A Review on Green Trustworthy Federated Edge Intelligence for Secure and Energy-Sustainable WSNs

Dr. J. Samuel Manoharan
Professor & Head/Dept. of Biomedical Engineering
Jerusalem College of Engineering
Chennai 600100, South India
samuel1530@gmail.com

Abstract: In healthcare, water management, air-quality monitoring, climate monitoring and smart infrastructure, the wireless sensor network (WSN) is used for long-term monitoring. The first energy limitation is that they are not sustainable in practice because of the depletion of energy resources, because nodes are unreliable, or malicious, because they generate too much communication overhead, or because they are unstable to route. Most of the existing research focuses on energy efficiency, federated learning, trust management, secure routing, and so on, as distinct concerns, without considering coordinated network level decision making. This paper suggests a Green Trustworthy Federated Edge Intelligence Systems in a single WSN architecture to tackle the challenges of multi-factor node trust evaluation, energy-aware federated participation and trust-based secure routing. It assesses the behaviour of nodes, the amount of energy they have left, the consistency of their sensing, and the reliability of their communications to facilitate the participation of trustworthy models and the selection of paths at the edge. An in-depth comparison of recent research reveals that trust, energy sustainability, federated learning and network-layer routing are well suited to be coupled more tightly. The framework proposed is suitable to be evaluated by means of Security, Sensing and WSN datasets, as well as network simulations under normal and adversarial conditions. The study offers quantitative basis for a secure, energy-efficient, deployment-driven WSNs for smart environments related to SDGs.

Keywords: Wireless Sensor Networks; Federated Edge Intelligence; Trust Management; Energy-Aware Routing; Secure Routing; Sustainable IoT

Introduction

Wireless sensor networks (WSNs) are the sensor backbone for numerous smart applications such as healthcare monitoring, water management, air-quality measurement, climate observation and intelligent infrastructure. But their life-time performance is limited due to the energy constraints of each node, communication overhead, unreliable and malicious nodes and routing instability. Therefore, in recent studies, the focus has been given to energy-efficient networking, federated learning, security and trust management, and secure communication as important mechanisms for enhancing the sustainability and reliability of WSN [1]–[3].

The benefits of federated learning are that sensor data does not need to be continuously transferred to centralized servers, so as to not expose privacy risks and move unnecessary data [1, 2].

In addition, for distributed learning, the residual energy, communication cost, and node participation are also important matters to consider, which is demonstrated by energy-aware federated learning [2], [3]. Conversely, intelligent routing techniques have been explored to enhance the routing process and communications efficiency in IoT-based WSN environments [4].

Recent federated learning studies in the field of trust also reveal that methods for using trust and residual energy in client selection and aggregation approach to enhance the reliability of edge learning [5, 6]. However, current solutions focus on either federated learning orchestration, energy efficiency, energy security, or routing. There is a lack of tight integration of the behavioural trust evaluation, energy-aware federated participation in trust issues, and network-layer secure routing [5], [6].

To fill the above mentioned gap, this paper introduces a trustworthy, green distributed edge intelligence solution for secure and energy-efficient WSNs. In the framework, multi-factor node trust evaluation, energy-aware federated participation and trust-based secure routing are all wrapped together in a unified architecture. Its goal is to minimize the nonessential communication, prevent the use of unreliable nodes, distribute energy usage evenly, and enable reliable operation of a long-term WSN for SDGs in a smart environment.

Related work

Data collection architectures have shifted from traditional to distributed and intelligent environments that can be used for the healthcare, environmental monitoring, industrial and smart infrastructure. The limited battery capacity, unreliable wireless links, limited processing power, non-homogeneity of sensing data, and exposure to malicious nodes still limit their long-term operation. In recent studies, therefore, several approaches such as federated learning, energy-aware routing, trust evaluation, edge intelligence and distributed security have been investigated as a way of enhancing network sustainability. While significant gains have been reported, most current work is optimizing selected aspects of the WSN operation, which motivates the need for increased coordination among the learning, trust, energy and routing mechanisms.

Numerous studies have focused on using FL in routing and distributed decision making for WSNs with IoT devices. In [7] federated deep reinforcement learning was used to enable adaptive routing in the dynamic network. Distributed learning allows to make local routing decisions but can still coordinate knowledge among participating nodes. This method considers various factors, including packet loss, latency, energy efficiency, scalability, communication overhead, and dynamic network conditions. This shows that federated learning is not limited to distributed classification tasks and can be used for optimisation at the network level. The routing process mostly focuses on adaptive and energy-efficient packet forwarding, however. There is no joint incorporation of behavioral trust assessment, consistency detection, malicious node reputation and trust-dependent collaborative learning participation. Thus, the security and trustworthiness of the nodes involved in federated routing should be given more consideration as in [7].

There have also been studies on secure and energy-aware routing that have not been connected to federated learning. [8] fuses the energy information and trust evaluation in the hierarchical WSN routing approach. Residual energy and communication behavior are taken into consideration when choosing appropriate forwarding nodes and cluster heads. This is necessary because energy-based selection may lead to unreliable/compromised nodes being selected for critical communication tasks. Therefore, adding trust can enhance the reliability of the route and network security. But the architecture is still mostly routing based. It does not promote a federated model

participation and distributed learning coordination. Moreover, the information gained within the nodes is not re-used in both learning and network layers. This separation restricts the power of the network to make the same decisions on the nodes that will learn, aggregate, forward, or be excluded.

A federated security mechanisms has since gained more focus since traditional centralised intrusion detection systems need sensor or IoT data to be shipped to the central servers. The work reported in [9] points out that federated learning can be an appropriate training method for distributed intrusion detection systems, where it is impossible to share the data collected locally. This type of architecture can minimize privacy issues and needless raw data transfers. Simultaneously, the study reveals some barriers, such as communication cost, a device diversity problem, non-identically distributed data, computational limitation and security issues that may arise during the federated-learning process. These are important challenges for WSNs because each node can have very different local distributions of data, sensing capabilities, communication reliability, and energy levels. But federated intrusion detection doesn't necessarily mean secure route formation, though. There needs to be a mechanism that links security observations with participation in the nodes, energy management and packet forwarding decisions.

Multi-factor trust evaluation is one potential answer to this constraint. In [10], multiple indicators are considered instead of relying on a single trust measure in the context of trust evaluation for federated learning. Overall assessment of a participating node includes node behaviour, node reliability, historical trust and reputation information. The method also deals with the uncertainty and inconsistency of recommendations and reputation information. This is important for distributed WSN environments as a node cannot be trusted by relying on a single communication event or isolated observation. Multiple reliability indicators and historical behaviour can yield more consistent trust estimates. However, the trust value in [10] is primarily used to assess the trustworthiness of the participants of federated learning. It has limited application to routing, secure forwarding, sensing consistency, and network-lifetime management in WSN, which are energy-balanced.

Four representative studies that are closely related to the proposed research are compared with a focus in Table 1.

Table 1. Comparison of representative related works

Ref.	Main Focus	Major Strength	Limitation Relevant to This Work
[7]	Federated deep reinforcement learning for WSN routing	Distributed and adaptive energy-aware routing	Does not jointly incorporate multi-factor trust into FL participation and routing
[10]	Multi-factor trust evaluation for federated learning	Behaviour, reliability, history, and reputation-based trust assessment	Trust is primarily learning-oriented and not integrated with WSN secure routing
[12]	Federated edge intelligence with trust-based security	Combines distributed learning, anomaly detection, and dynamic trust-based control	Limited emphasis on residual-energy balancing and network-lifetime-aware routing

[14]	Federated trust- and energy-aware routing	Integrates federated learning, trust, residual energy, and route selection	Designed for broader Fog–Cloud–IoT operation rather than a lightweight WSN-centred cross-layer framework

Another key challenge with the adoption of federated learning in sensor and edge networks is resource availability. In [11], federated learning is explored along with light-weight operation at the edge devices. Repeated exchange of model parameters can use up significant network resources, especially as far as communication reduction is concerned, computational capability and memory restrictions. This load can be lightened and collaborative learning become more feasible for limited devices by employing lightweight local processing and compressed communication. The results indicate that edge-level learning instead of regular transfer of the raw sensor observation to the cloud could be used in WSNs. However, the efficiency of communication is not sufficient to ensure sustainable operations of WSNs. Although nodes are able to compute, they might still not fit the above criterion due to battery depletion, link instability, abnormal sensing behavior, or malicious packet forwarding. Therefore, resource-aware learning needs to be facilitated with trust and network level reliability information.

In [12] the federated learning and dynamic trust-based security is further extended. This framework integrates anomaly detection at the edge, federated learning, and access decisions based on trust in a shared security design. The trust decision should be based on the current behaviour and operating context of a device rather than being based on a permanent trust or distrust of it. This is useful in WSN applications where sensor nodes can fail due to faulty operation or environmental changes, lack of energy resources, or malicious attacks. It also shows the feasibility of federated learning and trust management working together at the network edge. Its main goals, however, have to do with intrusion detection, privacy protection, and access control. The framework is not to optimize the selection of multi-hop trust-based routing, lifetime of the network, distribution of residual energy, and selection of energy-balanced routing. However, more integration is required for such an architecture to be able to fully support operation of long-duration WSNs.

In [13] authors take into consideration trustworthy and federated participation under resource constraints. The study aims to tackle the communication overhead of regular federated model exchanges and focuses on trusted engagement in multi-hierarchical edge settings. This paper supports the case against the automatic inclusion of all available nodes in each federated-learning round. Selective participation can minimize the amount of unnecessary communication and limit the contributions from unreliable sources to affect global knowledge. In WSNs, it is an important point since the low energy nodes can suffer from running out of battery. But the trustworthiness and communication efficiency of the model only partially represents node suitability. Certain important parameters of WSN nodes such as residual energy, packet-forwarding behavior, sensing consistency, link quality, and historical reliability, need to be considered as well. These indicators should affect the participation in the learning and routing in the network.

A more detailed study of federated learning, trust, energy consideration and routing is shared in [14]. The framework is based on collaborative learning for establishing trust and energy-aware routing in a Fog – Cloud – IoT system. Behavioural patterns, communication reliability are used to refine the values of trust; residual energy, latency, link stability are used for the route selection. This

is an important step forward as the process of evaluating trust is moving beyond network routing. The study shows that a combination of learning information with reliability information can be used to inform communication decisions and is feasible. But, it's a highly generalised Fog–Cloud–IoT architecture. In cases of highly constrained WSNs, a lightweight design with a limited cost of trust computation, model participation, routing control, and communications must be carefully weighed against limited node energy.

The other restriction found in [7]–[14] is the disorganized utilization of information created at various operation layers. Most of the energy-aware routing (EAR) algorithms rely on residual battery data only for routing and federated-learning mechanisms rely on node data or model characteristics to select participants. Likewise, trust-based systems can recognize malicious behavior without this information being used for route selection or energy management. This is because such stand-alone decisions can result in a different outcome. For instance, a node might have high residual energy, but might show poor forwarding behaviour, and another node might show excellent forwarding behaviour, but have a low level of energy to play a repeated game of federated training and forwarding. So, a sustainable WSN must be able to decide on a joint decision mechanism instead of individual optimisation of parameters.

In addition, there is a need for wider validation according to the literature. Most frameworks are tested with a single application, attack scenario or network environment. Different sensing distributions, communication loads, and node behaviours can be seen in sensor networks deployed in different domains such as healthcare, water monitoring, air-quality monitoring, climate monitoring, and infrastructure monitoring, among others, that are required to be sustainable. The considered framework for the deployment of the WSNs for SDG should be analyzed under a variety of sensing and security situations and not under a single one.

Overall, works related to federated routing [7]–[14] have set a solid ground for federated routing, trust-aware security, lightweight learning at the edge, and energy-efficient communication. However, an opportunity for research exists for a framework that is WSN-centred and where multi-factor behavioural trust, sensing consistency, residual energy, federated participation and secure route formation are interconnected components. This gap is addressed by the proposed work that proposes a green trustworthy, federated edge intelligence framework where common node reliability information has both learning-side and network-side applications. The proposed framework aims at supporting the reliable and long-term operation within heterogeneous SDG oriented WSN environments by integrating energy sustainability, trust evaluation, federated edge learning and secure communication in a unified decision process.

Key Contribution

The main contribution in this work is a unified green trustworthy, federated edge intelligence framework for secure and energy-sustainable operation of WSN. The proposed framework combines federated learning, trust evaluation, energy management and routing at a node level decision process, existing in an approach that regards them as separate processes. The Multi-factor trust is based on behavioural trustworthiness, sensing consistency, communication performance and energy state and it is supposed to affect the participation of federated actors and the secure selection of routes. Energy awareness has been added to avoid high energy nodes being used repeatedly, and to assist in the balanced operation of the network. Based on edge gateways, federated learning will be executed near the sensor nodes to reduce the amount of raw data transmission and reliance on the central processing center. Additionally, trust-based routing further reduces the number of nodes involved in

forwarding packets in the presence of unreliable or malicious nodes. The framework has been developed for heterogeneous applications, like healthcare, water monitoring, air-quality assessment, climate observation, and smart infrastructure, that can be used for SDGs. To validate, it uses security and sensing datasets that are integrated with the simulation of the WSN, thus enabling the evaluation of the learning performance, trust reliability, communication overhead, energy sustainability, packet delivery, latency, and network lifetime in a common experimental environment.

Inferences

Several important inferences can be drawn from the review of the existing studies [7] – [14]. On one hand, federated learning can help to decrease direct transfer of local data generated and facilitate distributed network intelligence, while on the other hand, communication overhead and the reliability of participants still are critical issues in constrained WSNs. Second, trust based routing provides protection against unreliable or malicious nodes, but this trust information is not typically used for federated participation as it is not re-used in other layers. Third, the mechanisms that make use of energy are effective in extending the life of the network, however, if only the energy is considered, high-energy nodes may be less reliable in terms of communication or abnormal behaviour. Thirdly, multi-factor trust evaluation is more reliable than single-parameter based assessment in evaluating the reliability of nodes when multiple factors are considered over time, including historical behavior, communication performance, sensing consistency, and energy status. Lastly, recent integrated approaches have shown the potential to integrate trust and federated learning with energy-aware routing, while lightweight WSN-centred coordination and validation in the context of heterogeneous SDG sensing environments are still relatively underdeveloped. Through these observation, it is concluded that there is a need for a cross layer framework, where the common node information plays a role in the learning participation, trust evaluation, energy balancing, and secure routing decision.

Conclusion

This work introduces the building blocks of a trustworthy edge intelligence framework in a green manner for secure and energy sustainable WSNs. The result of the literature review analysis reveals that federated learning, trust management, energy-aware operation and secure routing have individually proved to be potentially great solutions but their integration for the highly constrained WSN environment is still limited. The framework proposed in this paper aims to fill this shortcoming by incorporating multi-factor node trust, residual-energy awareness, federated edge participation and trust-guided secure routing into a single framework. The purpose of the framework is to decrease redundant communication, to not have any unreliable nodes, to balance the energy consumption of the network and to guarantee reliable long-term sensing. Security and sensing data will be used with the WSN simulation for validation, both in normal and adversarial scenarios. The evaluation of the performance will be based on network lifetime, packet delivery ratio, latency, communication overhead, trust accuracy, attack resilience and scalability. Proposed research thus paves a measurable path towards secure and sustainable deployment of WSNs in healthcare, environment, water resource management, climate monitoring and smart infrastructure applications.

REFERENCES

[1] T. M. Mengistu, T. Kim, and J.-W. Lin, “A survey on heterogeneity taxonomy, security and privacy preservation in the integration of IoT, wireless sensor networks and federated learning,” *Sensors*, vol. 24, no. 3, Art. no. 968, 2024, doi: 10.3390/s24030968.
[2] N. Taheri Javan, E. Zakizadeh Gharyeali, and S. Mostafavi, “An energy-efficient decentralized federated learning framework for mobile-IoT networks,” *Computer Networks*, vol. 263, Art. no. 111233, 2025, doi: 10.1016/j.comnet.2025.111233.
[3] M. Rahmati, “Energy-aware federated learning for secure edge computing in 5G-enabled IoT networks,” *Journal of Electrical Systems and Information Technology*, vol. 12, Art. no. 13, 2025, doi: 10.1186/s43067-025-00203-2.
[4] N. Manogaran, M. T. M. Raphael, R. Raja, A. K. Jayakumar, M. Nandagopal, B. Balusamy, and G. Ghinea, “Developing a novel adaptive double deep Q-learning-based routing strategy for IoT-based wireless sensor network with federated learning,” *Sensors*, vol. 25, no. 10, Art. no. 3084, 2025, doi: 10.3390/s25103084.
[5] M. J. C. S. Reis, “Trust-aware and energy-efficient federated learning for secure sensor networks at the edge,” *Sensors*, vol. 26, no. 8, Art. no. 2307, 2026, doi: 10.3390/s26082307.
[6] M. J. C. S. Reis, C. Serôdio, and F. Branco, “Trust- and energy-aware federated learning for wireless sensor networks: A lightweight orchestration framework for heterogeneous IoT environments,” *Electronics*, vol. 15, no. 11, Art. no. 2469, 2026, doi: 10.3390/electronics15112469.
[7] S. S. Suresh, V. Prabhu, V. Parthasarathy, G. Senthilkumar, and V. Gundu, “Intelligent data routing strategy based on federated deep reinforcement learning for IoT-enabled wireless sensor networks,” *Measurement: Sensors*, vol. 31, Art. no. 101012, 2024, doi: 10.1016/j.measen.2023.101012.
[8] B. S. V. Prasad and H. R. Roopashree, “Energy aware and secure routing for hierarchical cluster through trust evaluation,” *Measurement: Sensors*, vol. 33, Art. no. 101132, 2024, doi: 10.1016/j.measen.2024.101132.
[9] A. Belenguer, J. A. Pascual, and J. Navaridas, “A review of federated learning applications in intrusion detection systems,” *Computer Networks*, vol. 258, Art. no. 111023, 2025, doi: 10.1016/j.comnet.2024.111023.
[10] M. Cheng, W. Chen, W. Fang, Z. Wang, T. Xu, J. Liu, and V. C. M. Leung, “MFTE: Multifactor and fuzzy trust evaluation for federated learning in mobile edge computing,” *Computer Networks*, vol. 265, Art. no. 111340, 2025, doi: 10.1016/j.comnet.2025.111340.
[11] M. N. A. Ramadan, M. A. H. Ali, S. Y. Khoo, and M. Alkhedher, “Federated learning and TinyML on IoT edge devices: Challenges, advances, and future directions,” *ICT Express*, vol. 11, no. 4, pp. 754–768, 2025, doi: 10.1016/j.icte.2025.06.008.
[12] V. Padmavathi and R. Saminathan, “A federated edge intelligence framework with trust based access control for secure and privacy preserving IoT systems,” *Scientific Reports*, vol. 15, Art. no. 35832, 2025, doi: 10.1038/s41598-025-19712-1.
[13] A. Tariq, F. Sallabi, M. A. Serhani, E. S. Barka, T. Qayyum, I. Din, and I. Syed, “AI-driven lightweight and trustworthy federated learning framework for decision-making in resource-constrained Edge-IoT,” *IEEE Transactions on Consumer Electronics*, vol. 71, no. 4, pp. 12166–12180, 2025, doi: 10.1109/TCE.2025.3628207.
[14] F. Wang and K. Wang, “Federated learning-based trust and energy-aware routing in Fog–Cloud computing environments for the Internet of Things,” *Scientific Reports*, vol. 16, Art. no. 2244, 2026, doi: 10.1038/s41598-025-32010-0.