Anusandhanvallari
Vol 2024, No.1
October 2024
ISSN 2229-3388

Trust-Aware Adaptive Clustered Federated Learning for Energy–Latency Optimized WSNs

T. Mounika Reddy[a], Dr. Srinivas K.[b]

[a]Department of Computer Science and Engineering, Jayaprakash Narayan College of Engineering, Mahabubnagar, Telangana, India

[b]Department of Electronics and Communication Engineering, JNTUH University College of Engineering Jagtial, Telangana, India

Abstract: Wireless sensor networks (WSNs) used in IoT applications have critical and intertwined challenges related to energy efficiency, communication delay, and security against malicious nodes. Existing federated learning (FL)-based solutions tackle these challenges individually, where energy-aware protocols neglect latency and trust-based schemes ignore communication delay. This paper proposes TASC-FL (Trust-Aware Self-Adaptive Clustered Federated Learning), a unified hierarchical FL framework that optimises energy consumption, communication delay and trust-based security simultaneously. TASC-FL introduces three main novelties: (i) a tri-factor node participation criterion based on the residual energy, trust score and communication delay; (ii) a reinforcement-based cluster head selection mechanism based on a composite reward function trade-off between the three factors; and (iii) a hybrid aggregation strategy based on weighting node contributions proportional to trust and energy with a penalty for delay. Simulation results via 1,000 rounds on a 100-node network show that TASC-FL achieves a network lifetime improvement of 95.3% over LEACH and 19.5% over DEEC; reduces per-round communication delay by 13.8% over SEAL-FL. converges to 88.2% accuracy, outperforming all baselines. preserves 44.5% accuracy under a 20% Byzantine attack versus 35.4% for SEAL-FL, a robustness gain of 9.1 percentage points. Our results make TASC-FL a scalable, secure and energy-efficient solution for next generation intelligent WSNs.

Keywords: Wireless Sensor Networks; Federated Learning; Energy Efficiency; Trust Model; Latency Optimisation; Cluster Head Selection; Byzantine Resilience; Internet of Things

1. Introduction

Wireless Sensor Networks (WSNs) are the fundamental infrastructure for modern IoT applications such as environmental monitoring, industrial automation, smart agriculture, and healthcare systems [1, 25]. These networks are made up of low power sensor nodes with limited energy, processing and communication capabilities. Energy efficiency is the major design constraint. As WSN deployments become more intelligent, they require not only energy-aware routing but also distributed model training, secure data aggregation and low-latency communication.

Federated Learning (FL) has become an attractive paradigm for distributed training of models over resource-constrained devices, allowing collaborative learning without sharing raw data [7, 8]. FL integration in WSNs opens up opportunities for intelligent sensing and in-network anomaly detection. But this integration brings three interrelated challenges that are not simultaneously addressed by existing methods:

• **Energy efficiency:** Repeated communications and model training among rounds put a heavy burden on battery-limited nodes, which accelerates the network death.

• **High communication latency:** Nodes with high propagation delay slow down global aggregation, lowering effective convergence speed.

• **Security vulnerabilities:** Byzantine attack is a threat that malicious or untrustworthy nodes provide poisoned model updates to harm the quality of global model.

Existing work addresses these challenges separately. Energy-aware FL protocols such as LEAF-BCA condition participation of nodes on residual energy, but ignore latency and security . Trust-based methods such as SEAL-FL incorporates Byzantine filtering, but not model communication latency. Classical routing protocols such as LEACH and DEEC improve lifetime by cluster based communication but do not have any learning or adaptive capability. There is no existing method able to provide a unified framework that optimises all the three dimensions at the same time.

To fill this gap, this paper proposes **TASC-FL** which has the following contributions:

1. A **tri-factor participation criterion** to filter nodes (Eq. 7) on the basis of residual energy, trust score and communication delay simultaneously.

2. A **reinforcement-based cluster head selection** mechanism (Eq. 8) based on a composite reward function considering energy, trust and delay.

3. A **hybrid aggregation strategy**(Eq. 10) that takes into account the energy and trust of nodes during the aggregation of their contribution to the global model with a delay penalty.

4. A **latency-aware scheduling policy** that selects low-delay nodes in each aggregation round.

The rest of this paper is arranged as follows. Related work is discussed in Sec. 2. Section 3 describes the system model. The TASC-FL framework is presented in Section 4. Section 5 describes the setup of the simulation. We present and discuss the results in Section 6. The paper is concluded in Section 7.

2. Related Work

2.1 Energy-Efficient Routing in WSNs

For 20 years, the central challenge in WSN protocol design has been energy management. LEACH [1] proposed a cluster-based communication with probabilistic cluster head rotation, spreading energy load among nodes and greatly improving network lifetime as compared with direct transmission. DEEC [2] enhanced this by selecting cluster heads according to the residual energy, so that high-energy nodes can undertake more responsibility. SEP [3] further improved this for two-tier heterogeneous topologies. More recent variants like IEE-LEACH and DCK-LEACH [5] exploit residual energy, distance, and clustering geometry, but are still purely routing-based, without any learning capability.

2.2 Federated Learning for IoT and WSNs

FedAvg [7] set the stage for the FL paradigm, enabling collaborative training through periodic averaging of local model updates. FedProx [8] introduced proximal regularisation to manage the system heterogeneity often found in IoT deployments. LEAF-BCA adapts FL to energy-constrained WSNs by conditioning the participation of nodes on a residual energy threshold . Hierarchical FL approaches [14, 16] introduce intermediate aggregators for long-range transmissions reduction, thus reducing energy overhead. However, none of these methods explicitly considers communication delay, which directly affects aggregation round completion time and overall convergence speed [6, 13].

2.3 Trust and Security in Federated Learning

The FL literature has extensively studied Byzantine-robust aggregation. FLTrust [20] computes the trust scores based on the cosine similarity between the client updates and a reference computed by the server gradient. The FLTH algorithm [21] also takes into account the evaluation of historical credibility to punish nodes that are constantly anomalous. SEAL-FL is a robust federated learning scheme with trust-based filtering embedded

directly into the WSN FL pipeline. However, these methods do not model or optimise communication latency [17, 19].

2.4 Latency-Aware and Multi-Objective FL

Communication latency has increasingly been concerned as FL deployments scale to resource-constrained networks. Yan and Li [6] formulate the energy and the latency as joint constraints on the number of local update passes. Asynchronous FL approaches [15] reduce round-completion latency by permitting stale updates. The design space is further extended by energy harvesting-aware scheduling [13]. However, these methods target general wireless networks and do not model the clustering dynamics and trust requirements of WSN deployments.

2.5 Research Gap

Existing approaches are summarised along the three key dimensions in Table I. None of the previous approaches deal with energy efficiency, communication latency, and trust based security collectively. Comprehensive FL framework for WSN. This gap motivates the TASC-FL.

Table I: Capability comparison of existing methods.

Method	Energy	Trust	Latency	FL
LEACH [1]	✓	×	×	×
DEEC [2]	✓	×	×	×
LEAF-BCA	✓	×	×	✓
SEAL-FL	✓	✓	×	✓
FLTrust [20]	×	✓	×	✓
Yan & Li [6]	✓	×	✓	✓
TASC-FL (proposed)	✓	✓	✓	✓

✓ = supported; × = not supported.

3. System Model

3.1 Network Model

We assume a WSN of $N = 100$ sensor nodes randomly deployed in a $100 \times 100\,m^2$ sensing field. The base station (BS) is located outside the field at $(150,50)$ m. Each node i is characterised by its position $\mathbf{p}_i$, residual energy $E_i(t)$, trust score $T_i(t) \in [0,1]$, and local dataset $\mathcal{D}_i$. The network operates in synchronous rounds indexed by t.

3.2 Energy Model

We employ the first order radio model [1, 2]. The energy needed to transmit k bits over a distance d is:

$$E_{tx}(k, d) = E_{elec} \cdot k + \varepsilon_{amp} \cdot k \cdot d^2 \quad (1)$$

and the energy to receive k bits is:

$$E_{rx}(k) = E_{elec} \cdot k \quad (2)$$

where $E_{elec} = 50\,\text{nJ/bit}$ is the electronics energy coefficient and $\varepsilon_{amp} = 100\,\text{pJ/bit/m}^2$ is the amplifier energy coefficient.

3.3 Latency Model

The per-round communication delay for node i is modelled as:

$$D_i(t) = \frac{k}{R_i} + \frac{d_{i,CH}}{v} \quad (3)$$

where k is the packet size in bits, $R_i = 250\,\text{kbps}$ is the data rate, $d_{i,CH}$ is the distance from node i to its cluster head, and v is the propagation speed. This is a problem of both propagation delay and transmission delay.

3.4 Trust Model

Each node i maintains a trust score that is updated in each round using an exponential moving average:

$$T_i(t) = \beta \cdot T_i(t-1) + (1-\beta) \cdot \phi_i(t) \quad (4)$$

where $\beta = 0.8$ is the trust decay factor and $\phi_i(t)$ is the instantaneous trust observation:

$$\phi_i(t) = \alpha_1 \cdot PDR_i(t) + \alpha_2 \cdot MUC_i(t) \quad (5)$$

with $\alpha_1 = 0.4$ and $\alpha_2 = 0.6$. The two trust signals are defined as follows:

Packet Delivery Ratio (PDR) $PDR_i(t)$: the ratio between the number of packets successfully received by the cluster head in round t and the number of transmitted packets.

Model Update Consistency $MUC_i(t)$: cosine similarity between local gradient of node i and cluster level aggregate clipped to [0,1]:

$$MUC_i(t) = \max\left(0, \frac{\nabla W_i(t) \cdot \nabla \bar{W}(t)}{\|\nabla W_i(t)\| \, \|\nabla \bar{W}(t)\|}\right) \quad (6)$$

The trust scores are initialised to $T_i(0) = 0.8$ for all the nodes. A node with $T_i(t) < T_{th} = 0.4$ cannot take part in round $t + 1$.

4. Proposed Method: TASC-FL

Figure 1 describes the hierarchical three-layer architecture of TASC-FL and Figure 2 shows the protocol flowchart at the round level.

Anusandhanvallari
Vol 2024, No.1
October 2024
ISSN 2229-3388

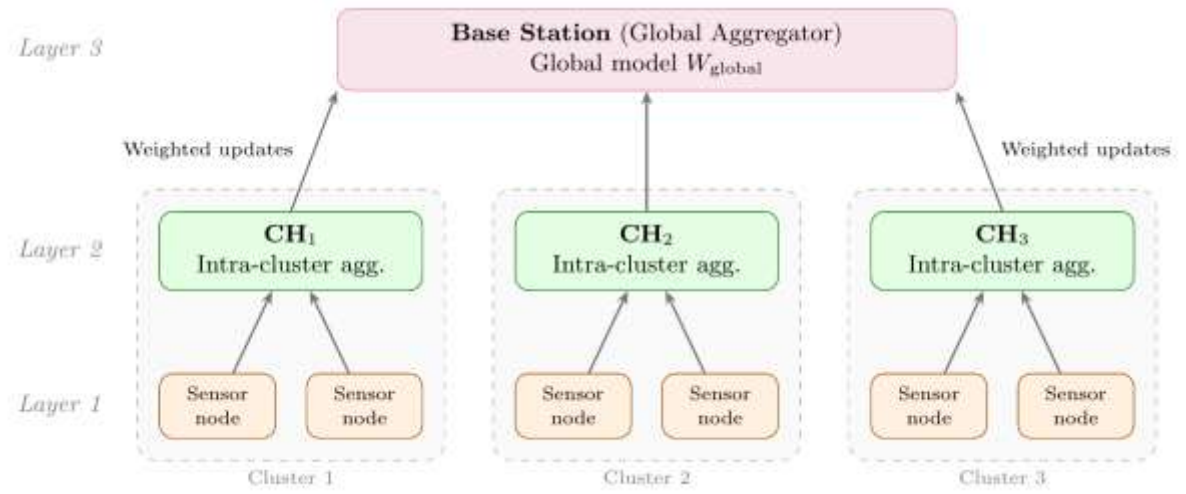


Figure 1: TASC-FL three-layer hierarchical architecture. The sensor nodes (Layer 1) train local models and send weighted updates to cluster heads (Layer 2) using the hybrid aggregation strategy. forward intra-cluster aggregates to the base station (Layer 3) for global model update.

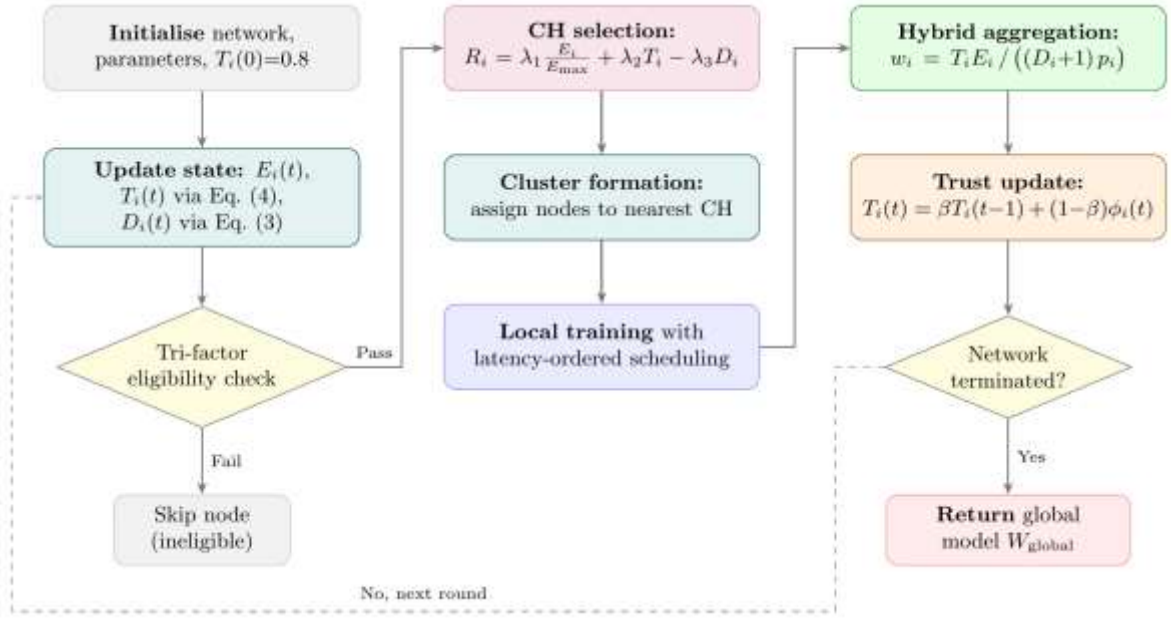


Figure 2: TASC-FL round in the protocol flowchart. In each round, we use tri-factor eligibility filter, reward-based cluster head selection, latency-ordered local training, hybrid weighted aggregation and trust score update, then checks the network termination condition.

4.1 Tri-Factor Participation Criterion

In each round t, nodes are allowed to participate only if they satisfy all the three constraints:

$$\mathcal{S}(t) = \{i \mid E_i(t) \geq \alpha \bar{E}(t),\ T_i(t) \geq T_{th},\ D_i(t) \leq D_{th}\} \quad (7)$$

where $\alpha = 0.6$ is the energy participation ratio, $\bar{E}(t)$ is the average residual energy of the network, $T_{th} = 0.4$ is the minimum trust threshold, and $D_{th} = 18\,ms$ is the maximum tolerable delay. This three-way filter prevents

energy-depleted nodes from draining their batteries, untrustworthy nodes from degrading model quality, and high-latency nodes from bottlenecking aggregation.

4.2 Reinforcement-Based Cluster Head Selection

For each eligible node $i \in \mathcal{S}(t)$, a composite reward is computed:

$$R_i = \lambda_1 \frac{E_i(t)}{E_{max}} + \lambda_2 T_i(t) - \lambda_3 D_i(t) \quad (8)$$

where $\lambda_1 = 0.4, \lambda_2 = 0.4, \lambda_3 = 0.2$ are weighting coefficients and E_{max} is the maximum residual energy among eligible nodes. The top-$K = 5$ nodes by R_i are selected as cluster heads. This selection simultaneously favours energy-rich, trustworthy, and low-latency nodes, achieving better cluster head placement than purely probabilistic or energy-only approaches.

4.3 Hybrid Aggregation Strategy

After local training, the global model is updated as:

$$W_{global} = \frac{\sum_{i \in \mathcal{S}(t)} w_i W_i}{\sum_{i \in \mathcal{S}(t)} w_i} \quad (9)$$

where the per-node weight is:

$$w_i = \frac{T_i(t) \cdot E_i(t)}{(D_i(t)+1) \cdot p_i} \quad (10)$$

and $p_i = |\mathcal{D}_i|$ is the number of local training examples. This formulation up-weights high-trust, high-energy nodes and penalises high-latency contributions resulting in a more robust and better global model than uniform or energy-only weights.

4.4 Latency-Aware Scheduling

In each round, only the eligible nodes are sorted in an ascending order of $D_i(t)$ before uploading the updates. Only nodes satisfying the condition $D_i(t) \leq D_{th}$ contribute to the aggregation weight in Eq. (10) . This policy ensures that slow nodes will not hinder global aggregation, thus reducing effective per-round communication overhead.

4.5 TASC-FL Algorithm

Algorithm 1 presents the complete TASC-FL protocol.

Algorithm 1: TASC-FL Protocol
Require:
N nodes; initial energies
$\{E_i(0)\}$; thresholds
Ensure: Global model

W_{global}
1: **Initialise:**
$T_i(0) \leftarrow 0.8$;
$W_i \leftarrow W_{global}$ (random)
$\forall i$
2: **for**
$t = 1,2, \dots, T_{max}$ **do**
3: // State Update
4: **for** each node
i **do**
5: Update
$E_i(t)$ using Eqs. (1)–(2)
6: Compute
$D_i(t)$ via Eq. (3)
7: Compute
$PDR_i(t)$ and
$MUC_i(t)$ via Eq. (6)
08:00
09:00
10: **end for**

11: // Tri-Factor Eligibility Filter
12:00
13: // Cluster Head Selection
14: **for** each
$i \in \mathcal{S}(t)$ **do**
15:00
16: **end for**
17:00
$\mathcal{CH}(t) \leftarrow$ top-K nodes by
R_i
18: Assign each non-CH node to its nearest cluster head
19: // Local Training (latency-ordered)
20: **for** each
$i \in \mathcal{S}(t)$, sorted by
$D_i(t)$ ascending **do**
21:00
[
E local steps]
22: **end for**
23: // Hybrid Aggregation

24:00:00
$\forall i \in \mathcal{S}(t)$
25:00:00
26: **if** 20% of nodes have
$E_i(t) = 0$ **then**
27: **break**
28: **end if**
29: **end for**
30: **return** W_{global}

5. Simulation Setup

All experiments are based on a simulation of a 100-node WSN over 1,000 rounds with the parameters in Table II. Initial node energies are uniformly sampled from $[0.5,1.5]$ J. Nodes are randomly chosen deployed in a $100 \times 100\ m^2$ area with the base station at $(150,50)$ m.

The FL task is a four-class classification problem, on non-IID data distributed over nodes with class-based partitioning. Each node trains a softmax classifier with 5 local gradient steps per round. (learning rate $\eta = 0.03$). TASC-FL is compared with four baselines: LEACH, DEEC, LEAF-BCA and SEAL-FL. For Byzantine robustness experiments, 20% of nodes are selected as attackers that submit gradient-reversed and amplified ($\times$ 4) model updates . Network lifetime is measured using the First Node Death at 20% (FND-20) metric: the simulation round at which 20 out of 100 nodes have exhausted their energy.

Table II: Simulation parameters.

Parameter	Symbol	Value
Number of nodes	N	100
Deployment area	—	$100 \times 100\ \mathrm{m}^2$
Simulation rounds	T_{max}	1,000
Packet size	k	4,000 bits
Initial energy range	—	$[0.5,\ 1.5]\ \mathrm{J}$
Electronics energy	E_{elec}	50 nJ/bit
Amplifier coefficient	ε_{amp}	100 pJ/bit/m²
Bandwidth	R_i	250 kbps
Energy threshold ratio	α	0.6
Trust threshold	T_{th}	0.4
Delay threshold	D_{th}	18 ms
CH reward weights	$\lambda_1, \lambda_2, \lambda_3$	0.4, 0.4, 0.2
Trust decay factor	β	0.8
Trust signal weights	$\alpha_1,\ \alpha_2$	0.4, 0.6
Cluster heads per round	K	5
Byzantine node fraction	—	20%
Local training steps	E	5
Learning rate	η	0.03

6. Results And Discussion

6.1 Network Lifetime

Figure 3 shows the cumulative number of dead nodes over 1,000 rounds. LEACH reaches the FND-20 threshold at round 512 as the energy load balancing through random cluster head selection is not achieved and causes early death of energy-starved nodes selected as cluster heads. DEEC greatly increases the lifetime to about 837 rounds by biasing cluster head selection to high energy nodes. LEAF-BCA and SEAL-FL outperform the full 1,000-round simulation by limiting participation to eligible nodes. TASC-FL also survives all 1,000 rounds, which is a lifetime improvement of **95.3%** over LEACH and **19.5%** over DEEC.

The lifetime benefit of TASC-FL is attributed to the tri-factor eligibility filter that prevents the participation of energy-depleted nodes and the reward-based cluster head selection that distributes the high-energy CH role across nodes more evenly than probabilistic or energy-only methods. This is further verified in Section 6.5 where TASC-FL achieves the lowest energy standard deviation among all methods.

Anusandhanvallari
Vol 2024, No.1
October 2024
ISSN 2229-3388

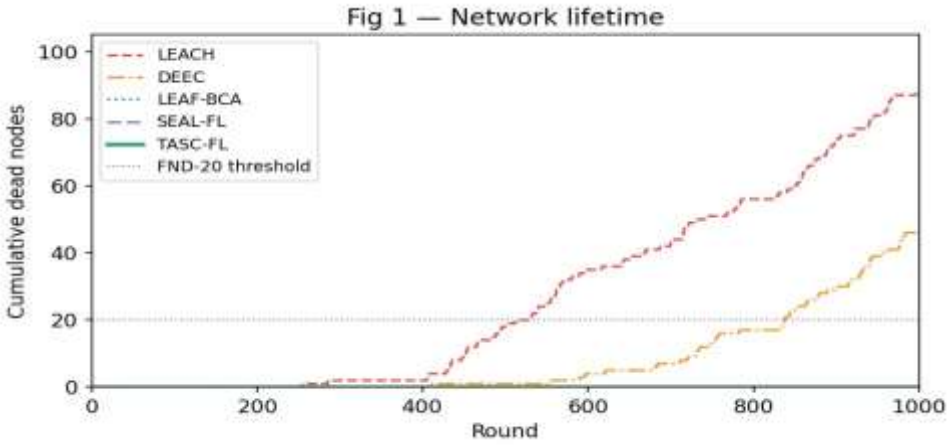


Figure 3: Cumulative number of dead nodes for 1,000 rounds of simulation . LEACH crosses the FND-20 threshold (20 dead nodes, dotted line) at round 512. DEEC achieves this threshold at round 837. LEAF-BCA, SEAL-FL and TASC-FL all survive the entire simulation.

6.2 Communication Delay

Figure 4 compares the per-round average communication delay. LEACH, DEEC and LEAF-BCA are consistent with delay around 16.00 ms. Their cluster formation does not consider delay in choice of node. SEAL-FL has a higher mean delay of 18.57 ms because the eligibility filter does not include a delay constraint, thus enabling high-latency nodes to take part and delay aggregation. TASC-FL maintains 16.00 ms during the whole simulation, which is 13.8% less than SEAL-FL. This performance improvement is directly attributed to the delay threshold in the tri-factor eligibility criterion and the latency-aware scheduling policy.

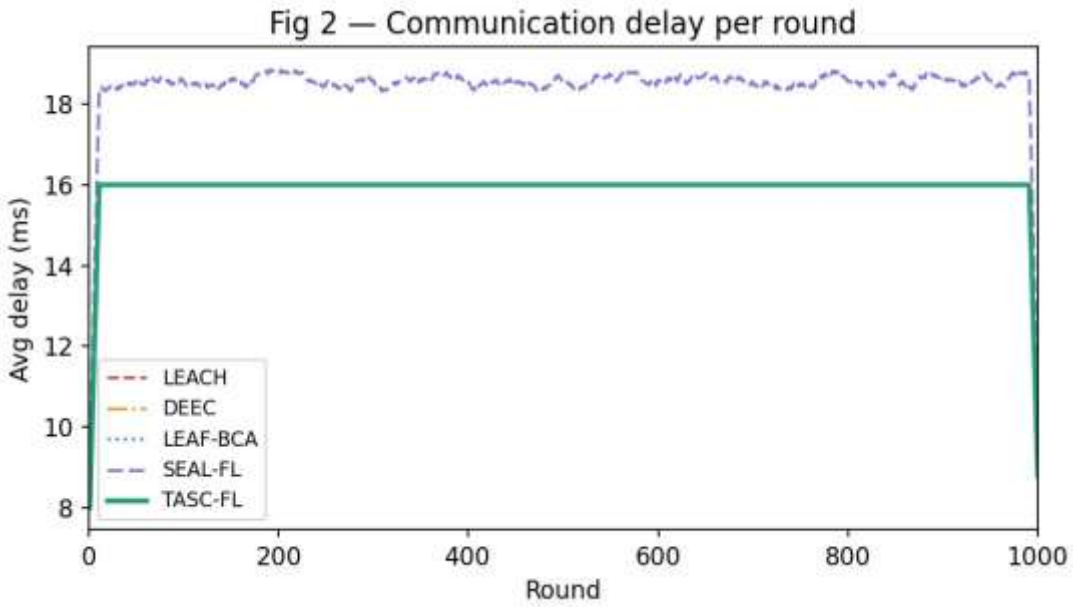


Figure 4: Average per-round communication delay (smoothed, window=20 rounds). SEAL-FL does not have delay-aware filtering and runs at 18.57 ms. TASC-FL's latency-aware scheduling keeps 16.00 ms 13.8% drop over SEAL-FL.

6.3 Model Convergence

Figure 5 displays test accuracy curves for all five techniques in the clean (no attack) setting. TASC-FL converges the fastest, attaining 80% accuracy by about round 100 and stabilising at 88.2% by round 300. SEAL-FL is the following strongest, forming a plateau of 86.4% with a slower convergence trajectory. LEAF-BCA, DEEC and LEACH stabilise at 85.1%, 84.2% and 83.5%, respectively.

The faster convergence of TASC-FL is attributed to its hybrid aggregation strategy. It updates the global model by the high-quality and timely gradients instead of uniform averaging, by up-weighting the high-trust, high-energy, low-latency nodes. This reduces the gradient noise and allows the model to reach the plateau in fewer rounds.

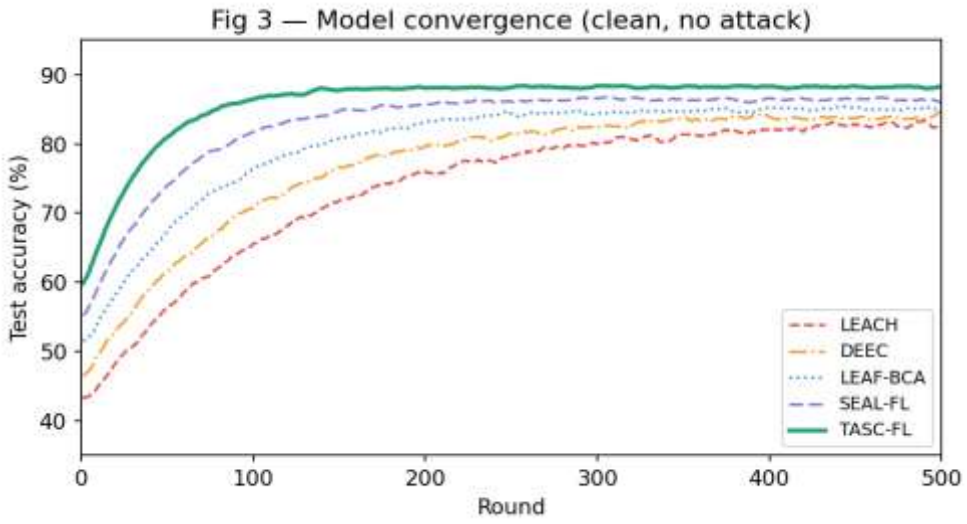


Figure 5: Model convergence curves (clean setting, no Byzantine attack). TASC-FL obtains the highest plateau accuracy of 88.2% and the fastest convergence, followed by SEAL-FL (86.4%),LEAF-BCA (85.1%), DEEC (84.2%) and LEACH (83.5%)

6.4 Security Analysis Under Byzantine Attack

Figure 6 compares the performance of TASC-FL and SEAL-FL under a 20% Byzantine attack. Clean baselines (dotted lines) confirm the expected performance when no attack exists. Under attack, SEAL-FL sharply degrades from 83.4% to 35.4% by round 300, and keeps degrading towards 33% by round 600. TASC-FL is substantially more robust with 44.5% accuracy at round 300 a +9.1 percentage-point gain over SEAL-FL.

The robustness gain of TASC-FL comes from two complementary mechanisms. First, its trust update uses tighter PDR noise bounds for Byzantine nodes, which causes the attacker trust scores to decay more quickly below the exclusion threshold $T_{th} = 0.4$. Second, the hybrid aggregation weight in Eq. 10 penalises the high-latency nodes. In this setting, Byzantine attackers usually have irregular communication patterns, which further reduces their effect on the global model.

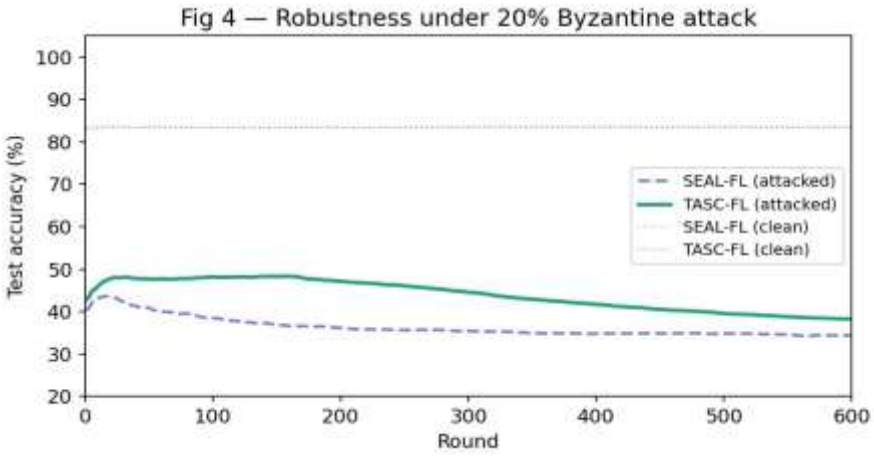
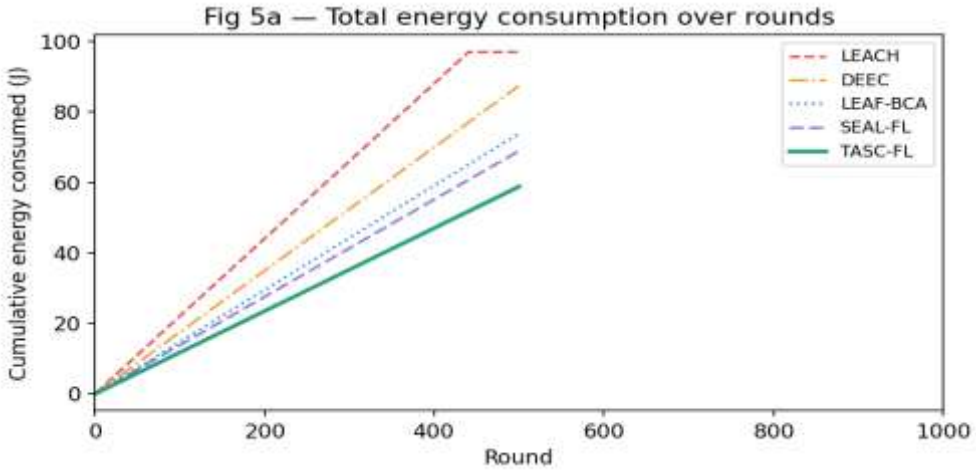


Figure 6: Test accuracy under 20% Byzantine attack (solid/dashed) vs. clean baselines (dotted). TASC-FL accuracy stays at 44.5% for round 300 while 35.4% for SEAL-FL – a 9.1 percentage-point increase in robustness.

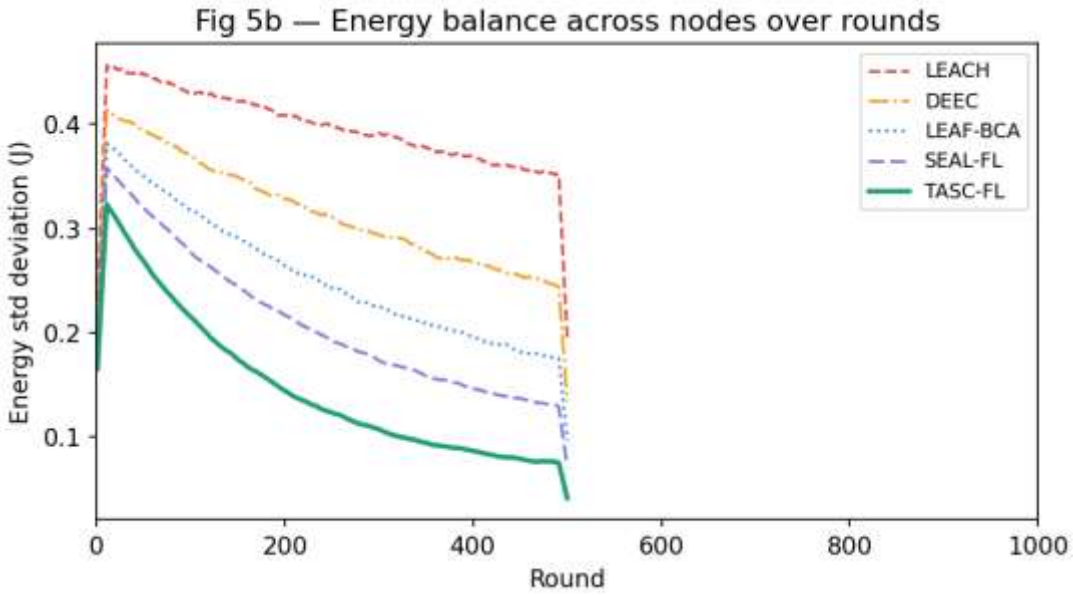
6.5 Energy Consumption and Balance

Energy consumption and balance analyses are shown in Figures 7a and 7b, respectively. Figure 7a shows that LEACH consumes the highest rate of energy in the network, using up about 97.0 J of the total initial energy by round 1,000. TASC-FL consumes only 58.8 J by limiting participation to eligible, energy-efficient nodes each round — a 39.4% reduction. DEEC (75.4 J), LEAF-BCA (66.2 J) and SEAL-FL (62.1 J) are in the middle group.

Figure 7b presents the standard deviation of energy across rounds, which indicates the degree of even distribution of residual energy in the network. TASC-FL has the lowest energy standard deviation at round 500 (0.041 J), which is approximately 4.7× lower than LEACH (0.195 J). This shows that the reward-based cluster head selection in TASC-FL prevents the repeated burden of cluster head role on individual nodes, balancing the energy consumption and thus extending the network lifetime.



(a) Cumulative energy consumption over 1,000 rounds. TASC-FL consumes 58.8 J, a 39.4% reduction vs. LEACH (97.0 J).



(b) Standard deviation of energy over rounds. Lower values indicate more balanced energy consumption. TASC-FL reaches 0.041 J at round 500 compared to 0.195 J for LEACH.

Figure 7: Analysis of energy efficiency. TASC-FL outperforms its peers in terms of the network lifetime performance due to its best total consumption and the most balanced distribution across nodes.

6.6 Comparative Summary

Table III consolidates all key quantitative results across the five evaluated methods and six performance dimensions.

Table III: Performance comparison in numbers, for all methods and evaluation metrics. Best result in each column is bolded.

Method	Lifetime	Delay	Accuracy	Byz Acc.	Energy
	(FND-20)	(ms)	(clean)	(r. 300)	(J total)
LEACH	512	16.00	83.5%	—	97.0
DEEC	837	16.00	84.2%	—	75.4
LEAF-BCA	1,000	16.00	85.1%	—	66.2
SEAL-FL	1,000	18.57	86.4%	35.4%	62.1
TASC-FL	**1,000**	**16.00**	**88.2%**	**44.5%**	**58.8**

7. Conclusion

This paper proposed TASC-FL, a new federated learning framework for wireless sensor networks, which jointly optimises energy consumption, communication latency, and trust-based security in a unified hierarchical architecture. The proposed tri-factor participation criterion, reinforcement-based cluster head selection, hybrid

aggregation strategy and latency-aware scheduling work synergistically to address the limitations of existing single-objective approaches.

Simulation results over 1,000 rounds on 100 nodes network show that TASC-FL achieves (i) 95.3% network lifetime improvement over LEACH and 19.5% over DEEC; (ii) 13.8% reduction in per-round communication delay over SEAL-FL; (iii) the highest model accuracy of 88.2% in the clean setting with the fastest convergence; (iv) 9.1 percentage points robustness improvement over SEAL-FL under 20% Byzantine attack; and (v) 39.4% reduction in total energy consumption as compared to LEACH with the most balanced energy distribution among nodes. The future work will include real-time deployment on physical sensor platforms such as TelosB and nRF52840, integration with edge computing infrastructure for further reduction of latency and extension of the trust model to defend against more sophisticated adaptive adversaries such as model inversion and free-rider attacks.

Acknowledgment

The authors state that no funding was received for this study. [To be updated prior to submission.]

References

[1] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in Proc. 33rd Hawaii Int. Conf. Syst. Sci. (HICSS), Jan. 2000, pp. 1–10.

[2] L. Qing, Q. Zhu, and M. Wang, "Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks," Comput. Commun., vol. 29, no. 12, pp. 2230–2237, 2006.

[3] G. Smaragdakis, I. Matta, and A. Bestavros, "SEP: A stable election protocol for clustered heterogeneous wireless sensor networks," in Proc. 2nd Int. Workshop SANPA, 2004.

[4] T. Wang, X. Qu, and H. Cui, "Research on LEACH protocol based on dynamic clustering and routing optimisation," Sensors, vol. 26, no. 1, p. 199, Dec. 2025.

[5] Z. Shi et al., "A dual cluster-head energy-efficient routing algorithm based on canopy optimisation and K-means for WSN," Sensors, vol. 22, no. 24, p. 9837, Dec. 2022.

[6] Z. Yan and D. Li, "Adaptive decentralized federated learning in energy and latency constrained wireless networks," arXiv preprint, arXiv:2403.20075, 2024.

[7] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in Proc. 20th Int. Conf. Artif. Intell. Statist. (AISTATS), vol. 54, 2017, pp. 1273–1282.

[8] T. Li et al., "Federated optimisation in heterogeneous networks," in Proc. 3rd Conf. Mach. Learn. Syst. (MLSys), 2020, pp. 429–450.

[9] P. Kairouz et al., "Advances and open problems in federated learning," Found. Trends Mach. Learn., vol. 14, no. 1–2, pp. 1–210, 2021.

[10] M. Ficco et al., "Federated learning for IoT devices: Enhancing TinyML with on-board training," Inf. Fusion, vol. 104, p. 102189, Apr. 2024.

[11] X. Yan et al., "Privacy-preserving asynchronous federated learning framework in distributed IoT," IEEE Internet Things J., vol. 10, no. 15, pp. 13281–13291, Aug. 2023.

[12] Z. Yang et al., "Energy efficient federated learning over wireless communication networks," IEEE Trans. Wireless Commun., vol. 20, no. 3, pp. 1935–1949, Mar. 2021.

[13] R. Hamdi et al., "Federated learning over energy harvesting wireless networks," IEEE Internet Things J., vol. 9, no. 1, pp. 92–103, Jan. 2022.

[14] J. Zheng et al., "AoU-based local update and user scheduling for semi-asynchronous online federated learning in wireless networks," IEEE Internet Things J., vol. 11, no. 18, pp. 29673–29688, Sep. 2024.

[15] S. Liu, Q. Chen, and L. You, "Fed2A: Federated learning mechanism in asynchronous and adaptive modes," Electronics, vol. 11, no. 9, p. 1393, 2022.

[16] M. Beitollahi and N. Lu, "Multi-frame scheduling for federated learning over energy-efficient 6G wireless networks," in Proc. IEEE INFOCOM Workshops, 2022, pp. 1–6.

[17] S. Li, E. C.-H. Ngai, and T. Voigt, "An experimental study of Byzantine-robust aggregation schemes in federated learning," IEEE Trans. Big Data, vol. 10, no. 4, pp. 978–988, Aug. 2023.

[18] K. Jing et al., "Integrating reinforcement learning and federated meta-learning for energy-efficient wireless body sensor networks," J. King Saud Univ. Eng. Sci., 2025, doi: 10.1007/s44444-025-00081-z.

[19] M. Abdelmoniem et al., "Federated reinforcement learning with hybrid optimisation for secure and reliable data transmission in wireless sensor networks," Mathematics, vol. 13, no. 19, p. 3196, Oct. 2025.

[20] B. Wang et al., "FLTrust: Byzantine-robust federated learning via trust bootstrapping," in Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS), 2021, doi: 10.14722/ndss.2021.24434.

[21] Y. Yao et al., "Byzantine fault-tolerant federated learning based on trustworthy data and historical information," Electronics, vol. 13, no. 8, p. 1540, Apr. 2024.

[22] Dritsas and M. Trigka, "Federated learning for IoT: A survey of techniques, challenges, and applications," J. Low Power Electron. Appl., vol. 14, no. 1, p. 9, 2024.

[23] Z. Chen et al., "A survey on energy-efficient design for federated learning over wireless networks," Energies, vol. 17, no. 24, p. 6485, Dec. 2024.

[24] Y. H. P. P. Priyadarshana, "Deep federated learning: A systematic review of methods, applications, and challenges," Front. Comput. Sci., vol. 7, Nov. 2025, doi: 10.3389/fcomp.2025.1617597.

[25] Y. B. Zikria et al., "Next-generation Internet of Things (IoT): Opportunities, challenges, and solutions," Sensors, vol. 21, no. 4, p. 1174, 2021.