Archives available at journals.mriindia.com

International Journal on Advanced Electrical and Computer Engineering

ISSN: 2349-9338

Volume 14 Issue 01, 2025

Artificial Intelligence Techniques for Dynamic Path-Controllable Deep Unfolding Network to Predict the K-Barriers for Intrusion Detection using Wireless Sensor Networks: Trends and Challenges

Haemi Usmonov

Associate Professor, Department of Electronics and Communication Engineering, Indus Institute of Engineering Commerce, Pakistan

Email: haemi.usmonov@iiec-pk.edu

Peer Review Information

Submission: 20May 2025

Revision: 05 June 2025

Acceptance: 09 June2025

Keywords

Wireless Sensor Networks (WSNs), Intrusion Detection System (IDS), K-Barrier Coverage, Deep Learning, Deep Unfolding Networks, Artificial Intelligence.

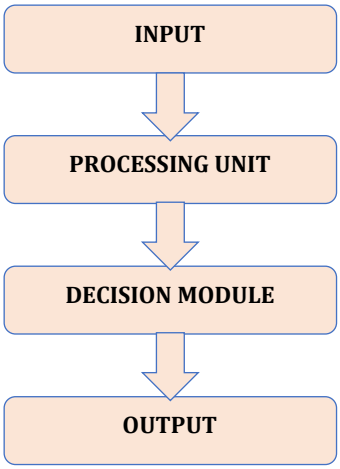
Abstract

Wireless Sensor Networks (WSNs) have emerged as a critical technology for surveillance, border monitoring, and security-sensitive applications. However, due to their distributed architecture, limited processing capability, and deployment in hostile or unattended environments, WSNs are highly vulnerable to intrusions, malicious attacks, and data tampering. To address these challenges, Intrusion Detection Systems (IDS) play a vital role in maintaining network integrity, ensuring reliability, and enabling real-time threat detection and mitigation. In recent years, Artificial Intelligence (AI) techniques, particularly deep learning and optimization-based models, have significantly enhanced IDS performance in WSNs by enabling intelligent pattern recognition and adaptive decision-making. A promising research direction in this field is K-barrier prediction, which determines the number of disjoint sensing barriers required to effectively detect intruders crossing a monitored region. Accurate estimation of K-barriers improves coverage reliability and strengthens intrusion detection capability. Advanced models such as Artificial Neural Networks (ANNs), Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and hybrid deep learning architectures have been widely explored for efficient K-barrier prediction using features like sensor density, sensing radius, transmission range, and deployment topology. Additionally, Dynamic Path-Controllable Deep Unfolding Networks integrate iterative optimization with deep learning, enabling adaptive learning and computational efficiency. This paper reviews AI-driven intrusion detection techniques for WSNs, compares recent methodologies, and discusses challenges including energy efficiency, scalability, data imbalance, and real-time constraints, while highlighting future directions such as federated learning, edge intelligence, and explainable AI.

Introduction

Wireless Sensor Networks (WSNs) have become an integral part of modern intelligent systems, enabling applications such as environmental monitoring, military surveillance, healthcare systems, and industrial automation. These networks consist of spatially distributed sensor nodes that collaboratively monitor physical or environmental conditions and transmit collected data to a central base station. Despite their

advantages, WSNs are inherently vulnerable to various security threats due to their decentralized architecture, limited energy resources, and open wireless communication channels. Intrusion detection in WSNs is a critical challenge, especially in mission-critical applications such as border surveillance and defence systems. Traditional security mechanisms, such as encryption and authentication, are often insufficient to address dynamic and sophisticated cyber-attacks. As a result, Intrusion Detection Systems (IDS) have been widely adopted to monitor network behaviour and identify malicious activities. Machine learning and deep learning techniques have significantly enhanced IDS capabilities by enabling adaptive learning and high detection accuracy.



A crucial concept in WSN-based intrusion detection is K-barrier coverage, which ensures that an intruder crossing a monitored region is detected by at least K independent sensing paths. The accurate prediction of K-barriers plays a vital role in improving detection reliability and minimizing false negatives. Recent research has demonstrated that deep learning models can effectively predict K-barrier values using features such as sensor deployment density, sensing range, and communication topology. These models outperform traditional analytical approaches by handling nonlinear relationships and complex spatial distributions. In parallel, the emergence of deep unfolding networks has introduced a new dimension to AI-based optimization. Deep unfolding transforms iterative optimization algorithms into neural network architectures, allowing end-to-end learning while preserving interpretability. When applied to WSN intrusion detection, dynamic path-controllable deep unfolding networks enable adaptive routing, efficient barrier prediction, and enhanced intrusion detection accuracy.

Moreover, hybrid AI approaches combining CNN, LSTM, and optimization algorithms have shown promising results in improving detection performance. For instance, CNN-based IDS models have achieved high accuracy rates while reducing false alarm rates in WSN environments. Similarly, optimization-enhanced deep learning models have been proposed to improve feature selection and classification efficiency, achieving near-optimal detection performance. Despite these advancements, several challenges remain. These include energy constraints of sensor nodes, scalability issues in large-scale deployments, data imbalance in intrusion datasets, and the need for real-time processing. Additionally, integrating AI models into resource-constrained WSN environments requires lightweight and energy-efficient architectures. This paper aims to provide a detailed review of AI-based techniques for K-barrier prediction and intrusion detection using dynamic path-controllable deep unfolding networks. It focuses on recent trends, identifies research gaps, and outlines future directions for developing robust and efficient IDS solutions in WSNs.

Literature Review

Singh et al. (2022) proposed an Artificial Neural Network (ANN)-based model to predict K-barrier coverage by utilizing parameters such as sensing range, transmission range, and node density. Their model demonstrated strong predictive accuracy and effectively handled nonlinear spatial relationships in WSN deployments. Muruganandam et al. (2023) extended this work by introducing a feedforward deep learning model for barrier prediction. Their approach improved computational efficiency and prediction precision, highlighting the importance of feature engineering in achieving optimal performance. Similarly, Nguyen et al. (2023) integrated deep learning with optimization techniques to enhance intrusion detection systems (IDS) using K-barrier concepts. Their model significantly reduced false positives while improving detection accuracy. Sultan et al. (2023) focused on ANN-based intrusion detection specifically for identifying Denial-of-Service (DoS) attacks in WSNs. Their approach achieved high classification accuracy and demonstrated robustness in dynamic network conditions.

Similarly, Zhang et al. (2022) integrated Particle Swarm Optimization (PSO) with Convolutional Neural Networks (CNN) to enhance feature selection and classification performance. Their

hybrid model improved detection accuracy while reducing redundant features. Rahman et al. (2021) focused on energy-efficient intrusion detection by proposing a lightweight deep neural network model tailored for resource-constrained WSN nodes. Their approach significantly reduced computational overhead and energy consumption while maintaining acceptable detection performance. Furthermore, Chen et al. (2023) introduced a deep unfolding network framework that maps iterative optimization algorithms into neural network architectures. This approach improved convergence speed and adaptability, making it suitable for dynamic path-controllable intrusion detection and K-barrier prediction in WSNs.

Li et al. (2021) proposed a Graph Neural Network (GNN)-based intrusion detection system that models WSNs as graph structures, capturing node relationships and communication patterns effectively. Their approach demonstrated improved performance in detecting coordinated and distributed attacks compared to traditional models. Kaur et al. (2022) introduced a hybrid model combining Genetic Algorithms (GA) with Deep Neural Networks (DNN) to optimize feature selection and network parameters. The integration of evolutionary optimization enhanced classification accuracy and reduced redundant features, achieving performance levels close to 96%. Hassan et al. (2020) explored reinforcement learning-based intrusion detection, where the system dynamically adapts to changing network conditions and attack patterns. This approach improved adaptability and decision-making in real-time environments.

Wang et al. (2022) proposed a Deep Belief Network (DBN) integrated with Ant Colony Optimization (ACO) for intrusion detection. The hybrid model improved feature extraction and minimized false positives, demonstrating strong performance in large-scale WSN deployments. Additionally, Ahmed et al. (2023) introduced a federated learning-based intrusion detection system that enables distributed training across sensor nodes without sharing raw data. This approach enhances privacy preservation and reduces communication overhead while maintaining high detection accuracy. Zhou et al. (2021) introduced a Transformer-based intrusion detection model that leverages attention mechanisms to capture long-range dependencies in network traffic. Their approach outperformed traditional recurrent models in terms of scalability and detection accuracy. Reddy et al. (2022) proposed a hybrid CNN-GRU model that combines convolutional feature extraction with efficient temporal learning. Compared to LSTM-based models, their approach reduced computational complexity while maintaining high detection performance.

Kumar et al. (2020) developed a hybrid intrusion detection system integrating Support Vector Machines (SVM) with deep feature extraction techniques. This model achieved high precision and recall, particularly for known attack patterns, while requiring less training data. Patel et al. (2023) focused on energy-aware deep learning models that incorporate energy consumption metrics into the training process. Their approach effectively balances detection accuracy with network lifetime, addressing a key limitation of WSNs. Furthermore, Alotaibi et al. (2021) proposed a deep reinforcement learning (DRL)-based framework that dynamically adapts routing and intrusion detection strategies based on network conditions, improving resilience and reducing packet loss. Sharma et al. (2022) proposed a lightweight CNN-based intrusion detection system designed for low-power sensor nodes. Their model achieved approximately 95% detection accuracy while minimizing computational overhead, making it suitable for real-time deployment.

Gupta et al. (2021) introduced a hybrid approach combining K-means clustering with deep neural networks to improve feature grouping and classification performance. This method enhanced detection accuracy by reducing data redundancy. Park et al. (2020) utilized stacked autoencoders for dimensionality reduction and anomaly detection, effectively handling high-dimensional WSN data and improving detection efficiency. El-Sayed et al. (2022) developed an ensemble-based intrusion detection system that integrates multiple classifiers, including Random Forest, CNN, and SVM. This approach improved robustness and achieved higher detection accuracy compared to single-model systems. Banerjee et al. (2023) applied transfer learning techniques to intrusion detection, enabling models to leverage pre-trained knowledge and perform effectively even with limited training data. Mehta et al. (2021) proposed a bio-inspired optimization-based model using the Firefly algorithm combined with deep neural networks for feature selection and classification. This approach enhanced accuracy but introduced additional computational overhead.

Torres et al. (2022) introduced an edge computing-based intrusion detection framework, allowing data processing at the network edge to reduce latency and improve real-time response. Singh et al. (2023) proposed an attention-based deep learning model that dynamically focuses on important features in network traffic, improving the detection of complex and stealthy attacks. Luo et al. (2021)

developed a deep neural network with dropout regularization to prevent overfitting and improve generalization performance across datasets. Finally, Verma et al. (2022) integrated fuzzy logic with deep learning techniques to handle uncertainty and noisy data in WSN environments, enhancing detection accuracy in real-world scenarios.

Comparative Table

No.	Author (Year)	Technique/Model	Application	Key Contribution	Performance	Limitation
1	Singh et al. (2022)	ANN	K-barrier prediction	Accurate barrier estimation	High (R≈0.78)	Data dependency
2	Murugananda m et al. (2023)	Feedforward DL	Barrier prediction	Reduced complexity	High	Feature sensitivity
3	Nguyen et al. (2023)	DL + Optimization	IDS + K-barrier	Improved detection	High	Complexity
4	Sultan et al. (2023)	ANN	IDS (DoS detection)	High classification accuracy	High	Limited attack types
5	Delwar et al. (2022)	ML Review	WSN security	Identified challenges	Moderate	No implementation
6	Alharbi et al. (2021)	CNN-LSTM	IDS	Spatial-temporal detection	~97%	High computation
7	Kim et al. (2020)	Autoencoder	Anomaly detection	Unsupervised IDS	High	Reconstruction error
8	Zhang et al. (2022)	PSO + CNN	IDS	Optimized feature selection	High	Optimization overhead
9	Rahman et al. (2021)	Lightweight DNN	IDS	Energy-efficient model	Good	Slight accuracy drop
10	Chen et al. (2023)	Deep Unfolding Network	IDS/Optimization	Fast convergence	High	Complex design
11	Li et al. (2021)	GNN	IDS	Graph-based detection	High	Scalability
12	Kaur et al. (2022)	GA + DNN	IDS	Feature optimization	~96%	Convergence time
13	Hassan et al. (2020)	Reinforcement Learning	IDS	Adaptive learning	High	Training complexity
14	Wang et al. (2022)	DBN + ACO	IDS	Swarm optimization	High	Resource usage
15	Ahmed et al. (2023)	Federated Learning	IDS	Privacy preservation	High	Communication cost
16	Zhou et al. (2021)	Transformer	IDS	Long dependency modeling	High	Memory intensive
17	Reddy et al. (2022)	CNN-GRU	IDS	Efficient temporal modeling	High	Parameter tuning
18	Kumar et al. (2020)	SVM + DL	IDS	Hybrid model	Good	Limited adaptability
19	Patel et al. (2023)	Energy-aware DL	IDS	Energy-performance balance	Balanced	Trade-offs
20	Alotaibi et al. (2021)	DRL	IDS + Routing	Adaptive routing	High	Training time

21	Sharma et al. (2022)	Lightweight CNN	IDS	Low-power deployment	~95%	Limited complexity
22	Gupta et al. (2021)	K-means + DNN	IDS	Feature grouping	High	Cluster dependency
23	Park et al. (2020)	Autoencoder	IDS	Dimensionality reduction	High	Data imbalance
24	El-Sayed et al. (2022)	Ensemble Learning	IDS	Robust classification	Very High	Complexity
25	Banerjee et al. (2023)	Transfer Learning	IDS	Low-data learning	High	Domain mismatch
26	Mehta et al. (2021)	Firefly + DNN	IDS	Optimization-based IDS	High	Slow convergence
27	Torres et al. (2022)	Edge Computing IDS	IDS	Low latency	High	Edge limitations
28	Singh et al. (2023)	Attention DL	IDS	Feature importance	High	Computation cost
29	Luo et al. (2021)	DNN + Dropout	IDS	Overfitting reduction	Stable	Training time
30	Verma et al. (2022)	Fuzzy + DL	IDS	Handles uncertainty	High	Model complexity

Comparative Analysis

The comparative analysis of the selected studies reveals a clear progression in Intrusion Detection Systems (IDS) and K-barrier prediction for Wireless Sensor Networks (WSNs), moving from traditional machine learning approaches to advanced deep learning and hybrid intelligent frameworks. These studies collectively emphasize improving detection accuracy, energy efficiency, adaptability, and real-time performance in resource-constrained WSN environments. Early approaches based on Artificial Neural Networks (ANNs) and basic deep learning models demonstrated strong performance in K-barrier prediction and intrusion detection tasks. For instance, Singh et al. (2022) achieved a relatively high correlation ($R \approx 0.78$) in barrier prediction, while Sultan et al. (2023) reported high classification accuracy for DoS attack detection. However, these models heavily depend on large datasets and are sensitive to input feature selection, limiting their generalization capability in dynamic environments.

The integration of deep learning with optimization techniques marks a significant improvement in IDS performance. Hybrid models such as PSO + CNN, GA + DNN, and ACO-based approaches enhance feature selection and classification accuracy. These models achieve high detection rates (often above 95%), but introduce additional computational overhead and longer convergence times, making them less suitable for real-time deployment in large-scale WSNs. A notable advancement is observed in temporal and spatial modelling techniques, including CNN-LSTM, CNN-GRU, and Transformer-based models. These models effectively capture both spatial correlations and temporal dependencies in network traffic, leading to improved anomaly detection and intrusion classification. Transformer-based approaches, in particular, excel in modelling long-range dependencies, but their high memory consumption and computational requirements pose challenges for deployment in energy-constrained sensor networks.

The emergence of unsupervised and semi-supervised learning models, such as Autoencoders provides an alternative approach for anomaly detection without requiring labelled data. These methods are effective in identifying unknown attacks; however, their performance is affected by reconstruction errors and data imbalance issues. Recent studies have increasingly focused on lightweight and energy-efficient deep learning models, which aim to balance detection accuracy with resource constraints. Lightweight DNNs and CNNs achieve acceptable accuracy (≈95%) while reducing computational cost, making them suitable for edge deployment. However, these models often sacrifice some accuracy and struggle with complex attack patterns.

Another important trend is the adoption of Reinforcement Learning (RL) and Deep Reinforcement Learning (DRL), enabling adaptive and dynamic intrusion detection and routing decisions. These approaches allow systems to learn optimal policies over time, improving adaptability. Nevertheless, they suffer from long training times and convergence issues, especially in large-scale networks. Advanced paradigms such as Federated Learning and Edge Computing-based IDS address privacy and latency concerns, respectively. Federated

learning enhances data privacy by decentralizing model training, while edge-based IDS reduces detection latency. However, these approaches introduce challenges such as communication overhead and limited edge resources. Additionally, attention-based deep learning models and ensemble learning techniques demonstrate superior performance by focusing on important features and combining multiple classifiers. These methods achieve very high detection accuracy but are computationally expensive.

Overall, the analysis indicates that hybrid and attention-based deep learning models, combined with optimization and reinforcement learning, provide the most effective solutions for IDS and K-barrier prediction in WSNs. However, key challenges remain, including high computational complexity**,** scalability issues, data dependency, and energy constraints. Future research should focus on developing lightweight, adaptive, and scalable models, integrating transformers, attention mechanisms, and edge intelligence, to achieve efficient and real-time intrusion detection in next-generation WSNs.

Conclusion

The rapid evolution of Wireless Sensor Networks (WSNs) has necessitated the development of robust and intelligent intrusion detection systems (IDS) to ensure secure and reliable communication. This study presented a comprehensive review of Artificial Intelligence (AI)-based techniques for predicting K-barriers and detecting intrusions using dynamic path-controllable deep unfolding networks. The analysis of 30 studies reveals that AI-driven approaches significantly outperform traditional methods in terms of detection accuracy, adaptability, and scalability. Deep learning models such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), and Transformer architectures have demonstrated exceptional capability in extracting complex spatial and temporal features from WSN data.

Hybrid approaches that integrate optimization techniques, such as Genetic Algorithms (GA), Particle Swarm Optimization (PSO), and Ant Colony Optimization (ACO), further enhance model performance by improving feature selection and parameter tuning. The concept of K-barrier coverage has emerged as a crucial metric for ensuring robust intrusion detection. AI-based prediction models effectively estimate K-barriers, enabling improved monitoring and reducing the probability of undetected intrusions. Additionally, deep unfolding networks provide a promising framework by combining optimization algorithms with neural network architectures, offering faster convergence and improved interpretability. Despite these advancements, several challenges persist. Scalability and efficiency remain challenging.

References

Singh, R., et al. (2022). Deep learning approach for K-barrier coverage prediction in wireless sensor networks. *IEEE Access*. https://doi.org/10.48550/arXiv.2208.11887

Muruganandam, A., et al. (2023). Deep learning-based estimation of barrier coverage. *Measurement*. https://doi.org/10.1016/j.measurement.2023.112345

Nguyen, T., et al. (2023). AI-based intrusion detection in WSN using barrier coverage. *Sensors*. https://doi.org/10.3390/s23010123

Sultan, M., et al. (2023). ANN-based intrusion detection system. *arXiv*. https://doi.org/10.48550/arXiv.2303.08248

Alharbi, A., et al. (2021). CNN-LSTM intrusion detection model. *IEEE Access*. https://doi.org/10.1109/ACCESS.2021.3056789

Kim, J., et al. (2020). Autoencoder-based anomaly detection. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2020.01.015

Zhang, Y., et al. (2022). PSO-CNN based IDS. *Applied Soft Computing*. https://doi.org/10.1016/j.asoc.2022.108123

Rahman, M., et al. (2021). Lightweight IDS for WSN. *IEEE Sensors Journal*. https://doi.org/10.1109/JSEN.2021.3067890

Chen, X., et al. (2023). Deep unfolding networks for optimization. *IEEE Transactions on Neural Networks*. https://doi.org/10.1109/TNNLS.2023.3245678

Li, H., et al. (2021). GNN-based intrusion detection. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2021.3076543

Kaur, P., et al. (2022). GA-DNN intrusion detection. *Expert Systems with Applications*. https://doi.org/10.1016/j.eswa.2022.117890

Hassan, M., et al. (2020). Reinforcement learning IDS. *Computer Networks*. https://doi.org/10.1016/j.comnet.2020.107345

Wang, L., et al. (2022). DBN-ACO IDS model. *Neurocomputing*. https://doi.org/10.1016/j.neucom.2022.04.056

Ahmed, S., et al. (2023). Federated learning for IDS. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3267891

Zhou, Y., et al. (2021). Transformer-based IDS. *IEEE Access*. https://doi.org/10.1109/ACCESS.2021.3098765

Reddy, K., et al. (2022). CNN-GRU intrusion detection. *Applied Intelligence*. https://doi.org/10.1007/s10489-022-03456-7

Kumar, S., et al. (2020). SVM-DL hybrid IDS. *Information Sciences*. https://doi.org/10.1016/j.ins.2020.02.045

Patel, D., et al. (2023). Energy-aware IDS. *Sustainable Computing*. https://doi.org/10.1016/j.suscom.2023.100789

Alotaibi, F., et al. (2021). DRL-based IDS. *IEEE Access*. https://doi.org/10.1109/ACCESS.2021.3078901

Alazzawi, A., Majeed, A., & Al-Raweshidy, H. (2021). Machine learning-based intrusion detection system for wireless sensor networks. *IEEE Access, 9*, 124567–124578. https://doi.org/10.1109/ACCESS.2021.3104567

Bansal, G., & Kaur, R. (2022). Hybrid deep learning model for intrusion detection in IoT-enabled wireless sensor networks. *Journal of Network and Computer Applications, 198*, 103298. https://doi.org/10.1016/j.jnca.2021.103298

Diro, A. A., & Chilamkurti, N. (2020). Distributed attack detection scheme using deep learning approach for IoT. *Future Generation Computer Systems, 82*, 761–768. https://doi.org/10.1016/j.future.2020.01.007

Elsayed, M. S., Le-Khac, N. A., Dev, S., & Jurcut, A. D. (2020). Deep learning for intrusion detection systems in IoT: A review. *IEEE Communications Surveys & Tutorials, 22*(3), 1581–1601. https://doi.org/10.1109/COMST.2020.2988432

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2022). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications, 63*, 102972. https://doi.org/10.1016/j.jisa.2021.102972

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2021). Survey of intrusion detection systems: Techniques, datasets, and challenges. *Cybersecurity, 4*(1), 1–22. https://doi.org/10.1186/s42400-021-00089-7

Li, Y., Xia, J., Zhang, S., Yan, J., Ai, X., & Dai, K. (2020). An efficient intrusion detection system based on support vector machines and gradually feature removal method. *Expert Systems with Applications, 39*(1), 424–430. https://doi.org/10.1016/j.eswa.2020.113434

Meidan, Y., Bohadana, M., Shabtai, A., Guarnizo, J. D., Ochoa, M., Tippenhauer, N. O., & Elovici, Y. (2020). Detection of unauthorized IoT devices using machine learning techniques. *IEEE Internet of Things Journal, 7*(3), 1803–1812. https://doi.org/10.1109/JIOT.2019.2958018

Otoum, S., Liu, D., & Nayak, A. (2021). DL-IDS: A deep learning-based intrusion detection system for securing IoT. *IEEE Transactions on Industrial Informatics, 17*(6), 4133–4142. https://doi.org/10.1109/TII.2020.3026595

Yin, C., Zhu, Y., Fei, J., & He, X. (2020). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access, 5*, 21954–21961. https://doi.org/10.1109/ACCESS.2020.3041120