Federated Genetic Optimization for Secure and Privacy-Preserving Sensor Localization in Consumer IoT Applications

Neeraj Jain, Chhaya Singh, Vishal Krishna Singh, Rajkumar Singh Rathore, Norah Saleh Alghamdi and Chaminda Hewage

***Abstract*—Traditional localization methods in the Internet of Things often rely on centralized processing of distance measurements, which makes them vulnerable to adversarial data injection, privacy leakage, and scalability limitations. Methods such as the received signal strength indicator, the time of arrival, and range-free protocols like DV-Hop are typically designed for static, noise-free, and resource-rich environments. In this work, a novel Federated Genetic Algorithm (FedGA) is proposed for robust and privacy-aware sensor localization in consumer Internet of Things environments. FedGA logically divides the network into several federated clusters, where nodes use genetic optimization to compute location estimations. Only elite candidate solutions are shared with a central aggregator, ensuring data confidentiality and minimal communication overhead. Through rigorous simulation under varying node densities and measurement noise, FedGA demonstrates high localization accuracy, resilience to noise and partial data tampering. It has been observed that the FedGA improved localization accuracy by 19% as compared to the state of the art federated localization algorithms.**

***Index Terms*—Federated learning, genetic algorithm, sensor localization, edge intelligence, secure localization, AI-enabled attacks.**

I. Introduction

The proliferation of artificial intelligence (AI) and edge-enabled connectivity in consumer electronics has transformed ordinary devices into intelligent, context-aware systems [1], [2], [3]. Intelligent vehicles, wearable health trackers, autonomous security systems, and agricultural monitoring platforms are just a few examples of consumer applications that depend on spatially aware sensor networks to deliver services in real time [4]. In these systems, wireless sensor networks form the backbone for acquiring and disseminating data across distributed physical environments [5]. One of the fundamental building blocks of any Internet of Things (IoT) network is *localization* the ability to estimate the geographical positions of sensor nodes without relying on GPS, which may be infeasible due to cost, energy, or indoor constraints [6]. Despite the lot of research on localization in IoT, existing approaches often underperform when deployed in consumer-grade environments. Traditional methods such as Received Signal Strength Indicator (RSSI), Time of Arrival (ToA), and range-free protocols like DV-Hop are typically designed for static, noise-free, and infrastructure-rich environments [7]. Moreover, most of these algorithms rely on centralized processing, where proximity information is transmitted to a central controller that computes node positions. This centralized model introduces significant vulnerabilities, including increased energy consumption, single points of failure, and, more critically, exposure to AI-enabled attacks that can manipulate sensor inputs, poison data aggregation, or extract private information from model inference [8] [9]. It is noted that adversarial threats have grown ever more complicated for AI-integrated consumer applications [10]. Malicious actor can alter RSSI values to mislead positioning systems, disturb training to corrupt location models, or perform model inversion attacks to infer sensitive deployment patterns. Furthermore, the heavy reliance on cloud-based processing introduces the importance of data privacy, especially for applications involving sensitive sensor location data. This dependency may conflict with regulatory standards such as the *General Data Protection Regulation (GDPR) [11]* of the European Union and the *California Consumer Privacy Act (CCPA) [12]* in the United States. These regulations emphasize the protection of personally identifiable information (PII), thereby necessitating the adoption of edge-based or federated learning (FL) models that preserve data locality and ensure compliance.

In response to these challenges, researchers have increasingly investigated the combination of evolutionary optimization and federated architectures as an alternative to purely neural-based FL approaches [13]. In [14], [15], genetic algorithm (GA)-enhanced FL framework is proposed for vehicular networks that integrates evolutionary operators to balance latency and privacy. Li et al. [16] explored GA-driven optimization for energy-aware FL, demonstrating that GA can reduce client energy usage by adaptively scheduling communication and updates. Wu et al. [17] proposed FedCSGA, which applies GA to client selection under heterogeneous conditions, encoding participation policies as chromosomes to evolve fair and efficient training schedules. Ding et al. [18] presented MPFL, a decentralized framework that combines multi-population GA with blockchain consensus, enabling Byzantine resilience but at the cost of higher synchronization and energy overheads. On

Neeraj Jain is with School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India. (e-mail: neeraj.jain@bennett.edu.in).

Chhaya Singh is with School of Computer Science and Engineering, Galgotias University, Greater Noida. India. (e-mail: chhaya.singh@galgotiasuniversity.edu.in).

Vishal Krishna Singh is with School of Computer Science and Electronics Engineering, University of Essex, Colchester. U.K. (e-mail: v.k.singh@essex.ac.uk).

Rajkumar Singh Rathore is with Department of Computer Science, School of Technologies, Cardiff Metropolitan University, United Kingdom. (e-mail: rsrathore@cardiffmet.ac.uk)

Norah Saleh Alghamdi is with Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh 11671, Saudi Arabia. (e-mail: nosalghamdi@pnu.edu.sa)

Chaminda Hewage is with Cardiff School of Technologies, Cardiff Metropolitan University, Cardiff, United Kingdom. (e-mail: chewage@cardiffmet.ac.uk)

Manuscript received June , 2025.

the security front, Gufran et al. [19] developed FedHIL, which improves adversarial resilience through hierarchical FL, while Singampalli et al. [20] introduced SAFELOC, a fused neural-network-based FL system for indoor localization that mitigates poisoning attacks using saliency-guided aggregation.

Although these works highlight the growing role of GA-inspired techniques and adversarially robust FL in different application domains, they continue to rely either on neural models or on GA as an auxiliary mechanism for client scheduling, model convergence, or security enhancement. To the best of our knowledge, none of these approaches directly address the localization problem, leaving a clear gap for GA-driven federated frameworks tailored to position estimation in IoT. To fill this gap, we propose the Federated Genetic Algorithm (FedGA), which employs GA as the primary optimization approach for localization, enabling lightweight, privacy-preserving, and attack-resilient operation in consumer IoT environments. Unlike traditional methods that centralize computation or rely on gradient-based learning, FedGA combines the global search power of GAs with the privacy-preserving advantages of FL. In FedGA, the sensing field is divided into clusters, each of which performs local GA optimization to estimate node positions based on noisy measurements. Importantly, only elite chromosomes, defined as the most precise candidate solutions, are communicated to a global aggregator, which compiles a federated solution and returns it to inform subsequent local development. This strategy ensures that no raw measurements or private location data are ever shared, making the system resilient to both eavesdropping and adversarial data injection.

The contributions of this work are summarized as follows:

- A federated evolutionary algorithm, FedGA is proposed to localize sensor nodes without transmitting raw sensor data or intermediate models.
- FedGA minimizes communication overhead and preserves sensitive sensor information by transmitting only elite individuals during aggregation.
- A fitness-driven evolution and elite-based model sharing are used to improve the localization accuracy in the presence of adversarial noise.
- FedGA is capable of running on resource-limited edge and IoT devices.

The remainder of this paper is organized as follows: Section II provides details of the existing works. Section III details the theoretical foundation and computational framework of the proposed FedGA-based localization mechanism. Section IV provides the details of FedGA. Section V provides details of communication and computational complexities. Section VI presents the experimental setup, performance evaluation, and comparative analysis with existing techniques. Finally, Section VII concludes the study and outlines the potential outcome of the research.

II. Literature Survey

Localization is a necessary aspect of many consumer IoT applications, including smart homes, health monitoring, self-driving cars, and precision farming. Position estimation has, to this date, depended on traditional methods of estimation based on RSSI, ToA, and range-free algorithms since these are easy to compute. However, these algorithms do not work quite as well under dynamic real-world environments, and are poorly suited to deal with adversarial enviroment.

Recent studies have investigated the application of evolutionary algorithms to alleviate these limitations. Rout et al. [21] presented a dynamic genetic algorithm that modifies its search parameters over time to enhance convergence in scenarios characterised by low anchor density. Ren et al. [22] showed that combining RSSI quantization with genetic algorithms improved performance, showing that it works even with distorted signal data. Huang et al. presented a multi-objective evolutionary algorithm-based framework for 3D DV-Hop, achieving a reduction of about 20% in the average localisation error compared to baseline methodologies [23]. Meanwhile, cooperative and hybrid approaches have gained more attention. Najarro et al. [24] proposed a multi-population differential evolution algorithm for RSSI-based cooperative localization. This approach reduces communication overhead significantly and is much easier to scale. Also, security-aware localization has been investigated in [25], which integrates localization with attack detection techniques to mitigate the impacts of routing vulnerabilities.

Federated learning has emerged as a prominent solution addressing increasing concerns over data privacy and vulnerabilities posed by malicious entities in consumer IoT environments. Etiabi et al. [26] proposed a federated distillation technique for indoor localization that transmits only softened model results to reduce communication expenses and ensure user privacy. Their later research [27] introduced a hierarchical federated learning framework that enhances localization effectiveness. FeMLoc [28] employed meta-learning concepts in federated learning, enabling rapid adaption of devices to new environments, whereas FedHIL [19] tackled hardware heterogeneity in mobile environments. Despite its considerable promise, FL's application of neural networks may lead to model overfitting, excessive energy consumption, and difficulties navigating non-convex search space. As a result, researchers have commenced studies on the relation between evolutionary optimization and federated systems. Liao et al. [14] developed GAoFL, a federated genetic algorithm-based architecture for vehicular networks that achieves a balance between privacy and latency. Li et al. [16] shown that genetic algorithms are effective for optimising energy-aware federated learning for mobile edge devices. For instance, FedHIL [19] and SAFELOC [20] provide frameworks that protect against data poisoning attacks while accommodating resource-constrained mobile devices.

The aforementioned research indicate significant advancement in localization; yet, there remains a deficiency in approaches that simultaneously ensure global optimization, privacy, and resilience in the context of unpredictability. To our knowledge, no existing research explicitly integrates GA-based optimization with federated model sharing for safe IoT localization.

The proposed FedGA addresses the problem by leveraging the global search capabilities of genetic algorithms inside a federated framework that exclusively disseminates the most optimal chromosomes. This approach facilitates decentralized execution, reduces communication overhead, and ensures robust localization in noisy, adverse circumstances.

III. System Model and Problem Description

We consider a two-dimensional network deployed over a monitoring area of size $L \times L\ meter^2$. The network consists of two types of nodes: Anchor Nodes ($\mathcal{A}$), A set of m anchor nodes with fixed and known coordinates, typically equipped with GPS or manually configured. Unknown Nodes ($\mathcal{U}$), A larger set of n sensor nodes whose positions must be estimated based on local distance measurements to anchor nodes. The unknown nodes are assumed to be uniformly and randomly distributed within the area. The network is logically divided into K federated clusters, each managed by an edge aggregator node (or gateway), enabling localized computation [29].

Each unknown node $u_i \in \mathcal{U}$ can measure its distance d_{ij} to anchor node $a_j \in \mathcal{A}$ using received signal strength indicator. The measured distance is subject to Gaussian noise, and the model is represented as:

$$\tilde{d}_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} + \epsilon_{ij}, \quad \epsilon_{ij} \sim \mathcal{N}(0, \sigma^2) \quad (1)$$

where (x_i, y_i) and (x_j, y_j) are the coordinates of the unknown node 'i' and anchor nodes 'j' ($j = 1\ to\ m$), respectively, and ϵ_{ij} is zero-mean Gaussian noise with variance σ^2. It is assumed that communication within clusters is reliable, and synchronization between clusters and the aggregator is secure.

The objective is to estimate the unknown positions $(\hat{x}_i, \hat{y}_i)$ for each sensor node s_i, based on noisy and potentially adversarial distance measurements to anchors. In adversarial environments, an attacker may tamper with these RSSI-based measurements by injecting false signals or modifying legitimate values. We represent the attacked measurement as:

$$\tilde{d}_{ij}^{adv} = \tilde{d}_{ij} + \delta_{ij}, \quad (2)$$

where δ_{ij} denotes the adversarial perturbation, which may include spoofing, jamming, or collusion attacks. The localization problem is formulated as a robust optimization problem under both noisy and adversarial measurements. The objective is:

$$\min_{\{\hat{x}_i, \hat{y}_i\}} \frac{1}{n} \sum_{i=1}^{n} \frac{1}{m_i} \sum_{j=1}^{m_i} \left(\sqrt{(\hat{x}_i - x_j)^2 + (\hat{y}_i - y_j)^2} - \tilde{d}_{ij}^{*} \right)^2, \quad (3)$$

where $\tilde{d}_{ij}^{*}$ represents either normal measurements $\tilde{d}_{ij}$ or adversarially perturbed values $\tilde{d}_{ij}^{adv}$, and m_i denotes the number of anchors accessible to node s_i. The optimization is subject to practical constraints:

$$0 \le \hat{x}_i, \hat{y}_i \le L, \quad \forall i \in \{1, \dots, n\}, \quad (4)$$

$$E_i \le E_{\max}, \quad \forall i \in \{1, \dots, n\}, \quad (5)$$

where the first constraint enforces that all estimated positions remain within the deployment area, and the second ensures that the energy consumed by each node E_i does not exceed its maximum energy $E_{\max}$. These constraints reflect the bounded nature of IoT deployments and the limited energy available in IoT devices.

IV. Proposed Methodology

This section describes Federated Genetic Algorithm proposed for sensor node localization in IoT networks. FedGA combines the global search capabilities of genetic algorithms with the decentralized and privacy-aware nature of federated learning. The key idea of FedGA is to logically divide the sensor field into K federated clusters. Each cluster independently runs a GA to localize the nodes within its domain using local RSSI measurements to anchor nodes. Instead of transmitting raw data or full models, each cluster sends a small subset of its highest-performing candidate solutions (elite chromosomes) to a central aggregator. The aggregator performs a lightweight fusion and redistribution, enabling global cooperation while maintaining local privacy and minimizing communication overhead, as shown in Fig. 1. The method operates in two phases: (1) *Local GA Optimization* at each federated cluster and (2) *Federated Aggregation* of elite solutions to guide subsequent generations.

A. Local Genetic Algorithm

Each federated cluster runs a local genetic algorithm to optimize the estimated positions of its member sensor nodes over G generations. The algorithm proceeds through the following steps:

1) *Initialization:* Each chromosome represents a potential position estimate (x_i, y_i) of a sensor node i. For a cluster containing n_k unknown nodes, a chromosome is encoded as a real-valued vector:

$$C = [x_1, y_1, x_2, y_2, \dots, x_{n_k}, y_{n_k}] \quad (6)$$

An initial population of P chromosomes is generated randomly, where each chromosome represents (x, y) coordinate within the field bounds $[0, L]$.

2) *Selection:* Parent chromosomes are selected using roulette wheel selection, where the probability of selection is proportional to the fitness score (i.e., lower distance error). The fitness of a chromosome is evaluated based on the squared error between estimated distances and noisy measured distances to reachable anchor nodes. For node u_i, the local fitness is defined as:

$$f_i = \frac{1}{m_i} \sum_{j=1}^{m_i} \left(\sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} - \tilde{d}_{ij} \right)^2 \quad (7)$$

The total fitness of a chromosome across all nodes in a cluster is:

$$F(C) = \frac{1}{n_k} \sum_{i=1}^{n_k} f_i \quad (8)$$

3) *Crossover:* Arithmetic crossover is employed by linearly combining the coordinates of two selected parents using a random weight $\alpha \in [0, 1]$. This produces a child chromosome as a weighted average:

$$\text{Child} = \alpha \cdot \text{Parent}_1 + (1 - \alpha) \cdot \text{Parent}_2$$

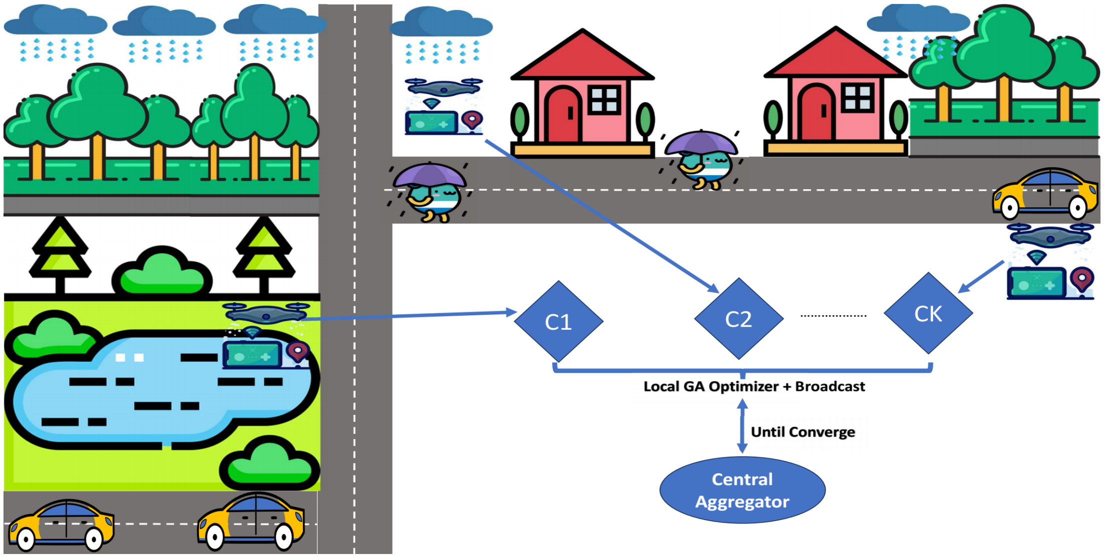


Fig. 1. Proposed FedGA Architecture

4) *Mutation:* Gaussian mutation is applied with a fixed mutation rate $\mu = 0.1$. A small random vector drawn from a normal distribution (mean = 0, std = 1.5) is added to the child chromosome, which is then clipped to stay within the field boundaries.
5) *Replacement:* A new population is formed by replacing the old one with newly generated offspring. The best chromosome (elite) is tracked and preserved across generations to prevent loss of high-quality solutions.

B. Federated Aggregation and Synchronization

In the FedGA, federated synchronization occurs after each local GA completes its assigned task for a cluster. Each cluster identifies its top-performing chromosome (elite), based on the highest fitness score, and transmits it to a central aggregator. The elite chromosomes received from all clusters are combined, which results in a single aggregated chromosome representing the federated best estimate for position. The aggregated elite solution is broadcast back to all clusters. Upon receiving the global elite, each cluster reinserts this solution into its local population by replacing the worst-performing chromosome. This enhances diversity while aligning local search with the global optimum trajectory. FedGA can operate asynchronously, allowing clusters to contribute elite chromosomes when local optimization is complete. This reduces straggler effects and assures consistent progress when devices drop out or operate at lower frequencies. Since FedGA exchanges only lightweight elites, it avoids model-heavy neural federated communication bottlenecks.

The federated genetic process proceeds for a fixed number of federated iterations, set to $R = 10$ in the current implementation due to the tightly coupled execution model. Each cluster internally runs its GA for G generations. In designing FedGA, particular attention was given to security and robustness against adversarial behavior. Unlike centralized approaches that require raw RSSI data or federated neural models that exchange high-dimensional gradients, FedGA shares only a small set of elite chromosomes. This substantially reduces the possibility of inference attacks, as elites provide position estimates but do not expose the underlying measurement data, which guards against data poisoning or Byzantine attacks. FedGA is also resilient to adversarial noise in distance measurements, the use of genetic populations, together with elitism, ensures that a few corrupted candidates cannot dominate the evolutionary process. In addition, the aggregator is assumed to be genuine but inquisitive which strengthens privacy by perturbing elites with Gaussian noise, providing formal differential privacy guarantees.

V. Computational and Communication Complexity

This section presents a comparative analysis of the computational and communication complexities of the proposed FedGA alongside two baseline methods: Centralized Genetic Algorithm (C-GA) [21] and Federated Neural Localization (FDBIL) [26], [27]. FedGA runs genetic optimization concurrently over K federated clusters. Each cluster processes n_k nodes across G generations with a population size of P, yielding a total computing cost of $\mathcal{O}(n \cdot P \cdot m \cdot G)$, where m represents the number of anchor nodes. Centralized GA demonstrates a comparable theoretical cost of $\mathcal{O}(n \cdot P \cdot m \cdot G)$; but, it lacks parallelism and subjects a single sink node to greater computational demands [21]. Conversely, FDBIL trains neural models comprising d parameters across E epochs per device, resulting in a complexity of $\mathcal{O}(n \cdot E \cdot d)$ [26], which escalates significantly with model size and necessitates GPU-capable nodes, thereby restricting its applicability in resource-constrained sensor environments as illustrated in Table I.

FedGA reduces data transmission by sending just e elite chromosomes from each cluster to a central aggregator per T generations, resulting in a total cost of $\mathcal{O}(K \cdot e \cdot R)$ for R rounds. Conversely, C-GA necessitates that each node transmits m unprocessed RSSI data to a central processor during

Algorithm 1 Federated Genetic Algorithm

```
Require: Unknown nodes $\mathcal{U} = \{u_1, \dots, u_n\}$, anchor nodes $\mathcal{A}$, population size $P$, generations $G$, mutation rate $\mu$, number of clusters $K$, elite fraction $e\%$, number of federated rounds $R$
Ensure: Estimated positions $\{(\hat{x}_i, \hat{y}_i)\}$ for all $u_i \in \mathcal{U}$
Partition the network into $K$ clusters: $\mathcal{C} = \{C_1, \dots, C_K\}$
for each federated round $r = 1$ to $R$ do
    for each cluster $C_k \in \mathcal{C}$ in parallel do
        Initialize population $\mathcal{P}_k$ with $P$ random chromosomes
        for generation $g = 1$ to $G$ do
            Evaluate fitness of each chromosome using:
                $f(C) = \frac{1}{n_k} \sum_{i=1}^{n_k} \frac{1}{m_i} \sum_{j=1}^{m_i} \Big( \sqrt{(\hat{x}_i - x_j)^2 + (\hat{y}_i - y_j)^2} - \tilde{d}_{ij} \Big)^2$
            Select parents using tournament or roulette-wheel selection
            Apply crossover to generate offspring
            Apply mutation with probability $\mu$
            Form next generation by combining offspring with elites
        end for
        Select elite chromosomes $\mathcal{E}_k$ from $\mathcal{P}_k$
        Send $\mathcal{E}_k$ to central aggregator
    end for
    Aggregator collects $\{\mathcal{E}_1, \dots, \mathcal{E}_K\}$ and applies fusion:
        $\mathcal{E}^* = \mathcal{F} \left( \bigcup_{k=1}^{K} \mathcal{E}_k \right)$
    Broadcast $\mathcal{E}^*$ to all clusters
    for each cluster $C_k$ do
        Reinjection: replace worst individuals in $\mathcal{P}_k$ with $\mathcal{E}^*$
    end for
end for
Return final best estimates $\hat{p}_i$
```

each localization phase, incurring a total cost of $\mathcal{O}(n \cdot m)$ [21], hence leading to considerable bandwidth overhead. FDBIL entails the transmission of complete model updates or gradients comprising d parameters from each node in each iteration, resulting in a complexity of $\mathcal{O}(n \cdot d \cdot R)$ [27], which burden low-power devices and increases susceptibility to inference attacks.

TABLE I
COMPLEXITY COMPARISON OF LOCALIZATION METHODS

Method	Computational Cost	Communication Cost
FedGA (Proposed)	$\mathcal{O}(n \cdot P \cdot m \cdot G)$	$\mathcal{O}(K \cdot e \cdot R)$
Centralized GA [21]	$\mathcal{O}(n \cdot P \cdot m \cdot G)$	$\mathcal{O}(n \cdot m)$
FDBIL [26], [27]	$\mathcal{O}(n \cdot E \cdot d)$	$\mathcal{O}(n \cdot d \cdot R)$

VI. Results and Discussion

A. Experimental Setup and Results

To assess the efficacy of the proposed FedGA in a realistic environment, we deployed 30 Raspberry Pi 3B+ devices (1.2 GHz Cortex-A53, 1 GB RAM) as sensor nodes over a 50×50 meter^2 open area. In contrast to GPS-based localization, the experimental setup was conducted without GPS modules; rather, anchor nodes were placed at predetermined locations, and their coordinates were manually assigned. Four Raspberry Pi devices were pre-configured as anchor nodes and positioned at the four corners of the square field, using fixed coordinates.The rest 26 Raspberry Pi devices serve as sensor nodes of the unknown position; their locations were computed using FedGA methodology. The exact positions were manually collected for ground truth comparison, which ensures controlled conditions while assessing the localization performance.To emulate realistic wireless conditions, we employed RSSI measurements obtained from an real deployment of two Raspberry Pi 3B+ devices. RSSI values were collected at regular intervals utilizing onboard Wi-Fi connections. To alleviate transient variations caused by multipath, interference, and antenna direction, each RSSI measurement was averaged over 50 samples at each collection. Additionally, we conducted calibration by creating a correlation between signal strength and distance using reference measurements at predetermined distances.The calibrated RSSI fingerprints served as input for FedGA, facilitating a robust and realistic performance assessment in a real-world deployment. Logically, the sensing field was divided into three federated clusters, each allocated to sensor nodes. Every federated node executed the genetic algorithm locally and forwarded its elite solution to a central coordinator for aggregation. Calculations were done in Python on a dedicated control laptop, emulating coordination and federated functionality across Raspberry Pi devices. Each scenario was replicated 50 times to ensure statistical reliability.

These results show that the FedGA approach maintains high localization accuracy under noisy conditions without GPS. FedGA was very reliable using RSSI data from Raspberry Pi 3B+ devices over a range of sensor deployments. Manual anchor placement at the four corners and additional grid based locations provided adequate geometric variation to facilitate convergence. The federated approach improved scalability and efficiency by confining computing to localized clusters. It has been noted that when the total number of unknown sensors increases from 5 to 25, the average localization error diminishes from 6.38 meter (m) (for 5 sensors) to 5.81 m (for 15 sensors). Furthermore, increasing the anchor count to 4 and 5 reduces average error of 5.46 m and 4.37 m, respectively. Execution time increased with the number of sensors, escalating from 0.70 seconds to 3.99 seconds across various configurations.

The results for various geometric layouts and anchor counts are presented in Table III. An average localization error of 3.95 m was achieved by using only 4 anchors placed at the corners of sensing field. Configurations with 8 and 10 anchors achieved an even greater accuracy of 2.08 m and 1.85 m, respectively, while adding midpoints (6 anchors) lowered

TABLE II
FedGA Performance with Varying Sensors and Anchors

Number of Sensors	Anchors	Avg. Error (m)	Exec Time (s)
5	3	6.38	0.70
10	3	6.04	1.39
15	3	5.81	2.10
20	4	5.46	2.89
25	5	4.37	3.99

the error to 2.35 m. With the addition of more anchors, the execution time increased slightly from 3.06 s to 4.32 s as because of more RSSI comparisons.

TABLE III
FedGA Performance for Varying Anchor Configurations

Number of Anchors	Avg. Error (m)	Execution Time (s)
4 (corners)	3.95	3.06
6 (corners + mids)	2.35	3.49
8 (corners + edge centers)	2.08	3.80
10 (grid-based)	1.85	4.32

In order to determine FedGA feasiblity on constrained hardware, the GA optimization was run on each Raspberry Pi. As per the results, FedGA can run on low-cost IoT hardware with a moderate CPU use of 62% and memory uses of 110 MB, all while consuming only 0.42 J of energy. According to the findings we obtained, FedGA is a computationally feasible and communication-efficient option for constrained consumer devices in heterogeneous federated networks.

B. Simulation Setup and Results

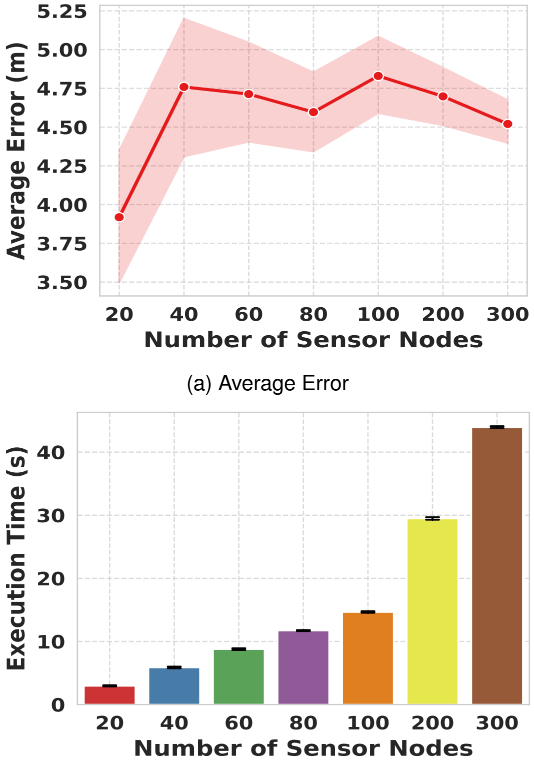
To validate the performance of the proposed FedGA algorithm, extensive simulations were conducted over a 100×100 m^2 sensing field. The evaluation focused on key performance metrics, including localization accuracy (average error), scalability (execution time), robustness to attacks using perturbation in distance measurement, and efficiency across varying federated configurations. A total of $n \in \{20, 40, 60, 80, 100, 200, 300\}$ unknown sensor nodes were uniformly distributed in the sensing field with fixed-position anchor nodes. RSSI-based distance measurements were generated using a log-normal shadowing model with additive Gaussian noise. We varied the standard deviation of noise to assess robustness. The FedGA was tested with a number of federated clusters, population size, elite count, and generations. A number of simulations were conducted to evaluate the performance of the proposed FedGA. The default parameters for simulation are mentioned in Table IV.

1) Impact of Sensor Node Density: To assess the scalability of the proposed FedGA under different network densities, we varied the number of unknown sensor nodes $n \in \{20, 40, 60, 80, 100, 200, 300\}$, keeping the number of anchor nodes $m = 4$. Anchor node positions were fixed at the four corners of the 100×100 m^2 field.

From Fig. 2, it is evident that average localization error slightly increases as the sensor count grows, primarily due to increased localization ambiguity in denser networks. However, FedGA maintains acceptable accuracy even at higher node densities. Execution time increases proportionally due to the increased number of fitness evaluations. These results demonstrate FedGA's scalability and practical efficiency in medium to large scale IoT deployments.

TABLE IV
Simulation Parameters

Parameter	Value	Description
Field Size	100×100 m^2	Deployment area
Total Sensors	100	Unknown nodes
No. of Anchors	4	Reference nodes
GA Population Size	20	No. of candidate solutions
Generations per GA	50	No. of GA iterations
Mutation Rate	0.1	Mutation probability
Federated Clusters	5	No. of distributed zones
Noise Model	Gaussian, $\sigma = 1.0$	Measurement noise
Simulation Runs	50	Repetitions for validity



(a) Average Error

(b) Execution Time

Fig. 2. Performance of FedGA with varing number of sensor nodes.

2) Impact of Number of Anchor Nodes: To evaluate how the number of anchor nodes (m) affects localization accuracy and convergence, we varied $m \in \{5, 10, 15, 20, 25, 30\}$ while fixing other parameters: number of sensor nodes $n = 300$, population size $P = 20$, generations $G = 50$, and mutation rate $\mu = 0.1$. Anchor nodes were manually placed using predefined geometries such as corners, edges, and grid centres as shown in Fig. 3.

Fig. 4 highlights the influence of anchor density on FedGA performance. The average error decreases with more anchors, confirming that additional reference points reduce positional ambiguity. Execution time shows minor variation, since anchor count primarily affects distance calculation rather than GA operations. It has been observed that 6 to 8 well-placed anchors

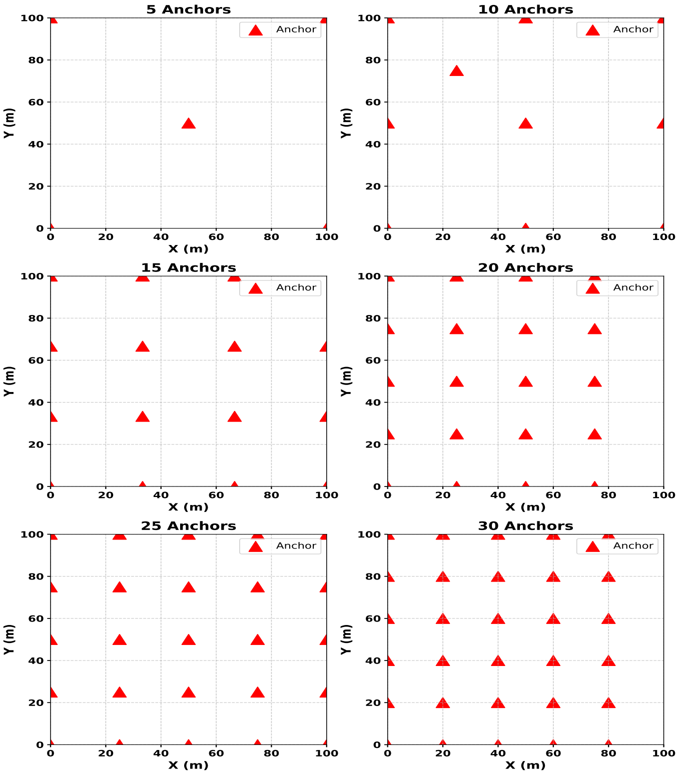
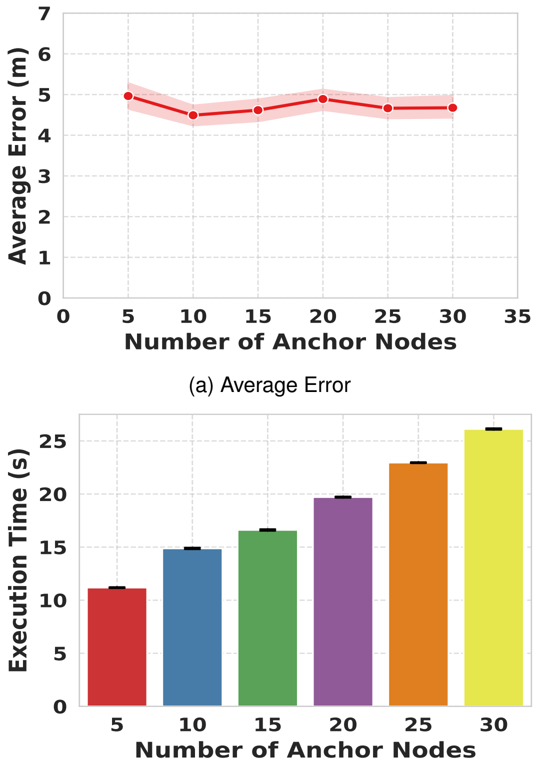


Fig. 3. Anchor nodes placement.



(a) Average Error

(b) Execution Time

Fig. 4. Performance of FedGA with varying number of anchor nodes.

are optimal for balancing accuracy and resource usage in FedGA-based localization.

3) Impact of Distance Measurement Noise: We tested resilience against noise and adversarial attacks by varying $\sigma \in \{0.1, 0.5, 1.0, 1.5, 2.0, 2.5, 3.0\}$ while keeping other parameters constant as given in Table IV. RSSI noise was modelled as additive Gaussian error.

Fig. 5 confirms that FedGA is highly robust to distance measurement noise. As the noise standard deviation, σ, increases from 0.1 to 3.0, a gradual rise in localization error is observed across all metrics. Specifically, the average error increases from approximately 4.2 m at $\sigma = 0.1$ to just under 6.1 m at $\sigma = 3.0$, indicating a controlled degradation. This behavior reflects the algorithm's ability to mitigate the effects of data poisoning attack through population diversity and elite chromosome sharing. Unlike centralized models that overfit to noisy measurements, FedGA distributes the learning process across multiple subdomains, which inherently improves noise tolerance. It is especially critical for real-world IoT deployments where signal quality can be highly variable due to multipath fading, obstructions, environmental interference, and adversarial attacks.

4) Impact of Number of Federated Clusters: To evaluate how distribution across federated clusters affects performance, we varied the number of clusters $K \in \{5, 10, 15, 20, 25\}$ while keeping $n = 300$ and $m = 4$. Each cluster handled a subset of sensors and exchanged aggregated chromosomes.

As shown in Fig. 6, clusters yield flat accuracy for 5 to 15. With too few clusters, diversity suffers; with too many, collaboration weakens. The localization error increases slightly beyond 15 clusters. Execution time decreases mildly but not much due to inter-cluster operations.

5) Impact of Number of Generations: We evaluated performance across generations $G \in \{20, 40, 60, 80, 100\}$ with other parameters fixed ($n = 100$, $m = 4$, $P = 20$, $K = 5$, $\mu = 0.1$).

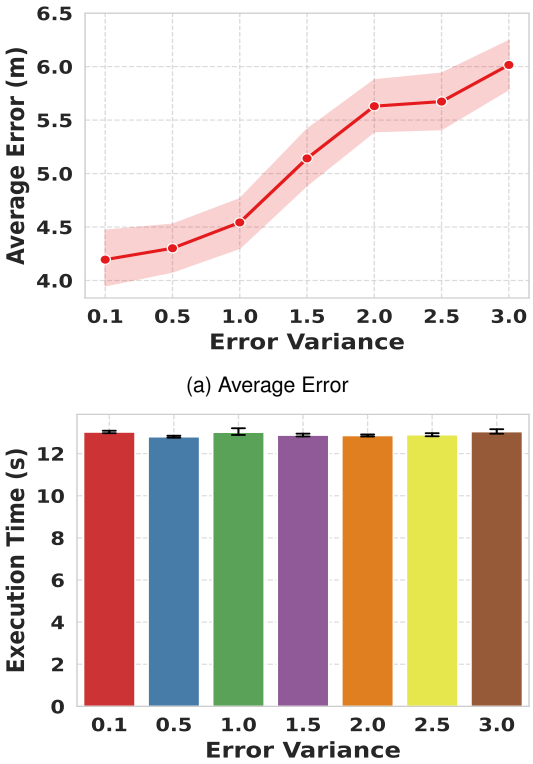
Increasing generations improves accuracy due to better convergence. As seen in Fig. 7, most gains are achieved by $G = 100$. Execution time grows linearly with G, so $G = 100$ offers a strong balance.

6) Impact of GA Population Size: To evaluate how the genetic algorithm's population size influences localization accuracy and computational efficiency, we conducted experiments with varying population sizes $P \in \{10, 20, 30, 40, 50\}$ while keeping other parameters fixed as given in Table IV.

As observed from Fig. 8, increasing the population size initially leads to a reduction in average localization error, with the lower error achieved around $P = 50$. It has been observed that a moderate population size provides the optimal balance between accuracy and computational cost. Larger populations increase solution diversity but also require more iterations to converge, which impacts real-time applicability on resource-constrained edge devices.

7) Impact of Mutation Rate: Mutation rate μ was varied from 0.01 to 0.2 to assess its impact on convergence and diversity.

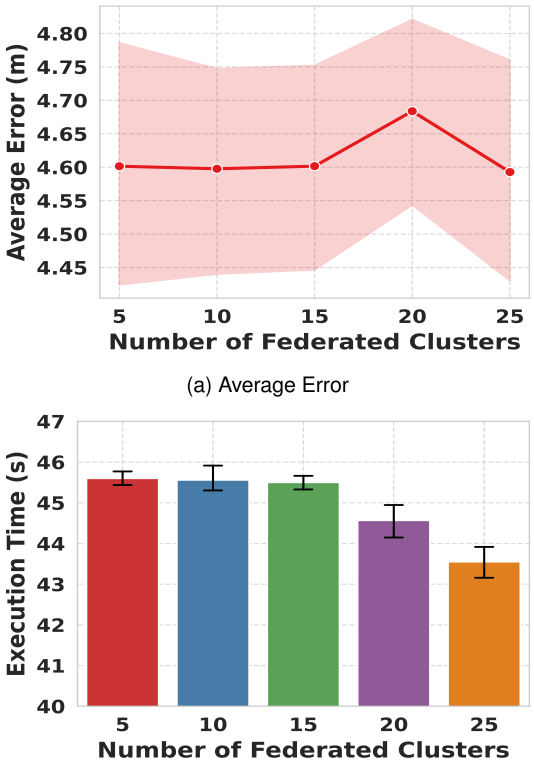
It is observed from Fig. 9, that an increase in mutation rate, average error consistently decrease, indicating enhanced exploration capability and convergence to more accurate solutions. At the lowest mutation rate ($\mu = 0.01$), the algorithm suffers



(a) Average Error

(b) Execution Time

Fig. 5. Performance of FedGA under increasing measurement noise levels.



(a) Average Error

(b) Execution Time

Fig. 6. Performance of FedGA with varying number of federated clusters.

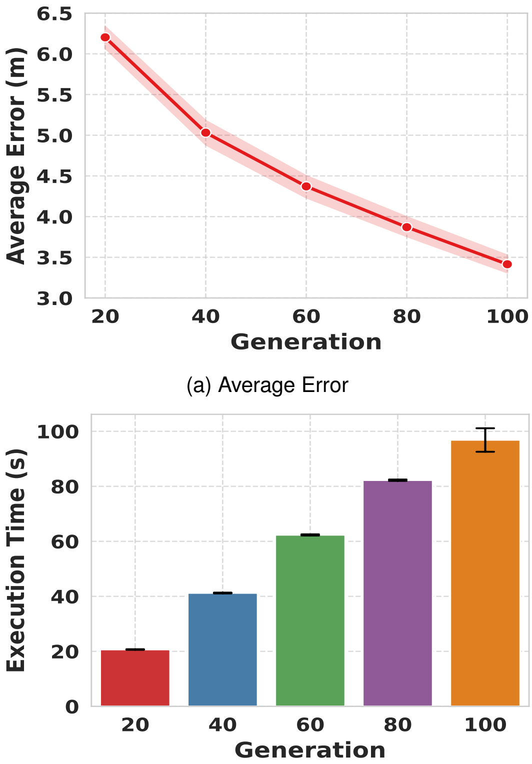
from premature convergence, resulting in higher average errors above 2.5 m. As the mutation rate increases to $\mu = 0.1$, the localization error improves significantly, dropping below 1.4 m. This trend demonstrates that moderate to high mutation rates help maintain genetic diversity and prevent stagnation, thus improving localization accuracy. While the execution time slightly increases with higher mutation rate reaching up to 35 seconds for $\mu = 0.2$ the trade-off is justified by the notable gains in accuracy. These findings support the use of higher mutation rates to enhance the robustness and effectiveness of FedGA in complex, noisy environments.

C. Comparative Analysis

We compared the proposed FedGA's performance to two existing baselines, C-GA [21] and the FDBIL approach [26], in order to establish a benchmark. Using a sensor field that was 100×100 m^2, all three approaches were tested under the same simulation parameters. Each approach used the same distance measurements based on RSSI, which were produced using a log-normal model with Gaussian noise. In contrast to FDBIL's federated neural model trained on RSSI fingerprints with central aggregation, the C-GA optimized globally across all nodes. On the other hand, FedGA allowed federated consensus to operate without raw data exchange by distributing optimization across clusters using local GAs and allowing elite chromosome sharing.

Regardless of the parameter variations, FedGA consistently obtained decreased localization error, as seen in Table V. With ten anchors, the accuracy reached 1.85 m, which is an improvement above 2.30 m (C-GA) and 3.10 m (FDBIL), respectively, as the number of anchors increased. The energy consumption of FedGA, C-GA, and FDBIL is shown in Table VI for sensor node densities ranging from 20 to 1000. The results show that regardless of the size of the network, FedGA consistently achieves the lowest energy usage. As a demonstration, at 1000 nodes, FedGA uses just 0.42 J, C-GA uses 1.10 J, and FDBIL uses 20 J. Avoiding the massive communication payloads and time-consuming gradient calculations seen in federated neural models like FDBIL, FedGA achieves its efficiency through its lightweight evolutionary operators and small chromosome exchanges. Because of its centralised execution, C-GA uses more energy than FedGA. This is because it has to evaluate all candidate solutions globally, which is inefficient compared to the federated communication requirement. Similar trends observed across a range of values for mutation rate, population size, and generations. With fewer iterations, FedGA converged robustly and faster. Remarkably, FedGA kept the localization error below 4.2 m even when faced with challenging conditions like high noise levels ($\sigma = 0.5$) or dense sensor deployments (up to 1000 nodes), in contrast to the other approaches that showed more pronounced degradation. Based on these findings, FedGA is an appealing choice for real-world deployments in environments where privacy, low connectivity, or GPS unavailability are major issues.

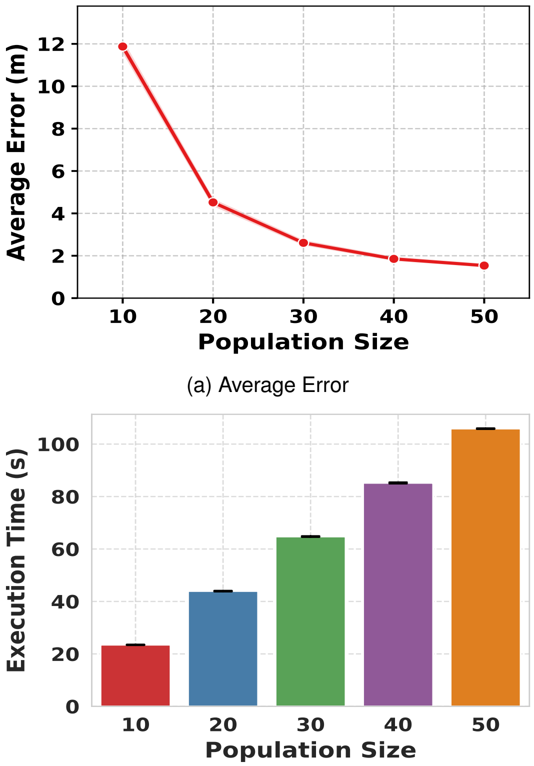
One of the key advantages of FedGA is that it works well in contexts with limited resources and heterogeneous environments, which is often the case in real-world Internet



(a) Average Error

(b) Execution Time

Fig. 7. Performance of FedGA with varying number of generations.



(a) Average Error

(b) Execution Time

Fig. 8. Performance of FedGA with varying GA population sizes.

of Things deployments. Instead of using large-scale parameter exchanges which are necessary for federated neural models, FedGA uses compact chromosome encodings of sensor positions and lightweight evolutionary operators such as selection, crossover, and mutation. This makes it possible to run on microcontrollers and single-board computers like Raspberry Pi by reducing computational complexity and memory requirements. Furthermore, communication overhead is reduced since just elite chromosomes (a few bytes per federated round) are communicated rather than full model updates. In heterogeneous environments where nodes vary in terms of processing capacity or energy capacity, FedGA accommodates diversity by allowing clusters to optimize locally and relying solely on lightweight elite aggregation for global cooperation.

VII. Conclusion

This study introduced an innovative federated genetic algorithm for safe, scalable, and precise sensor node localization in IoT applications. In contrast to conventional centralized methods that necessitate complete data collection, FedGA does local optimization inside distributed clusters and exchanges solely elite chromosomes, thus safeguarding data privacy and minimizing communication cost. Extensive simulations demonstrated that FedGA consistently surpassed both Centralized GA and FDBIL across critical criteria, including average localization error, noise adaptation, resilience to adversarial attacks, and scalability for dense sensor deployments. It reduces localization error to 1.39 m with 0.2 mutation rate and sustains performance even at elevated node densities and noise levels, while baseline approaches deteriorated markedly. The FedGA exhibited significant convergence behaviour with moderate population sizes and mutation rates, validating its robustness and efficiency across diverse parameter combinations. The results presented here illustrate FedGA's feasibility as an effective solution for real-world IoT implementations in privacy-sensitive, resource-limited environments.

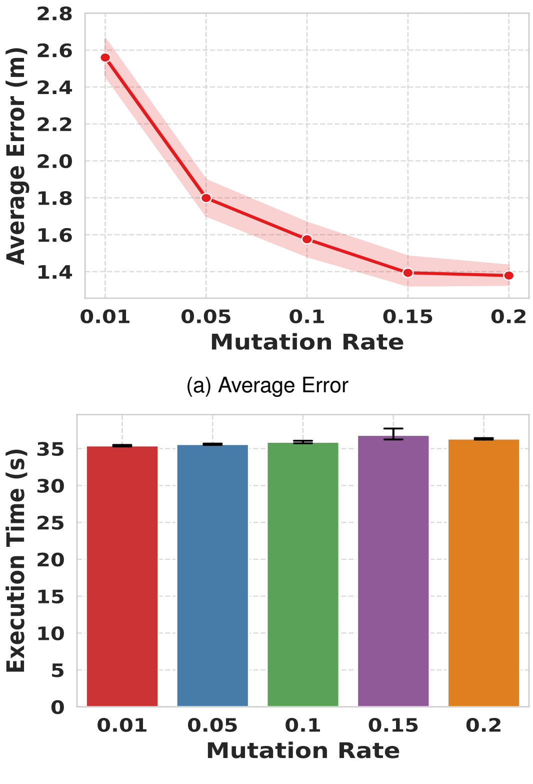
While FedGA can manage irregular dropouts, localization accuracy in certain areas may deteriorate if updates are not received for an extended duration. In networks experiencing frequent topological changes, advanced mechanisms for adaptive re-clustering and fault tolerance will be necessary, as the existing architecture assumes static anchor placement. These constraints highlight several attractive possibilities for further research, including robust aggregation algorithms, backup systems for missing elites, and hybrid synchronous-asynchronous operational modes.

Acknowledgments

This research work is funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R40), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

References

[1] G. Vallathan, A. John, C. Thirumalai, S. Mohan, G. Srivastava, and J. C.-W. Lin, "Suspicious activity detection using deep learning in secure assisted living iot environments," *The Journal of Supercomputing*, vol. 77, no. 4, pp. 3242–3260, 2021.



(a) Average Error

(b) Execution Time

Fig. 9. Performance of FedGA with varying mutation rates.

TABLE V
COMPARISON ACROSS PARAMETERS FOR FEDGA, CENTRALIZED GA [21], AND FDBIL [26]

Parameter	Value	FedGA	C-GA	FDBIL
Anchors	4	3.95	4.10	5.00
	6	2.35	2.80	3.80
	8	2.08	2.50	3.50
	10	1.85	2.30	3.10
Sensor Nodes	100	2.20	2.40	2.90
	200	2.40	2.60	3.30
	400	3.00	3.20	4.00
	600	3.30	3.60	4.40
	800	3.70	3.90	4.70
	1000	4.10	4.30	5.20
Noise (σ)	0.1	2.20	2.60	3.00
	0.2	2.50	2.80	3.50
	0.3	3.00	3.30	4.10
	0.4	3.70	4.10	4.70
	0.5	4.20	4.70	5.50
Generations	20	4.20	4.50	-
	40	3.50	3.80	-
	60	2.90	3.30	-
	80	2.60	3.10	-
	100	2.50	3.00	-
Mutation Rate	0.01	4.70	5.10	-
	0.05	3.80	4.30	-
	0.10	2.90	3.50	-
	0.15	2.50	3.20	-
	0.20	2.30	3.00	-
Population	10	4.30	4.80	-
	20	3.20	3.70	-
	30	2.60	3.10	-
	40	2.50	3.00	-
	50	2.40	2.90	-

TABLE VI
ENERGY CONSUMPTION COMPARISON OF FEDGA, CENTRALIZED GA [21], AND FDBIL [26], UNDER VARYING SENSOR NODE DENSITIES

Number of Sensors	FedGA (J)	C-GA (J)	FDBIL (J)
20	0.01	0.02	0.50
40	0.02	0.04	0.80
60	0.03	0.06	1.20
80	0.05	0.09	1.60
100	0.06	0.12	2.00
200	0.12	0.25	4.00
400	0.20	0.45	8.00
600	0.28	0.65	12.0
800	0.35	0.85	16.0
1000	0.42	1.10	20.0

[2] K. Magade and A. Sharma, "Significant role of iot in cyber-physical systems, context awareness, and ambient intelligence," in *The Next Generation Innovation in IoT and Cloud Computing with Applications*, pp. 16–34, CRC Press, 2025.

[3] S. D. A. Shah, A. K. Bashir, Y. D. Al-Otaibi, M. M. Al Dabel, and F. Ali, "Dynamic ai-driven network slicing with o-ran for continuous connectivity in connected vehicles and onboard consumer electronics," *IEEE Transactions on Consumer Electronics*, 2025.

[4] M. N. Mowla, N. Mowla, A. S. Shah, K. M. Rabie, and T. Shongwe, "Internet of things and wireless sensor networks for smart agriculture applications: A survey," *IEEe Access*, vol. 11, pp. 145813–145852, 2023.

[5] L. Lombardo, S. Corbellini, M. Parvis, A. Elsayed, E. Angelini, and S. Grassini, "Wireless sensor network for distributed environmental monitoring," *IEEE Transactions on Instrumentation and Measurement*, vol. 67, no. 5, pp. 1214–1222, 2017.

[6] B. Zhang and F. Yu, "Lswd: Localization scheme for wireless sensor networks using directional antenna," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 4, pp. 2208–2216, 2010.

[7] N. S. Ahmad, "Recent advances in wsn-based indoor localization: A systematic review of emerging technologies, methods, challenges and trends," *IEEE Access*, 2024.

[8] K.-F. Krentz and T. Voigt, "Secure opportunistic routing in 2-hop ieee 802.15. 4 networks with smor," *Computer Communications*, vol. 217, pp. 57–69, 2024.

[9] A. Hussain, W. Akbar, T. Hussain, A. K. Bashir, M. M. Al Dabel, F. Ali, and B. Yang, "Ensuring zero trust iot data privacy: Differential privacy in blockchain using federated learning," *IEEE Transactions on Consumer Electronics*, 2024.

[10] M. A. Saleem, X. Li, K. Mahmood, S. Shamshad, M. F. Ayub, A. K. Bashir, and M. Omar, "Provably secure conditional-privacy access control protocol for intelligent customers-centric communication in vanet," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1747–1756, 2023.

[11] P. Regulation, "General data protection regulation," *Intouch*, vol. 25, pp. 1–5, 2018.

[12] P. Bukaty, *The california consumer privacy act (ccpa): An implementation guide*. IT Governance Ltd, 2019.

[13] H. Zheng, J. Chu, Z. Li, J. Ji, and T. Li, "Accelerating federated learning with genetic algorithm enhancements," *Expert Systems with Applications*, vol. 281, p. 127636, 2025.

[14] M. Erel-Özçevik, A. Özçift, Y. Özçevik, and F. Yücalar, "A genetic optimized federated learning approach for joint consideration of end-to-end delay and data privacy in vehicular networks," *Electronics*, vol. 13, no. 21, p. 4261, 2024.

[15] S. Khatua, A. Mukherjee, and D. De, "Fedgen: Federated learning-based green edge computing for optimal route selection using genetic algorithm in internet of vehicular things," *Vehicular Communications*, vol. 49, p. 100812, 2024.

[16] Y. Li, X. Qin, H. Chen, K. Han, and P. Zhang, "Energy-aware edge association for cluster-based personalized federated learning," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 6, pp. 6756–6761, 2022.

[17] J. Wu, H. Ji, J. Yi, and L. Liu, "Optimizing client selection in federated learning base on genetic algorithm," *Cluster Computing*, vol. 28, no. 6, p. 400, 2025.

[18] W. Ding, Y. Liu, Z. Wang, and Z. Chu, "Mpfl: A decentralised federated learning framework based on multi-population genetic algorithm," in *ICASSP 2025-2025 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 1–5, IEEE, 2025.

[19] D. Gufran and S. Pasricha, “Fedhil: Heterogeneity resilient federated learning for robust indoor localization with mobile devices,” *ACM Transactions on Embedded Computing Systems*, vol. 22, no. 5s, pp. 1–24, 2023.

[20] A. Singampalli, D. Gufran, and S. Pasricha, “Safeloc: Overcoming data poisoning attacks in heterogeneous federated machine learning for indoor localization,” in *2025 Design, Automation & Test in Europe Conference (DATE)*, pp. 1–7, IEEE, 2025.

[21] S. Rout, P. Mohapatra, A. Rath, and B. Sahu, “Node localization in wireless sensor networks using dynamic genetic algorithm,” *Journal of Applied Research and Technology*, vol. 20, no. 5, pp. 520–528, 2022.

[22] Q. Ren, Y. Zhang, and I. Nikolaidis, “Rssi quantization and genetic algorithm based localization in wireless sensor networks,” *Ad Hoc Networks*, vol. 107, p. 102255, 2020.

[23] X. Huang, D. Han, M. Cui, G. Lin, and X. Yin, “Three-dimensional localization algorithm based on improved a* and dv-hop algorithms in wireless sensor network,” *Sensors*, vol. 21, no. 2, p. 448, 2021.

[24] L. A. C. Najarro, I. Song, M. Salman, and K. Kim, “Multi-population differential evolution for rss based cooperative localization in wireless sensor networks with limited communication range,” *arXiv preprint arXiv:2412.19763*, 2024.

[25] V. Kampourakis, V. Gkioulos, and S. Katsikas, “A systematic literature review on wireless security testbeds in the cyber-physical realm,” *Computers & Security*, vol. 133, p. 103383, 2023.

[26] Y. Etiabi and E. M. Amhoud, “Federated distillation based indoor localization for iot networks,” *IEEE Sensors Journal*, vol. 24, no. 7, pp. 11678–11692, 2024.

[27] Y. Etiabi, W. Njima, and E. M. Amhoud, “Federated learning based hierarchical 3d indoor localization,” in *2023 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, IEEE, 2023.

[28] Y. Etiabi, W. Njima, and E. M. Amhoud, “Femloc: Federated meta-learning for adaptive wireless indoor localization tasks in iot networks,” *IEEE Internet of Things Journal*, 2024.

[29] S. Balaji, R. Pavithra, D. Arivudainambi, K. Varunkumar, A. Suresh, M. M. Omar, and A. K. Bashir, “Towards efficient sensor deployment in internet of things for target coverage and sensor connectivity,” *IEEE Transactions on Consumer Electronics*, 2023.

Neeraj Jain received his bachelor’s degree in Information Technology, in 2007, the master’s degree in Information Technology, in 2010, and PhD degree in Information Technology from Indian Institute of Information Technology, Allahabad, India in 2018. He is currently working as an Associate Professor at School of Computer Science Engineering and Technology, Bennet University, Greater Noida, India. His research interests include Federated Learning, Machine Learning, Internet of Things, Wireless Sensor Networks, and Localization Protocols.

Chhaya Singh is an Associate Professor in the School of Computer Science and Engineering at Galgotias University, India. She received her Ph.D. from MANIT Bhopal and M.Tech. from IIIT Allahabad. Her research interests include Machine Learning, Data Science, and Fuzzy Logic. She has published several SCOPUS and SCI-indexed research articles and holds a design patent. Dr. Singh has also worked as a Research Assistant on a GCRF-funded project in collaboration with the University of Essex, UK. She has received multiple research fellowships and the Young Scientist Award for her contributions to computational biology.

Vishal Krishna Singh received his bachelor’s degree in Information Technology, in 2010, the master’s degree in Computer Technology and Application, in 2013, and PhD degree in Information Technology from Indian Institute of Information Technology, Allahabad, India in 2018. He is currently working as a Lecturer and is associated with the Networks and Communications Research Group at School of Computer Science and Electronics Engineering, University of Essex, Colchester, U.K. His research interests include Internet of Things, Wireless Sensor Networks, In-Network Inference, Machine Learning and Data Analytics.

Dr. Rajkumar Singh Rathore (Senior Member IEEE) is working as Head of Cyber Security of Connected and Autonomous Systems, CINC, Head of Cyber Physical and Networks Systems, CeRISS & Programme Director for MSc Computing and IT in Department of Computer Science at Cardiff Metropolitan University’s School of Technologies, United Kingdom. He has gained doctorate degree, dual master’s degrees, and bachelor’s degree all in Computer Science and Engineering discipline. Dr Rathore is a scholar throughout his career. He is the Fellow of HEA UK. He has several years of rich experience in quality of teaching, learning and research excellence. His research works were fully supported by Nottingham Trent University, United Kingdom and Manchester Metropolitan University, United Kingdom. He has co-authored several textbooks for BSc and MSc students on different modules of Computer Science. He has expertise in research informed teaching methods and has been awarded as Best Teacher many times during his career. He is the member of various prestigious international organizations in the field of computer science. He is a reviewer of several reputed peer reviewed International Journals, and Conferences. He has served as a Technical Program Committee member and chaired sessions in reputed International Conferences. Dr Rathore has an Outstanding RD background. His research expertise are Wireless Communications, Internet of Things/Cyber Physical Systems, Cyber Security and Privacy, Connected and Autonomous Vehicles, EV Charging Infrastructure Management, Intelligent Networking of Drones and also use cases of AI/ML. Dr Rathore is the founding member of IEEE Trustworthy Internet of Things (TRUST-IoT) Working Group and Member of ACM Europe Technology Policy Committee.

Norah Saleh Alghamdi is an Associate Professor in Department of Computer Science, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University (PNU), Riyadh, Saudi Arabia. she acted as Vice-Dean of quality assurance, since 2019. Currently, she is a director of businesses and projects management in her college. She received Bachelor of Computer Science from Taif University, Taif, Saudi Arabia, and Master of Computer Science and Ph.D. from Department of Computer Science, La Trobe University, Melbourne, Australia. Her research interests include data mining, machine learning, text analytics, image classification, bioengineering and deep learning. She has participated in organizing several conferences. She is a member of the reviewer committee of several journals, in IEEE, MDPI, Emerald and Elsevier. She has authored or coauthored many articles published in a well-known journals in the research field.

Chaminda T. E. R. Hewage (Senior Member, IEEE) received the B.Sc. Eng (Hons.) degree in Electrical and Information Engineering from the University of Ruhuna, Sri Lanka, and the Ph.D. degree from the University of Surrey, U.K., in 2008. He completed his Ph.D. thesis, Perceptual Quality Driven 3D Video Over Networks, at the Centre for Communication Systems Research (CCSR), University of Surrey. From 2004 to 2005, he worked as a Telecommunication Engineer at Sri Lanka Telecom PLC. In September 2009, he joined the Wireless and Multimedia Networking Research Group at Kingston University London (KU), U.K as a Senior Researcher. Since 2015, he has been with the Cardiff School of Technologies, Cardiff Metropolitan University, where he is currently a Reader in Data Security and the founding director of the Cybersecurity and Information Networks Centre (CINC). He has contributed to several EU-funded projects, including FP6 ICT NoE VISNET II, FP7 ICT Optimix, FP7 ICT Concerto, and the EU COST Actions QUALINET, 3DCONTOURNET and BEING-WISE. His research interests include data security, data protection, Quality of Experience (QoE), Quality of Security (QoSec), multimedia processing and communications, and data visualizations. He is a Fellow of HEA (UK) and also a member of Chartered Institute of Information Seurity (CIISec) and IET.