Engineering Applications of Artificial Intelligence 162 (2025) 112783

Contents lists available at ScienceDirect

Engineering Applications of Artificial Intelligence

journal homepage: www.elsevier.com/locate/engappai

Neuro inspired deep learning based secure and energy efficient routing with autonomous intrusion prevention in wireless sensor networks

A. Babu Karuppiah [a,*], Vijayalakshmi Nanjappan [b], R. RajaRaja [c], S. Vishnu Priyan [d]

[a] Department of Electronics and Communication Engineering, Sri Eshwar College of Engineering, Coimbatore, Tamilnadu, India
[b] Department of Computer Science and Engineering, Alliance School of Advanced Computing, Alliance University, Anekal, Bangalore, India
[c] Department of Electronics and Communication Engineering, PSG Institute of Technology and Applied Research, Coimbatore, India
[d] Department of Biomedical Engineering, Kings Engineering College, Chennai, India

ARTICLE INFO

Keywords:
Neuro-inspired deep learning
Spiking neural networks
Intrusion prevention
Energy-efficient routing
Wireless sensor networks
Trust-aware routing

ABSTRACT

Wireless Sensor Networks (WSNs) are crucial in mission-driven domains such as environmental monitoring, industrial control, and military surveillance. However, their open communication medium, constrained resources, and unattended deployment make them prone to routing-layer attacks. Existing security frameworks mostly rely on reactive intrusion detection systems or conventional deep learning models, which incur high computational overhead and fail to adapt effectively under dynamic network conditions. To overcome these limitations, this study proposes a Neuro-Inspired Deep Learning Framework based on Spiking Neural Networks (SNNs) for autonomous intrusion prevention and energy-aware routing. The proposed model leverages latency-based spike encoding of key behavioral metrics (e.g., residual energy, latency, routing frequency, and packet delivery ratio) and utilizes a Leaky Integrate-and-Fire neuron architecture for proactive vulnerability prediction. Implementation using the Network Simulator-3 (NS-3) simulation tool and validation on the Wireless Sensor Network Dataset (WSN-DS), the framework achieves 99.72 % prediction accuracy, 99.98 % precision, 99.33 % recall, and 99.12 % F1-score, outperforming existing studies in attack detection rate. The proposed Secure Energy-Aware Routing Metric (SEARM) protocol achieves an average energy consumption of 0.32 J and a packet delivery ratio of 99.1 % while maintaining performance across varying network sizes (30–150 nodes) and attack intensities (up to 50 %). Additionally, the model features a self-healing mechanism that reintegrates previously blocked nodes based on dynamic trust recovery. This research establishes a proactive, low-power, and intelligent security paradigm for WSNs and sets the foundation for future innovations in biologically inspired and scalable network protection strategies.

1. Introduction

WSNs have become a fundamental technology for pervasive and distributed sensing in important areas, including infrastructure monitoring, environmental sensing, military observation, and industrial process automation. WSNs jointly carry out data sensing, forwarding, and transmission using multi-hop communication making use of spatially distributed, low-power, and limited-resource sensor nodes. Yet, because of their open wireless medium, limited power, and computational capabilities, WSNs are extremely vulnerable to a wide range of security threats, especially routing-layer attacks like sinkhole, wormhole, and selective forwarding (Kumari and Tyagi, 2024), (Daousis et al., 2024). Providing such limited environments with secure and energy-efficient routing is an intricate and crucial research challenge that is essential to the integrity of data and network longevity. Traditional intrusion detection methods often use extensive training, static rules specifications, and reactive mitigation strategies, each of which introduces significant latency and energy costs (Khatami et al., 2025), (Almarri et al., 2025). These factors create challenges for traditional intrusion detection methods to be effective as real-time intrusion prevention methods for WSNs. As such, there is a critical need for low-weight, intelligent, and adaptive security methods to proactively attack routing-based attacks, before meaningful degradation occurs within the network (Ahmed et al., 2024), (Vishwas and Ramesh, 2025).

* Corresponding author.
E-mail addresses: babkarofficial@gmail.com (A.B. Karuppiah), viji365@gmail.com (V. Nanjappan), birneraja@gmail.com (R. RajaRaja), rsv.priyan@gmail.com (S.V. Priyan).

https://doi.org/10.1016/j.engappai.2025.112783
Received 2 June 2025; Received in revised form 3 October 2025; Accepted 11 October 2025
Available online 18 October 2025

Previous research in WSN security has focused primarily on reactive Intrusion Detection Systems (IDS), anomaly detection using conventional machine learning-based classifiers, and trust-aware routing protocols (UmaRani et al., 2025), (Ramalingam et al., 2024). Even though these techniques improve the recognition accuracy after an attack, they all rely on a post-detection, defensive mechanism; once malicious activity has occurred, any action taken to assess the situation makes the WSN increasingly vulnerable and less effective (Lakshminarayanan et al., 2024), (Wu et al., 2025). Additionally, deep learning models such as CNN or LSTM networks, although able to extract spatial and temporal features, they are computationally expensive and generally unsuitable for deployment on highly constrained sensor nodes (Delwar et al., 2024), (Yesodha et al., 2024), (Robacky Mbongo et al., 2025), (Kalodanis et al., 2025). To overcome these constraints, this study presents a neuro-inspired deep learning architecture based on SNNs for autonomous intrusion detection and energy-efficient routing in WSNs. Compared to conventional IDS design, the proposed technique exploits the event-driven processing and temporal coding features of biological neurons to anticipate and block malicious routing activity before it affects the network. This architecture combines unsupervised spatiotemporal learning and biologically inspired inference to enable real-time energy-efficient and smart routing choices. By shifting from reactive protection towards proactive defense, the system improves network security and operational life in mission-critical and resource-limited WSN settings.

1.1. Research motivation

The growing deployment of WSNs in mission-critical areas requires strong security measures that support operations under constrained resources. The existing intrusion detection frameworks make use of lots of energy while working on a reaction-based model, but have little success in preventing attacks before network breaches. A lightweight, smart system with the capability to autonomously avoid intrusions without recourse to detection is needed. Neuro-inspired architectures, especially SNN, are a promising means for proactive threat mitigation in real-time WSN scenarios.

1.2. Significance of the study

This study presents a neuro-inspired autonomous intrusion prevention framework that supports real-time threat anticipation and secure routing with low computational overhead. Through the use of SNN, the framework improves temporal perception and decision latency while being compatible with WSN hardware constraints. The method minimizes packet loss, saves energy, and avoids network performance degradation due to routing-based attacks. It represents a shift from reactive to preventive security measures in resource-limited IoT systems.

1.3. Problem statement

WSNs play a central role in numerous applications, but securing them from malicious attacks with energy efficiency is still a challenging issue. Existing studies like Aruchamy (Aruchamy et al., 2023) suggest AI-driven IDS and secure routing protocols, showing high detection rates and energy conservation. However, they do not support adaptability to changing network situations and prevention of attacks in advance before their occurrence. In Wang, Liu, and Jiang (Wang et al., 2024), even though trust-based detection mechanisms have adaptive reactions to internal attacks, the trust computation creates latency and complexity, which degrades real-time performance under limited environments. In addition, Jeevanantham and Rebekka (2022) suggested an Energy-Aware Neuro-Fuzzy Routing model that also increases QoS by saving energy and increasing the network lifetime. However, the model mainly works for static systems and lacks built-in security attributes or dynamic attack adaptability. These constraints identify the necessity of a new framework that integrates real-time autonomous intrusion prevention, neuro-inspired deep learning models, and energy-efficient routing to deliver both proactive security and effective performance in dynamic and large-scale WSN environments.

1.4. Recent innovations and challenges

Recent advances have explored deep learning models like CNNs, RNNs, and LSTMs for WSN security, providing better intrusion detection accuracy (Ra' et al., 2025), (Haque and Soliman, 2025). However, these models are still not suitable for use on energy-limited sensor nodes because they have high computational complexity and slow response rates. The main challenges are real-time execution, energy efficiency, and the absence of proactive routing defense techniques. In addition, the incorporation of temporal cognition and neuro-inspired adaptability is unexplored in existing intrusion prevention systems.

1.5. Key contributions of the study

- Spiking Neural Network-Based Intrusion Prevention: Presents a latency-aware SNN model for pre-emptive intrusion detection in WSNs based on temporal spike encoding of real-time behavioral indicators of sensor nodes to identify routing-layer attacks.
- Secure Energy-Aware Routing Metric (SEARM): Presents an innovative routing metric that combines dynamic trust evaluation with link quality estimation to improve secure data transmission while minimizing energy expenditure.
- Autonomous Self-Healing Framework: Forms a feedback-based system that enables the re-admission and reintegration of stranded nodes after normalizing their behavior, leading to long-term robustness and prolonged network resilience.
- Enhanced Security and Network Performance in Adversarial Scenarios: Exhibits enhanced performance in threat detection accuracy, packet delivery ratio, and energy efficiency under diverse simulated attack scenarios, supporting its efficacy for large-scale WSN deployment.

1.6. Rest of section of the study

- Section 2: Related Works – Overview of existing reactive WSN security approaches and their gaps.
- Section 3: Methodology – Proposed SNN-based proactive intrusion prevention and routing framework.
- Section 4: Results and Analysis – Comparative evaluation showing enhanced security and efficiency.
- Section 5: Conclusion and Future Works – Summary of contributions with future directions for scalability and adaptability.

2. Related Works

2.1. AI-based intrusion detection and secure routing

The traditional secure routing protocols have been enhanced with schemes like Enhanced DMR by Alnawafa and Allaymoun (2025), which added sleep-aided cluster disabling to save energy and prevent redundant transmissions. Their Enhanced Dynamic Multi-Hop Routing (EDMR) protocol was better than DMR, EMDHT-LEACH, and LEACH in terms of energy use and throughput, but failed with highly dynamic topologies or high frequency data generation. These non-AI approaches are still restricted to dealing with unpredictable intrusion patterns, leading to a switch towards AI-based secure routing. The model proposed by Aruchamy (Aruchamy et al., 2023) is an AI-based Energy-aware Intrusion Detection and Secure Routing model that combines intrusion detection, a decision strategy based on game theory, and an energy-aware AODV algorithm. The model achieved a 95 % detection

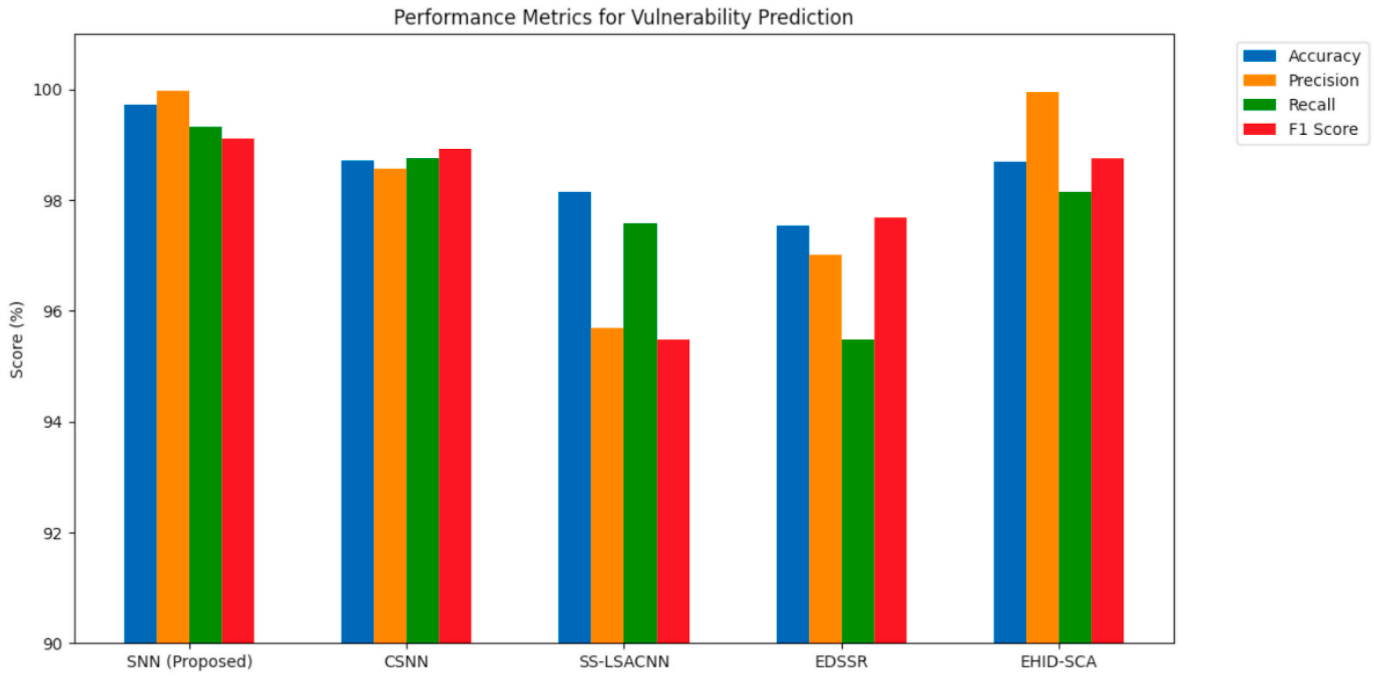

Fig. 19. Vulnerability prediction performance comparison.

Table 10
Performance comparison.

Model	Attack Detection Rate (%)
Proposed Approach	98.5
EDSSR (Yang et al., 2024)	97.5
EAT-MR (Yin et al., 2022)	94.8
EA-AODV (Aruchamy et al., 2023)	95.1
RPL-AOVD (Kipongo et al., 2023)	97.2

detection performance comparison is given in Fig. 20.

4.10. Discussion

The proposed neuro-inspired framework transforms WSN security through the combination of a biologically realistic SNN with trust-aware, energy-efficient routing to support proactive and real-time intrusion blocking. In contrast to conventional schemes that are largely based on reactive detection mechanisms, this study employs temporal coding and spike-based learning to predict vulnerabilities as a function of deviations from normal behavioral patterns. Through the use of behavioral metrics like residual energy, routing update interval, and packet delivery ratio, the SNN can identify anomalies in advance before they become active threats. The Trust Evaluation System also enhances the process by periodically updating a node's credibility to ensure that nodes with high reliability are the ones involved in making routing decisions. These two mechanisms, when combined, enable direct node exclusion without the generation of alerts or central monitoring, lowering response latency and energy overhead tremendously.

Experimental results validate the robustness of the framework in various performance aspects. The proposed approach has a vulnerability prediction accuracy of 99.72 %, surpassing all the compared baselines. Its routing protocol, SEARM, strikes a balance between energy, trust, and link quality, resulting in the minimum energy consumption (0.32 J) while having a packet delivery ratio of 99.1 %. The model responds to changing network states and recovers nodes after an anomaly through a self-healing mechanism, which is imperative for long-term network robustness. Additionally, it exhibits robust scalability and attack detection efficacy even as the threat level and node count increase. Although this work emphasized Wireless Sensor Networks, the neuro-inspired, trust-aware architecture is not limited to any particular domain. Behavioral metric spike-based encoding, active vulnerability prediction, and self-healing trust mechanism are generic attributes applicable to any cyber-physical system. For example, energy usage and packet delivery ratio in smart grids can be replaced by load stability and false-data injection resilience for predictive and low-latency intrusion detection. Similarly, latency and routing frequency can be reconfigured in vehicular ad hoc networks for safety-critical message broadcasting and mobility-imposed topology dynamics. As only the domain-specific communication protocols and performance metrics must be accommodated, the framework retains its energy-efficient, distributed, and predictive security benefits along with its scalability to various IoT-driven infrastructures. The proactive design of the system, in conjunction with its distributed nature, presents a high-performance defense mechanism without sacrificing energy or computational constraints. This makes the model an end-to-end solution for actual WSN deployment in mission-critical and resource-constrained environments.

5. Conclusion and future work

This study has introduced a novel neuro-inspired deep learning framework for energy-efficient and secure routing in WSNs that combines SNNs for predictive vulnerability analysis and an autonomous intrusion prevention system. Through deviations from the conventional reactive paradigms, the proposed method outperforms in both energy efficiency and security improvement aspects. Empirical verifications ensure better performance in vulnerability forecasting (accuracy: 99.72 %), energy saving (0.32 J/node), and packet delivery rate (99.1 %) against state-of-the-art approaches such as EDSSR and EA-AODV. The approach also demonstrates strength in diverse attack levels and network sizes, establishing it as a prime candidate for dynamic, real-time deployment settings. This study includes a self-adaptive feedback module that facilitates effortless reintegration of nodes, thereby ensuring long-term network sustainability and performance.

Even with these improvements, the system does face some limitations. Firstly, the higher computational load during intense attack situations results in perceptible energy spikes that could impact battery-constrained nodes. Secondly, the system so far utilizes optimized pre-

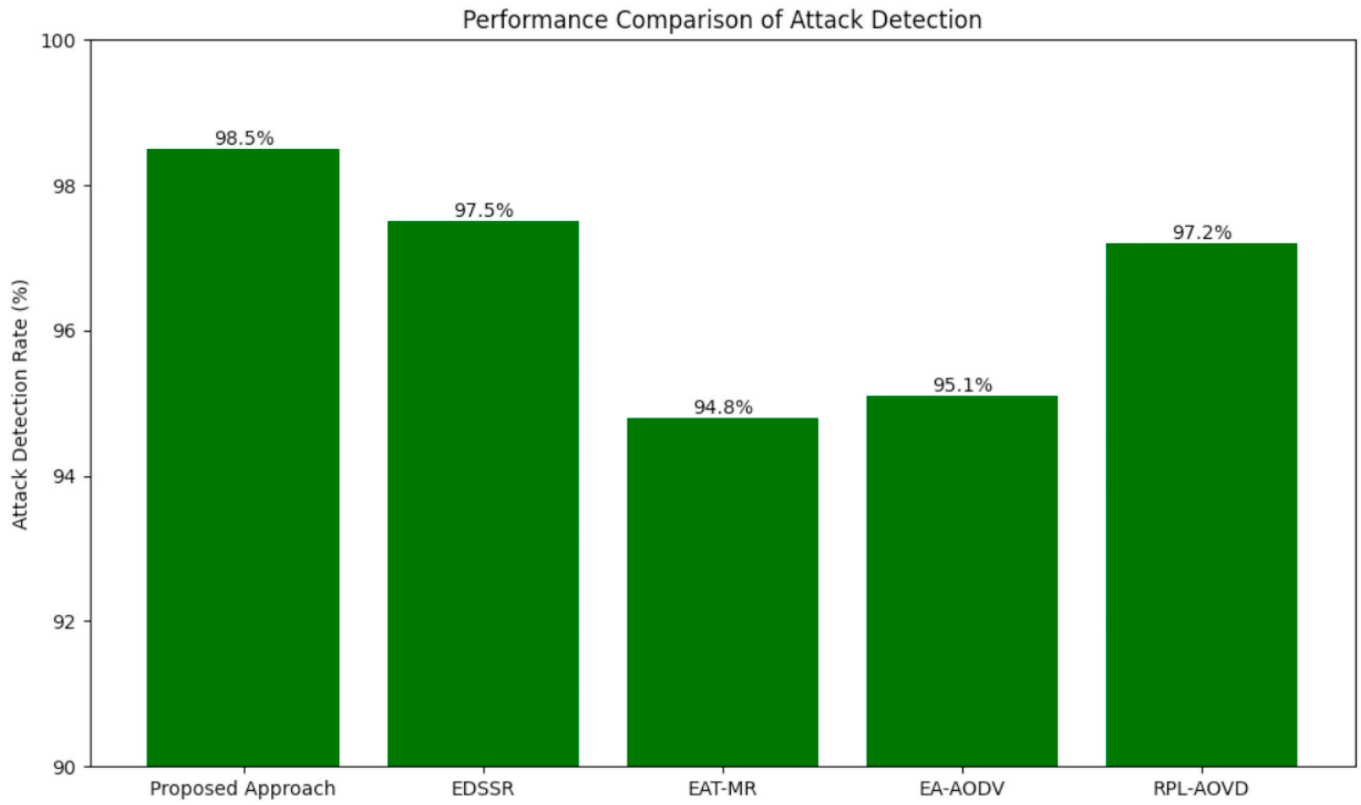

Fig. 20. Attack detection comparison across models.

determined behavior features from the WSN-DS dataset, which restricts its applicability to diverse WSN deployments with varying sensor dynamics or environmental conditions. Addressing these issues involves more adaptive feature extraction and energy consumption under extreme danger levels. The future work can investigate in-sensor SNN deployment with low-weight hardware-based implementation for real-time inference and low energy consumption. The implementation path can include the transfer of SNN models onto microcontrollers or neuromorphic chips to assess their viability under memory as well as computational limitations. Furthermore, incorporating model adaptation for dynamic feature evolution and adversarial attack patterns makes the model more realistic. Compatibility with federated learning systems or blockchain-based identity management architectures can yield improved scalability and decentralized trust mechanisms. These areas of research hold the potential to develop next-generation secure and sustainable WSN infrastructures; hence, this study is not an end goal but a milestone towards comprehensive investigation in proactive and intelligent intrusion prevention systems.

CRediT authorship contribution statement

A. Babu Karuppiah: Writing – original draft, Software, Methodology, Conceptualization. **Vijayalakshmi Nanjappan:** Supervision, Project administration, Investigation. **R. RajaRaja:** Validation, Resources, Formal analysis, Data curation. **S. Vishnu Priyan:** Writing – review & editing, Visualization, Funding acquisition.

Consent to publish

All authors gave permission to consent to publish.

Funding

No fundings.

Declaration of competing interest

The authors declare no conflicts of interest(s).

Data availability

The Datasets used and/or analysed during the current study available from the corresponding author on reasonable request.

References

Ahmed, K.M., Shams, R., Khan, F.H., Luque-Nieto, M.-A., 2024. Securing underwater wireless sensor networks: a review of attacks and mitigation techniques. IEEE Access.

Almarri, S., Al Safwan, H., Al Qisoom, S., Gdaim, S., Zitouni, A., 2025. Optimized wireless sensor network architecture for AI-Based wildfire detection in remote areas. Fire 8 (7), 245.

Alnawafa, E., Allaymoun, M., 2025. EDMR: an enhanced dynamic multi-hop routing protocol with a novel sleeping mechanism for wireless sensor networks. Sensors 25 (14), 4510.

Aruchamy, P., Gnanaselvi, S., Sowndarya, D., Naveenkumar, P., 2023. An artificial intelligence approach for energy-aware intrusion detection and secure routing in internet of things-enabled wireless sensor networks. Concurrency Comput. Pract. Ex. 35 (23), e7818.

Bassam Kasasbeh. WSN-DS [Online]. Available: https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds. (Accessed 21 April 2025).

Chavan, P., et al., 2024. Enhanced hybrid intrusion detection system with attention mechanism using deep learning. SN Computer Science 5 (5), 534.

Daousis, S., Peladarinos, N., Cheimaras, V., Papageorgas, P., Piromalis, D.D., Munteanu, R.A., 2024. Overview of protocols and standards for wireless sensor networks in critical infrastructures. Future Internet 16 (1), 33.

Delwar, T.S., et al., 2024. The intersection of machine learning and wireless sensor network security for cyber-attack detection: a detailed analysis. Sensors 24 (19), 6377.

Dogra, R., Rani, S., Kavita, Shafi, J., Kim, S., Ijaz, M.F., 2022. ESEERP: enhanced smart energy efficient routing protocol for internet of things in wireless sensor nodes. Sensors 22 (16), 6109.

Gangwani, P., Perez-Pons, A., Upadhyay, H., 2024. Evaluating trust management frameworks for wireless sensor networks. Sensors 24 (9), 2852.

Haque, A., Soliman, H., 2025. A transformer-based autoencoder with isolation forest and XGBoost for malfunction and intrusion detection in wireless sensor networks for forest fire prediction. Future Internet 17 (4), 164.
Jeevanantham, S., Rebekka, B., 2022. Energy-aware neuro-fuzzy routing model for WSN based-IoT. Telecommun. Syst. 81 (3), 441–459.
Kalodanis, K., Papapavlou, C., Feretzakis, G., 2025. Enhancing security in 5G and future 6G networks: machine learning approaches for adaptive intrusion detection and prevention. Future Internet 17 (7), 312.
Khatami, S.S., Shoeibi, M., Salehi, R., Kaveh, M., 2025. Energy-efficient and secure double RIS-aided wireless sensor networks: a QoS-aware fuzzy deep reinforcement learning approach. J. Sens. Actuator Netw. 14 (1), 18.
Kipongo, J., Swart, T.G., Esenogho, E., 2023. Design and implementation of intrusion detection systems using RPL and AOVD protocols-based wireless sensor networks. International Journal of Electronics and Telecommunications 309–318.
Krishnan, R., et al., 2022. An intrusion detection and prevention protocol for internet of things based wireless sensor networks. Wirel. Pers. Commun. 124 (4), 3461–3483.
Kumari, S., Tyagi, A.K., 2024. Wireless sensor networks: an introduction. Digital Twin and Blockchain for Smart Cities, pp. 495–528.
Lakshminarayanan, R., Dhanasekaran, S., Vinod Kumar, R., Selvaraj, A., 2024. Optimizing federated learning approaches with hybrid convolutional neural networks-bidirectional encoder representations from transformers for precise estimation of average localization errors in wireless sensor networks. Int. J. Commun. Syst. 37 (13), e5822.
Lin, Y., Xu, X., Xu, H., 2024. A revolutionary approach to use convolutional spiking neural networks for robust intrusion detection. Clust. Comput. 27 (9), 13333–13352.
Nait Abbou, A., Manner, J., 2023. ETXRE: energy and delay efficient routing metric for RPL protocol and wireless sensor networks. IET Wirel. Sens. Syst. 13 (6), 235–246.
Narayana, P., et al., 2024. Energy-efficient and secure routing strategy for opportunistic data transmission in WSNs. Journal of Cyber Security Technology 1–36.
Newton, P., Felix, A., 2022. ETX-aware energy-efficient algorithm to reduce packet retransmissions in the internet of things. Indian J. Sci. Technol. 15 (1), 28–43.
Ramalingam, S., Dhanasekaran, S., Sinnasamy, S.S., Salau, A.O., Alagarsamy, M., 2024. Performance enhancement of efficient clustering and routing protocol for wireless sensor networks using improved elephant herd optimization algorithm. Wirel. Netw. 30 (3), 1773–1789.
Ra', M., Heilat, L., Qudah, W., Alhatamleh, S., Al-Khateeb, A., 2025. A novel improved deep learning model based on Bi-LSTM algorithm for intrusion detection in WSN. Netw. Heterogeneous Media 20 (2), 532–565.
Robacky Mbongo, K.H., et al., 2025. Conv1D-GRU-Self attention: an efficient deep learning framework for detecting intrusions in wireless sensor networks. Future Internet 17 (7), 301.
Sarath Kumar, R., Sampath, P., Ramkumar, M., 2023. Enhanced Elman Spike neural network fostered intrusion detection framework for securing wireless sensor network. Peer-to-Peer Networking and Applications 16 (4), 1819–1833.
Sharma, V., Beniwal, R., Kumar, V., 2024. Multi-level trust-based secure and optimal IoT-WSN routing for environmental monitoring applications. J. Supercomput. 80 (8), 11338–11381.
Siamantas, G., Rountos, D., Kandris, D., 2025. Energy saving in wireless sensor networks via LEACH-Based, energy-efficient routing protocols. J. Low Power Electron. Appl. 15 (2), 19.
Siddiq, A., Ghazwani, Y.J., 2024. Hybrid optimized deep neural network based intrusion node detection and modified energy efficient centralized clustering routing protocol for wireless sensor network. IEEE Trans. Consum. Electron.
Singh, V.K., Sivashankar, D., Kundan, K., Kumari, S., 2024. An efficient intrusion detection and prevention system for DDOS attack in WSN using SS-LSACNN and TCSLR. Journal of Cyber Security and Mobility 135–160.
Soni, A., Bhalerao, S., Maddineni, T., Ali, S.M., Rajini, J., Khare, S., 2024. Optimized deep learning-based intrusion detection and secure, energy-efficient routing in wireless sensor networks. In: 2024 IEEE 4th International Conference on ICT in Business Industry & Government (ICTBIG). IEEE, pp. 1–6.
Tewari, P., Tripathi, S., 2023. An energy efficient routing scheme in internet of things enabled WSN: neuro-fuzzy approach. J. Supercomput. 79 (10), 11134–11158.
UmaRani, C., Ramalingam, S., Dhanasekaran, S., Baskaran, K., 2025. An hybrid machine learning and improved social spider optimization based clustering and routing protocol for wireless sensor network. Wirel. Netw. 31 (2), 1885–1910.
Vikas, C. Wahi, Sagar, B.B., Manjul, M., 2025. Trusted energy-aware hierarchical routing (TEAHR) for wireless sensor networks. Sensors 25 (8), 2519.
Vishwas, H., Ramesh, T., 2025. Recent trends in localization, routing, and security for wireless sensor networks. IEEE Access.
Wang, C., Liu, G., Jiang, T., 2024. Malicious Node Detection in Wireless Weak-Link Sensor Networks Using Dynamic Trust Management. IEEE Transactions on Mobile Computing.
Wu, N.-I., Feng, T.-H., Hwang, M.-S., 2025. A fuzzy-based relay security algorithm for wireless sensor networks. Sensors 25 (14), 4422.
Xie, Y., Chen, H., 2024. A novel method for effective intrusion detection based on convolutional speaking neural networks. Journal of King Saud University-Computer and Information Sciences 36 (2), 101975.
Yang, R., et al., 2024. EDSSR: a secure and power-aware opportunistic routing scheme for WSNs. Sci. Rep. 14 (1), 28625.
Yesodha, K., Krishnamurthy, M., Thangaramya, K., Kannan, A., 2024. Elliptic curve encryption-based energy-efficient secured ACO routing protocol for wireless sensor networks. J. Supercomput. 80 (13), 18866–18899.
Yin, H., Yang, H., Shahmoradi, S., 2022. EATMR: an energy-aware trust algorithm based the AODV protocol and multi-path routing approach in wireless sensor networks. Telecommun. Syst. 81 (1), 1–19.