12th INTERNATIONAL SCIENTIFIC CONFERENCE ON DEFENSIVE TECHNOLOGIES
OTEH 2026
Serbia, Tara, 21 - 24 October 2026

FEDERATED LEARNING FOR AUTONOMOUS DISTRIBUTED GNSS JAMMING SWARMING STATIONS

BOBAN SAZDIĆ-JOTIĆ
Military Technical Institute, Belgrade, boban.sazdic.jotic@vs.rs

DRAGANA BOJIĆ
Military Technical Institute, Belgrade, dragana.bojic@mod.gov.rs

RADIANA BRUSIN
Military Technical Institute, Belgrade, radiana.brusin@mod.gov.rs

Abstract: *The wide implementation of Global Navigation Satellite Systems has declared these technologies critical assets in both military operations and civilian infrastructure. Consequently, Global Navigation Satellite Systems have become a critical target for Electromagnetic Spectrum Operations. Traditional centralized jamming systems, however, are often inadequate in complex and dynamic electromagnetic environments and in large geographic areas due to weaknesses such as single-point failures, increased latency, and restricted signal range. To overcome these limitations, there is a need for autonomous, distributed jamming architectures capable of adapting to dynamic electromagnetic environments. This paper proposes a decentralized approach powered by Federated Learning to enable a swarm of jamming agents to collaboratively learn and execute electronic attack. Federated Learning was selected to reduce communication overhead and enable effective coordination among multiple agents in complex, large-scale environments where synchronization is essential for neutralizing dynamic military targets. To evaluate system performance, we observed the Jamming-to-Signal Ratio at the Global Navigation Satellite Systems receiver point, ensuring the effectiveness of the distributed electronic attack strategy. Our results show that this approach provides excellent adaptability in non-stationary, high-mobility scenario compared to traditional centralized jamming strategies. Exploiting the collective intelligence of multiple autonomous agents and improving the Jamming-to-Signal Ratio at the target receiver, the proposed approach achieves higher operational efficiency and resilience against counter-jamming measures. The Federated Learning framework sets up a scalable and robust foundation for future multi-agent coordination in military electromagnetic spectrum operations.*

Keywords: *agents, artificial intelligence (AI), electromagnetic spectrum operations (EMSO), Federated Learning (FL), Global Navigation Satellite Systems (GNSS), Jamming-to-Signal Ratio (JSR).*

1. INTRODUCTION

Electromagnetic Spectrum Operations (EMSO) include coordinated combat military actions to profile, exploit, and protect the electromagnetic environment, combining electronic warfare (EW) with spectrum management. The primary purpose of EMSO is to achieve superiority and unrestricted access to the electromagnetic spectrum (EMS) for friendly forces while at the same time denying its use to foes. In modern multi-domain conflicts, this is obtained by enabling precision electronic attack (EA), covered and secure communication, and early warning capabilities. However, modern EMSO cope with severe limitations due to the extreme congestion of the radio frequency (RF) environment, the proliferation of commercial off-the-shelf (COTS) software-defined radios (SDR), and the vulnerability of centralized EW architectures [1].

Crucial and specific aspect of successful EMSO is the exploitation of possibly weakens point which are Position, Navigation, and Timing (PNT) signals, most notably the Global Navigation Satellite System (GNSS) [2]. The primary military purpose of GNSS, that engages satellite constellations such as GPS, GLONASS, Galileo, and BeiDou, is to serve as the primary and global tool for giving precise, real-time spatial and temporal information. The critical limitation of GNSS comes from its extreme vulnerability to electronic interference [3], [4], both intentional and unintentional. Unintentional interference arises from civilian infrastructure, space weather phenomena, or RF cosmic radiation and harmonic emissions from nearby communication equipment, which inadvertently degrade sensitivity of GNSS receiver (GNSS RX). Intentional interference stands for a deliberate tactical deployment and engagement of EA assets. From an EMSO perspective, GNSS jamming and spoofing offers profound tactical benefits by creating localized denial-of-service (DoS) zones for PNT signals [4].

In response to these general threats, modern defensive doctrines have integrated advanced GNSS protection mechanisms, complicating the EMSO scene [5]. Current military GNSS RXs are increasingly equipped with anti-jamming capabilities, such as spatial-temporal anti-jamming processing (STAP) [6], Controlled Reception Pattern Antennas (CRPA) [7], and multi-constellation fallback algorithms. While these electronic protection (EP) techniques enhance PTN resilience, they turn the EMS into

Corresponding author: B. Sazdić-Jotić;
E-mail: boban.sazdic.jotic@vs.rs
DOI: 10.5937/OTEH26058S

a highly dynamic, asymmetric environment. For offensive EMSO, traditional high-power, centralized jamming stations or jammer (JX) are no longer fully effective, as protection techniques can nullify static interference sources [7].

To overcome these sophisticated defense techniques, this paper proposes a distributed autonomous GNSS jamming framework based on artificial intelligence (AI). Rather than relying on a single vulnerable JX, the proposed architecture coordinates a swarm of geographically distributed, low-cost and low-power JX capable of executing synchronized jamming [1], [8]. To navigate dynamic RF environments, each JX employs Reinforcement Learning (RL) to autonomously adapt its position and power based on real-time feedback. To address communication limits and data privacy constraints, a Federated Learning (FL) framework [9] is integrated across the swarm, allowing jammers to collaboratively optimize a global model by exchanging compact weight updates instead of raw telemetry [10], [11], [12].

The integration of RL and FL for distributed GNSS jamming offers key EMSO advantages:

- **Resilience.** Spatial distribution eliminates single points of failure, protecting against hard-kill threats.
- **Adaptability.** RL-driven local control allows real-time optimization of position and power against dynamic electronic protection (EP) upgrades.
- **Anti-Jam Evasion.** Multiple low-power JXs effectively bypass modern protections like Controlled Reception Pattern Antennas (CRPA).
- **Communication Efficiency.** FL preserves bandwidth and privacy by exchanging compact model weights instead of raw telemetry.

Conversely, architecture faces operational challenges, including swarm convergence complexity, heterogeneity penalties during federated aggregation (due to varying hardware/communication limits), and the requirement for strict synchronization between JXs to prevent mutual self-interference.

The rest of this paper is organized as follows: chapter 2 presents the literature review, chapter 3 shows the architectural design of the proposed approach, chapter 4 shows the results and discussion, and chapter 5 summarizes the core findings of the study.

2. LITERATURE

2.1. GNSS OVERVIEW

Technologies of GNSS have become a crucial part of modern infrastructure, with broad applications in transportation, telecommunications, scientific research, and numerous civilian and military systems. In recent years, GNSS is again in the focus because of the recent military conflicts around the world. Official GPS interface specification documents [13] provide the basis for understanding the structure of PTN signals, message formats, and the characteristics of individual frequency bands. Additionally, authors in [14] addressed GNSS modernization and analyzed the development of new signals and services, as well as improvements in positioning accuracy. New ideas are presented in [15] giving attention to multi-constellation GNSS RXs, which provide greater positioning reliability and availability in complex environments. Finally, authors in [16] investigated the application of AI to improve GNSS performance, particularly in position estimation and signal-quality analysis.

2.2. GNSS INTERFERENCE (JAMMING & SPOOFING)

Signals of GNSS reach the Earth's surface at extremely low power levels, generally below the GNSS RX thermal-noise floor, which makes it particularly vulnerable to various forms of interference and deliberate attacks. Jamming [17] and spoofing [5] are widely regarded as the most serious EA threats to reliable GNSS operation. In addition, review studies in [18], [19], analyze the effects of interference on GNSS RX performance using parameters such as automatic gain control (AGC), carrier-to-noise density ratio (C/N0), signal spectral characteristics, and in-phase/quadrature (I/Q) samples. Additionally, authors in [20] introduced distributed systems for detecting and localizing interference sources, as well as to sensor networks for monitoring large geographical areas. Modern approaches in [21] increasingly employ AI algorithms for the automatic detection and classification of different interference types. Although many existing algorithms achieve high detection accuracy, most rely on centralized data processing, which represents a limitation in distributed GNSS systems.

2.3. REINFORCEMENT LEARNING AND FEDERATED LEARNING

The integration of RL approaches in the domain of GNSS technologies represents a fundamental innovation in modern EMSO, particularly under conditions of intentional jamming and spectrum vulnerability [22], [23]. By interacting with dynamic EMS, intelligent autonomous unmanned systems can adopt alternative navigation strategies and mitigate GNSS loss [24]. This capability enables systems to adapt to unpredictable spatial variations without requiring predefined, static scenarios. Moreover, FL is a modern distributed AI approach that enables collaborative model training without exchanging raw data among agents. In communication networks, edge computing, and distributed systems, FL has been successfully applied to distributed spectrum sensing, interference classification, and jammer recognition [25]. In the GNSS domain, recent studies demonstrate the potential of FL for spoofing-attack detection [26], GNSS interference classification [27], and the development of personalized models for different receivers and operating environments.

Despite substantial progress, the application of RL and FL in EMSO for distributed GNSS jamming remains underexplored, especially in scenarios involving autonomous JXs and real-time data processing. This research gap provides the primary motivation for the solution proposed in this paper.

3. METHODOLOGY

This chapter defines the proposed simulation model for analyzing and improving the AI distributed jamming of GNSS RX in the context of EMSO. The system model combines RL algorithm for the autonomous positioning of *N* JXs organized in a swarm with a simple FL framework to collaboratively watch and evaluate the cooperative EA effects. The simulation model defines a two-dimensional square, Region of Interest (ROI), $\mathcal{A}$, centered at the coordinate origin, and defined by the set:

$$\mathcal{A} = \{(x, y) \in \mathbb{R}^2 | -D/2 \leq x \leq D/2, -D/2 \leq y \leq D/2 \quad (1)$$

where *x* and *y* are planar coordinates, and $D \times D = 20 \times 20$ km are ROI dimensions (empirically chosen for operational EMSO level).

3.1. ROI CONFIGURATION AND RASTERIZATION

The ROI is discretized using a raster grid with a resolution step of $\Delta = 0.025$ km (empirically chosen for operational EMSO level), defining a finite matrix of possible positions where the swarm of JXs can exist in. To stand for real EMSO deployment limits, the ROI is divided along the *y*-axis into two distinct operational zones:

- **Area of Interest (AOI)** is a foe territory and the part of ROI, resolute for deployment and maneuvering of one enemy GNSS RX:

$$\text{AOI} \cap \mathcal{A}, \forall x \geq 0 \quad (2)$$

- **Area of Responsibility (AOR)** is a friendly territory and the part of ROI, resolute for deployment and maneuvering of swarm of JXs:

$$\text{AOR} \cap \mathcal{A}, \forall x < 0 \quad (3)$$

The fixed GNSS RX is positioned at $\mathbf{x}_{\text{RX}} = [0, 5]$, while JXs can maneuver in the AOR. At time step *t*, the position of *i*-th ($i = 1,2, \ldots, N = 10$) JX is $\mathbf{x}_{i,t} = [x_{i,t}, y_{i,t}]$. At the beginning of simulation ($t = 0$), the JXs start the mission from separate positions and can move inside the AOR maneuvering boundary ($\forall x \leq -5$). Such constraints show the real EMSO conditions and help to simulate the swarm jamming keeping the minimum distance from GNSS RX.

3.2. RADIO PROPAGATION MODEL

The research focuses particularly on GNSS L1 frequency band (1575.42 MHz), which power level ($P_{\text{GNSS,RX}}$) at the whole ROI randomly fluctuated in the range from -125 dBm to -130 dBm that is simply presented with Normal Gaussian distribution. The jamming signal arriving at the targeted GNSS RX position is modeled using a Free Space Path Loss (FSPL) propagation model:

$$L_i = 20\log_{10}(d_{i,t}) + 20\log_{10}(f) + 32.45 \quad (4)$$

where L_i is signal propagation loss from *i*-th JX to the targeted GNSS RX, $d_{i,t} = \|\mathbf{x}_{i,t} - \mathbf{x}_{\text{RX}}\|_2$ is the Euclidean 2D distance between the *i*-th JX and the targeted GNSS RX in km, *f* is GNSS RX frequency in MHz, and 32.45 is FSPL constant. To guarantee a successful EA, the cumulative Jamming-to-Signal Ratio (*JSR*) at the GNSS RX position must satisfy a predefined effectiveness threshold, which is set to $\gamma_{\text{JSR}} = 20.005$ dB. The critical threshold value (γ_{JSR}) for effective EA can be observed through the cumulative power:

$$P_{\text{J,RX}}^{\gamma} = P_{\text{GNSS,RX}} + \gamma_{\text{JSR}} \quad (5)$$

$$p_{\text{J,RX}}^{\gamma} = 10^{\frac{P_{\text{J,RX}}^{\gamma}}{10}} \quad (6)$$

Next, assuming all JXs transmit with the same power, the required uniform power per JX is:

$$p_t^{\text{JX}} = \frac{p_{\text{J,RX}}^{\gamma}}{\sum_{i=1}^{N} g_i} \quad (7)$$

$$P_t^{\text{JX}} = 10\log_{10}(p_t^{\text{JX}}) \quad (8)$$

where P_t^{JX} is resulting jamming signal at the GNSS RX position and $g_i = 10^{(G_{JX} + G_{RX} - L_i/10)}$ is the linear path gain from *i*-th JX towards the GNSS RX, where G_{JX} is antenna gain of each JX, G_{RX} is antenna gain of GNSS RX and L_i is defined in equation (4). It is important to note that P_t^{JX} is power term used inside the reward function explained in chapter 3.1.

3.3. OPTIMIZATION VIA RL

Building upon the foundational concepts proved in our prior work [28], the problem of finding the best spatial distribution of the JXs is solved by engaging Proximal Policy Optimization (PPO) [29] due to its superior stability and clipped objective constraints in non-stationary multi-agent settings.

State Space (*s*). Comprises the current coordinates of all JXs in the AOR with the boundary restriction, alongside the current estimated *JSR* derived from direct feedback loops. The PPO agent was implemented using an actor–critic neural-network architecture. For each JX, the input state is a four-dimensional normalized vector composed of the current JX spatial coordinates, the required uniform JX power, and the estimated joint JSR at the GNSS RX:

$$s_{i,t} = \left[\frac{x_{i,t}}{D/2}, \frac{y_{i,t}}{D/2}, \frac{P_t^{\text{JX}}}{50}, \frac{JSR_t}{50}\right] \quad (9)$$

Action Space (*a*). Defines the permitted directional steps of the agent on the raster grid across the four primary basic directions (North, South, East, West) with a discrete step size of Δ_d, or a possibility to remain stationary:

$$a_{i,t} = [N(\uparrow), S(\downarrow), E(\rightarrow), W(\leftarrow), Stay(\cdot)] \quad (10)$$

Reward Function (*r*). The reward function was designed to guide the swarm of JXs toward spatial configurations that satisfy the required *JSR* at the GNSS RX while minimizing the required uniform JX power. Each JX receives a local reward composed of a shared power-efficiency term, a local distance-improvement term, a *JSR* tracking penalty, an invalid-action penalty, and a pairwise separation penalty. The power-efficiency term encourages configurations that reduce the uniform transmit power needed to achieve the target joint *JSR*. The distance-reduction term encourages each JX to move toward the RX within the allowed rasterized maneuvering region. The *JSR* tracking term penalizes deviations from the required *JSR*, while the invalid-movement action and JX-to-JX separation penalties enforce motion feasibility and

discourage unrealistic JX co-location. A compact form of the reward function is:

$$r_{i,t} = w_P(\Delta P_t) + w_d \Delta d_{i,t} - w_J e_{JSR,t} - w_B\left(I_{i,t}^{invalid}\right) - w_S(S_t) \quad (11)$$

where the power-efficiency reward is product of scaling factor (w_P=3.0) and power difference ($\Delta P_t = P_{t-1}^{JX} - P_t^{JX}$); the distance-reduction reward is product of scaling factor (w_d=0.75) and distance difference ($\Delta d_{i,t} = \frac{d_{i,t-1} - d_{i,t}}{\Delta}$); the *JSR* tracking penalty is product of scaling factor (w_J=0.05) and *JSR* mismatch ($e_{JSR,t} = \frac{|JSR_t - \gamma|}{\max(|\gamma|,1)}$); the invalid movement penalty is product of scaling factor (w_B=0.05) and invalid movement (when JXs try to leave the allowed maneuvering region); the JX-to-JX separation penalty is product of scaling factor (w_S=0.10) and JXs co-location or unwanted clustering. The scaling factors are empirically chosen during the training process.

The PPO network consists of a shared fully connected backbone with two hidden layers, each having 96 neurons and hyperbolic tangent (Tanh) activation functions. The actor head maps the hidden representation to logits over the five discrete raster actions (a). A categorical distribution is then formed from these logits to sample the JX movement action. In parallel, the critic head maps the same hidden representation to a scalar state-value estimate used for advantage estimation. The PPO network parameters are optimized using the Adam optimizer with a learning rate of $\alpha=3\times10^{-4}$. Training uses the clipped PPO objective (ε=0.2), generalized advantage estimation with ζ=0.97 and λ=0.95, a value-loss coefficient of 0.50, an entropy coefficient of 0.02, and gradient-norm clipping at 0.50. The PPO network training was implemented in PyTorch using a custom JX swarm environment rather than the OpenAI Gymnasium interface. Evaluation is performed with 1000 steps and greedy-polish mechanism. The proposed environment directly represents the multi-JX raster movement problem, RF link-budget evaluation, JSR computation, reward calculation, and movement constraints.

3.4. FL FRAMEWORK FOR JAMMING EFFECTIVENESS MONITORING

Centralized data aggregation between JXs in EMSO could be disrupted due to bandwidth constraints, communication masking, or the deployment of electronic counter-counter measurement (ECCM) assets. To mitigate this weakness, we propose an FL framework consisting of the distributed JXs as local FL clients. The purpose of the FL framework (FL-PPO) is to allow the JXs to improve their PPO policies without sending raw local trajectories, observations, rewards, or full training data to a central controller - aggregator. At the beginning of each federated round (r), the aggregator JX broadcasts the current global actor's weights ($\theta_i^{(r)} \leftarrow \theta^{(r)}$) to the other JXs. Each JX then performs local PPO training using its own local states, actions, rewards, and *JSR* feedback. After local training, i-th JX obtains updated local weights ($\theta_i^{(r,local)}$). Instead of sending the full local model or raw training data, each JX computes a compact weight increment. Moreover, only increment ($\Delta\theta_i^{(r)} = \theta_i^{(r,local)} - \theta^{(r)}$) is transmitted to the aggregator JX. Although the framework is federated, it still uses central aggregation. The difference from conventional architecture is that the central aggregator is one of the JX stations. The selected aggregator JX performs five main operations:

- **Global model initialization**. At round r=0, the aggregator JX initializes the global PPO actor model ($\theta^{(0)}$).
- **Weight-increment collection**. After local PPO training, each JX sends only its compact update ($\Delta\theta_a^{(r)}$) to the aggregator JX.
- **Compact update compression**. The weight increments are compressed before transmission with top-k FP16 compression.
- **Federated averaging**. The aggregator JX periodically executes a Federated Averaging routine to compute the updated global model parameters:

$$\Delta\theta_{golbal}^{(r)} = \frac{1}{N}\sum_{i=1}^{N} \Delta\theta_i^{(r)} \quad (12)$$

The aggregator JX reconstructs the sparse updates, computes their average, and the global model is then updated and broadcasted back to the JXs. This decentralized pipeline yields system robustness, enables collaborative observation of the ESM, and accelerates the convergence rate of the RL agents toward globally the best spatial coordination within highly fluid EMSO conditions.

4. RESULTS AND DISCUSSION

This section presents the simulation results, which were conducted to analyze the efficacy of jamming, and the prediction of the best locations for distributed JXs (two JXs, five JXs and ten JXs towards one GNSS RX). The results show that the proposed approach can be used for AI distributed jamming of GNSS RX in the context of EMSO. The FL-PPO framework can achieve stable convergence toward the best locations, with *JSR* values consistently supported within the specified threshold. Visual analysis of the agent's trajectories reveals that the model avoids EMS inefficient regions, focusing instead on positions that help the best *JSR*. Results of the optimal positions of two JXs with FL-PPO framework when GNSS RX is asymmetrically positioned are shown in Figure 1.

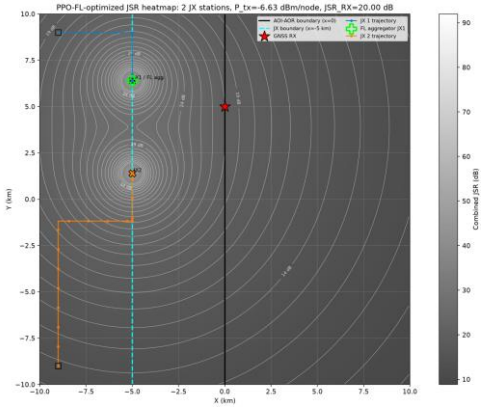


Figure 1. Optimal position of two JXs with FL-PPO when GNSS RX is asymmetrically positioned

The trajectories shown in Figure 1 demonstrate how the JXs focus on maneuvering toward the GNSS RX coordinates, optimizing their positions to maximize the *JSR* while minimizing transmit power. Results of the optimal positions of five JXs with FL-PPO framework

when GNSS RX is asymmetrically positioned are shown in Figure 2.

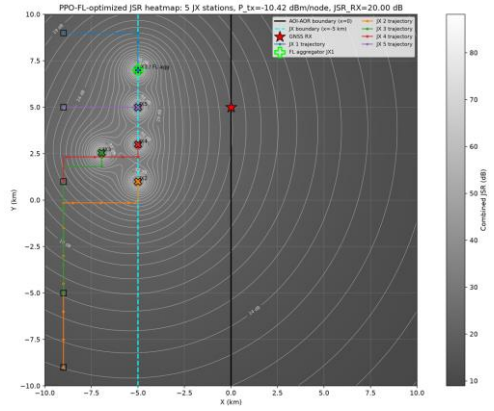
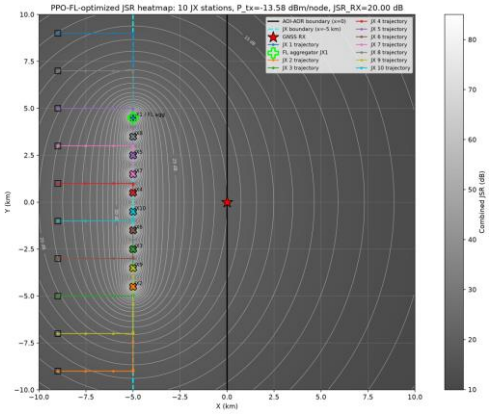
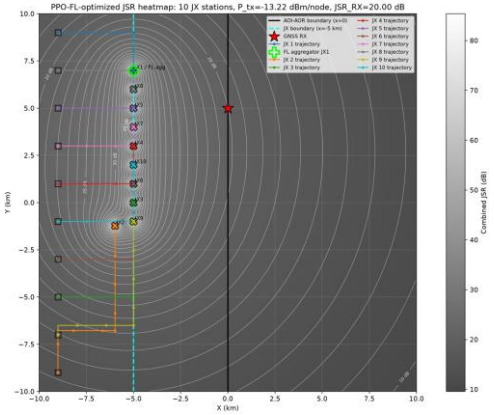


Figure 2. Optimal position of five JXs with FL-PPO when GNSS RX is asymmetrically positioned

It can be noticed that the higher density of JX trajectories occurs near the GNSS RX which confirms the FL-PPO framework adaptation when GNSS RX is asymmetrically positioned. Figures 1 and 2 show that the asymmetric setup shifts optimal JX locations toward the displaced GNNS RX, proving the proposed approach dynamically adapts to varying GNSS RX geometries rather than converging to fixed configurations. The improvement in the proposed approach can easily be seen with scenario when ten JXs are engaged, that is presented in Figure 3.



a)



b)

Figure 3. Optimal spatial distribution of ten JXs using FL-PPO: a) GNSS RX at the ROI center, and b) GNSS RX asymmetrically positioned at (0,5).

Figure 3 illustrates the optimized spatial deployment of ten JXs under two GNSS RX placement scenarios using the FL-PPO framework. It can be noticed that the spatial distribution contours confirm that individual JXs autonomously place themselves to avoid overlapping redundancies, ensuring a uniform *JSR* coverage over the GNSS RX position. During evaluations of edge cases (JXs were initialized at the border of the ROI), the FL-PPO framework successfully guided isolated JXs toward the globally optimal positions. The results demonstrate that the FL-PPO framework balance effectively from small configurations to larger JX's swarms, successfully satisfying joint *JSR* while minimizing transmit power through cooperative spatial positioning. These properties of the FL-PPO framework support findings and emphasize that RL models can outperform traditional heuristic and deterministic search algorithms in situations with expansive search domains or dynamically changing conditions [12], [22]. This can be supported by quantitative comparison shown in Table 1.

Table 1. Quantitative comparison.

Method	N JX	RX	P_t^{JX}/JX, [dBm]	Mean $d_{i,t}$ [km]	"greedy-polish" steps
PPO	2	(0,0)	-6.67	5.5901	18
		(0,5)	-6.39	6.0443	78
FL-PPO		(0,0)	-6.67	5.5917	63
		(0,5)	-6.63	5.6801	104
PPO	5	(0,0)	-10.59	5.7153	97
		(0,5)	-10.31	6.0822	221
FL-PPO		(0,0)	-10.59	5.7153	200
		(0,5)	-10.42	5.9085	206
PPO	10	(0,0)	-13.58	5.7332	146
		(0,5)	-13.17	6.2686	212
FL-PPO		(0,0)	-13.58	5.7330	180
		(0,5)	-13.22	6.1712	222

Table 1 demonstrates that FL-PPO framework achieves same or better spatial optimization and jamming effectiveness to centralized PPO, especially in the scenario when GNSS RX is asymmetrically positioned. Despite its advantages, the FL-PPO framework introduces a minor heterogeneity penalty. Specifically, in the ten JXs swarm scenario, the FL-PPO framework required 23% more total evaluation steps to achieve a stable spatial convergence when GNSS RX is symmetrically positioned, and 5% when GNSS RX is symmetrically positioned. Such delay in global model synchronization is an expected trade-off, attributed to the periodic nature of the federated weight aggregation phase compared to the continuous, immediate centralized updates.

5. CONCLUSION

This paper introduced a FL-PPO framework for autonomous distributed GNSS jamming using PPO-based local control and a peer-selected aggregation JX. By exchanging only compact model-weight increments rather than raw trajectory data, the architecture eliminates central dependence while maintaining communication efficiency. Simulation results confirm that both PPO and FL-PPO frameworks successfully adapt jammer deployment to target geometries—converging symmetrically for centered GNSS receivers and shifting dynamically toward asymmetric placements to minimize transmit power while

satisfying target JSR constraints. While the FL-PPO framework introduces a slight delay in convergence compared to a centralized PPO, it provides critical advantages in tactical EMSO: immunity to single-point communication failures and the ability to dynamically adapt to asymmetric target geometries. Furthermore, scalability tests demonstrate that the FL-PPO framework effectively coordinates larger swarms. The primary contribution lies in merging distributed spatial optimization with federated weight-sharing for communication-constrained environments. Future work will incorporate terrain-induced multipath propagation, dynamic jamming power and receiver mobility over predefined trajectory, network latencies, and hardware-in-the-loop validation.

Acknowledgements: This work was supported by the Ministry of Science, Technological development and Innovations of the Republic of Serbia, Contract No. 451-03-34/2026-03/200325.

References

[1] Joint Chiefs of Staff, *CJCS: Joint Publication 3-85: Joint Electromagnetic Spectrum Operations (JEMSO)*. 2022. Accessed: Jun. 28, 2026. [Online]. Available: https://www.waru.edu/sites/default/files/Migrated/CopDocuments/Joint_Pub_3-85.pdf

[2] V. Renaudin, M. I. Sayyaf, F. Le Bourhis, and M. Ortiz, "GNSS Positioning Under Threat: The Rising Risk to Existing Systems and The Role of Alternative Indoor and Seamless Navigation Technologies," *IEEE Journal of Indoor and Seamless Positioning and Navigation*, vol. 3, pp. 246–259, Nov. 2025, doi: 10.1109/JISPIN.2025.3629705.

[3] O. Sushych, O. Pogurelskiy, V. Konin, O. Kutsenko, I. Prykhodko, and T. Maliutenko, "Performance Analysis of Intentional Interference on Multi-GNSS Receivers," *Lecture Notes in Networks and Systems*, vol. 992 LNNS, pp. 114–124, 2024, doi: 10.1007/978-3-031-60196-5_10/SAVE-RESEARCH.

[4] A. Blatnik and B. Batagelj, "Evaluating GNSS Receiver Resilience: A Study on Simulation Environment Repeatability," *Electronics 2025, Vol. 14, Page 1797*, vol. 14, no. 9, p. 1797, Apr. 2025, doi: 10.3390/ELECTRONICS14091797.

[5] B. Gattis, J. Cydejko, and D. Akos, "Baltic sea GNSS jamming and spoofing emitter detection and localization in real-time using a time difference of arrival (TDOA) system," *GPS Solutions*, vol. 30, no. 2, p. 96, Apr. 2026, doi: 10.1007/s10291-026-02061-5.

[6] Z. Meng and F. Shen, "Robust Space-Time Adaptive Processing Method for GNSS Receivers in Coherent Signal Environments," *Remote Sens. (Basel).*, vol. 15, no. 17, p. 4212, Aug. 2023, doi: 10.3390/rs15174212.

[7] J. W. Harris and D. M. Bevly, "Beam Steering Adaptive Noise Cancellation with a Controlled Reception Pattern Antenna for GNSS Anti-Jamming," in *2025 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, IEEE, Apr. 2025, pp. 337–344. doi: 10.1109/PLANS61210.2025.11028269.

[8] A. M. D. Barbu, "The Cognitive Electronic Warfare in the Age of Artificial Intelligence," *STRATEGIES XXI - National Defence College*, vol. 2, no. 1, pp. 15–24, Nov. 2024, doi: 10.53477/2784-2487-24-02.

[9] T. Wang, Y. Li, Y. Wu, and T. Q. S. Quek, "Secrecy Driven Federated Learning via Cooperative Jamming: An Approach of Latency Minimization," *IEEE Trans. Emerg. Top. Comput.*, vol. 10, no. 4, pp. 1687–1703, Oct. 2022, doi: 10.1109/TETC.2022.3159282.

[10] A. Alhosban, "Electronic Warfare in NAVWAR: Impact of Electronic Attacks on GNSS / GBAS Approach Service Types C and D Landing systems and their proposed Electronic Protection Measures (EPM)," *Hadmérnök*, vol. 14, no. 2, pp. 238–255, Jun. 2019, doi: 10.32567/hm.2019.2.20.

[11] A. Meftah, T. N. Do, G. Kaddoum, C. Talhi, and S. Singh, "Federated Learning-Enabled Jamming Detection and Waveform Classification for Distributed Tactical Wireless Networks," *IEEE Transactions on Network and Service Management*, vol. 20, no. 4, pp. 5053–5072, Dec. 2023, doi: 10.1109/TNSM.2023.3271578.

[12] Z. A. El Houda, H. Moudoud, and B. Brik, "Federated Deep Reinforcement Learning for Efficient Jamming Attack Mitigation in O-RAN," *IEEE Trans. Veh. Technol.*, vol. 73, no. 7, pp. 9334–9343, 2024, doi: 10.1109/TVT.2024.3359998.

[13] Tony Anthony, "NAVSTAR GPS Space Segment/Navigation User Segment Interfaces," 2023.

[14] K. Špoljar, M. Zrinjski, A. Tupek, and K. Stipetić, "Modernization of GNSS, RNSS, and SBAS," *Technologies (Basel).*, vol. 13, no. 11, p. 494, Oct. 2025, doi: 10.3390/technologies13110494.

[15] S. Jin, X. Meng, G. Dardanelli, and Y. Zhu, "Multi-Global Navigation Satellite System for Earth Observation: Recent Developments and New Progress," *Remote Sens. (Basel).*, vol. 16, no. 24, p. 4800, Dec. 2024, doi: 10.3390/rs16244800.

[16] A. Mohanty and G. Gao, "A survey of machine learning techniques for improving Global Navigation Satellite Systems," *EURASIP J. Adv. Signal Process.*, vol. 2024, no. 1, p. 73, Jun. 2024, doi: 10.1186/s13634-024-01167-7.

[17] A. Morrison *et al.*, "Jammertest 2022: Jamming and Spoofing Lessons Learned," in *ENC 2023*, Basel Switzerland: MDPI, Oct. 2023, p. 22. doi: 10.3390/ENC2023-15445.

[18] L. Marata *et al.*, "Trends and Challenges in Next-Generation GNSS Interference Management," Oct. 2025, doi: 10.48550/arXiv.2510.27576.

[19] K. Radoš, M. Brkić, and D. Begušić, "Recent Advances on Jamming and Spoofing Detection in GNSS," *Sensors*, vol. 24, no. 13, p. 4210, Jun. 2024, doi: 10.3390/s24134210.

[20] A. Ghanbarzadeh, M. Soleimani, and H. Soleimani, "GNSS/GPS Spoofing and Jamming

Identification Using Machine Learning and Deep Learning," Jan. 2025. doi: 10.48550/arXiv.2501.02352.

[21] Y. K. Esfandabadi, A. Tabatabaei, and R. Hein, "AI-Driven Detection, Characterization and Localization of GNSS Interference: A Comprehensive Approach Using Portable Sensors," in *European Navigation Conference 2025*, Basel Switzerland: MDPI, Mar. 2026, p. 43. doi: 10.3390/engproc2026126043.

[22] S. You, M. Diao, and L. Gao, "Deep Reinforcement Learning for Target Searching in Cognitive Electronic Warfare," *IEEE Access*, vol. 7, pp. 37432–37447, 2019, doi: 10.1109/ACCESS.2019.2905649.

[23] X. Xiong *et al.*, "Intelligent jamming decision-making system based on reinforcement learning," *Computers and Electrical Engineering*, vol. 123, p. 110288, Apr. 2025, doi: 10.1016/j.compeleceng.2025.110288.

[24] W. Zhang, M. Zhang, Z. Zhao, F. Sun, and F. Liu, "Frequency jamming resource allocation method based on temporal reinforcement learning," *Signal Processing*, vol. 239, p. 110330, Feb. 2026, doi: 10.1016/j.sigpro.2025.110330.

[25] S. Barkatsa, M. Diamanti, P. Charatsaris, S. Voikos, E. E. Tsiropoulou, and S. Papavassiliou, "Coordinated Jamming and Poisoning Attack Detection and Mitigation in Wireless Federated Learning Networks," *IEEE Open Journal of the Communications Society*, vol. 6, pp. 3745–3759, 2025, doi: 10.1109/OJCOMS.2025.3558672.

[26] S. Liu, W. Liu, A. Hussain, and P. Papadimitratos, "G2FL: Robust Federated Learning for GNSS Spoofing Detection," in *IEEE ICC 2026 Fifth Workshop on Machine Learning and Deep Learning for Wireless Security Proceedings and IEEE Xplore*,

[27] M. Jiang, Z. Ye, Y. Xiao, and X. Gou, "Federated Transfer Learning Aided Interference Classification in GNSS Signals," Jun. 2024, doi: 10.48550/arXiv.2406.16102.

[28] O. Pejčić, N. Šepa, and B. Sazdić-Jotić, "Predikcija efikasnosti radio-ometanja primenom algoritma veštačke inteligencije," in *Zbornik radova 69. konferencije ETRAN*, Društvo za ETRAN i Akademska misao, Beograd, Srbija, 2025, pp. 251–256. doi: 10.69994/69E25049.

[29] J. Schulman, F. Wolski, P. Dhariwal, A. Radford, and O. Klimov, "Proximal Policy Optimization Algorithms," Aug. 2017, doi: 10.48550/arXiv.1707.06347.