

LIGHTWEIGHT DEEP LEARNING IDS FOR ENERGY-CONSTRAINED WIRELESS SENSOR NETWORKS

D. Malarvizhi¹, M. Varshikasree², G. Kavi Bharathi³

¹ Assistant Professor, Department of Software System and AIML, Sri Krishna Arts and Science College, Coimbatore, Tamilnadu, India.

^{2,3} Student, Department of Commerce IT and E-Commerce, Sri Krishna Arts and Science College, Coimbatore, Tamilnadu, India.

Article Info

Article History:

Published: 06 Sept 2026

Publication Issue:

Volume 3, Issue 9
September-2026

Page Number:

92-98

Corresponding Author:

D. Malarvizhi

Abstract:

Wireless Sensor Networks (WSNs) are widely used in applications such as environmental monitoring, industrial automation, healthcare, smart cities, and agriculture. These networks consist of small sensor nodes with limited energy, memory, and computational capacity. Due to these limitations and the use of open wireless communication channels, WSNs are vulnerable to security attacks such as Denial of Service (DoS), sinkhole, blackhole, spoofing, and selective forwarding attacks [1], [15]. Traditional Intrusion Detection Systems (IDS) often require high computational power and communication resources, making them unsuitable for energy-constrained sensor networks [2]. Lightweight Deep Learning-based IDS offers a practical solution by using compact neural network models and energy-efficient detection techniques. The proposed approach uses a hierarchical detection strategy in which sensor nodes perform initial anomaly detection using ultra-lightweight models, while cluster heads perform more detailed classification. Techniques such as model pruning, quantization, feature selection, and knowledge distillation help reduce memory usage and energy consumption [4], [6], [16]. The system aims to achieve high intrusion detection accuracy while minimizing energy consumption and communication overhead, making intelligent security more suitable for resource-constrained WSN environments [8], [18].

Keywords: Wireless Sensor Networks, Intrusion Detection System, Lightweight Deep Learning, Energy Efficiency, TinyML, Anomaly Detection, Model Compression, CNN, LSTM, Network Security

1.INTRODUCTION

Wireless Sensor Networks are groups of sensor devices that gather, handle and send data using wireless links. Wireless Sensor Networks are widely used in modern settings that need constant monitoring [1]. However sensor nodes normally run on batteries. Have small memory, weak processing power and low communication capacity. This makes Wireless Sensor Networks face security problems. Attackers can take advantage of sensor nodes or wireless links to break Wireless Sensor Networks operations change data or shorten the life of Wireless Sensor Networks [15]. Intrusion Detection Systems watch network activity and spot strange actions.. Usual Intrusion Detection Systems methods may rely on central monitoring or heavy machine learning models that use a lot of energy and add communication load [2]. Deep learning can find patterns and spot new attacks. Yet older deep learning models are often too big to run on sensor nodes directly [13] [19]. Therefore small deep learning methods are needed to make intrusion detection work, in Wireless Sensor Networks while keeping security, detection accuracy and use of resources in balance [9] [18].

2.FUNDAMENTAL CONCEPTS OF WSN AND IDS

A Wireless Sensor Network consists of a number of small sensor nodes that communicate wirelessly to collect, process and transmit information from the surrounding environment. Each sensor node generally contains sensing components, a processor, memory, a wireless communication module and a power source. WSNs are widely used in monitoring, healthcare, industrial automation and smart systems but they operate under limitations related to battery energy, processing capability, memory, bandwidth and wireless communication reliability. An Intrusion Detection System monitors network traffic and node behavior to identify activities. Anomaly-based IDS learns network behavior and identifies deviations as possible attacks whereas signature-based IDS identifies attacks by comparing activities with known attack patterns.

Deep learning models can automatically learn patterns from network data with CNNs supporting feature extraction and LSTM-based models analyzing temporal patterns in network traffic. However standard deep learning models require memory and computational power making lightweight techniques necessary for deployment, in resource-constrained environments.

3.PROPOSED METHODOLOGY

The proposed Lightweight Deep Learning IDS follows an energy-aware methodology that fits the limits of Wireless Sensor Networks. The network is split into three levels: sensor nodes, cluster heads and a base station. The sensor nodes sense data. Do a first check for intrusions. The cluster heads gather alerts. Run a thorough attack classification. The base station performs analysis manages the model and monitors security. Data from the network can be gathered when things run normally or when attacks happen. It is processed using features such as packet inter-arrival time, packet transmission rate, neighbor consistency, RSSI variations, retransmission counts and routing anomalies. The models are trained offline on datasets that contain both malicious traffic. After training the models are compressed before they are put onto sensor nodes and cluster heads [12]. The base station can update the models from time to time when new attack patterns appear so the Lightweight Deep Learning IDS stays strong, against threats [11].

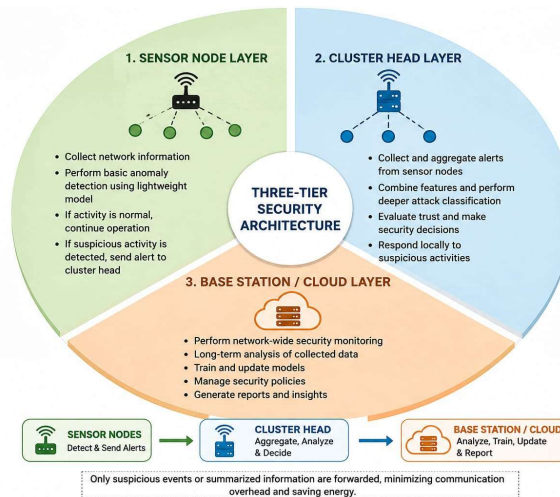
4.LIGHTWEIGHT DEEP LEARNING TECHNIQUES

Lightweight Deep Learning is, about building models that work well for intrusion detection but use less computational power, memory and energy. Compact CNNs are used to extract features. Lightweight LSTM or GRU models help analyze time-based network patterns. Autoencoders support detecting behavior in data. When a few features are available small fully connected networks can still be effective [13] [19].

Model compression plays a role. Pruning removes weights and neurons. Quantization reduces the precision of numbers, which cuts down on memory use and processing needs. Knowledge distillation lets a smaller model learn the parts of a larger model [4] [6] [16].

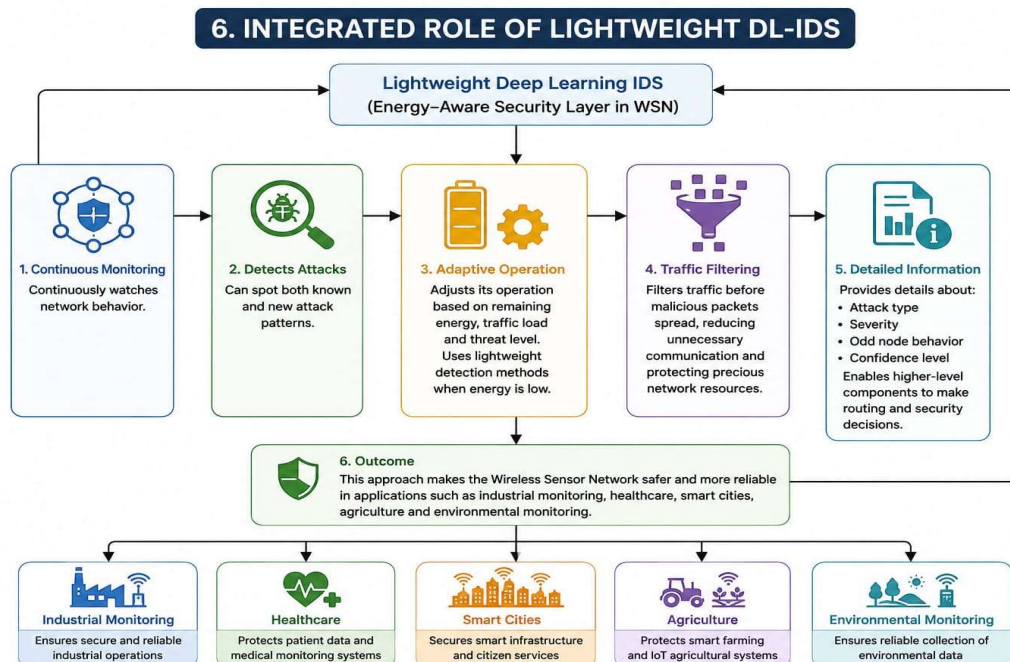
Energy-aware feature selection helps by choosing the most useful data from network traffic. This reduces processing. Local feature. Anomaly screening lower the amount of data sent over the network. In sensor networks sending data uses a lot of energy so reducing communication makes the system more efficient [9] [18].

5.SYSTEM ARCHITECTURE



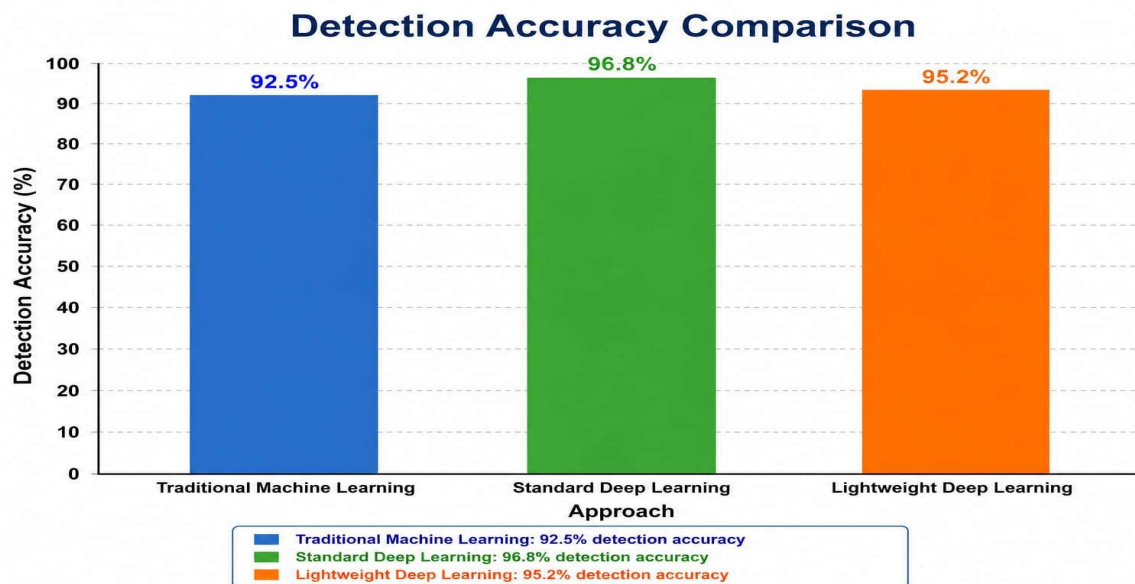
The system that is being suggested uses a three-tier structure that is arranged in a hierarchy to spread out security tasks across the network. In the tier sensor nodes gather information about the network and do basic detection of anything unusual using a model that is extremely light in terms of resources. When the activity is normal the node keeps working as usual. When something unusual is found the node sends a report to the cluster head. In the tier the cluster heads take care of combining alerts mixing features doing a deeper classification of attacks making decisions based on trust and responding locally to anything that seems suspicious. In the tier the base station or the cloud layer deals with checking the whole network for security analyzing things over a long period training models and updating them changing security policies and providing reports. Because of this tasks that need a lot of computing power are not handled by the battery-powered sensor nodes. Only the events that are considered suspicious or information that has been summarized move, from the sensor nodes to the cluster heads and then to the base station. This helps reduce the amount of communication needed and makes the system work in a way that uses energy efficiently [9] [11].

6. INTEGRATED ROLE OF LIGHTWEIGHT DL-IDS



Lightweight Deep Learning IDS serves as an energy-aware security layer inside the Wireless Sensor Network. Lightweight Deep Learning IDS continuously watches network behavior. Can spot both known and new attack patterns [2] [13]. Lightweight Deep Learning IDS can change its operation based on remaining energy, traffic load and threat level which lets it use detection methods when energy is low. Lightweight Deep Learning IDS also filters traffic before malicious packets spread, cutting unnecessary communication and protecting precious network resources [15]. Lightweight Deep Learning IDS supplies details about attack type, severity, odd node behavior and confidence enabling higher-level parts to make routing and security choices. This approach lets the Wireless Sensor Network be safer and more reliable in uses such, as industrial monitoring, healthcare, smart cities, agriculture and environmental monitoring [1] [15].

7.RESULT ANALYSIS



The performance analysis shows that Lightweight Deep Learning IDS can achieve detection accuracy close to standard deep learning approaches while requiring significantly fewer resources. In the proposed comparison, traditional machine learning achieved a detection accuracy of 92.5%, standard deep learning achieved 96.8%, and lightweight deep learning achieved 95.2%. Lightweight Deep Learning also demonstrated competitive precision, recall, and F1-score while maintaining a significantly smaller model size and lower energy consumption. These results show that model compression and efficient neural network design can preserve much of the detection capability of larger models while reducing memory and computational requirements [4], [16]. The proposed approach therefore supports faster local decision-making, improved network lifetime, and the detection of multiple attack types while maintaining a balance between security and energy efficiency [9], [18].

8.DISCUSSION

The proposed Lightweight Deep Learning-based IDS offers a balance between security performance and the limited resources available in Wireless Sensor Networks. Standard deep learning models may offer detection accuracy but their large size and computational requirements make them hard to deploy directly on battery-powered sensor nodes. Lightweight deep learning addresses this problem through architectures, model compression, feature selection and hierarchical decision-making [4] [9]. However the effectiveness of the system depends on the quality and diversity of

training data the level of model compression and changing network conditions [2] [13]. Therefore an effective Lightweight DL-IDS must carefully balance detection accuracy, energy efficiency and deployment complexity.

9.ADVANTAGES

The proposed Lightweight Deep Learning IDS offers advantages for energy-constrained Wireless Sensor Networks. It can achieve detection performance while using fewer computational resources than conventional deep learning models [16]. Local anomaly detection reduces communication and helps conserve battery power resulting in improved energy efficiency and an extended network lifetime. The hierarchical architecture distributes tasks among sensor nodes, cluster heads and the base station supporting scalability in large-scale WSN deployments. In addition deep learning techniques can identify patterns and adapt to different types of attacks making the system more flexible and intelligent [13] [19]. The major advantage of the proposed approach is its ability to provide security while minimizing the impact, on the limited energy, memory and processing resources of sensor nodes [9] [18].

10.LIMITATIONS

Despite its advantages Lightweight Deep Learning IDS has limitations. Lightweight Deep Learning IDS relies largely on high-quality and varied training data. If the data is limited or unrepresentative detection performance may fall [2] [12]. Lightweight Deep Learning IDS faces an accuracy-compression trade-off; much pruning or quantization can lower the model's performance [4] [16]. Managing updates for Lightweight Deep Learning IDS across sensor nodes can be hard and changes in network layout or environment can hurt detection performance and raise false alarms. Most sensor nodes cannot run deep-learning training on their own because of low power and limited compute so centralized or distributed model management becomes necessary [9] [18].

11.FUTURE DIRECTIONS

Many new ideas could make Lightweight Deep Learning IDS for Wireless Sensor Networks. Federated learning lets many devices work together to improve Lightweight Deep Learning IDS models without sending all data to one place, which cuts down on communication and supports learning everywhere [8] [11]. Future Lightweight Deep Learning IDS can also use IDS methods that change detection thresholds, model size and sampling rates by themselves based on network conditions. Trust-based security tools can join with Lightweight Deep Learning IDS results to give safety against bad nodes and cross-layer detection can pull data from several network layers to spot clever attacks more easily [15]. Building hardware-aware neural networks and testing Lightweight Deep Learning IDS, on sensor boards and standard data sets can also make Lightweight Deep Learning IDS more dependable and useful [16] [18].

12.CONCLUSION

Wireless Sensor Networks need security methods that can work inside limits of power, memory and calculation. Traditional Intrusion Detection Systems and normal deep learning models can give security but are usually too heavy for a sensor node to run. Lightweight Deep Learning IDS supplies an answer by using tiny models choosing only the best features cutting away extra parts, shrinking data size and using layered detection. These techniques lower the load while still detecting attacks well. [4] [6] [16] The new design spreads detection work across the sensor nodes, the cluster leaders and the base station. This spread cuts down on communication and saves energy. Results show that Lightweight Deep Learning IDS can reach security performance close to that of deep learning while letting the network last longer and grow more easily. [9] [18] Overall Lightweight Deep Learning IDS looks promising for protecting power-tight Wireless Sensor Networks. Future changes, in learning, federated learning, trust systems and hardware-aware model design can make security, speed and real-world use even better. [8] [15]

References

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347–2376.
2. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176.
3. Cook, D. J., & Das, S. K. (2004). *Smart environments: Technology, protocols, and applications*. John Wiley & Sons.
4. Deng, L., Li, G., Han, S., Shi, L., & Xie, Y. (2020). Model compression and hardware acceleration for neural networks: A comprehensive survey. *Proceedings of the IEEE*, 108(4), 485–532.
5. Doshi, R., Aphorpe, N., & Feamster, N. (2018). Machine learning DDoS detection for consumer Internet of Things devices. In *Proceedings of the 2018 IEEE Security and Privacy Workshops* (pp. 29–35).
6. Hinton, G., Vinyals, O., & Dean, J. (2015). Distilling the knowledge in a neural network. *arXiv preprint arXiv:1503.02531*.
7. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2019). A sybil attack detection scheme for a centralized Internet of Things. *Future Generation Computer Systems*, 100, 139–149.
8. Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., et al. (2021). Advances and open problems in federated learning. *Foundations and Trends in Machine Learning*, 14(1–2), 1–210.
9. Lane, N. D., Bhattacharya, S., Mathur, A., Forlivesi, C., Kawsar, F., & Georgiev, P. (2017). Squeezing deep learning into mobile and embedded devices. *IEEE Pervasive Computing*, 16(3), 82–88.
10. Lu, Y., & Da Xu, L. (2019). Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, 6(2), 2103–2115.
11. McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. Y. (2017). Communication-efficient learning of deep networks from decentralized data. In *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics* (pp. 1273–1282).
12. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. In *2015 Military Communications and Information Systems Conference* (pp. 1–6).
13. Pang, G., Shen, C., Cao, L., & Van Den Hengel, A. (2021). Deep learning for anomaly detection: A review. *ACM Computing Surveys*, 54(2), 1–38.
14. Ren, J., Zhang, Y., Zhang, K., & Shen, X. (2017). Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks. *IEEE Transactions on Wireless Communications*, 16(2), 1134–1147.
15. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164.
16. Sze, V., Chen, Y.-H., Yang, T.-J., & Emer, J. S. (2017). Efficient processing of deep neural networks: A tutorial and survey. *Proceedings of the IEEE*, 105(12), 2295–2329.
17. Tang, T. A., Mhamdi, L., McLernon, D., Zaidi, S. A. R., & Ghogho, M. (2020). Deep learning approach for network intrusion detection in software defined networking. *IEEE Transactions on Network and Service Management*, 17(1), 236–248.

18. Xu, X., Sun, Q., Luo, Y., Huang, L., Wang, S., & Wang, C. (2021). TinyML: A systematic review and synthesis of existing research. *ACM Transactions on Embedded Computing Systems*, 20(5), 1–38.
19. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access*, 5, 21954–21961.
20. Zhang, C., Patras, P., & Haddadi, H. (2019). Deep learning in mobile and wireless networking: A survey. *IEEE Communications Surveys & Tutorials*, 21(3), 2224–2287.