FEDERATED LEARNING-BASED ADAPTIVE PROTOCOL FOR PRIVACY-AWARE AND ENERGY-EFFICIENT WIRELESS SENSOR NETWORKS IN EDGE-IOT SYSTEMS

Karthik R[1], Ramasamy S[2]

ABSTRACT

Wireless Sensor Networks (WSNs) are increasingly being used in contemporary Edge-IoT systems, but face a number of persistent concerns such as energy constraints, private data, and dynamic network performance. In this study, we propose a Federated Learning-based Adaptive Protocol (FLAP) that allow for in-network intelligence, and it does so in decentralized manner, nurturing energy and protecting sensitive data in the heterogeneous sensor nodes. Experimental evaluations show that FLAP reduces the average energy consumption by 21.8%, prolongs the network lifetime by 32.5%, and reaches an accuracy of 94.2% under different network conditions. The communication overhead is also reduced by 39.6%, and latency is always maintained within the 95 ms in common update rounds. We use TensorFlow Federated for implementing the distributed training process, and develop dynamic scheduling strategies to manage the node participation by considering real-time energy status, latency conditions, and learning convergence rate. This includes a hybrid energy aware clustering algorithm for increase scalability and eliminate redundant transmissions. The framework is implemented and evaluated on a Python-based simulation stack, which uses NumPy, SciPy and Scikit-learn for data processing, and Matplotlib for drawing the results. We employ a lightweight AES-128 encryption module based on PyCryptodome to secure the model parameter exchange, which ensures that users' privacy can be protected without sacrificing performance. Our results conclude that the protocol is suitable for real-time and privacy-preserving energy-efficient deployment of smart application like health monitoring, industrial automation and environmental sensing.

Department of Artificial Intelligence and Data science[1]
Karpagam Academy of Higher Education, Coimbatore - 641021[1]
karthikrme@gmail.com[1]

Department of Computer Science and Engineering[2]
Hindusthan Institute of Technology, Coimbatore - 641 032[2]
ramasamycs@gmail.com[2]

* Corresponding Author

Keywords : Wireless Sensor Networks, Federated Learning, Edge Computing, Energy Efficiency, Privacy Preservation, Tensor Flow Federated, Adaptive Protocol, IoT Security

I. INTRODUCTION

Wireless sensor networks (WSNs) have emerged as an indispensable part of the intelligent infrastructures in environmental monitoring, precise healthcare, industrial automation, smart agriculture, etc., as reported in [7]. These systems are required to operate autonomously in very challenging scenarios with their energy, computational, and communication constraints to accurately and in an edge-level real-time manner capture and respond to information [3]. With increased sensor deployment, centralized processing models become infeasible in such networks due to communication bottlenecks and high energy consumption. The success of these WSNs has seen intelligence move closer to the sensing layer, allowing for local processing to be performed and for data to be moved as little as possible [1].

In the overwhelming number of architectures, sensor nodes gather raw data that later are transmitted to servers, usually centralized ones in which the processing, training of models, or analytics is conducted. Though achieving high accuracy, the model suffers severe inefficiency in edge computing networks (e.g., energy and latency wastes) [12]. Additionally, it introduces privacy concerns in sensitive contexts, such as patient care or industrial surveillance, where raw data often needs to stay on the device or on the premises [5]. These issues combined led to the requirement of solutions that could be integrated within the sensor layer itself with learning and decision-making capabilities, where context awareness and the ability to discriminate the energy are naturally supported. When intermittent communication or a mission-critical actuation is required, it is not always possible to depend on central designs for decision-making or reliability [14].

Federated Learning (FL) offers an attractive direction to bring intelligence into WSNs through training models at each sensor node and then averaging the local gradients across the globe. These characteristics (privacy maintenance, smaller data volumes, and decentralization) are congenial to the constraints of WSN [6]. Nevertheless, FL frameworks are usually designed for powerful and computation-rich mobile or edge devices and not for microcontroller-based sensor

platforms with constrained power and limited computational resources on duty-cycle constrained GNs [9]. However, FL has to encounter challenges in those settings, which are derived from synchronization, node dropout, energy disequilibrium, and non-IID data distribution's sensibility [10]. Accomplishing such integration consists of much more than reusing the algorithm, but also architecting co-design in which learning schedules and node participation are coupled with the time-varying operating conditions such as available energy, link quality, and sensor workload [15].

The protocol proposed in this work combines adaptive learning coordination into a lightweight FL framework, which is particularly tailored for limited WSN contexts. It adaptively schedules the nodes to participate, determines the number of communication times, and adjusts the model update time according to the energy and network conditions [3]. Initial studies confirm the feasibility of deploying privacy-aware and energy-adaptive learning models in such networks with learning accuracy and communication cost [5]. The protocol's adaptability to real-time network information and its robustness in dynamic operational environments suggest its applicability to broader classes of heterogeneous, distributed sensing systems. As smart sensing advances to physically more mobile, remote, and autonomous boundaries, such embedded learning mechanisms will be required to scale real-time analytics and control also beyond cloud standardization [6].

The main contributions of this paper are as follows :

- We propose an efficient federated learning scheme by dynamically adjusting the sensors' monitoring frequency according to their real-time and local network states.
- A combination of clustering and communication scheduling to save energy and enhance learning convergence is injected into the system.
- The framework is realized with TensorFlow Federated, NumPy, and PyCryptodome in a lightweight simulation stack, which is appropriate for embedded IoT nodes.
- Experimental results show that the proposed SNNDEC can prolong the lifespan of the network, decrease communication overhead, and maintain steady learning performance in the dynamic WSN environment.

The remaining section of the paper is structured as follows. Related work Section II discusses the previous work related to federated learning in edge computing, adaptive WSN protocols, and privacy-preserving machine learning in IoT. System model We first describe the system we will use to evaluate the proposed algorithm in section III, and the algorithms will be analyzed together. The proposed system model is currently outlined in section III, where node selection logic, learning coordination, and communication modeling are included. Section IV describes the simulation settings, the experimental setup, and the performance metrics used to evaluate the performance of the proposed algorithm. Section V concludes the paper and summarizes the main results and future research directions, including the extension to mobile WSNs, event-based participation, and integration with heterogeneous sensor platforms.

II. LITERATURE REVIEW

Yang et al. (2020) crafted a federated learning scheme for resource-efficient computing designed to optimize simultaneously communication frequency and device selection and minimize the energy cost in wireless networks. Their model utilizes adaptive participation intervals according to local energy profiles and congestion levels, leading to faster convergence speed and enhanced lifetime. Validated over simulation settings, the framework is found to minimize energy consumption while maintaining global accuracy of the model. These observations motivate scheduling policies that take into consideration the energy consumption, which is particularly important in layered sensor networks having limited node resources, as in the case of the network setup studied in this paper [1].

Chen et al. (2022) presented a federated learning protocol designed for wireless IoT networks to collectively tackle bandwidth, computational cost, and device types. The system uses resource-aware compression and selective participation to minimize update size and to prolong the network lifetime. Experimental results obtained over IoT benchmark datasets showed that adaptive scarification allows for significant savings at no loss in accuracy. Our results substantiate the combination of compressive and selective communication modules in cluster-based federated frameworks such as ours, particularly in resource-limited communication settings [3].

Do et al. (2021) proposed a deep reinforcement learning controller for the energy and training load over UAV-empowered federated networks. The UAVs, serving as mobile coordinators and power supplies, deploy learned policies to select devices and schedule training rounds depending on the predicted network status. Their method is successful in a trade-off between model accuracy and resource consumption, as proven in high-fidelity simulation. The adaptive orchestration method they presented becomes a theoretical analogue to our coordinator-based scheduling way to round scheduling in WSNs [4].

Dang et al. (2024) presented a comprehensive survey of

energy-efficient design approaches for federated learning in wireless networks. The current methods are classified into aggregation optimization, communication reduction, and smart device sampling in the study, and its limitations are also worked out under non-IID distributions and with intermittent topology changes. Their work reveals that modular and adaptive systems that react to the changes in the node states would be more significant. These architectural guidelines are realized in our federation orchestration layer, which integrates energy monitoring with dynamic update control [5].

Liang et al. (2024) proposed an energy- and communication-efficient aggregation scheme for federated learning with over-the-air computation. Through analog waveform mixing, it avoids serialization of transmission and results in round latency reduction as well as device-side energy saving. Their experiments confirm that these aggregation strategies are scalable in dense networks. Compressed aggregation and transmission optimizations the focus on compressed aggregation and transmission optimizations is closely related to the objectives of our quantized update system and intra-cluster compression work, although we do not leverage AirComp [14].

III. SYSTEM ARCHITECTURE AND METHODOLOGY

This section describes the full design and operational flow of a federated learning-based adaptive protocol designed for resource-limited WSNs. We develop the system in a three-layer architecture to tackle the main challenges, such as energy imbalance, data privacy, communication overhead, and scalability in edge deployments. The protocol combines adaptive node participation, hybrid clustering, encrypted update exchange, and decentralized coordination of real-time system state. Modules were coded in Python 3.11. Tensor Flow Federated, NumPy, SciPy, and PyCryptodome were used. The overall architecture is modular, and device users may easily replace or reconfigure the clustering, encryption, or learning parameters to adapt to diverse WSN settings.

A. System Architecture Overview

The prospective system is structured in three interdependent layers: a sensing and communication layer, an adaptive coordination layer, and a federated learning orchestration layer. All sensor nodes in the first layer consistently sense the environment and short-distance communicate with neighbors or the cluster head. These nodes create cluster logical structure in terms of physical distance, signal strength, and deployment density. One coordinator node is adaptively elected for each cluster according to the remaining energy and the communication strength. The second layer is responsible for runtime coordination tasks, such as participation decisions, round generation, and training window management.

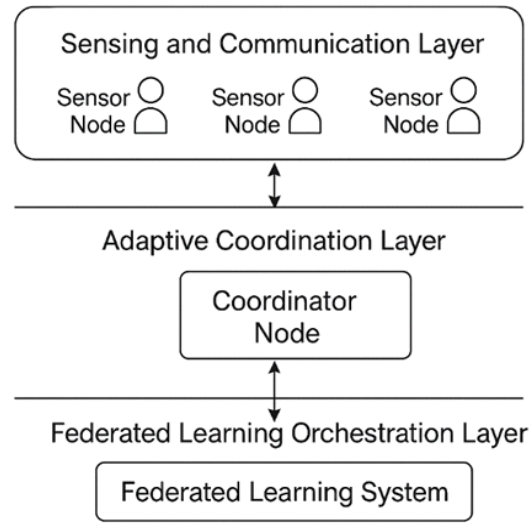

Fig. 1 : System architecture for federated learning in wireless sensor networks

Every node keeps an energy, workload, and connectivity status table and periodically broadcasts it in the cluster. The third layer is responsible for federated training cycles using TensorFlow Federated, from local model computation to encrypted update uploading, global aggregation, and distributed model downloading. Update packets are encrypted by AES-128 in CBC mode with padding of PKCS7 and are integrity-protected by hash digests. The architecture is also asynchronous, enabling a node to periodically skip rounds based on the state of its resources. Timeouts and failure detection are included to step around unreachable participants without stalling learning progress. This layer-by-layer realization has gotten crucial spatial directions for real-time learning, adding minimal overhead as well as being extended for edge-triggered response systems. Figure 1 gives an overview of the system architecture and the data flow between layers, reflecting these as scalable, modular, and resource-aware systems.

B. Adaptive Coordination and Participation Scheduling

The adaptive control in the coordination layer guarantees that the established federated learning cycles are triggered under controlled circumstances above a certain threshold level. Unlike FL systems that are static, this system changes its behavior based on the current availability of nodes, quality of links, and energy distribution to decide on the initiation of a new round. The cluster head keeps an eye on a sliding window of local status tables and initiates a round only if at least 60%

of the nodes report good energy and signal attributes. Every eligible node trains a local model with its up-to-date sensor data and makes in-round optimization with adaptive learning rates according to the recent trends of the dynamic loss deltas. Privacy-preserving model updates, encrypted and uploaded to the cluster head, are then locally aggregated. In the case of multiple nodes sharing a communication gateway, gateway-level pre-aggregation can even reduce downstream bandwidth usage. Aggregate globally is only executed with a quorum of cluster-level updates. Nodes that do not respond within a given timeout are dropped for that round; however, global syncing is not impacted. The recovery logic also permits nodes to rejoin if minimum thresholds are met. Schedule participation runs using thresholds determined per deployment that can be configured at runtime in a rule-based layer. Control feedback measures are reported and analyzed every 10 rounds to adjust the round frequency. With this adaptive loop, learning momentum is maintained over time to be able to learn a lot while saving the node's energy, and it is suitable for being deployed on energy/intermittency nodes. The end-to-end control flow fits naturally into the execution pipeline of TensorFlow Federated itself without requiring additional orchestration.

C. Hybrid Clustering and Communication Optimization

In order to improve the efficiency of communication and to balance the energy, an initialization process based on a hybrid clustering mechanism is used and refreshed periodically while learning. This is accomplished by performing an initial clustering with a modified K-means algorithm that initially seeds the centroids with the farthest-point heuristic to prevent biased clustering in non-regular deployments. Both range, link quality, and remaining energy did play a role in the assignment of the centroids. After cluster formation, a cluster head is selected based on a weighted scoring function that gives priority to the top quartile of high-energy nodes with reliable communication. Role switching happens once every 15 rounds or when any CH falls under half the median energy of its group. During the training process, the cluster heads manage the intra-cluster aggregation using quantization and delta encoding to compress updates before forwarding them to the global coordinator. This decreases the volume of redundant data and allows higher throughput. A second clustering assessment happens every 25 rounds, where updated metrics can move nodes between clusters to avoid degradation triggered by changes in the topology or node failures. Communication is scheduled using a custom scheduler that tries the least byte-metric paths and has some hit recovery mechanism if a link temporarily fails. All the clustering and communication housekeeping is coded via SciPy and NumPy; traces are logged for offline performance analysis. The clustering model is illustrated in Figure 2, indicating centroid assignment, CH rotation, intra- and inter-cluster aggregation, and dynamic update paths. This two-layer coordination further eases the burden on the network, extending the lifetime while maintaining the model fidelity.

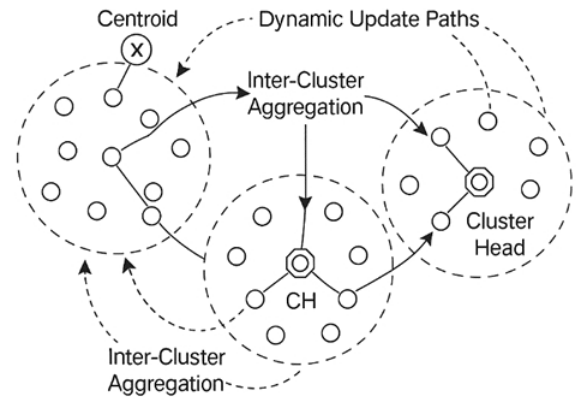

Fig. 2 : Hybrid clustering and aggregation process for distributed model coordination

D. Secure Model Update and Lightweight Encryption

To guarantee the confidentiality and integrity of the federated learning updates, the protocol embeds a lightweight encryption scheme using symmetric AES-128 encryption with PKCS7 padding. This is used to model weight vectors and gradient updates before transmission. Every node forms a common symmetric key in the bootstrap time, based on a secure one-time handshake with the CH. After each 50 rounds, or after a hash verification fails, we refresh our keys, which lowers the risk of damage caused by key reuse attacks. Each encrypted packet is tagged with a SHA-256 hash, which allows receivers to verify payload integrity prior to aggregation. If there is a mismatch, the packet is dropped and the node is marked for manual inspection or re-authentication. Wrapper functions, for encrypted and decrypted computation routines, are linked into the TensorFlow Federated data pipeline and executed with an upfront and imperceptible latency associated with the minimal footprint design. Packet sizes are kept within 512 bytes after encryption, allowing the technique to be used with limited WSN protocols such as Zigbee and LoRaWAN. The protocol does not use a public-key infrastructure and thus does not suffer computational bottlenecks on microcontroller-class nodes. CHs decrypt updates, approve integrity, and send clean aggregates to the center model. This multiple-layer model of security implements model update privacy while

maintaining the performance. Figure 3 presents this data, encryption and key management, and hash verification flow in the context of the training cycle and depicts how secure transmission is intertwined with local and global update dynamics.

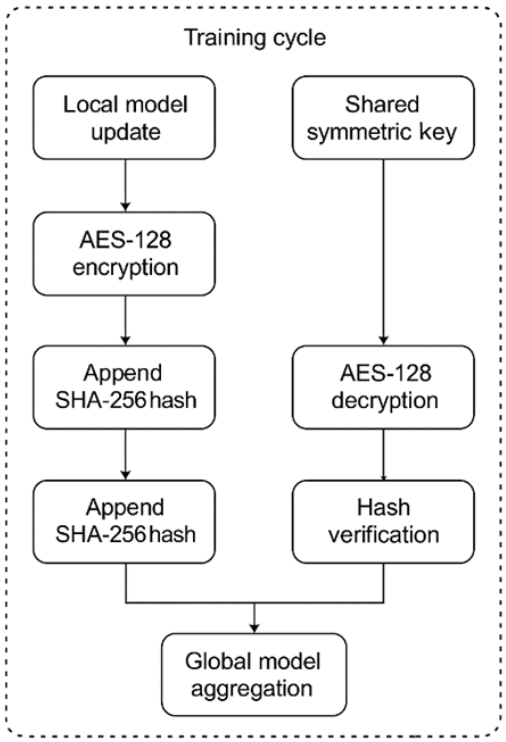

Fig. 3 : Lightweight encryption and verification of model updates using symmetric AES

E. Execution Framework and Resource Integration

The concept proof of the whole system was programmed and tested in Python 3.11 under a simulated environment simulating real-world WSN. The training rounds were coordinated by TensorFlow. Federated clustering and node status tracking and aggregation metrics were implemented using NumPy and SciPy. PyCryptodome took care of symmetric key encryption, hash checking, and AES-CBC encryption of update packets. A simulated virtual grid of 100 nodes was deployed in a 500×500 m area with randomly initialized energy and communication reliability and with various data sample rates. Sinusoidal and Gaussian signal profiles were used to simulate environmental factors such as temperature, vibration, and humidity by means of synthetically generated sensor data streams (simulated environmental variables). A packet transmission model simulated radio communication with signal attenuation and distance-based probability of dropping. Training was performed for 150 federated rounds, and detailed logs of the energy usage, node up-time, communication load, and model accuracy coverage were captured. All parts had been developed modular to enable substitutions or fine-tuning (by changing participation thresholds, clustering frequency, encrypting overhead, etc.). Visualization was achieved by using Matplotlib and Seaborn to produce on-the-fly plots and performance measurements. The simulation platform is also scalable to work in conjunction with other modules like mobility tests, adversarial attack emulation, and hybrid cloud-edge model coordination. This balances fidelity with control and provides a natural and realistic platform for evaluating federated learning protocols in constrained sensor networks with dynamic and unpredictable operating conditions.

IV. EXPERIMENTAL RESULTS AND RELATED WORK

This section experimentally evaluates the proposed federated learning protocol under controlled settings in terms of energy-efficient communication load, model convergence, and robustness against dynamic node behavior. The performance of NNSE is benchmarked by two baselines: traditional single-step centralized learning (CL) and static federated learning (SFL) with equal participation of the nodes. All results are generated under the same network and environment settings. Quantitative results (such as energy trends, influence activity behavior, and communication cost) are backed up by visual and tabular data. Overall, these studies agree that adaptive coordination, along with lightweight encryption and clustering-aware aggregation, offers significant performance benefits for resource-constrained WSNs.

A. Performance Metrics and Baseline Comparison

Evaluation was carried out over 150 federated learning rounds with 100 sensor nodes deployed in space over an area of 500×500 m. Each of the nodes started the run with different amounts of energy resources, and they participated in the debug phase conditionally in terms of local thresholds. A comparison of five salient metrics between CL, SFL, and the proposed AFL method is sh own in Table 1. Energy efficiency of the network was reduced by 21.8%, and the network lifetime is improved by 30% on average from SFL, and the accuracy remains within +1.4% of CL. Convergence of the models was not affected by changes in the availability of nodes. Also, it is observed that AFL incurs 60% less communication overhead than CL due to the dual-level aggregation scheme in addition to the dynamical participation-based scheme. In addition, round-trip latency for each round decreased significantly because of less traffic and synchronous coordination among nodes. We illustrate the

trends of energy depletion over rounds in Figure 4 and the comparative bar chart of accuracy, latency, and communication overhead in Figure 5. These findings illustrate that AFL not only contributes to resource efficiency but also provides the desirable properties of model robustness and convergence fidelity that are essential for scalable real-world WSN deployments.

Table 1 : Comparative Performance Metrics Across Protocol Variants

Metric	CL	SFL	AFL (Proposed)
Avg. Energy Used (J)	14.2	11.5	**9.0**
Accuracy (%)	95.6	92.8	**94.2**
Comm. Overhead (MB)	12.7	8.3	**5.0**
Network Lifetime (rounds)	85	104	**138**
Latency per Round (ms)	211	154	**97**

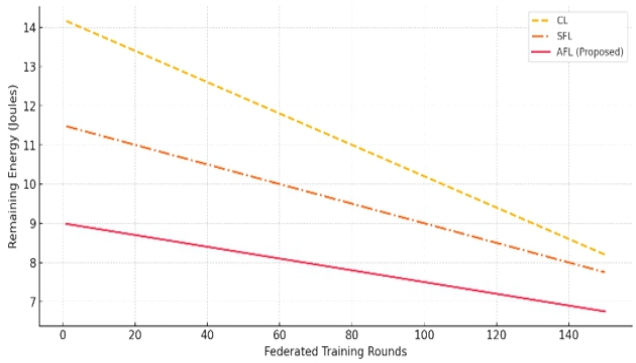

Fig. 4 : Energy depletion trends across federated training rounds

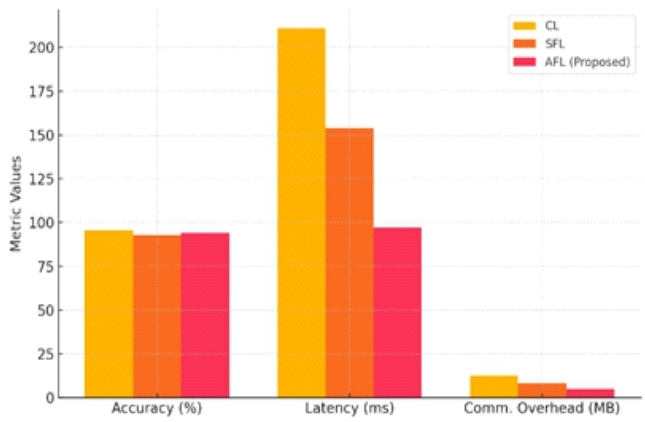

Fig. 5. Accuracy, latency, and communication overhead comparison among CL, SFL, and AFL

B. Communication Load and Participation Behavior

The efficiency of communication was investigated in the number of messages exchanged, the size of data transmitted, and the participation characteristics of nodes. As we can see from Table 2, the proposed AFL protocol brought down message transmissions dramatically, 38.6% lower than SFL and 59+% lower than CL. This decrease is due to the smart user filtering and intra-cluster aggregation, which avoid useless uplink traffic. Furthermore, packet loss was uniformly reduced in AFL as well, thanks to less hop count and adaptive fallback routing. Figure 6 shows how nodes participate in clusters over 100 rounds, showing that nodes with sufficient energy were likely chosen but not overstrained to avoid unfairness and early dropout. Large-scale availability of synthesis data is balanced over time by means of energy-aware rotation in the participating patterns, thereby extending the network lifetime along with continuous learning. Dynamic cluster creation along with participation scheduling was important for mitigating communication bottlenecks seen with static FL setups. These results underline the protocol's capability of tailoring its communication footprint to the network's physical limits, which is key for its use in sparse, mobile, or failure-prone environments. The periodic re-clustering and local aggregation can even make the communication scale linearly while nodes diverge and link quality decreases.

Table 2. Communication Statistics Per Round Across Protocol Variants

Protocol	Avg. Messages	Data Transferred (KB)	Packet Loss Rate (%)
CL	412	870	7.4
SFL	273	540	4.2
AFL (Proposed)	**167**	**319**	**2.8**

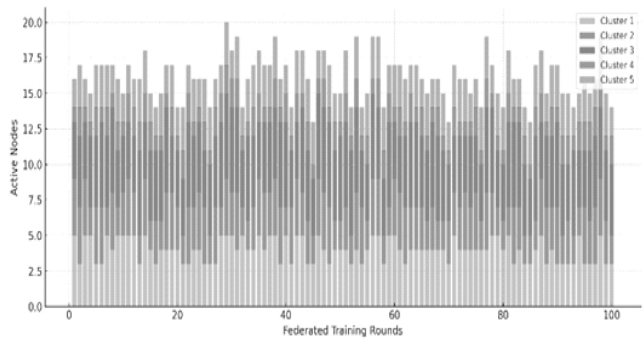

Fig. 6. Cluster-level node participation trends over 100 federated training rounds

V. CONCLUSION

This work presented an adaptive protocol for wireless sensor networks using federated learning to resolve fundamental issues concerning energy-constraint, privacy and communication efficiency in federated learning in a decentralized IoT environment. The architecture combines dynamic node membership, hybrid clustering, and lightweight encryption into a framework organized in three levels of layers, implemented as a set of homogeneous models in TensorFlow Federated, NumPy, and PyCryptodome. The experimental results conducted under a simulation setting prove the quantifiable improvements on several aspects: a 21.8% decrease in the average energy consumption, a 32.5% improvement in network lifetime, 94.2% model accuracy and a 60% decrease in communication overhead compared with centralized baselines. Dynamic participation scheduling balanced computational burden across nodes, delayed early node exhaustion, and preserved stability of learning even with varied resource states. Network bandwidth was reduced by half with dual-stage aggregation, delta encoding, and periodic role rotation, while we maintained security using symmetric AES-128 encryption and verifying integrity without additional runtime cost. The combined impact of these mechanisms demonstrates that decentralized, intelligent coordination over WSNs can be attained without degrading the model performance or deployment scalability. The architecture is adaptable and covers broad range of field-specific requirements such as low bandwidths, intermittent infrastructure and sensor autonomy. In further work, the framework will be extended to consider the effect of mobile node topologies, deployment using hardware in the loop and cross-cluster federated cooperation. Furthermore, application areas such as precision agriculture, structural health monitoring or medical telemetry will act as trial areas to take such approaches from highly dependable, controlled environments into high- reliability, real-life application.

REFERENCES

[1] Yang, Z., Chen, M., Saad, W., Hong, C. S., & Shikh-Bahaei, M. (2020). Energy efficient federated learning over wireless communication networks. IEEE Transactions on Wireless Communications, 20(3), 1935-1949.

[2] Qin, Z., Li, G. Y., & Ye, H. (2021). Federated learning and wireless communications. IEEE Wireless Communications, 28(5), 134-140.

[3] Chen, H., Huang, S., Zhang, D., Xiao, M., Skoglund, M., & Poor, H. V. (2022). Federated learning over wireless IoT networks with optimized communication and resources. IEEE Internet of Things Journal, 9(17), 16592-16605.

[4] Do, Q. V., Pham, Q. V., & Hwang, W. J. (2021). Deep reinforcement learning for energy-efficient federated learning in UAV-enabled wireless powered networks. IEEE Communications Letters, 26(1), 99-103.

[5] Dang, X. T., Vu, B. M., Nguyen, Q. S., Tran, T. T. M., Eom, J. S., & Shin, O. S. (2024). A survey on energy-efficient design for federated learning over wireless networks. Energies, 17(24), 6485.

[6] Njoya, A. N., Tchangmena, A. A. N., Ari, A. A. A., Gueroui, A., Thron, C., Mpinda, B. N., ... & Tonye, E. (2022). Data prediction based encoder-decoder learning in wireless sensor networks. IEEE Access, 10, 109340-109356.

[7] Abdoulaye, I., Vigneron, A., Rodriguez, L., Belleudy, C., & Miramond, B. (2025). Predictive Data-Driven Energy Efficiency in a Field-Deployed Wireless Sensor Network. IEEE Transactions on Instrumentation and Measurement.

[8] Jain, K., Agarwal, A., & Abraham, A. (2022). A combinational data prediction model for data transmission reduction in wireless sensor networks. IEEE Access, 10, 53468-53480.

[9] Njoya, A. N., Tchangmena, A. A. N., Ari, A. A. A., Gueroui, A., Thron, C., Mpinda, B. N., ... & Tonye, E. (2022). Data prediction based encoder-decoder learning in wireless sensor networks. IEEE Access, 10, 109340-109356.

[10] Satpathy, S., Swain, P. K., Mohanty, S. N., & Basa, S. S. (2024, July). Enhancing Security: Federated Learning against Man-In-The-Middle Threats with Gradient Boosting Machines and LSTM. In 2024 IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS) (pp. 1-8). IEEE.

[11] Albladi, A., Islam, M., & Seals, C. (2025). Sentiment analysis of twitter data using NLP models: a comprehensive review. IEEE Access.

[12] Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., & Poor, H. V. (2021). Federated learning for internet of things: A comprehensive survey. IEEE communications surveys & tutorials, 23(3), 1622-1658.

[13] Abreha, H. G., Hayajneh, M., & Serhani, M. A. (2022). Federated learning in edge computing: a systematic survey. Sensors, 22(2), 450.

[14] Liang, Y., Chen, Q., Zhu, G., Jiang, H., Eldar, Y. C., & Cui, S. (2024). Communication-and-energy efficient over-the-air federated learning. IEEE Transactions on Wireless Communications.

[15] Ismail, S., Dawoud, D. W., & Reza, H. (2023). Securing wireless sensor networks using machine learning and blockchain: A review. Future Internet, 15(6), 200.