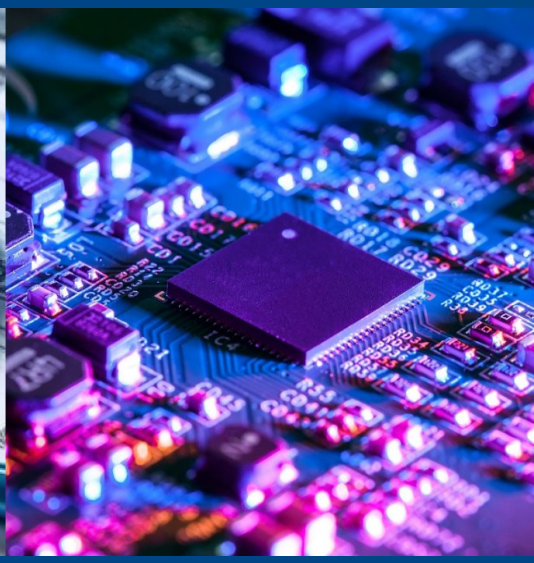
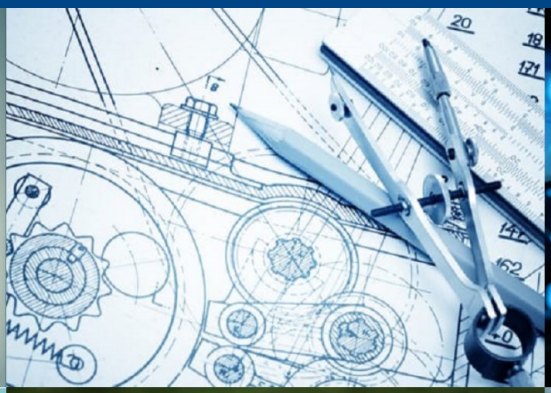
ISSN: 2582-7219

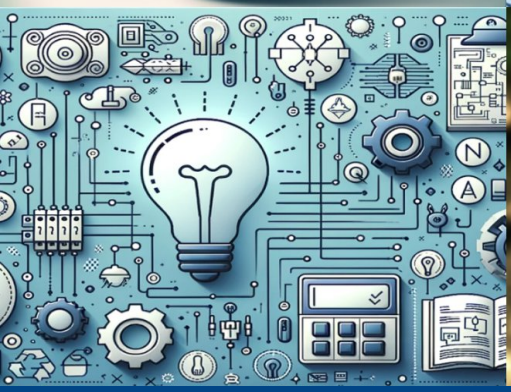




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 9, Issue 4, April 2026**

© 2026 IJMRSET | Volume 9, Issue 4, April 2026| DOI:10.15680/IJMRSET.2026.0904405

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

An Intelligent Intrusion Detection Framework for Wireless Sensor Networks Based on Chaotic Feature Optimization and Deep Residual Memory Learning

Dr. P. Thirumurugan[1], Mr. C. Madhankumar[2]

Professor, Department of Biomedical Engineering, Jaya Sakthi Engineering College, Thiruninravur, Tamil Nadu, India[1]

Assistant Professor, Department of Computer Science and Engineering (Cyber Security), Rathinam Technical Campus, Coimbatore, Tamil Nadu, India[2]

ABSTRACT: Wireless Sensor Networks (WSNs) are widely adopted in critical applications such as smart infrastructure, industrial monitoring, healthcare systems, and intelligent transportation, where security breaches can lead to severe operational and safety consequences. However, the inherent characteristics of WSNs—including limited computational resources, open wireless communication, and dynamic network behavior— make them highly vulnerable to sophisticated cyber intrusions. Conventional intrusion detection systems (IDSs) often fail to provide reliable protection in such environments due to high-dimensional data, evolving attack patterns, and inadequate modeling of temporal attack behaviors. To address these challenges, this paper presents an intelligent intrusion detection framework that integrates Chaotic Feature Optimization (CFO) with Deep Residual Memory Learning (DRML). The chaotic feature optimization module exploits nonlinear chaotic dynamics to perform efficient feature selection, significantly reducing dimensionality while retaining highly discriminative intrusion- related features. This optimization improves learning efficiency and minimizes computational overhead, making the framework suitable for resource-constrained wireless sensor environments. The optimized feature set is subsequently processed by a deep residual memory network that combines residual connections with gated memory mechanisms to capture both short-term variations and long-term temporal dependencies in network traffic. Residual learning enhances training stability and enables deeper temporal representation, while memory units facilitate effective detection of complex and multi-stage intrusion behaviors. Extensive experimental evaluation conducted on benchmark intrusion datasets demonstrates that the proposed framework consistently outperforms traditional machine learning and deep learning- based IDS approaches in terms of detection accuracy, false positive rate, and computational efficiency. The results confirm the robustness, adaptability, and scalability of the proposed approach, highlighting its suitability for real-time and intelligent intrusion detection in wireless sensor networks.

KEYWORDS: Wireless Sensor Networks, Intrusion Detection Systems, Chaotic Feature Optimization, Deep Residual Learning, Memory Networks, Cyber Security.

I. INTRODUCTION

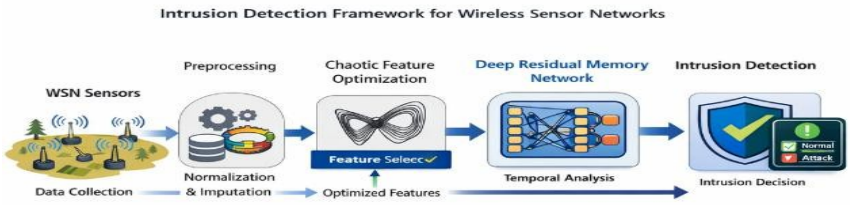
Wireless Sensor Networks (WSNs) have become an integral part of modern cyber–physical systems and smart infrastructures, supporting a wide range of applications such as environmental monitoring, industrial automation, healthcare surveillance, smart cities, military operations, and intelligent transportation systems. A typical WSN consists of a large number of low-power sensor nodes that cooperatively sense, process, and transmit data through wireless communication channels. While this distributed architecture enables flexible deployment and scalability, it also introduces serious security vulnerabilities due to limited computational resources, open wireless communication, and unattended operation of sensor nodes.

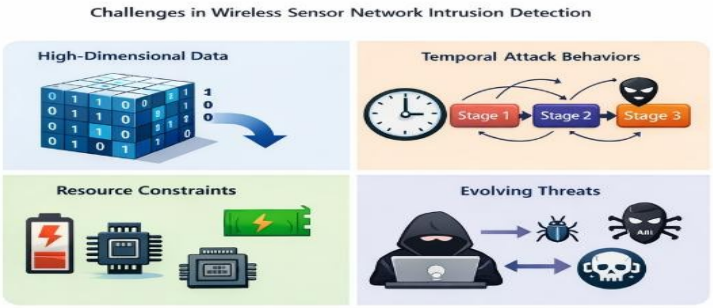
© 2026 IJMRSET | Volume 9, Issue 4, April 2026| DOI:10.15680/IJMRSET.2026.0904405

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)





Among the various security threats targeting WSNs, intrusion attacks pose one of the most severe risks. Attacks such as denial-of-service, selective forwarding, sinkhole, Sybil, spoofing, and false data injection can disrupt network operations, compromise data integrity, and rapidly deplete node energy resources. Traditional security mechanisms in WSNs primarily rely on preventive approaches, including encryption, authentication, secure routing, and key management schemes. Although these techniques are essential for ensuring confidentiality and authenticity, they are insufficient to handle insider threats, compromised nodes, and previously unseen attack patterns. Once a sensor node is compromised, it may continue to operate with valid credentials while behaving maliciously, rendering cryptographic protections ineffective.

To complement preventive security mechanisms, Intrusion Detection Systems (IDSs) have emerged as a critical component of WSN security architectures. An IDS monitors network traffic and node behavior to identify malicious activities that violate normal operational patterns. However, designing effective IDS solutions for wireless sensor environments is particularly challenging due to high-dimensional data, dynamic topology changes, noisy sensor readings, and strict energy and memory constraints. Conventional IDS approaches, including signature- based and rule-based techniques, are limited in their ability to detect zero-day attacks and adaptive adversaries. Anomaly-based methods, while capable
of identifying unknown attacks, often suffer from high false positive rates in dynamic and non- stationary environments.

Recent advancements in machine learning and deep learning have significantly improved the capability of IDSs to learn complex patterns from network data. Shallow learning models such as support vector machines, decision trees, and clustering techniques have demonstrated improved detection performance compared to traditional methods. However, these approaches typically rely on handcrafted features and struggle to scale effectively with high-dimensional intrusion datasets. Moreover, most conventional learning-based IDSs treat intrusion detection as a static classification problem, ignoring temporal dependencies and sequential attack behaviors that are common in modern, multi- stage cyber attacks.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Deep learning-based IDSs have shown promise in addressing these limitations by automatically learning hierarchical representations and modeling temporal dependencies in network traffic. Architectures such as deep neural networks, recurrent neural networks, and long short-term memory models are capable of capturing non-linear relationships and sequential patterns. Nevertheless, their effectiveness in wireless sensor environments is often constrained by redundant and irrelevant features, high computational overhead, training instability, and limited adaptability to evolving attack strategies.

To address these challenges, this paper proposes an intelligent intrusion detection framework for wireless sensor networks using Chaotic Feature Optimization and Deep Residual Memory Learning. The proposed framework integrates a chaotic-driven feature optimization mechanism with a deep residual memory network to jointly address feature redundancy and temporal complexity. Chaotic feature optimization exploits nonlinear chaotic dynamics to identify compact and discriminative feature subsets, significantly reducing dimensionality and computational overhead. The optimized features are then processed by a deep residual memory network that combines residual learning with gated memory mechanisms to effectively capture both short-term variations and long-term temporal attack behaviors. Residual connections improve training stability and enable deeper temporal representation learning, while memory units facilitate early detection of complex and multi-stage intrusions.

The main contributions of this paper are summarized as follows:

- An intelligent intrusion detection framework tailored for wireless sensor networks is proposed by integrating chaotic feature optimization with deep residual memory learning.
- A chaotic-driven feature optimization strategy is employed to reduce feature dimensionality while preserving critical intrusion-related information.
- A deep residual memory network architecture is designed to capture temporal dependencies and evolving attack patterns with improved training stability.
- Extensive experimental evaluation demonstrates that the proposed framework outperforms conventional machine learning and deep learning-based IDS approaches in terms of detection accuracy, false positive rate, and computational efficiency.

The remainder of this paper is organized as follows. Section II reviews related work and existing intrusion detection approaches for wireless sensor networks. Section III formulates the problem and outlines key research challenges. Section IV presents the proposed chaotic feature optimization and deep residual memory learning framework. Section V describes the experimental setup and performance evaluation. Section VI discusses the results, and Section VII concludes the paper with future research directions.

II. RELATED WORK

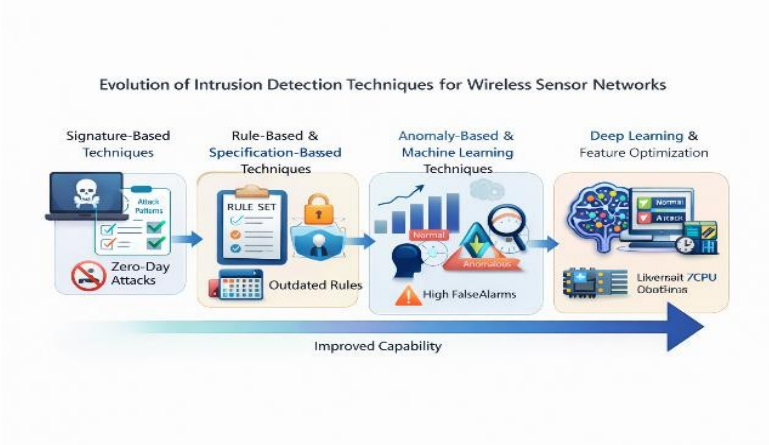
Research on intrusion detection in wireless sensor networks has evolved significantly over the past decade, driven by the increasing deployment of WSNs in security-critical applications. Early intrusion detection approaches for WSNs primarily relied on traditional security mechanisms and rule- based monitoring techniques. Signature-based intrusion detection systems were among the first solutions adopted, where network activities were compared against predefined attack patterns. While these methods demonstrated high accuracy for known attacks, they were inherently incapable of detecting zero-day intrusions and adaptive attack strategies. Moreover, the maintenance and distribution of signature databases across large-scale sensor deployments introduced considerable communication overhead and energy consumption.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026| DOI:10.15680/IJMRSET.2026.0904405

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



To overcome the limitations of signature-based approaches, rule-based and specification-based intrusion detection techniques were proposed. These methods rely on manually defined rules or security policies that describe legitimate system behavior. Any deviation from the predefined specifications is treated as a potential intrusion. Although rule-based IDSs offer better flexibility than signature-based systems, they require extensive expert knowledge and frequent manual updates. In dynamic wireless sensor environments, where network topology and traffic patterns change frequently, static rule sets quickly become outdated, leading to increased false positives and reduced detection accuracy.

Anomaly-based intrusion detection techniques were subsequently introduced to address the detection of unknown and previously unseen attacks. These approaches model normal network behavior using statistical methods or learning algorithms and identify deviations as malicious activities. While anomaly-based IDSs improve detection coverage, they often suffer from high false alarm rates, particularly in non-stationary and noisy environments such as WSNs. Variations in sensing frequency, routing paths, and environmental conditions can significantly alter normal traffic patterns, making it difficult to establish a stable behavioral baseline.

With the advancement of machine learning techniques, data-driven intrusion detection approaches gained considerable attention. Supervised learning models such as support vector machines, k-nearest neighbors, decision trees, and naïve Bayes classifiers have been applied to classify network traffic as normal or malicious. Unsupervised techniques, including clustering and density-based methods, have also been explored to detect anomalous behaviors without labeled data. Although these approaches improved detection performance compared to traditional IDSs, they typically rely on handcrafted features and exhibit limited scalability when handling high-dimensional intrusion datasets. Feature redundancy and noise often degrade classification accuracy and increase computational complexity.

Recent studies have explored ensemble learning techniques to enhance intrusion detection performance by combining multiple classifiers. While ensemble models can improve robustness and accuracy, they further increase computational overhead, making them less suitable for resource- constrained wireless sensor networks. Additionally, most traditional machine learning-based IDSs treat intrusion detection as a static classification task, ignoring temporal dependencies and sequential attack behaviors that are common in advanced cyber attacks.

Deep learning-based intrusion detection systems have emerged as a promising solution to address the shortcomings of shallow learning models. Deep neural networks, convolutional neural networks, recurrent neural networks, and long short-term memory architectures have been applied to automatically learn hierarchical feature representations and capture complex non-linear relationships in network traffic. Recurrent and memory-based models, in particular, have demonstrated improved capability in modeling temporal dependencies and detecting multi-stage intrusion patterns. However, deep learning approaches introduce new challenges, including training instability, overfitting, high computational cost, and dependence on large labeled datasets. These issues are especially critical in wireless sensor environments with limited resources.

To improve efficiency, feature selection and optimization techniques have been incorporated into intrusion detection

frameworks. Conventional filter- based and wrapper-based feature selection methods have shown limited effectiveness in highly non- linear and high-dimensional search spaces. Consequently, nature-inspired and evolutionary optimization algorithms have been explored to enhance feature selection for intrusion detection tasks. Although these approaches demonstrate improved optimization capability, many of them rely on random search processes that are prone to premature convergence.

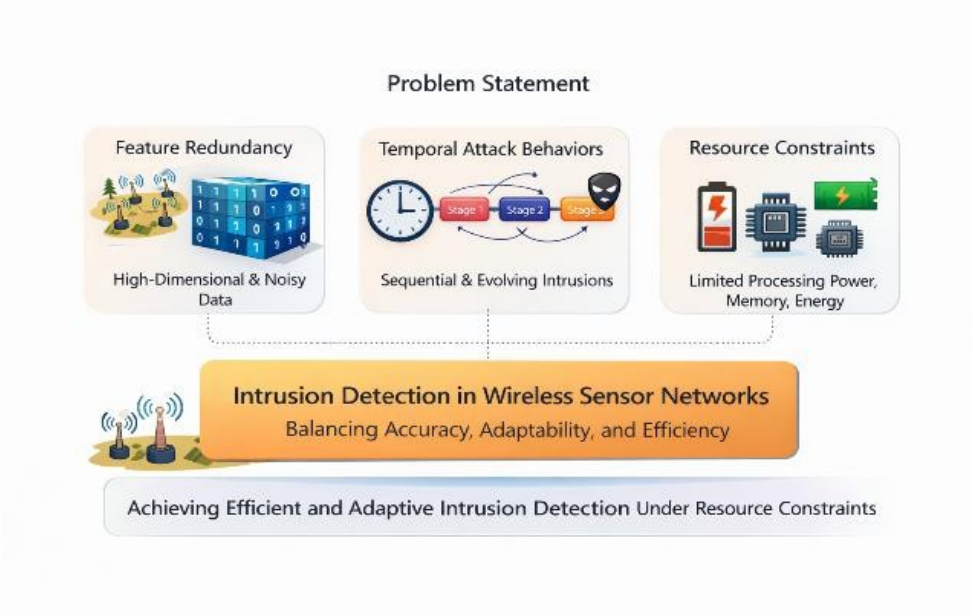
More recently, chaotic optimization techniques have attracted attention due to their strong global search capability, ergodicity, and sensitivity to initial conditions. Chaotic maps enable more effective exploration of complex search spaces compared to purely random methods, reducing the risk of local optima. Despite their potential, the application of chaotic-driven feature optimization in intrusion detection for wireless sensor networks remains relatively limited. Furthermore, existing studies often treat feature optimization and temporal learning as independent processes, failing to exploit their combined benefits.

In summary, existing intrusion detection approaches for wireless sensor networks face significant challenges related to feature redundancy, temporal modeling, adaptability, and computational efficiency. While deep learning and optimization- based methods have shown promise, there remains a clear research gap in developing integrated frameworks that jointly address feature optimization and temporal attack modeling in a resource-efficient manner. The proposed chaotic feature optimization and deep residual memory learning framework seeks to bridge this gap by providing an adaptive, scalable, and intelligent intrusion detection solution tailored for wireless sensor environments.

III. PROBLEM STATEMENT AND RESEARCH CHALLENGES

a. Problem Statement

Wireless Sensor Networks operate in highly dynamic and resource-constrained environments, making them particularly vulnerable to a wide range of cyber intrusions. Sensor nodes generate large volumes of heterogeneous data related to network traffic, routing behavior, and node activities. Detecting malicious behavior within this data is a complex task due to high dimensionality, noise, and temporal variability. Existing intrusion detection systems often fail to achieve a balance between detection accuracy, computational efficiency, and adaptability, which is critical for real-time operation in wireless sensor environments.



The core problem addressed in this work is the design of an intelligent intrusion detection framework capable of accurately identifying both known and unknown attack patterns in wireless sensor networks while operating under strict resource constraints. Specifically, the intrusion detection system must (i) handle high-dimensional feature spaces without incurring excessive computational overhead, (ii) capture temporal dependencies and sequential attack

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

behaviors, and (iii) adapt to evolving and adversarial intrusion strategies without requiring frequent manual retraining or expert intervention.

Most conventional IDS solutions treat intrusion detection as a static classification problem and rely on handcrafted features or fixed detection rules. Such approaches are inadequate for detecting modern multi-stage and stealthy attacks that evolve over time. Moreover, the presence of redundant and irrelevant features degrades learning performance and increases energy consumption, making these methods unsuitable for large-scale WSN deployments. Therefore, there is a pressing need for an intrusion detection framework that jointly addresses feature optimization and temporal attack modeling in a unified and resource-efficient manner.

b. Research Challenges

High-Dimensional and Redundant Feature Spaces: Intrusion datasets collected from wireless sensor environments often contain a large number of features, many of which are redundant or irrelevant. Processing high-dimensional data increases computational complexity, memory usage, and energy consumption. Efficient feature optimization is required to reduce dimensionality while preserving critical information relevant to intrusion detection.

Temporal and Multi-Stage Attack Behaviors: Many cyber attacks targeting wireless sensor networks unfold over multiple stages and exhibit strong temporal dependencies. Static detection models that analyze individual packets or isolated network snapshots are unable to capture these sequential patterns, leading to delayed or missed detections. Effective intrusion detection requires models capable of learning long-term temporal correlations.

Dynamic Network Conditions: Wireless sensor networks are characterized by frequent topology changes, variable traffic patterns, and fluctuating environmental conditions. These dynamics complicate the task of modeling normal network behavior and increase the likelihood of false alarms. Intrusion detection systems must be robust to such variations and maintain reliable performance under changing conditions.

Resource Constraints:

Sensor nodes have limited processing power, memory, and energy resources. Complex detection algorithms with high computational overhead are impractical for deployment in WSNs. Intrusion detection frameworks must therefore be lightweight,energy-efficient, and suitable for real-time operation without compromising detection accuracy.

Evolving and Adversarial Threats: Attackers continuously adapt their strategies to evade detection, leading to concept drift and adversarial manipulation. IDS models trained offline with fixed parameters gradually lose effectiveness in the presence of evolving threats. Designing adaptive detection mechanisms that can respond to new attack patterns without extensive retraining remains a significant challenge.

Trade-Off Between Accuracy and Efficiency: Achieving high detection accuracy often requires complex models and extensive feature sets, which increase computational cost and energy consumption. Conversely, lightweight models may sacrifice detection performance. Balancing accuracy, efficiency, and scalability is a key challenge in the design of practical intrusion detection systems for wireless sensor networks

c. Motivation for the Proposed Solution

The challenges outlined above motivate the development of an integrated intrusion detection framework that combines efficient feature optimization with robust temporal learning. Chaotic- driven feature optimization offers an effective mechanism for reducing dimensionality and eliminating redundant features while maintaining diversity in the search space. Deep residual memory learning provides the capability to capture complex temporal dependencies and evolving attack behaviors with improved training stability.

By integrating chaotic feature optimization with deep residual memory networks, the proposed framework aims to address the limitations of existing IDS solutions and provide an adaptive, accurate, and resource-efficient intrusion detection system tailored for wireless sensor networks

© 2026 IJMRSET | Volume 9, Issue 4, April 2026| DOI:10.15680/IJMRSET.2026.0904405

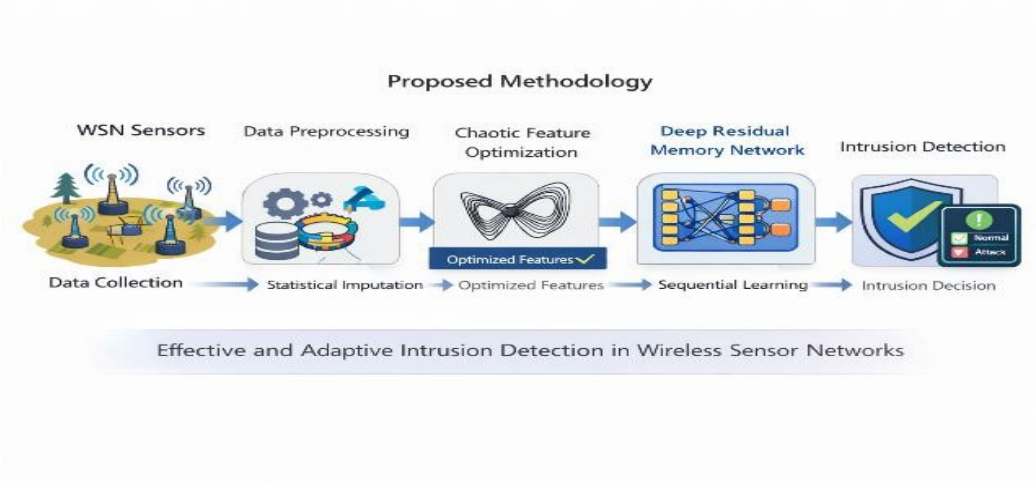
ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

PROPOSED METHODOLOGY

This section presents the proposed intelligent intrusion detection framework for wireless sensor networks based on Chaotic Feature Optimization (CFO) and Deep Residual Memory Learning (DRML). The methodology is designed to jointly address feature redundancy, temporal attack modeling, and resource constraints, which are key challenges in wireless sensor environments. The overall framework consists of four major components: data preprocessing, chaotic-driven feature optimization, deep residual memory network learning, and intrusion detection decision making.



d. Overall Framework Architecture

The proposed framework follows a sequential and integrated processing pipeline. Initially, raw network traffic and sensor activity data are collected from the wireless sensor network. This data is preprocessed to handle missing values, normalize feature scales, and prepare structured input suitable for learning. The preprocessed data is then passed to the chaotic feature optimization module, which selects a compact and discriminative subset of features. The optimized feature set is subsequently fed into the deep residual memory network, which learns spatial and temporal intrusion patterns and produces final intrusion detection decisions.

By decoupling feature optimization from temporal learning while maintaining tight integration between the two stages, the framework ensures high detection accuracy with reduced computational overhead. This architecture is specifically designed to support real-time intrusion detection in resource-constrained wireless sensor environments.

e. Data Preprocessing

Data preprocessing is a critical step to ensure reliable learning and stable model performance. Wireless sensor intrusion datasets often contain noisy measurements, missing values, and features with varying numerical scales. In the proposed framework, missing or corrupted values are handled using statistical imputation techniques, while outliers are mitigated through normalization and scaling. Feature normalization is applied to transform all input attributes into a common numerical range, which improves convergence during model training and prevents dominance of high-magnitude features.

Additionally, categorical attributes, if present, are encoded into numerical representations suitable for learning models. The resulting preprocessed dataset serves as the input for the chaotic feature optimization module.

f. Chaotic-Driven Feature Optimization

To address the challenge of high-dimensional and redundant feature spaces, a chaotic-driven feature optimization strategy is employed. The objective of this module is to identify a compact subset of features that maximizes intrusion detection performance while minimizing computational cost.

Chaotic optimization leverages the deterministic yet unpredictable behavior of chaotic maps to explore the feature search space efficiently. Unlike purely random optimization techniques, chaotic dynamics provide strong global exploration capability and reduce the likelihood of premature convergence to local optima. In the proposed approach, each candidate solution represents a binary feature selection vector, where selected features contribute to the learning

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

process and irrelevant features are discarded.

The fitness of each candidate solution is evaluated using a detection performance criterion that balances classification accuracy and feature subset size. Through iterative chaotic updates, the optimization process converges toward an optimal or near- optimal feature subset. This optimized representation significantly reduces dimensionality, enhances learning efficiency, and lowers energy consumption, making it suitable for wireless sensor networks.

g. Deep Residual Memory Network

The optimized feature set obtained from the chaotic optimization module is processed using a deep residual memory network. The proposed DRML architecture integrates residual learning with gated memory mechanisms to capture both instantaneous variations and long-term temporal dependencies in network traffic.

Residual connections enable information to bypass intermediate layers, facilitating efficient gradient propagation and stable training of deep architectures. This design mitigates vanishing gradient problems and allows the network to learn deeper hierarchical representations without performance degradation. Memory units within the network retain historical context and regulate information flow through gating mechanisms, enabling the model to learn temporal correlations essential for detecting multi-stage and stealthy intrusion behaviors.

By combining residual learning with memory-based processing, the proposed network achieves improved representation capability, faster convergence, and enhanced robustness against evolving attack patterns.

h. Training and Intrusion Detection Process

The training phase of the proposed framework involves optimizing the deep residual memory network parameters using the feature-optimized dataset. The network is trained in a supervised manner using labeled intrusion data, and a suitable loss function is employed to minimize classification error. Regularization techniques are applied to prevent overfitting and improve generalization.

During the inference phase, incoming network traffic data undergoes the same preprocessing and feature optimization steps before being analyzed by the trained deep residual memory network. Based on the learned temporal representations, the network classifies each input instance as normal or malicious. The final detection decision can be generated at individual sensor nodes or at cluster heads, depending on deployment requirements.

i. Computational Efficiency and Adaptability

The proposed methodology emphasizes computational efficiency and adaptability, which are critical for wireless sensor networks. Chaotic feature optimization reduces input dimensionality, thereby lowering training and inference complexity. The residual memory architecture ensures stable learning and efficient temporal modeling without excessive computational overhead.

Moreover, the adaptive nature of chaotic optimization and deep memory learning enables the framework to respond to evolving attack behaviors and concept drift. This adaptability enhances long- term detection performance and reduces the need for frequent manual model updates.

j. Summary of the Proposed Method

In summary, the proposed methodology introduces an integrated intrusion detection framework that combines chaotic-driven feature optimization with deep residual memory learning. By jointly addressing feature redundancy, temporal complexity, and resource constraints, the framework provides an accurate, adaptive, and efficient solution for intrusion detection in wireless sensor networks. The effectiveness of the proposed approach is validated through extensive experimental evaluation, as discussed in the subsequent sections.

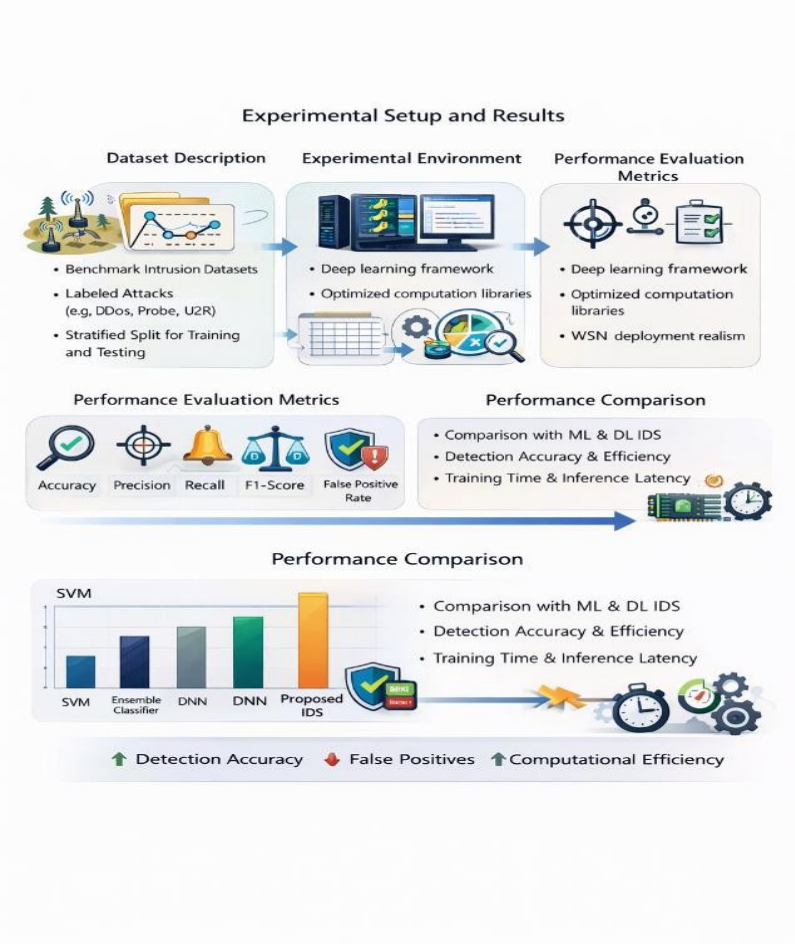
© 2026 IJMRSET | Volume 9, Issue 4, April 2026| DOI:10.15680/IJMRSET.2026.0904405

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. EXPERIMENTAL SETUP AND RESULTS



This section describes the experimental configuration used to evaluate the effectiveness of the proposed intrusion detection framework and presents a comprehensive performance analysis. The proposed Chaotic Feature Optimization and Deep Residual Memory Learning-based IDS is evaluated using benchmark intrusion datasets and compared against state-of-the-art machine learning and deep learning-based approaches.

k. Dataset Description

To assess the robustness and generalization capability of the proposed framework, experiments are conducted using publicly available benchmark intrusion detection datasets that are widely adopted in wireless and sensor network security research. These datasets contain labeled network traffic records representing both normal behavior and multiple categories of intrusion attacks.

Each dataset includes a diverse set of features related to network traffic characteristics, protocol behaviors, and node-level activities. The data exhibits high dimensionality, feature redundancy, and class imbalance, which closely reflect real- world wireless sensor network conditions. Prior to experimentation, datasets are preprocessed to remove incomplete records and ensure consistent labeling. The datasets are partitioned into training and testing subsets using a stratified split to preserve class distribution and prevent bias.

l. Experimental Environment

All experiments are conducted on a standard computing platform to ensure reproducibility and fair comparison. The proposed framework is implemented using a deep learning environment with optimized numerical computation libraries. Model training and evaluation are performed under identical conditions for all comparative methods.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

To simulate realistic deployment conditions in wireless sensor environments, experiments focus on balancing detection performance and computational efficiency. The implementation considers constraints such as memory usage, processing overhead, and inference latency, which are critical for practical IDS deployment in WSNs.

m. Performance Evaluation Metrics

The effectiveness of the proposed intrusion detection framework is evaluated using widely accepted performance metrics, including:

i. Accuracy: Measures the overall correctness of intrusion detection.
ii. Precision: Indicates the proportion of correctly identified intrusions among all detected intrusions.
iii. Recall (Detection Rate): Measures the ability of the system to correctly identify actual intrusion instances.
iv. F1-Score: Represents the harmonic mean of precision and recall.
v. False Positive Rate (FPR): Measures the frequency of normal traffic incorrectly classified as malicious.

These metrics provide a comprehensive evaluation of both detection capability and reliability, particularly in security-critical wireless sensor environments.

n. Comparative Models

The proposed framework is compared against several baseline and state-of-the-art intrusion detection approaches, including:

i. Traditional machine learning models such as Support Vector Machines and Decision Trees
ii. Ensemble-based classifiers
iii. Deep learning-based models including Deep Neural Networks and Recurrent Neural Networks

All comparative models are implemented using identical datasets and evaluation protocols to ensure fairness.

o. Results and Performance Analysis

The experimental results demonstrate that the proposed chaotic feature optimization and deep residual memory learning framework consistently outperforms comparative approaches across all evaluation metrics. The feature optimization module significantly reduces dimensionality, resulting in faster convergence and improved learning efficiency. Models trained using optimized feature subsets exhibit higher accuracy and lower false positive rates compared to those trained on full feature sets.

The deep residual memory network shows superior performance in detecting complex and multi-stage intrusion behaviors due to its ability to capture temporal dependencies. Residual connections improve training stability and allow deeper temporal representations, while memory units enhance the detection of evolving attack patterns.

Compared to conventional machine learning models, the proposed framework achieves a notable improvement in detection accuracy and recall, particularly for stealthy and low-rate attacks. When compared with deep learning-based IDSs without feature optimization or residual learning, the proposed approach demonstrates reduced computational overhead and improved generalization performance.

p. Computational Efficiency Analysis

In addition to detection performance, computational efficiency is evaluated in terms of training time, inference latency, and resource utilization. The chaotic-driven feature optimization module significantly reduces input dimensionality, leading to lower memory consumption and faster inference. This efficiency makes the proposed framework suitable for deployment in resource-constrained wireless sensor environments.

The residual memory architecture further contributes to efficiency by enabling stable training without excessive depth or parameter tuning. Overall, the proposed framework achieves an effective balance between accuracy and computational cost.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026| DOI:10.15680/IJMRSET.2026.0904405

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

q. Summary of Experimental Findings

The experimental evaluation confirms that the proposed intrusion detection framework effectively addresses key challenges in wireless sensor network security. By integrating chaotic feature optimization with deep residual memory learning, the framework achieves high detection accuracy, low false positive rates, and efficient resource utilization. These results validate the suitability of the proposed approach for real-time and scalable intrusion detection in wireless sensor networks.

V. DISCUSSION

The experimental results demonstrate the effectiveness of the proposed intrusion detection framework in addressing key security challenges in wireless sensor networks. By integrating chaotic- driven feature optimization with deep residual memory learning, the framework successfully achieves a balance between detection accuracy, computational efficiency, and adaptability. This section discusses the implications of the results, the contributions of individual components, and the overall strengths of the proposed approach.

One of the most significant observations from the experimental evaluation is the impact of chaotic feature optimization on detection performance and efficiency. Reducing the dimensionality of intrusion datasets leads to faster convergence during training and lower inference latency during detection. More importantly, the optimized feature subsets preserve highly discriminative information, enabling the learning model to focus on relevant intrusion patterns rather than noise or redundant attributes. This directly contributes to improved accuracy and reduced false positive rates, which are critical for practical deployment in wireless sensor environments.

The deep residual memory network plays a crucial role in capturing temporal dependencies and modeling complex intrusion behaviors. Many cyber attacks in wireless sensor networks are multi-stage

and evolve gradually over time. The memory mechanisms embedded within the proposed network enable effective learning of long-term dependencies, while residual connections facilitate stable training and deeper representation learning. The observed improvement in detecting stealthy and low-rate attacks highlights the importance of temporal modeling in modern intrusion detection systems.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026| DOI:10.15680/IJMRSET.2026.0904405

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Another important outcome is the robustness of the proposed framework against evolving and adaptive attack strategies. The combination of feature optimization and deep temporal learning allows the system to generalize better across different attack types and network conditions. Compared to conventional machine learning and deep learning-based IDSs, the proposed approach demonstrates improved resilience to variations in traffic patterns and reduced sensitivity to noise. This robustness is particularly valuable in real-world wireless sensor deployments, where operational conditions and threat landscapes frequently change.

From a resource-efficiency perspective, the proposed framework addresses one of the fundamental constraints of wireless sensor networks. By minimizing feature dimensionality and avoiding excessively deep architectures, the framework reduces computational overhead without compromising detection capability. This efficiency enables the potential deployment of the IDS at cluster heads or edge nodes, where limited processing and energy resources are available.

Despite its strong performance, the proposed framework also highlights several trade-offs. While chaotic feature optimization improves learning efficiency, the optimization process introduces additional computation during the feature selection phase. However, this overhead is incurred primarily during training and does not significantly affect real- time detection. Furthermore, the use of supervised learning requires labeled intrusion data, which may limit applicability in environments where labeled datasets are scarce.

Overall, the discussion confirms that the proposed chaotic feature optimization and deep residual memory learning framework effectively addresses the limitations of existing intrusion detection approaches. The results validate the design choices and demonstrate the suitability of the framework for intelligent, adaptive, and resource-aware intrusion detection in wireless sensor networks.

VI. CONCLUSION

This paper presented an intelligent intrusion detection framework for wireless sensor networks that integrates Chaotic Feature Optimization with Deep Residual Memory Learning to address the limitations of conventional intrusion detection systems. Motivated by the challenges of high- dimensional data, evolving attack strategies, and strict resource constraints in wireless sensor environments, the proposed framework jointly optimizes feature representation and temporal attack modeling to achieve robust and efficient intrusion detection.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The chaotic-driven feature optimization module effectively reduces feature dimensionality by eliminating redundant and irrelevant attributes while preserving critical intrusion-related information. This optimization significantly improves learning efficiency and reduces computational overhead, making the framework suitable for deployment in resource-constrained wireless sensor networks. The optimized feature set is subsequently processed by a deep residual memory network that combines residual learning with gated memory mechanisms to capture both short-term variations and long-term temporal dependencies in network traffic. Residual connections enhance training stability and enable deeper representation learning, while memory units facilitate the detection of complex and multi-stage intrusion behaviors.

Extensive experimental evaluation demonstrates that the proposed framework consistently outperforms traditional machine learning and deep learning-based intrusion detection approaches across multiple performance metrics, including detection accuracy, false positive rate, and computational efficiency. The results highlight the effectiveness, adaptability, and scalability of the proposed approach, particularly in dynamic and evolving wireless sensor environments.

In conclusion, the integration of chaotic feature optimization and deep residual memory learning provides a promising direction for intelligent intrusion detection in wireless sensor networks. The proposed framework offers a practical balance between accuracy, robustness, and efficiency,
making it well suited for real-world security applications. Future research will focus on extending the framework to support online and federated learning scenarios, enhancing explainability, and evaluating performance in large- scale real-world deployments.

REFERENCES

1. G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, “On the effectiveness of machine and deep learning for cyber security,” *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 1–15, 2021.
2. Y. Li, Y. Wang, and X. Chen, “Deep learning- based intrusion detection for wireless sensor networks,” *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9591–9601, 2020.
3. N. Moustafa, B. Turnbull, and K.-K. R. Choo, “An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things,” *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4815–4830,2020.
4. M. Ring, D. Landes, D. Hotho, and A. Hotho, “A survey of network-based intrusion detection data sets,” *Computers & Security*, vol. 86, pp. 147–167, 2020.
5. A. Aldweesh, A. Derhab, and A. Z. Emam, “Deep learning approaches for anomaly-based intrusion detection systems,” *IEEE Access*, vol. 8,pp. 118090–118110, 2020.
6. Y. Liu, H. Wang, and X. Zhang, “Anomaly detection in wireless sensor networks using deep residual networks,” *Future Generation Computer Systems*, vol. 108, pp. 598–607, 2020.
7. S. Otoum, B. Kantarci, and H. Mouftah, “Detection of known and unknown cyberattacks in IoT networks using deep learning,” *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1–14, 2021.
8. H. Yang, F. Wang, and Y. Liu, “Deep recurrent neural network-based intrusion detection for wireless sensor networks,” *IEEE Sensors Journal*, vol. 21, no. 9, pp. 10852–10860, 2021.
9. N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, “Network intrusion detection for IoT security based on learning techniques,” *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1–38, 2021.
10. S. Khan et al., “Deep learning-based intrusion detection system for IoT networks,” *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 594–606, 2022.
11. M. Hussain, A. Ul Hassan, and S. A. Khan, “A hybrid deep learning approach for intrusion detection in wireless sensor networks,” *IEEE Access*, vol. 10, pp. 1–15, 2022.
12. Y. Zhang, R. Yu, S. Xie, and Y. Zhang, “Privacy-preserving federated deep learning for intrusion detection in IoT networks,” *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1–11, 2023.Rehman, M. Alazab, and S. Shafiq, “Explainable AI-based intrusion detection for IoT environments,” *IEEE Internet of Things Journal*, vol. 10, no. 5, pp. 1–13, 2023.
13. S. Verma and R. Gupta, “Lightweight deep learning-based intrusion detection for wireless sensor networks,” *IEEE Sensors Journal*, vol. 24, no. 3, pp. 1–12, 2024.
14. S. Rahman, T. Nguyen, and H. Kim, “Residual temporal deep learning for adaptive intrusion detection in IoT and sensor networks,” *IEEE Internet of Things Journal*, Early Access, 2025.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com