikhmin, A., Yang, H., Larsson, E.G. and Marzetta, T.L., 2017. Cell-free massive MIMO versus small cells. *In IEEE Transactions on Wireless Communications*. pp. 1834–1850. https://doi.org/10.1109/TWC.2017.2655515.

Ngo, H.Q., Tran, L.N., Duong, T.Q., Matthaiou, M. and Larsson, E.G., 2018. On the total energy efficiency of cell-free massive MIMO. *In IEEE Transactions on Green Communications and Networking*. pp. 25–39. https://doi.org/10.1109/TGCN.2017.2770215.

Nguyen, N.P., Ngo, H.Q., Duong, T.Q., Tuan, H.D. and Tourki, K., 2018. Secure massive MIMO with the artificial noise-aided downlink training. *In IEEE Journal on Selected Areas in Communications*, 36(4), pp. 802–816. https://doi.org/10.1109/JSAC.2018.2825140.

Park, J., Yun, S. and Ha, J., 2024. Secure power control for downlink cell-free massive MIMO with passive eavesdroppers. *IEEE Transactions on Vehicular Technology*, 73(6), pp. 9038-9043. https://doi: 10.1109/TVT.2023.3348485.

Solaija, M.S.J., Salman, H. and Arslan, H., 2022. Towards a Unified framework for physical layer security in 5G and beyond networks. *IEEE Open Journal of Vehicular Technology*, 3, pp. 321–343. https://doi: 10.1109/OJVT.2022.3183218.

Tubail, D.A., Alsmadi, M. and Ikki, S., 2023. Physical layer security in downlink of cell-free massive MIMO with imperfect CSI. *IEEE Transactions on Information Forensics and Security*, 18, pp. 2945–2960. https://doi.org/10.1109/TIFS.2023.3272769.

Wang, X., Gao, Y., Zhang, G., Guo, M. and Xu, K., 2022. Security performance analysis for cell-free massive multiple-input multiple-output system with multi-antenna access points deployment in presence of active eavesdropping. *International Journal of Distributed Sensor Networks*, 18(8), P. 15501329221114536. https://doi.org/10.1177/15501329221114535.

Wu, Y., Wen, C.K., Chen, W., Jin, S., Schober, R. and Caire, G., 2018. Data-aided secure massive MIMO transmission with active eavesdropping. *IEEE International Conference on Communications (ICC)*, pp. 1-6, https://doi.org/10.1109/ICC.2018.8422338.

Xing, C., Jing, Y., Wang, S., Ma, S. and Poor, H.V., 2020. New viewpoint and algorithms for water-filling solutions in wireless communications. *IEEE Transactions on Signal Processing*, 68, pp. 1618–1634. https://doi.org/10.1109/TSP.2020.2973488.

Zaher, M., Demir, O.T., Bjornson, E. and Petrova, M., 2023. Learning-based downlink power allocation in cell-free massive MIMO systems. *IEEE Transactions on Wireless Communications*, 22(1), pp. 174–188. https://doi.org/10.1109/TWC.2022.3192203.

Zhang, X., Guo, D., An, K., Ding, Z. and Zhang, B., 2019. Secrecy analysis and active pilot spoofing attack detection for multigroup multicasting cell-free massive MIMO systems. *IEEE Access*, 7, pp. 57332–57340. https://doi.org/10.1109/ACCESS.2019.2914028.

Zhang, X., Liang, T., An, K., Zheng, G. and Chatzinotas, S., 2021. Secure transmission in cell-free massive MIMO with RF impairments and low-resolution ADCs/DACs. *IEEE Transactions on Vehicular Technology*, *70*(9), pp. 8937-8949. https://doi.org/10.1109/TVT.2021.3098693.

Zhang, Y., Xia, W., Zheng, G., Zhao, H., Yang, L., and Zhu, H., 2022. Secure transmission in cell-free massive MIMO with low-resolution DACs over Rician fading channels. *IEEE Transactions on Communications*, 70(4), pp. 2606–2621. https://doi.org/10.1109/TCOMM.2022.3147241.

الاختيار المشترك لنقاط الوصول وتخصيص القدرة لأنظمة MIMO الضخمة الآمنة الخالية من الخلايا في ظل التنصّت النشط

غيداء علاء حسين* ، عقيل نعمة المعموري

قسم هندسة الإلكترونيات والاتصالات، كلية الهندسة، جامعة بغداد، بغداد، العراق

الخلاصة

تُعد أنظمة MIMO الضخمة الخالية من الخلايا من أكثر البنى الواعدة لشبكات الاتصالات اللاسلكية المستقبلية، وذلك بسبب قدرتها على توفير تغطية أوسع وموثوقية أعلى وكفاءة طيفية محسّنة، مع دعم الاتصالات الآمنة من خلال التعاون بين نقاط الوصول الموزعة (APs) . ومع ذلك، يصبح تأمين الإرسال الهابط في انظمة (CF-mMIMO) تحديًا كبيرًا ولا سيما عند وجود متنصّت نشط (Eve) بالقرب من المستخدم المستهدف. ولتحقيق كفاءة طيفية سرية عالية (SSE) مع عدد محدود من نقاط الوصول النشطة وضمن ميزانية قدرة محدودة في ظل قنوات Nakagami-m ومع معلومات حالة قناة غير مثالية (CSI) تم اقتراح خوارزمية لاختيار نقاط الوصول موجهة نحو تعزيز السرّية، وذلك بالاعتماد على(MRT) كما تم اعتماد مخططين لتخصيص القدرة، هما التخصيص المتساوي للقدرة (EPA) و تخصيص القدرة بطريقة ملء الماء (WF) . تشير نتائج المحاكاة إلى أن طريقة التفعيل المقترحة لنقاط الوصول القائمة على التحسين المشترك تحسّن معدل السرّية للمستخدم المستهدف مقارنةً باستراتيجيات الاختيار غير المحسّنة. فعند مستوى خطأ تقدير لمعلومات حالة القناة مقداره 0.1، تحقق الطريقة المقترحة تحسينًا في كفاءة السرّية الطيفية بنسبة 149%باستخدام WF وبنسبة 317% باستخدام EPA. أما عند مستوى اعلى لخطأ تقدير معلومات حالة القناة إلى 0.4، فتبلغ نسب التحسين 144.5%باستخدام WF و 280.6%باستخدام EPA.

الكلمات المفتاحية: أنظمة MIMO الخالية من الخلايا، معدل السرية، MIMO متعدد المستخدمين، تلاشي Nakagami-m، أمن الطبقة المادية.