

Beyond LLM-GA: Secure Fluid Antenna Systems with ReEvo-Designed Memetic Algorithm

Hanyong Xu, Zhaolai Dang, and Tong Zhang

Abstract—Fluid antenna systems (FASs) offer significant spatial flexibility, yet securing them against eavesdropping is critical for practical FAS deployment in military, satellite, and internet-of-things networks. Although large language model (LLM)-assisted genetic algorithms (LLM-GAs) can address this secure FAS port selection problem, whether further algorithmic improvement is possible warrants deeper investigation. To this end, we propose a memetic algorithm based on reflective evolution (ReEvo). Unlike the state-of-the-art LLM-GAs, which design only crossover or mutation operators with an LLM, our algorithm leverages an LLM to evolve dedicated crossover, mutation, and local-search operators offline. These operators are then embedded into a memetic search framework, thereby obviating any online LLM queries during execution. Simulation results at equal generation counts demonstrate that our proposed algorithm achieves a higher secure sum-rate than the conventional GA and the state-of-the-art LLM-GAs.

Index Terms—Fluid antenna system, large language model, memetic algorithm, physical-layer security.

I. INTRODUCTION

The ever-increasing demand for high data rates and massive connectivity in next-generation wireless networks calls for new degrees of freedom to enhance spectral efficiency and link reliability. To this end, fluid antenna systems (FASs) enable antenna port selection over a dense aperture, improving signal strength, interference suppression, and spatial diversity without extra radio frequency (RF) chains [1]–[3]. Unfortunately, joint port selection and beamforming, if optimally designed, holds the key to fully unlocking the potential of FAS, yet it poses a mixed-integer nonconvex problem that is computationally challenging [4]–[6].

Securing FAS wireless communications against passive eavesdropping poses a distinct and formidable challenge. This, combined with the need to jointly optimize discrete port selections and continuous beamforming vectors, significantly complicates the design, as the secrecy objective is nonconvex and intricately coupled with multiuser interference and power limitations. Analytical studies characterize secrecy capacity, outage probability, and the impact of spatial channel asymmetry between legitimate users and eavesdroppers [7] and [8]. Recent works jointly optimize beamforming and antenna positions in FAS-aided non-orthogonal multiple access (NOMA) systems [9], or use penalty and majorization–minimization

TABLE I
COMPARISON OF THE LLM-DESIGNED OPERATORS IN [13], [14], AND THE PROPOSED ALGORITHM.

Operator class	Ref. [13] (crossover only)	Ref. [14] (mutation only)	Proposed (memetic)
LLM-Designed Mutation	No	Yes	Yes
LLM-Designed Crossover	Yes	No	Yes
LLM-Designed Local Search	No	No	Yes

procedures for secure and covert links [10]. However, none of the above works has fully addressed the secure port selection problem.

Large language models (LLMs) have recently been used to address the port selection/antenna position selection problem [11]–[14]. In particular, Wang *et al.* [13] applied reflective evolution (ReEvo) [15] to a binary-genetic algorithm (GA) crossover for power minimization. Their crossover uses population fitness, elite-port frequencies, and port co-occurrences, with conventional selection, mutation, elitism, and repair. The learned crossover is generated offline, has no explicit local-search stage, and is not evaluated with a secrecy objective. In addition, Zheng *et al.* [14] proposed an efficient LLM-GA algorithm, which combines a frequency-based crossover with an LLM-designed one-port mutation. Its exchange probability and displacement range are prescribed, after which standard GA selection, elitism, and repair are applied; the target is nonsecure multiuser performance such as max-min signal-to-interference-plus-noise ratio (SINR). Thus, [13] learns only the crossover operator, whereas [14] learns only the mutation operator. Port prediction has also been investigated in [16].

In this paper, we propose a ReEvo-designed memetic optimizer [17] for secure port selection in downlink multiuser FASs, which outperforms state-of-the-art LLM-GAs in terms of secure sum-rate. Each candidate port subset is scored by its achievable secure sum rate, computed via a secure weighted minimum mean-square error (WMMSE) beamforming procedure. Under this secrecy-driven fitness, ReEvo successively evolves three complementary operators offline, namely crossover, mutation, and local-search. The learned crossover exploits elite-port statistics and grid topology; the mutation performs feasible one-in-one-out swaps at both local and global scales; and the local-search operator generates four complementary one-swap neighbors per offspring. All three operators are frozen after offline evolution and embedded into a memetic search framework, requiring no LLM queries during online execution. Unlike prior LLM-GAs that design only crossover or mutation operators without security considera-

This work was supported in part by the National Natural Science Foundation of China under Grant 62401229.

H. Xu and Z. Dang are with the School of Information, Harbin Institute of Technology, Shenzhen, Shenzhen 518055, China (e-mail: {2025311252, 2025310700}@stu.hit.edu.cn).

T. Zhang is with Guangdong Provincial Key Laboratory of Aerospace Communication and Networking Technology, Harbin Institute of Technology, Shenzhen, 518055, China (e-mail: tongzhang@hit.edu.cn).

tion, our method covers all discrete search stages, explicitly accounts for eavesdropper leakage, and performs systematic local refinement, all under the same secrecy-aware fitness. Table I contrasts the LLM-designed operators of [13] and [14] with those of the proposed algorithm. Simulation results demonstrate that our proposed algorithm achieves a higher secure sum-rate than the conventional GA and the state-of-the-art LLM-GAs.

II. SYSTEM MODEL AND PROBLEM FORMULATION

We first define the system model, and then formulate joint secure port selection and beamforming Problem.

A. System Model

We consider a multiuser downlink fluid antenna system (FAS) in which a base station (BS) serves K single-antenna users in the presence of a passive single-antenna eavesdropper. Let $\mathcal{K} \triangleq \{1, \dots, K\}$ denote the user index set. The BS has a rectangular FAS aperture of dimensions $\lambda W_x \times \lambda W_y$, where $\lambda = c/f_c$ and W_x, W_y are normalized by the carrier wavelength. A uniform $N_x \times N_y$ grid provides $N_s = N_x N_y$ candidate ports, of which exactly n_s are active.

Let $(n_{x,i}, n_{y,i})$ denote the two-dimensional grid index of port i , where $1 \leq n_{x,i} \leq N_x$, $1 \leq n_{y,i} \leq N_y$, and $i = n_{y,i} + (n_{x,i} - 1)N_y$. The physical distance between ports i and j is $d_{i,j} = \sqrt{\left(\frac{n_{x,i} - n_{x,j}}{N_x - 1} \lambda W_x\right)^2 + \left(\frac{n_{y,i} - n_{y,j}}{N_y - 1} \lambda W_y\right)^2}$. Consistent with the channel generator, define $J_{i,j} = j_0(2\pi d_{i,j}/\lambda)$, where $j_0(x) = \sin(x)/x$ and $j_0(0) = 1$. This isotropic three-dimensional model differs from the cylindrical Bessel correlation in Jakes' model [18]. The spatial correlation matrix is

$$\mathbf{J} = \begin{bmatrix} J_{1,1} & J_{1,2} & \cdots & J_{1,N_s} \\ J_{2,1} & J_{2,2} & \cdots & J_{2,N_s} \\ \vdots & \vdots & \ddots & \vdots \\ J_{N_s,1} & J_{N_s,2} & \cdots & J_{N_s,N_s} \end{bmatrix} \in \mathbb{R}^{N_s \times N_s}. \quad (1)$$

Because $\mathbf{J}$ is real and symmetric, write its eigendecomposition as $\mathbf{J} = \mathbf{U} \mathbf{\Lambda} \mathbf{U}^T$, where $\mathbf{U}$ is real and orthogonal. Let r_k and r_e denote the BS-to-user and BS-to-eavesdropper distances, respectively. We model the large-scale power gains by $\beta_k = \beta_0(r_k/r_0)^{-\alpha}$ for $k \in \mathcal{K}$ and $\beta_e = \beta_0(r_e/r_0)^{-\alpha}$, where β_0 is the reference gain at distance r_0 and α is the path-loss exponent. The channel vector of user $k \in \mathcal{K}$ is

$$\mathbf{h}_k^H = \sqrt{\beta_k} \mathbf{g}_k^H \mathbf{\Lambda}^{1/2} \mathbf{U}^T, \quad k \in \mathcal{K}, \quad (2)$$

where $\mathbf{g}_k \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_s})$ for $k \in \mathcal{K}$. The eavesdropper channel is

$$\mathbf{h}_e^H = \sqrt{\beta_e} \mathbf{g}_e^H \mathbf{\Lambda}^{1/2} \mathbf{U}^T \quad (3)$$

where $\mathbf{g}_e \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_s})$. Independent Gaussian vectors are drawn for the users and the eavesdropper, and are mapped through the same correlation matrix; hence, the links share spatial correlation but have independent small-scale fading. Shadowing is omitted. As an upper-bound benchmark, we assume that the BS has perfect instantaneous channel state information (CSI) for every link; eavesdropper CSI may have

been acquired while that terminal was previously active. The channels remain quasi-static within each optimization run, so all candidate configurations share the same propagation state. Robust design under imperfect or delayed CSI is outside the present scope.

Let $\mathbf{e}_i$ denote the i th column of $\mathbf{I}_{N_s}$. When n_s distinct ports with indices $m_1, \dots, m_{n_s}$ are activated, their port selection matrix is defined as $\mathbf{E}_{n_s} \triangleq [\mathbf{e}_{m_1}, \dots, \mathbf{e}_{m_{n_s}}] \in \mathbb{R}^{N_s \times n_s}$. Each column of $\mathbf{E}_{n_s}$ selects one physical port, so feasibility requires

$$\mathbf{E}_{n_s}(:, \ell) \in \{\mathbf{e}_1, \dots, \mathbf{e}_{N_s}\}, \quad \ell = 1, \dots, n_s. \quad (4)$$

and the selected ports must be distinct:

$$\mathbf{E}_{n_s}(:, \ell) \neq \mathbf{E}_{n_s}(:, q), \quad \ell \neq q. \quad (5)$$

Together, these constraints activate exactly n_s distinct ports. Define the effective channel vectors $\bar{\mathbf{h}}_k = \mathbf{E}_{n_s}^H \mathbf{h}_k$ and $\bar{\mathbf{h}}_e = \mathbf{E}_{n_s}^H \mathbf{h}_e$. Stacking the user channels gives $\bar{\mathbf{H}} = [\bar{\mathbf{h}}_1, \dots, \bar{\mathbf{h}}_K]^H \in \mathbb{C}^{K \times n_s}$. The BS jointly designs the port selection matrix $\mathbf{E}_{n_s}$ and the beamforming matrix $\mathbf{W} = [\mathbf{w}_1, \dots, \mathbf{w}_K]$, where $\mathbf{w}_k \in \mathbb{C}^{n_s \times 1}$ is the beamformer for legitimate user $k \in \mathcal{K}$. Let $\mathbf{x}_d = [x_1, \dots, x_K]^T$ collect the unit-power data symbols, i.e., $\mathbb{E}[|x_k|^2] = 1$. The transmitted signal is

$$\mathbf{x} = \mathbf{E}_{n_s} \mathbf{W} \mathbf{x}_d = \sum_{k \in \mathcal{K}} \mathbf{E}_{n_s} \mathbf{w}_k x_k, \quad (6)$$

Because the columns of $\mathbf{E}_{n_s}$ are orthonormal, the transmit-power constraint becomes

$$\|\mathbf{E}_{n_s} \mathbf{W}\|_F^2 = \|\mathbf{W}\|_F^2 = \sum_{k \in \mathcal{K}} \|\mathbf{w}_k\|_2^2 \leq P_{\max}. \quad (7)$$

The receiver noises satisfy $n_k \sim \mathcal{CN}(0, \sigma_k^2)$ and $n_e \sim \mathcal{CN}(0, \sigma_e^2)$. The received signals are

$$y_k = \mathbf{h}_k^H \mathbf{E}_{n_s} \mathbf{w}_k x_k + \sum_{j \neq k} \mathbf{h}_k^H \mathbf{E}_{n_s} \mathbf{w}_j x_j + n_k, \quad (8a)$$

$$y_e = \sum_{k \in \mathcal{K}} \mathbf{h}_e^H \mathbf{E}_{n_s} \mathbf{w}_k x_k + n_e. \quad (8b)$$

Under single-user decoding, the eavesdropper treats all other streams as interference. The resulting SINRs are

$$\gamma_k = \frac{|\mathbf{h}_k^H \mathbf{E}_{n_s} \mathbf{w}_k|^2}{\sum_{j \in \mathcal{K} \setminus \{k\}} |\mathbf{h}_k^H \mathbf{E}_{n_s} \mathbf{w}_j|^2 + \sigma_k^2}, \quad k \in \mathcal{K}, \quad (9a)$$

$$\gamma_{e,k} = \frac{|\mathbf{h}_e^H \mathbf{E}_{n_s} \mathbf{w}_k|^2}{\sum_{j \in \mathcal{K} \setminus \{k\}} |\mathbf{h}_e^H \mathbf{E}_{n_s} \mathbf{w}_j|^2 + \sigma_e^2}, \quad k \in \mathcal{K}. \quad (9b)$$

Accordingly, the achievable secrecy rate of user k is

$$R_k^s = [\log_2(1 + \gamma_k) - \log_2(1 + \gamma_{e,k})]^+, \quad k \in \mathcal{K}, \quad (10)$$

following the standard wiretap-rate construction [19].

B. Joint Secure Port Selection and Beamforming Problem

Mathematically, the joint secure port selection and beamforming problem for the downlink multiuser FAS is formulated as follows:

$$\begin{aligned} \text{P1: } & \max_{\mathbf{E}_{n_s}, \mathbf{W}} \sum_{k \in \mathcal{K}} R_k^s(\mathbf{E}_{n_s}, \mathbf{W}) \\ & \text{s.t. } (4), (5), \text{ and } (7). \end{aligned}$$

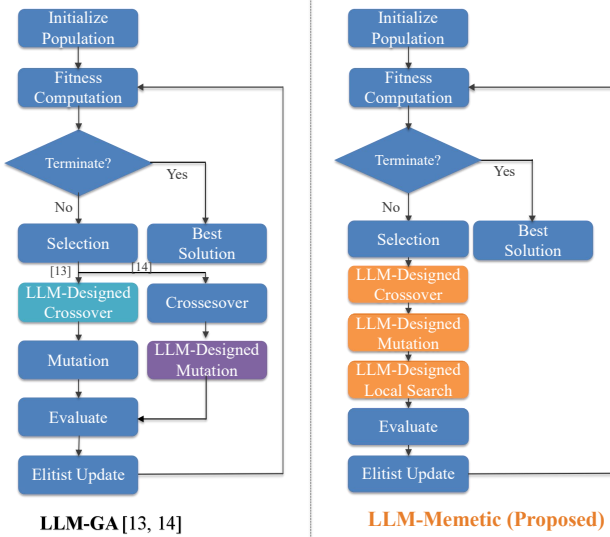


Fig. 1. Flowchart comparison of [13] and [14] with the proposed algorithm.

Physically, selecting a port changes the sampled channels of every user and of the eavesdropper at the same time. The objective therefore rewards ports that strengthen the desired links while suppressing multiuser interference and information leakage, subject to the total transmit power. Since the port-selection constraints introduce a combinatorial discrete space and the secrecy sum-rate is nonlinear in the selection and beamforming variables, Problem P1 is a nonlinear mixed-integer nonconvex program.

III. REEVO-DESIGNED MEMETIC ALGORITHM

To solve Problem P1, we develop a ReEvo-designed memetic algorithm comprising an offline LLM-driven operator design stage and an online memetic search stage that requires no LLM application programming interface (API) calls. In the offline stage, ReEvo evolves three complementary discrete operators (crossover, mutation, and local search) under a secrecy-driven fitness evaluated via secure WMMSE beamforming. In the online stage, each candidate port subset generated by the frozen operators is scored via secure WMMSE beamforming; the memetic search then evolves toward higher secure sum-rates without any LLM queries. Fig. 1 illustrates the overall architecture and highlights the distinction between our method and prior LLM-GAs that design only a crossover operator [13] or only a mutation operator [14].

A. Secure WMMSE Beamforming

For a fixed $\mathbf{E}_{n_s}$, we use a safeguarded WMMSE-based procedure [20]. Initialize $\mathbf{V} = \bar{\mathbf{H}}^H(\bar{\mathbf{H}}\bar{\mathbf{H}}^H + 10^{-6}\mathbf{I})^{-1}$ and $\mathbf{W}^{(0)} = \sqrt{P_{\max}}\mathbf{V}/\|\mathbf{V}\|_F$; if the solve fails, use $\mathbf{V} = \bar{\mathbf{H}}^H$. With the scalar estimate $\hat{x}_k = u_k^*y_k$, the user's minimum mean-square error (MMSE) receiver, mean-square error (MSE), and weight are

$$T_k = \sum_{j \in \mathcal{K}} |\bar{\mathbf{h}}_k^H \mathbf{w}_j|^2 + \sigma_k^2, \quad (11a)$$

$$u_k = \frac{\bar{\mathbf{h}}_k^H \mathbf{w}_k}{T_k}, \quad \varepsilon_k = 1 - \frac{|\bar{\mathbf{h}}_k^H \mathbf{w}_k|^2}{T_k}, \quad (11b)$$

$$q_k = \varepsilon_k^{-1}. \quad (11c)$$

When the eavesdropper decodes stream k and treats the remaining streams as interference, its corresponding variables are

$$T_e = \sum_{j \in \mathcal{K}} |\bar{\mathbf{h}}_e^H \mathbf{w}_j|^2 + \sigma_e^2, \quad (12a)$$

$$u_{e,k} = \frac{\bar{\mathbf{h}}_e^H \mathbf{w}_k}{T_e}, \quad \varepsilon_{e,k} = 1 - \frac{|\bar{\mathbf{h}}_e^H \mathbf{w}_k|^2}{T_e}, \quad (12b)$$

$$q_{e,k} = \varepsilon_{e,k}^{-1}. \quad (12c)$$

For an arbitrary receiver u , the MSE is $e_k(u, \mathbf{W}) = |u|^2 T_k - 2 \operatorname{Re}\{u^* \bar{\mathbf{h}}_k^H \mathbf{w}_k\} + 1$. The rate identity is $\ln(1 + \gamma_k) = \max_{u \in \mathbb{C}, q > 0} \{\ln q - q e_k + 1\}$, attained at (11). For the eavesdropper, $-\ln(1 + \gamma_{e,k}) = \min_{u \in \mathbb{C}, q > 0} \{q e_{e,k} - \ln q - 1\}$, attained at (12). Frozen auxiliary variables lower-bound the legitimate rate but upper-bound the negative eavesdropper rate. Thus the following linearization yields a trial model for the unclipped rate difference, not a guaranteed secrecy-rate lower bound. Omitting the common $1/\ln 2$ factor and constants gives

$$\widetilde{\mathbf{W}} = \arg \max_{\|\mathbf{W}\|_F^2 \leq P_{\max}} -\operatorname{tr}(\mathbf{W}^H \mathbf{A} \mathbf{W}) + 2 \operatorname{Re}\{\operatorname{tr}(\mathbf{B}^H \mathbf{W})\}, \quad (13)$$

where

$$\mathbf{A} = \sum_{k \in \mathcal{K}} q_k |u_k|^2 \bar{\mathbf{h}}_k \bar{\mathbf{h}}_k^H, \quad (14a)$$

$$\mathbf{b}_k = q_k u_k \bar{\mathbf{h}}_k + c_e \bar{\mathbf{h}}_e \bar{\mathbf{h}}_e^H \mathbf{w}_k^{(t)} - q_{e,k} u_{e,k} \bar{\mathbf{h}}_e, \quad (14b)$$

$$c_e = \sum_{j \in \mathcal{K}} q_{e,j} |u_{e,j}|^2, \quad \mathbf{B} = [\mathbf{b}_1, \dots, \mathbf{b}_K]. \quad (14c)$$

Specifically, for the positive quadratic $\mathbf{w}_k^H \mathbf{C}_e \mathbf{w}_k$, where $\mathbf{C}_e = c_e \bar{\mathbf{h}}_e \bar{\mathbf{h}}_e^H \succeq 0$, convexity gives $\mathbf{w}_k^H \mathbf{C}_e \mathbf{w}_k \geq 2 \operatorname{Re}\{(\mathbf{w}_k^{(t)})^H \mathbf{C}_e \mathbf{w}_k\} - (\mathbf{w}_k^{(t)})^H \mathbf{C}_e \mathbf{w}_k^{(t)}$. This affine minorization produces the $\mathbf{C}_e \mathbf{w}_k^{(t)}$ term in (14b). The Lagrangian stationarity condition of (13) is $(\mathbf{A} + \mu \mathbf{I}) \widetilde{\mathbf{W}} = \mathbf{B}$, and hence, when nonsingular, we have

$$\widetilde{\mathbf{W}} = (\mathbf{A} + \mu \mathbf{I})^{-1} \mathbf{B}. \quad (15)$$

Since $\mathbf{A} \succeq 0$, the KKT conditions solve (13) globally: $\mu = 0$ for a feasible unconstrained solution, otherwise bisection enforces $\|\widetilde{\mathbf{W}}\|_F^2 = P_{\max}$ with $\mu > 0$. The implementation adds $10^{-10} \mathbf{I}$ if the zero-multiplier linear solve fails.

For each trial $\mathbf{W}(\eta) = (1 - \eta) \mathbf{W}^{(t)} + \eta \widetilde{\mathbf{W}}$, evaluate $\sum_{k \in \mathcal{K}} R_k^s$ using the per-user secrecy rates in (10). A negative per-user difference contributes zero, while that stream still causes interference. The unclipped trial model retains all streams. Start at $\eta = 1$ and halve it for at most 20 trials; retain the incumbent and stop if none is accepted. The acceptance tolerance is 10^{-10} ; termination also occurs after 30 iterations or improvement below $10^{-6} \max(1, |\sum_{k \in \mathcal{K}} R_k^s|)$. In exact arithmetic, accepting only nondecreasing steps preserves feasibility and gives

$$0 \leq \sum_{k \in \mathcal{K}} R_k^s \leq \sum_k \log_2 \left(1 + \frac{P_{\max} \|\bar{\mathbf{h}}_k\|_2^2}{\sigma_k^2} \right).$$

Thus exact monotone objective values converge if continued indefinitely; this is not a beamformer or stationary-point convergence guarantee.

Algorithm 1 Offline LLM operator design and API-free secure FAS optimization

```

1: for  $q \in \{c, m, l\}$  in order do
2:   Initialize program population  $\Phi_q$  from seed and LLM code.
3:   while fewer than  $N_{\text{eval}}$  programs have been evaluated do
4:     Evaluate training fitness  $F_q$  by secure WMMSE.
5:     Reflect on higher/lower-fitness code; generate programs and update  $\Phi_q$ .
6:   end while
7:   Freeze the best program  $\chi_q^*$  by training fitness.
8: end for
9: Initialize  $P$  feasible chromosomes; evaluate and cache fitness and beamformers.
10: for  $g = 1, \dots, G$  do
11:   Preserve  $E$  elites and select parents for  $P - E$  children.
12:   Apply  $\chi_c^*$  and  $\chi_m^*$ ; repair cardinality.
13:   Apply  $\chi_l^*$  to create  $N_l$  neighbors per child.
14:   Score uncached candidates by secure WMMSE.
15:   Retain the best  $P - E$  candidates with the  $E$  elites.
16: end for
17: return Best chromosome and its cached beamformer.

```

B. ReEvo-Designed Memetic Port Search

We encode a port subset as a binary chromosome $\mathbf{s} \in \{0, 1\}^{N_s}$ satisfying $\mathbf{1}^T \mathbf{s} = n_s$. Following [15], the LLM acts as a hyper-heuristic. Let $\mathcal{Q} = \{c, m, l\}$ denote the crossover, mutation, and local-search operator classes, respectively. DeepSeek Reasoner evolves each class separately. For class q , each program χ_q is an individual in population Φ_q . Its meta-fitness is the best secure sum-rate attained when an inner GA-based search uses χ_q on the fixed training channel set:

$$R_{\text{sec}}(\mathbf{s}) = \sum_{k \in K} R_k^s(\mathbf{s}), \quad (16a)$$

$$F_q(\chi_q) = \max_{\mathbf{s} \in \text{GA}_q(\chi_q)} R_{\text{sec}}(\mathbf{s}), \quad (16b)$$

Because (16) includes secure WMMSE optimization, programs are selected by the target secrecy objective rather than a surrogate port score.

The three operator classes receive feasible binary chromosomes and grid indices; crossover also receives population fitness and ranks. Crossover combines two parents, mutation performs a one-in-one-out swap, and local search generates four neighbors: nearby, long-distance, same-row/column, and crowded-to-sparse relocation. Returned chromosomes are repaired to contain exactly n_s active ports; invalid programs are discarded. All fitness evaluations use the same training channels, beamformer initialization, and stopping rule.

Algorithm 1 summarizes the procedure. Crossover is trained with conventional mutation and no local search; mutation is trained with crossover fixed; local search is trained with both fixed. Programs are selected by training fitness and then checked on separate validation channels.

During online execution, the three frozen operators generate offspring and neighbors, while caching and elitist replacement control the WMMSE evaluations.

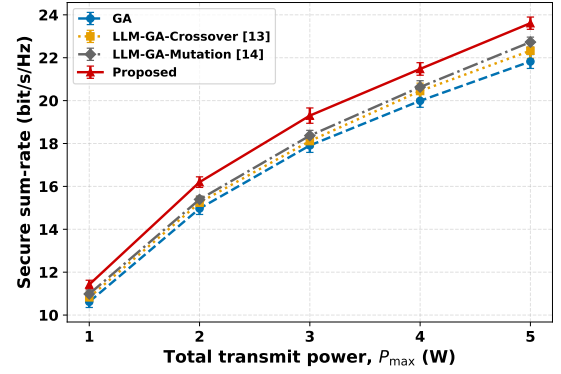


Fig. 2. Mean secure sum-rate versus total transmit power.

TABLE II
SIMULATION PARAMETERS.

Parameter	Setting
Grid / aperture	$20 \times 20 / 0.5 \times 0.5 \text{ m}^2$
Carrier frequency	3.4 GHz
Users / eavesdropper	$K = 10 / 1$
Active ports	$n_s = 10$
Distances / path loss	$r_k = r_e = r_0; \beta_k = \beta_e = 1$
Noise variance	$\sigma_k^2 = \sigma_e^2 = 1$ (normalized)
Transmit power	$P_{\text{max}} \in \{1, 2, 3, 4, 5\} \text{ W}$
Population / elites	$P = 20 / E = 4$
Offspring / generations	16 / 100
Mutation probability	0.2
Operator train / validation	10 / 20 disjoint channels
Test channels / random seeds	20 paired / 20 seeds
LLM / programs	DeepSeek / 10-program population

IV. SIMULATIONS

Table II summarizes the simulation parameters. The power sweep uses normalized gains $\beta_k = \beta_e = 1$ and noise variances $\sigma_k^2 = \sigma_e^2 = 1$. Equivalently, $r_k = r_e = r_0$, $\beta_0 = 1$, and the path-loss exponent cancels. Each realization includes all K user channels and one eavesdropper channel. All methods share test channels, initial populations, and random seeds at each power. Offline ReEvo uses DeepSeek to generate operator code with 10 programs in the population. Fitness uses 10 training channels; selected programs are checked on 20 disjoint validation channels without reranking. Training and validation searches use 20 and 50 generations at power 2.5, respectively. Final testing uses 20 separate channels and 20 random seeds; training and validation use 10 and 20 channel realizations, respectively. The online optimizer uses frozen code, with no trainable neural-network layers or hidden dimensions and no LLM calls.

Throughout, the reported rate is the total secrecy rate summed over users and averaged over test channels, never divided by K . The same test channels are reused across all total transmit power levels. The error bars show one sample standard deviation of the 20 per-channel total rates.

Fig. 2 shows that the secure sum-rate of all four methods increases as P_{max} grows from 1 to 5 W, with the proposed algorithm remaining the highest at every point. At 1 W, it achieves 11.423 bit/s/Hz, corresponding to gains of 7.6%, approximately 6%, and approximately 4% over GA, LLM-GA-crossover [13], and LLM-GA-mutation [14], respectively. At 5 W, it achieves 23.611 bit/s/Hz, yielding gains of 8.2%, approximately 5%, and approximately 4% over the same

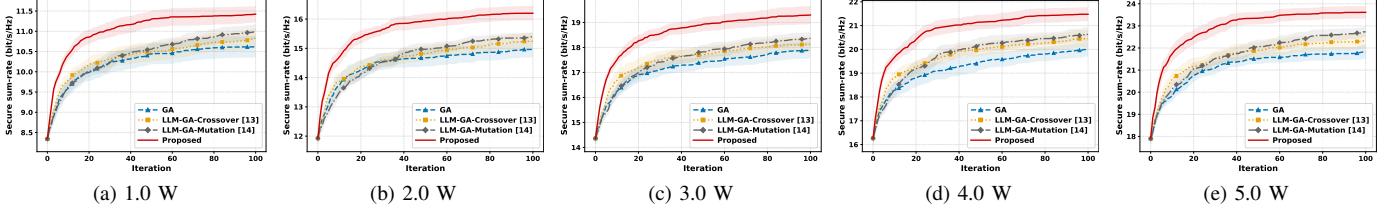


Fig. 3. Secure sum-rate convergence for five total transmit power levels.

three baselines. The two LLM-GA baselines consistently lie between GA and the proposed algorithm, with visibly overlapping error bars at some operating points. A possible explanation is that elite-aware recombination preserves useful spatial patterns, while local and global exchanges explore the tradeoffs among signal strength, interference, and leakage. This ordering holds at equal generation counts, though the additional local-search evaluations may particularly account for the gains obtained by the proposed algorithm. Note that each operating point plotted in Fig. 2 is the generation-100 terminal value of the corresponding convergence curve in Fig. 3; that is, Fig. 2 summarizes the final (generation-100) data of Fig. 3 as a function of transmit power.

Fig. 3 shows secure sum-rate convergence over 100 generations. The proposed algorithm separates from the baselines early and stays ahead in all five power panels, while all curves gradually flatten as the populations approach stable incumbents. The terminal values at generation 100 correspond to the respective operating-point results summarized in Fig. 2, linking the convergence endpoint to the power-sweep comparison. Local search evaluates additional one-swap neighbors, so these curves do not establish faster convergence in runtime or evaluation count.

V. CONCLUSION

This paper presented a ReEvo-designed memetic optimizer for joint port selection and secure beamforming in multiuser fluid antenna systems. An LLM evolves dedicated crossover, mutation, and local-search operators offline under a secrecy-driven fitness, and the frozen programs incur no online LLM-query overhead. For each candidate port configuration, the beamformer is optimized by secure WMMSE.

Across the tested total transmit power levels, the proposed method consistently obtains the highest mean secure sum-rate among the conventional GA and both LLM-GA baselines, with gains that remain visible from low to high transmit power. These results indicate that evolving all three discrete search operators offline can outperform LLM-GAs that design only a single operator. Extending the framework to imperfect or delayed CSI and to more general multiuser and multi-antenna scenarios is left as future work.

REFERENCES

- [1] W. K. New *et al.*, “A tutorial on fluid antenna system for 6G networks: Encompassing communication theory, optimization methods and hardware designs,” *IEEE Commun. Surveys Tuts.*, vol. 27, no. 4, pp. 2325–2377, Aug. 2025.
- [2] J. Peng, Y. Wan, T. Zhang, and S. Wang, “Fluid antenna-assisted edge Gaussian splatting using grey wolf algorithm,” in *Proc. 2nd Asia Conf. Commun. 6G (ACC6G)*, Shenzhen, China, 2026, pp. 45–50, doi: 10.1109/ACC6G70208.2026.11605699.
- [3] J. Peng, T. Zhang, S. Wang, M. Shao, H. Xu, and R. Wang, “Group relative policy optimization for robust blind interference alignment with fluid antennas,” in *Proc. IEEE Int. Conf. Commun. (ICC)*, Glasgow, U.K., May 2026, pp. 1–6.
- [4] Q. Zhang, M. Shao, T. Zhang *et al.*, “An efficient sum-rate maximization algorithm for fluid antenna-assisted ISAC system,” *IEEE Commun. Lett.*, vol. 29, no. 1, pp. 200–204, 2025.
- [5] T. Zhang *et al.*, “Indoor fluid antenna systems enabled by layout-specific modeling and group relative policy optimization,” *IEEE Trans. Wireless Commun.*, vol. 25, pp. 9313–9329, 2026.
- [6] W. Wang, T. Zhang, H. Xu, S. Wang, R. Wang, and K.-K. Wong, “MA-GRPO: Accelerated MARL training for fluid antenna-assisted wireless network optimization,” arXiv:2604.17379, 2026.
- [7] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security: Technical challenges, recent advances, and future trends,” *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.
- [8] F. R. Ghadi, K.-K. Wong, F. J. Lopez-Martinez, W. K. New, H. Xu, and C.-B. Chae, “Physical layer security over fluid antenna systems: Secrecy performance analysis,” *IEEE Trans. Wireless Commun.*, vol. 23, no. 12, pp. 18201–18213, Dec. 2024.
- [9] L. Mai, J. Yao, J. Tang, T. Wu, K.-K. Wong, H. Shin, and F. Adachi, “A secure beamforming design: When fluid antenna meets NOMA,” arXiv:2411.08386, 2024.
- [10] J. Yao, L. Xin, T. Wu, M. Jin, K.-K. Wong, C. Yuen, and H. Shin, “FAS for secure and covert communications,” *IEEE Internet Things J.*, vol. 12, no. 11, pp. 18414–18418, Jun. 2025.
- [11] C. Wang, K.-K. Wong, Z. Li, L. Jin, and C.-B. Chae, “Large language model empowered design of fluid antenna systems: Challenges, frameworks, and case studies for 6G,” *IEEE Wireless Commun.*, vol. 33, no. 2, pp. 117–125, Apr. 2026.
- [12] T. Deng, Y. Gao, T. Zhang, M. Shao, W. Ni, and H. Xu, “Integrating large language models into fluid antenna systems: A survey,” *Sensors*, vol. 25, no. 16, Art. no. 5177, Aug. 2025.
- [13] C. Wang, B. Zhang, Z. Li, K.-K. Wong, H. Xu, G. Zheng, and C.-B. Chae, “LLM-driven design for fluid antenna systems,” *IEEE Wireless Commun. Lett.*, vol. 15, pp. 1065–1069, 2026.
- [14] G. Zheng, F. Liu, and Q. Zhang, “LLM-enabled automated algorithm design for multiuser fluid antenna communications,” *IEEE Trans. Wireless Commun.*, vol. 25, pp. 18811–18823, 2026.
- [15] H. Ye *et al.*, “ReEvo: Large language models as hyper-heuristics with reflective evolution,” in *Proc. Adv. Neural Inf. Process. Syst.*, 2024, pp. 1–14.
- [16] Y. Zhang, H. Yin, W. Li, E. Bjornson, and M. Debbah, “Port-LLM: A port prediction method for fluid antenna based on large language models,” *IEEE Trans. Commun.*, vol. 73, no. 12, pp. 14534–14547, Dec. 2025.
- [17] P. Moscato, “Memetic algorithms: A short introduction,” in *New Ideas in Optimization*, D. Corne, M. Dorigo, and F. Glover, Eds. New York: McGraw-Hill, 1999, pp. 219–234.
- [18] W. C. Jakes, *Microwave Mobile Communications*. New York, NY, USA: Wiley, 1974.
- [19] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [20] Q. Shi, E. Razaviyayn, Z.-Q. Luo, and C. He, “An iteratively weighted MMSE approach to distributed sum-utility maximization for a MIMO interfering channel,” *IEEE Trans. Signal Process.*, vol. 59, no. 9, pp. 4331–4340, Sep. 2011.