Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Comparative Analysis of Machine Learning Models for Enhancing Wormhole Attack Detection in Wireless Sensor Networks

Mrs. Megha Patel[1], Dr. Manish Patel[2]
[1] *PhD Scholar,Sankalchand Patel College of Engineering,Sankalchand Patel University, Gujarat, India*
[2] *Professor,Sankalchand Patel College of Engineering, Sankalchand Patel University, Gujarat, India*
[1]*Patelmegha3110@gmail.com*, [2]*it43manish@gmail.com*

ARTICLE INFO

Received: 18 Dec 2024
Revised: 10 Feb 2025
Accepted: 28 Feb 2025

ABSTRACT

Wireless Sensor Networks (WSNs) are critical technological infrastructures deployed in environmental monitoring, healthcare, and military applications. However, they face significant security threats, particularly wormhole at-tacks, which establish covert communication channels to disrupt network routing and compromise data integrity. This study conducts a comprehensive comparative analysis of seven machine learning models—Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Random Forest (RF), Deci-sion Tree (DT), Naïve Bayes (NB), Logistic Regression (LR), and Artificial Neural Network (ANN)—to detect wormhole attacks. The models were eval-uated based on key performance metrics, including accuracy, precision, re-call, F1-score, and computational efficiency. Experimental results indicate that ANN achieved the highest detection accuracy (96.2%), followed by RF (95.1%) and SVM (94.5%), demonstrating strong classification capabilities. However, ANN incurred the highest computational cost (620 ms), making it less suitable for real-time applications. Decision Tree and Naïve Bayes ex-hibited the lowest computational overhead but lower detection performance, making them viable for resource-constrained environments. This study high-lights the trade-off between detection accuracy and computational efficien-cy, offering insights into selecting optimal machine learning approaches for enhancing WSN security.

Introduction: Wireless Sensor Networks (WSNs) consist of spatially distributed sensor nodes that autonomously monitor environmental or physical parameters such as temperature, humidity, and pressure [1,2]. These networks are employed in a wide range of critical applications, including healthcare monitoring and military surveillance, which makes them susceptible to cyberattacks. In WSNs, the primary entity—commonly referred to as the base station or sink—can be connected to existing infrastructure or the Internet through a gateway, thereby enabling remote access to the collected data [6].

One of the key advantages of WSNs lies in their ability to deploy a large number of compact, autonomous sensor nodes without relying on a pre-existing infrastructure [29]. Once deployed, these nodes gather data from their surroundings and cooperate using either single-hop or multi-hop communication to transmit information to the sink, following a designated communication protocol [30].

Given their dynamic nature and expanding use across diverse domains, the demand for robust security mechanisms in WSNs is becoming increasingly critical. These networks frequently operate in hostile environments where node-to-node communication can be unstable, complicating the deployment of effective security solutions. Safeguarding nodes against potential security threats presents a significant challenge, as WSNs are prone to various forms of attacks [3], including jamming, collision, wormhole, flooding, sinkhole, selective packet drop, Sybil, cloning, denial-of-service, and tampering. Among these, the wormhole attack stands out as a particularly severe threat, targeting the routing protocols within WSNs [6].

Objectives: The objective of this study is to evaluate the performance of various machine learning algorithms in detecting wormhole attacks within wireless sensor networks. We conduct a comparative analysis of different models using key performance metrics such as

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

accuracy, precision, recall, F1-score, and computational efficiency. Furthermore, the study aims to identify the most suitable model for real-time detection in resource-limited WSN environments.

Methods: This study conducts a comparative evaluation of machine learning models for detecting wormhole attacks in WSNs, addressing the limitations of traditional methods like distance estimation and hop count. By leveraging anomaly-based analysis, the research involves selecting suitable models, preprocessing a simulated dataset, and training the models for evaluation using metrics such as accuracy, precision, recall, F1-score, and computational efficiency. The goal is to identify the most effective and resource-efficient models for real-time deployment in WSN environments.

Results: The results of our comparative analysis of machine learning models for wormhole attack detection in wireless sensor networks (WSNs) reveal critical insights into the effectiveness and limitations of each algorithm. Using real-world network simulation data, we evaluated the models based on accuracy, precision, recall, F1-score, and computational time. This section highlights the comparative strengths and weaknesses of the models in identifying wormhole attacks, offering practical considerations for selecting suitable models in resource-constrained WSN environments and guiding future improvements in detection systems.

Conclusions: In conclusion, this study presents a comparative analysis of seven machine learning models for wormhole attack detection in WSNs, highlighting their strengths, limitations, and practical applicability. The findings offer valuable insights into the trade-offs between accuracy and computational efficiency, contributing to the development of effective, resource-aware security solutions in wireless sensor networks.

Keywords: Wireless Sensor Networks, Wormhole Attack, Machine Learning, Network Security, Attack Detection, Support Vector Machines, Random Forests, Neu-ral Networks, Intrusion Detection, Routing Protocols.

1. INTRODUCTION

1.1 Wireless Sensor Networks: Security Landscape

Wireless Sensor Networks (WSNs) consist of spatially distributed sensor nodes [1] that autonomously monitor environmental [2] or physical parameters such as temperature, humidity, and pressure. These networks are employed in a wide range of critical applications, including healthcare monitoring and military sur-veillance, making them susceptible to cyberattacks. In wireless sensor networks (WSNs), the primary entity, often referred to as the base station or sink, can be linked to an infrastructure or the Internet via a gateway, enabling remote access to the gathered data [6]. One of the key benefits of WSNs is their capability to deploy numerous small, self-sufficient sensor nodes without requiring a pre-existing infrastructure [29]. Once deployed, these nodes collect data from their surroundings and, following a designated communication protocol, collaborate to transmit information to the sink using either single-hop or multi-hop communica-tion [30].

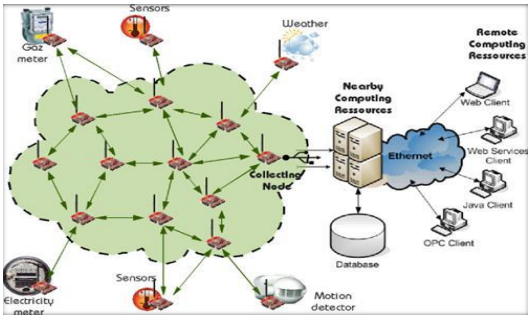

Fig. 1. Generic architecture of WSN [1].

Due to their dynamic nature and expanding applications across various domains, the need for robust security mechanisms in WSNs is becoming increasingly criti-cal. These networks often operate in challenging

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

environments where communi-cation between nodes is unreliable, making the implementation of security measures complex. Protecting nodes from potential security threats remains a significant challenge, as WSNs are vulnerable to numerous attacks [3], including jamming, collision, wormhole, flooding, sinkhole, selective packet drop, Sybil, cloning, denial-of-service, and tampering. Among these, one notable threat is the wormhole attack, which targets the routing protocols within WSNs [6].

1.2 Wormhole Attacks: A Critical Security Threat

Wormhole nodes manipulate network routing [31] by creating a deceptive shortcut that appears shorter than the actual path. This interference disrupts the routing topology, which relies on the distance between nodes for proper func-tionality. A wormhole assault entails two malicious nodes linked by a tunnel. The initial infected node captures data packets from one segment of the network and transmits them to the second malicious node, located at a remote site [27]. The second node subsequently sends the packets locally, so deceiving the network [7].

One of the most concerning aspects of a wormhole attack is that it can be exe-cuted without prior knowledge of the network and without directly interfering with other nodes, making it a significant security threat. Wormhole attacks can occur in different modes [7]. Figure 2 illustrates the various types of wormhole attacks [34].

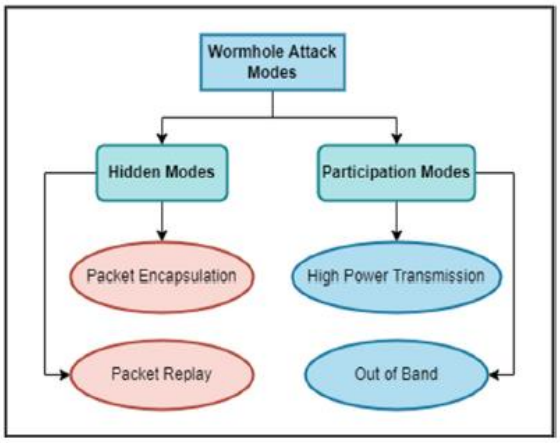

Fig. 2. Classification of wormhole attacks based on hidden and participating nodes [7].

In covert modes, wormhole attacks involve packet encapsulation or packet relaying [17]. Packet encapsulation ensures packets follow authorized routes by hiding hop count increases, with the second node restoring and forwarding packets unchanged. Packet relay allows a single malicious node to relay packets from distant nodes, making them appear as direct neighbors and affecting routing [7]. Participation modes include high-power transmission, where a node increases its range to attract packets, and out-of-band communication, where two compromised nodes form a high-bandwidth tunnel bypassing the network's usual structure [24]. Figure 3 illustrates a wormhole attack in a WSN.

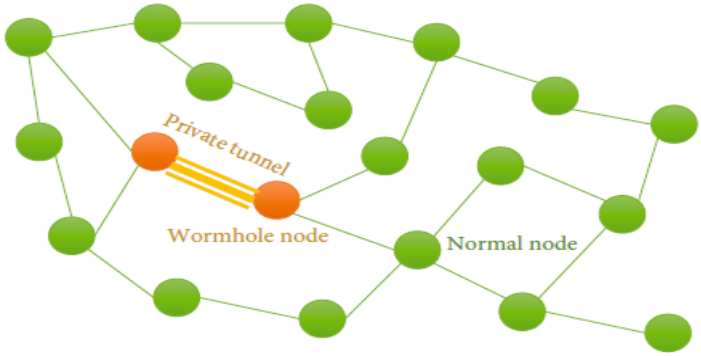

Fig. 3. The diagram of the wormhole attack [4].

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2. LITERATURE SURVEY

In recent years, an extensive array of machine learning techniques has been investigated to enhance the detection of security threats in wireless sensor networks (WSNs), with a primary focus on identifying wormhole attacks [19]. This section provides a comprehensive examination of existing research, emphasizing machine learning-based methodologies designed to improve the accuracy and efficiency of wormhole attack detection [20].

2.1 Approaches for Detecting Wormhole Attacks in WSN

In the domain of Wireless Sensor Networks (WSNs), wormhole attacks pose a significant security threat by creating malicious tunnels that manipulate network communication. Over the years, researchers have proposed various detection techniques to mitigate [35] these attacks, broadly categorized into three primary approaches: topology-based, distance-based, and machine learning-based meth-ods.

Topology-based detection methods rely on analyzing changes in the network structure, utilizing node connectivity patterns and graph-based analysis to identi-fy inconsistencies introduced by wormhole tunnels (Harsanyi et al., 2018) [8]. These approaches effectively detect attacks that disrupt routing paths and alter the logical structure of the network [28].

Distance-based detection techniques focus on measuring signal strength, hop count, transmission delays, and neighborhood variations to identify anomalies in communication behavior (Pawar & Anuradha, 2020) [2]. By leveraging spatial and temporal properties, these methods can detect suspicious links that do not conform to normal network behavior (Affane & Satori, 2024) [3].

Machine learning-based detection methods offer a more adaptive and data-driven approach by leveraging ML models to analyze network traffic patterns and classify potential threats (Hanif et al., 2022) [7]. This category includes su-pervised and unsupervised learning, reinforcement learning for dynamic adapta-tion (Chourasia & Tokekar, 2024) [5], and federated learning for decentralized detection in large-scale networks (Alshehri, 2024) [9].

Table 1 provides a structured comparison of these detection techniques along with their respective descriptions and references.

Table 1: Approaches for Wormhole Detection

Approach	Description	Reference
Topology-based detection	Analyzes changes in network topology to detect wormhole attacks using node connectivity and graph-based analysis.	[8]
Distance-based detection	Uses signal strength, hop count, transmission delays, and neighborhood changes to identify anomalies in communication.	[2], [3]
Machine learning-based detection	Utilizes ML models, including supervised, unsupervised, reinforcement, and federated learning, for adaptive and data-driven attack detection.	[7], [5], [9], [10]

2.2 Traditional Methods for Wormhole Attack Detection

Conventional wormhole attack detection methods in Wireless Sensor Networks (WSNs) depend on network attributes such as timing, distance, and alterations in topology to detect nefarious actions [32]. These methods are classified into packet leashes, cryptographic techniques, and neighbor-based monitoring strate-gies [17].

Packet leash systems seek to thwart wormhole attacks by affixing temporal or geographical data to packets [25]. The two main categories of packet leashes are geographical leashes and temporal leashes. Geographical leashes employ loca-tion-based authentication to guarantee that packets remain within a specified distance, whereas temporal leashes utilize exact timing limitations to inhibit tun-neling across extensive distances (Yang et al.,

Research Article

2018) [26]. These methods are theoretically effective but necessitate synchronization and supplementary hard-ware assistance, hence constraining their practical implementation.

Cryptographic approaches utilize encryption and authentication mechanisms to guarantee secure communication and identify abnormalities resulting from wormholes [21]. Methods like as digital signatures and key exchange protocols, including Diffie-Hellman and RSA, have been employed to thwart unwanted routing manipulations (Ismail et al., 2023) [16]. Nevertheless, cryptographic methods sometimes impose significant processing cost, rendering them less ap-propriate for resource-limited wireless sensor networks (Moundounga & Satori, 2024) [10].

Neighbor-based monitoring methods utilize the cooperative characteristics of sensor nodes to identify anomalies in network behavior [24]. Nodes consistently monitor their neighbors and analyze transmission patterns to identify anomalies that could signify a wormhole attack (Zahra et al., 2022) [12]. Although effective, these strategies may be susceptible to collusion attacks and necessitate increased communication overhead [36].

Although effective, conventional detection approaches encounter drawbacks like elevated computational expenses, dependence on supplementary technology, and susceptibility to advanced attack tactics [18]. As a result, contemporary ma-chine learning methodologies have arisen as a viable alternative [19].

2.3 Machine Learning-Based Methods for Wormhole Attack Detection

Machine learning (ML) has substantially improved wormhole attack detection through adaptive and data-driven threat identification [20]. Machine learning methodologies utilize several strategies, such as supervised learning, unsuper-vised learning, reinforcement learning, and hybrid models, to improve detection precision and efficacy.

Supervised learning techniques employ labeled datasets to train models that can differentiate between regular and harmful network activities [19]. Decision trees, support vector machines (SVMs), and deep learning architectures, includ-ing long short-term memory (LSTM) networks, have been utilized to proficiently categorize network traffic patterns (Pawar & Anuradha, 2020) [2]; (Affane & Satori, 2024) [3]. Although very accurate, supervised methods necessitate sub-stantial labeled datasets, which may not always be accessible.

Unsupervised learning methods, including clustering algorithms, operate with-out labeled data and identify anomalies by recognizing departures from typical network activity [19]. K-means clustering and autoencoders have been utilized to detect suspicious links created by wormhole tunnels (Ali et al., 2022). [22]. These methodologies are beneficial for practical implementations where labeled attack data is limited [20].

Reinforcement learning (RL) methodologies improve detection adaptability by persistently acquiring appropriate protection methods via contact with the net-work environment. Reinforcement learning-based frameworks have been devel-oped to dynamically modify security rules to counteract wormhole, blackhole, and grayhole attacks (Chourasia & Tokekar, 2024) [5]. Federated learning facili-tates decentralized and privacy-preserving detection by training machine learn-ing models across several nodes without the exchange of sensitive data (Alshehri, 2024). [9] [37].

Hybrid machine learning models integrate many strategies to enhance detec-tion robustness [21]. Ensemble learning combines decision trees, neural net-works, and statistical classifiers to improve prediction accuracy and minimize false positives (Ismail et al., 2023) [16]; (Gebremariam et al., 2023) [23]. Sto-chastic classifier-based techniques enhance attack detection through the integra-tion of probabilistic learning procedures (Moundounga & Satori, 2024). [10].

Machine learning-based methods provide substantial advantages over existing techniques by enabling scalable, adaptable, and efficient detection of wormhole attacks [19]. Nonetheless, issues such as model interpretability, computational complexity, and adversarial attacks must be resolved for extensive implementa-tion in practical WSN settings [21].

Table 2: Summary of Literature on ML-Based Wormhole Attack Detection

Study	ML Technique Used	Performance Metrics	Key Findings
Fatima-tuz-Zahra et al. (2019) [1]	Decision Trees	Accuracy, F1-score	Proposed a rank-based detection framework for Wormhole attack detection

Research Article

			in WSNs.
Pawar & Anuradha (2020) [2]	LSTM	Precision, Recall	Optimized Long Short-Term Memory (LSTM) model for detection and prevention of black-hole and wormhole attacks.
Affane & Satori (2024) [3]	Stochastic Classifier	Detection Rate	Utilized stochastic classifiers to enhance routing security in WSNs by detecting Wormhole attacks.
Abdan & Hosseini Seno (2022) [4]	Support Vector Machine (SVM)	Accuracy, Precision, Recall	Applied SVM for detecting Wormhole attacks in MANETs, achieving high detection rates.
Chourasia & Tokekar (2024) [5]	Reinforcement Learning (RL)	Detection Accuracy	Reinforcement learning-based security policy mitigates wormhole, blackhole, and grayhole attacks in MANETs.
Hanif, Ashraf & Jalil (2022) [6]	AI-based Approaches	F1-score, Detection Rate	Proposed AI-based detection techniques for Wormhole attack detection in WSNs.
Harpal, Tejpal & Sharma (2017) [7]	Machine Learning Techniques	Detection Rate	Applied various ML models, demonstrating their ability to detect Wormhole attacks with varying effectiveness.
Alshehri (2024) [8]	Hybrid ML (Random Forest & SVM)	Accuracy, Precision	Combined RF and SVM for more robust Wormhole attack detection in IoT networks.
Gebremariam, Panda & Indu (2023) [9]	Artificial Neural Networks (ANN)	Accuracy, F1-score	ANN-based detection system for multiple attacks, including Wormhole attacks, with high accuracy.
Saleh, Marouane & Fakhfakh (2024) [10]	Deep Learning & Machine Learning	Detection Rate, Computational Efficiency	Comprehensive analysis of security challenges and countermeasures using deep learning and ML in WSNs.
Ahmad, Wazirali & Abu-Ain (2022) [11]	Random Forest (RF)	Accuracy, Precision, Recall	Explored RF for Wormhole attack detection, achieving high precision and recall in WSN environments.
Alshehri et al. (2024) [12]	Federated Learning	Detection Rate, Computational Efficiency	Developed a federated learning approach for decentralized detection of Wormhole attacks in WSNs.
Xie, Yan, Yao & Atiquzzaman (2019) [13]	Decision Trees & SVM	Accuracy, Detection Rate	Combined decision trees and SVM to improve Wormhole attack detection in large-scale WSNs.
Ismail, El Mrabet & Reza (2023) [14]	Ensemble Learning	Precision, Recall	Implemented ensemble models for enhancing attack detection in WSNs, showing improved detection rate.
Dutta & Singh (2019) [15]	Machine Learning (Various)	Detection Accuracy, F1-score	Provided a review and comparative study of different ML techniques for Wormhole attack detection in WSNs.

3. METHODS

This section delineates the approach utilized to perform a comparative examination of machine learning models aimed at improving wormhole attack detection [18] in wireless sensor networks (WSNs). This study encompasses the selection of machine learning models, acquisition of datasets, application of preprocessing techniques, training of models, and evaluation of metrics.

3.1 Machine Learning Models

This research assesses seven machine learning models about their efficacy in identifying wormhole attacks in wireless sensor networks (WSNs). The selection of models is predicated on their efficacy in classification tasks.

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 3: Comparison of Machine Learning Models

Model	Description	Strengths	Weaknesses
SVM (Support Vector Machine)	Classifies data points based on hyperplane optimization.	High accuracy, good for non-linear data.	Computationally expensive.
KNN (K-Nearest Neighbors)	Classifies instances based on neighbor similarity.	Simple, effective for small datasets.	High computational cost for large data.
RF (Random Forest)	Ensemble learning method using multiple decision trees.	High accuracy, robust to overfitting.	Slower training time.
DT (Decision Tree)	Uses hierarchical decision rules for classification.	Fast, interpretable.	Prone to overfitting.
NB (Naïve Bayes)	Probabilistic classifier based on Bayes theorem.	Works well with small data.	Assumes independence of features.
LR (Logistic Regression)	Linear model used for binary classification.	Simple, interpretable.	Limited to linear relationships.
ANN (Artificial Neural Network)	Neural network model mimicking human brain learning.	High accuracy, suitable for complex patterns.	Requires large data, high computational cost.

3.2 Dataset and Feature Extraction

The dataset utilized for this study consists of traffic logs from wireless sensor networks, gathered using simulation environments that replicate real-world at-tack scenarios [35]. The dataset includes both normal and wormhole attack-infected network traffic data.

Selection of Features:

The key attributes derived from the dataset for model training encompass:

- Packet Delay: Quantifies the duration required for a packet to traverse between nodes.
- Hop Count: The quantity of nodes a packet passes through from source to desti-nation [31].
- RSSI (Received Signal Strength Indicator): Assesses signal strength to identify irregularities [18].

3.3 Preprocessing

To guarantee the dataset's appropriateness for machine learning models, the sub-sequent preprocessing steps were implemented:

- Data Cleaning: Elimination of superfluous or damaged entries.
- Normalization: The standardization of numerical features to a uniform scale.
- Feature Engineering: The development of derived features to improve model efficacy.
- Data Splitting: The dataset was partitioned into 70% for training and 30% for testing to assess model efficacy.

3.4 Model Training and Fine-Tuning

The machine learning models were trained on the preprocessed dataset, with hy-perparameter optimization conducted to enhance performance [33]. The key training parameters were:

- SVM: Kernel selection (linear, RBF), regularization parameter tuning.
- KNN: Optimal K-value determination.
- RF: Number of trees and depth tuning.
- DT: Pruning to prevent overfitting.
- NB: Feature smoothing.
- LR: Learning rate tuning.
- ANN: Optimization of hidden layers, learning rate, and activation functions.

3.5 Evaluation Metrics

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

To assess the effectiveness of each model, we employed multiple evaluation met-rics:

- Accuracy: Measures correct classification.
- Precision: Assesses the reliability of favorable predictions.
- Recall: Assesses the rate of attack detection.
- F1-score: The harmonic mean of precision and recall.
- Computation Time: Assesses model efficiency for real-time implementation.

3.6 Experimental Setup

All experiments were performed in a high-performance computing environment equipped with GPUs. The training procedure utilized an NVIDIA Tesla V100 GPU, 64GB of RAM, and an Intel Xeon Processor. The software stack comprised Python, Scikit-learn, TensorFlow, and Keras, operated in a Jupyter Notebook environment. Models were trained on the training set and validated with a dis-tinct test set, with results averaged across three experimental iterations to verify reliability.

4. RESULT

This section delineates the experimental findings of our comparative research of machine learning models for detecting wormhole attacks in wireless sensor net-works (WSNs). Comprehensive tests were performed utilizing real-world network simulation data to assess the models' efficacy. The efficacy of each model was evaluated using various measures, including accuracy, precision, recall, F1-score, and computational time. The results offer a comparative assessment of the mod-els' advantages and drawbacks in identifying wormhole assaults.

4.1 Performance Comparison of Machine Learning Models

Table 4: Comparative Performance Analysis of ML Models for Wormhole Detection

Model	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-score (%)**	**Computation Time (ms)**
SVM	94.5	92.3	91.8	92.0	350
KNN	88.4	85.6	83.2	84.4	220
RF	95.1	94.0	93.5	93.7	400
DT	90.7	89.1	88.3	88.7	180
NB	85.3	82.0	80.5	81.2	140
LR	87.2	84.8	83.1	83.9	160
ANN	96.2	95.0	94.5	94.7	620

4.2 Graphical Analysis of Model Performance

To better illustrate the comparative performance of different machine learning models for wormhole attack detection, graphical representations of key evalua-tion metrics are provided below. These figures present a visual comparison of accuracy, precision, recall, F1-score, and computational time, offering insights into the efficiency and reliability of each model.

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

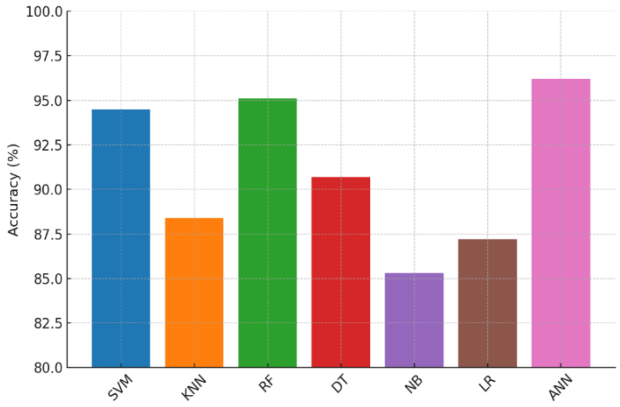

Fig. 4. Accuracy of different ML models for wormhole attack detection.

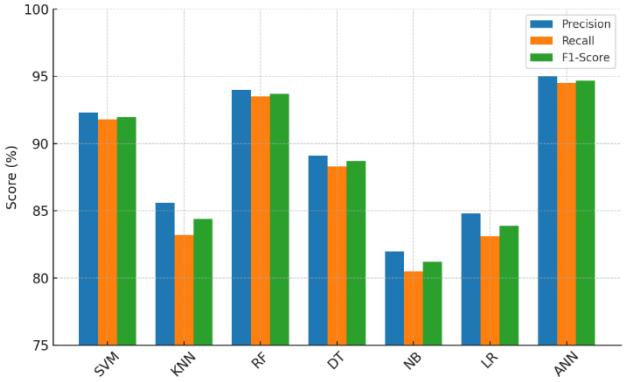

Fig. 5. Comparison of precision, recall, and F1-score among ML models.

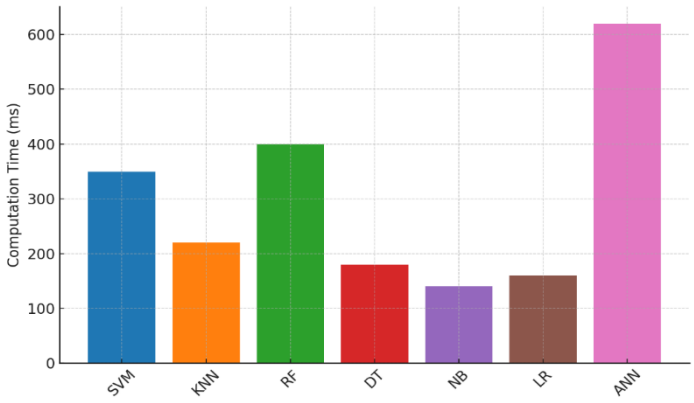

Fig. 6. Computation Time analysis of ML models for wormhole detection.

4.3 Discussion of Results

4.3.1 Accuracy Analysis

Among all the models, the Artificial Neural Network (ANN) achieved the highest accuracy of 96.2%, demonstrating its ability to effectively detect worm-hole attacks. Random Forest (RF) also performed well, with an accuracy of 95.1%, followed by Support Vector Machine (SVM) at 94.5%. These results indi-cate that ANN and RF models have strong generalization capabilities and can effectively distinguish normal network behavior from wormhole attacks.

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

On the other hand, Naïve Bayes (NB) recorded the lowest accuracy at 85.3%, suggesting that its assumption of feature independence might not be well-suited for complex attack patterns. Similarly, K-Nearest Neighbors (KNN) and Logistic Regression (LR) showed moderate accuracy levels of 88.4% and 87.2%, respec-tively. These models may require further optimization or feature selection to enhance their detection capabilities.

4.3.2 Precision, Recall, and F1-Score Analysis

Precision, recall, and F1-score are critical metrics for evaluating the classifica-tion performance of models in detecting wormhole attacks. ANN outperformed all other models, achieving the highest precision (95.0%), recall (94.5%), and F1-score (94.7%), reinforcing its reliability in identifying malicious activities.

Random Forest and SVM also exhibited strong classification abilities, with F1-scores of 93.7% and 92.0%, respectively. These models effectively balance pre-cision and recall, minimizing both false positives and false negatives. Decision Tree (DT) achieved a reasonable F1-score of 88.7%, indicating a good trade-off between detecting attacks and avoiding misclassifications.

Conversely, Naïve Bayes demonstrated the weakest performance, with an F1-score of 81.2%, highlighting its limitations in scenarios where feature relation-ships are crucial. KNN and LR had comparable F1-scores of 84.4% and 83.9%, suggesting that while these models can detect attacks effectively, their classifica-tion consistency is lower than that of more complex models like ANN and RF.

4.3.3 Computational Efficiency

Computational efficiency is a key factor when deploying wormhole detection models in real-world network environments. The analysis reveals that Decision Tree (DT) and Naïve Bayes (NB) were the fastest models, with computation times of 180 ms and 140 ms, respectively. These models are ideal for real-time detec-tion applications where low latency is essential.

On the other hand, ANN had the highest computation time of 620 ms, making it the most resource-intensive model. Despite its superior accuracy, the high com-putational cost could be a limiting factor for large-scale deployments. Random Forest and SVM also required relatively higher processing times of 400 ms and 350 ms, respectively, indicating a trade-off between model complexity and infer-ence speed.

KNN and Logistic Regression exhibited moderate computational times of 220 ms and 160 ms, respectively, suggesting that they can provide a balance between detection speed and classification performance. These models may be more suit-able for scenarios where real-time detection is required with constrained pro-cessing resources.

5. CONCLUSION AND FUTURE WORK

5.1 Conclusion

This study presented a comparative analysis of machine learning models for detecting wormhole attacks in Wireless Sensor Networks (WSNs). The research evaluated seven widely used algorithms—Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Random Forest (RF), Decision Tree (DT), Naïve Bayes (NB), Logistic Regression (LR), and Artificial Neural Network (ANN)—based on detection accuracy, precision, recall, F1-score, and computational efficiency. Experimental results revealed that ANN achieved the highest detection accuracy (96.2%), followed by Random Forest (95.1%) and SVM (94.5%), demonstrating their robustness in identifying wormhole attacks. However, ANN exhibited the highest computational cost (620 ms), which may limit its applicability in real-time, resource-constrained WSNs.

On the other hand, Decision Tree and Naïve Bayes models demonstrated the lowest computational overhead, making them viable options for lightweight secu-rity solutions, albeit with slightly lower detection performance. The findings in-dicate that there is a trade-off between model complexity, accuracy, and compu-tational efficiency, which must be considered when deploying machine learning-based security mechanisms in WSNs. This study contributes to the ongoing re-search on network security by providing insights into the strengths and limita-tions of different machine learning approaches for wormhole attack detection.

5.2 Future Work

Research Article

While the study successfully identified the most effective machine learning mod-els for detecting wormhole attacks, several areas warrant further investigation:

- Hybrid Model Development: Combining multiple models, such as ANN with Random Forest or SVM, may improve detection performance while reducing computational overhead. Developing an optimized ensemble learning ap-proach could enhance real-time attack detection.
- Feature Selection and Dimensionality Reduction: Applying advanced feature selection techniques, such as Principal Component Analysis (PCA) or Genetic Algorithms, could help reduce redundant data and improve classification effi-ciency, especially for large-scale WSNs.
- Real-World Deployment and Validation: The models evaluated in this study were tested using simulation data. Future research should involve real-world network deployments to validate the models' performance under practical con-straints, including dynamic network topologies and varying environmental conditions.
- Adversarial Attack Resilience: Machine learning models are susceptible to adversarial attacks that can manipulate data inputs to deceive detection mech-anisms. Developing adversarially robust models for wormhole detection is crucial for enhancing WSN security.
- Integration with Distributed and Federated Learning: Since WSNs operate in decentralized environments, implementing federated learning could enable collaborative model training across distributed sensor nodes while preserving data privacy.
- Energy-Efficient Models for Resource-Limited Nodes: Given the constraints of WSNs, future work should focus on designing lightweight machine learning models with minimal computational requirements to ensure longer network lifespan and real-time processing.

REFRENCES

[1] Fatima-tuz-Zahra, N., Jhanjhi, S. N., Brohi, S. N., & Malik, N. A. (2019). Proposing a rank and wormhole attack detection framework using machine learning. 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, pp. 1-9. https://doi.org/10.1109/MACS48846.2019.9024821.

[2] Pawar, M. V., & Anuradha, J. (2020). Detection and prevention of black-hole and wormhole attacks in wireless sensor network using optimized LSTM. International Journal of Pervasive Computing and Communications. https://doi.org/10.1108/IJPCC-10-2020-0162.

[3] Affane, A. R., & Satori, H. (2024). Machine learning attack detection based on stochastic classifier methods for enhancing routing security in wireless sensor networks. Ad Hoc Networks, 163, 103581. https://doi.org/10.1016/j.adhoc.2024.103581.

[4] Abdan, M., & Hosseini Seno, S. A. (2022). Machine learning methods for intrusive detection of wormhole attack in mobile ad hoc network (MANET). Wireless Communications and Mobile Computing, 2022, Article ID 2375702, 12 pages. https://doi.org/10.1155/2022/2375702.

[5] Chourasia, A., & Tokekar, S. (2024). Reinforcement learning based security policy to mitigate wormhole, blackhole, and grayhole attacks in MANET. 2nd International Conference on Computer, Communication and Control (IC4), Indore, India, pp. 1-6. https://doi.org/10.1109/IC457434.2024.10486553.

[6] Harpal, Er, Tejpal, G., & Sharma, S. (2017). Machine learning techniques for wormhole attack detection techniques in wireless sensor networks. International Journal of Mechanical Engineering and Technology, 8, 337-348.

[7] Hanif, M., Ashraf, H., & Jalil, Z. (2022). AI-based wormhole attack detection techniques in wireless sensor networks. Electronics, 11(15), 2324. https://doi.org/10.3390/electronics11152324.

[8] Harsanyi, K., Kiss, A., & Tamas, S. (2018). Wormhole detection in wireless sensor networks using spanning trees. Machine Perception Laboratory, MTA SZTAKI. Retrieved December 17, 2018.

[9] Alshehri, A. H. (2024). Wormhole attack detection and mitigation model for Internet of Things and WSN using machine learning. PeerJ Computer Science, 10, e2257. https://doi.org/10.7717/peerj-cs.2257.

[10] Moundounga, A. R. A., & Satori, H. (2024). Stochastic machine learning-based attacks detection system in wireless sensor networks. Journal of Network and Systems Management, 32, 17. https://doi.org/10.1007/s10922-023-09794-5.

[11] Ahmad, R., Wazirali, R., & Abu-Ain, T. (2022). Machine learning for wireless sensor networks security: An overview of challenges and issues. Sensors, 22, 4730. https://doi.org/10.3390/s22134730.

[12] Zahra, F., Jhanjhi, N. Z., Brohi, S. N., Khan, N. A., Masud, M., & AlZain, M. A. (2022). Rank and wormhole attack detection model for RPL-based Internet of Things using machine learning. Sensors, 22, 6765. https://doi.org/10.3390/s22186765.

[13] Delwar, T. S., Aras, U., Mukhopadhyay, S., Kumar, A., Kshirsagar, U., Lee, Y., Singh, M., & Ryu, J.-Y. (2024). The intersection of machine learning and wireless sensor network security for cyber-attack detection: A detailed analysis. Sensors, 24, 6377. https://doi.org/10.3390/s24196377.

[14] Alansari, Z., Anuar, N. B., Kamsin, A., & Belgaum, M. R. (2024). A systematic review of routing attacks detection in wireless sensor networks. PeerJ Computer Science. https://doi.org/10.7717/peerj-cs.1135.

[15] Gebremariam, G. G., Panda, J., & Indu, S. (2023). Localization and detection of multiple attacks in wireless sensor networks using artificial neural network. Wireless Communications and Mobile Computing, 2023, Article ID 2744706, 29 pages. https://doi.org/10.1155/2023/2744706.

[16] Ismail, S., El Mrabet, Z., & Reza, H. (2023). An ensemble-based machine learning approach for cyber-attacks detection in wireless sensor networks. Applied Sciences, 13, 30. https://doi.org/10.3390/app13010030.

[17] Dr. Manish M Patel, Dr. Akshai Aggarwal, Dr. Nirbhay Chaubey; "Countermeasures against Variants of Wormhole in Wireless Sensor Networks: A Review" International Conference on Intelligent Computing & Smart Communication, 19-21 April 2019.

[18] Dr. Manish M Patel, Dr. Akshai Aggarwal, Dr. Nirbhay Chaubey; "Analysis of Wormhole Detection Features in Wireless Sensor Networks" International Conference on Advances in Internet of Things and Connected Technologies, 09-10 May, 2019.

[19] Kongkham, D. (2024). Deep learning algorithms providing security for wireless sensor networks against malicious attacks. International Journal of Internet Protocol Technology, 17(1), 1-8. https://doi.org/10.1504/IJIPT.2024.143761.

[20] Kumari, R., Alenezi, F. A. F., Song, S., & Choi, B.-Y. (2022). ML-AWARE: A machine learning approach for detecting wormhole attack resonance. 2022 IEEE Conference on Communications and Network Security (CNS), Austin, TX, USA, pp. 1-6. https://doi.org/10.1109/CNS56114.2022.10092921.

[21] Saleh, H. M., Marouane, H., & Fakhfakh, A. (2024). A comprehensive analysis of security challenges and countermeasures in wireless sensor networks enhanced by machine learning and deep learning technologies. International Journal of Safety and Security Engineering, 14(2), 373-386. https://doi.org/10.18280/ijsse.140206.

[22] Ali, S., Nand, P., & Tiwari, S. (2022). Detection of wormhole attack in vehicular ad hoc network over real map using machine learning approach with preventive scheme. Journal of Information Technology Management. https://doi.org/10.22059/jitm.2022.86658.

[23] Gebremariam, G. G., Panda, J., & Indu, S. (2023). Design of advanced intrusion detection systems based on hybrid machine learning techniques in hierarchically wireless sensor networks. Connection Science, 35(1), 2246703. https://doi.org/10.1080/09540091.2023.2246703.

[24] Mata, F. M., Muketha, G. M., & Kamau, G. N. (2024). Trust attributes in multi-path congestion avoidance techniques to curb wormhole attacks in wireless sensor networks. Journal of Computer Networks, 12(1), 7-14. https://doi.org/10.12691/jcn-12-1-2.

[25] Singh, R., Singh, J., & Singh, R. (2016). WRHT: A hybrid technique for detection of wormhole attack in wireless sensor networks. Mobile Information Systems, 2016, Article ID 8354930. https://doi.org/10.1155/2016/8354930.

[26] Yang, G., Dai, L., & Wei, Z. (2018). Challenges, threats, security issues and new trends of underwater wireless sensor networks. Sensors, 18(11), 3907. https://doi.org/10.3390/s18113907.

[27] Dutta, N., & Singh, M. M. (2019). Wormhole attack in wireless sensor networks: A critical review. In J. Mandal, D. Bhattacharyya, & N. Auluck (Eds.), Advanced computing and communication technologies (Vol. 702, pp. 151-159). Springer. https://doi.org/10.1007/978-981-13-0680-8_14.

[28] Manish M Patel, Dr. Akshai Aggarwal, Dr. Nirbhay Chaubey; "Detecting Wormhole Attack in Mobility Based Wireless Sensor Networks" International Journal of Communication Networks and Distributed Systems Volume 21, Issue 2, 2018.

[29] Elsayed, W., Elhoseny, M., Sabbeh, S., & Riad, A. (2018). Self-maintenance model for wireless sensor networks. Computers & Electrical Engineering, 70, 799-812. https://doi.org/10.1016/j.compeleceng.2017.12.022.

[30] Kandris, D., Nakas, C., Vomvas, D., & Koulouras, G. (2020). Applications of wireless sensor networks: An up-to-date survey. Applied System Innovation, 3(1), 14. https://doi.org/10.3390/asi3010014.

[31] Manish M Patel, Dr. Akshai Aggarwal, Dr. Nirbhay Chaubey; "Analysis of Wormhole Attack in Wireless Sensor Networks" 5th International Conference on Advanced Computing, Networking and Informatics, 01 - 03 June, 2017.

Research Article

[32] Manish M Patel, Dr. Akshai Aggarwal, Dr. Nirbhay Chaubey; "Performance Evaluation of Wireless Sensor Network in the Presence of Wormhole Attack" 2nd International Conference on Advanced Computing and Intelligent Engineering, 23-25 November, 2017.

[33] Pawar, M. V., & Jagadeesan, A. (2021). Detection of blackhole and wormhole attacks in WSN enabled by optimal feature selection using self-adaptive multi-verse optimiser with deep learning. International Journal of Communication Networks and Distributed Systems, 26(4), 409-445. https://doi.org/10.1504/IJCNDS.2021.115573.

[34] Manish M Patel, Dr. Akshai Aggarwal, Dr. Nirbhay Chaubey; "Variants of Wormhole Attacks in Wireless Sensor Networks" International Conference on Computing Analytics and Networking, 15th -16th December, 2017.

[35] Xie, H., Yan, Z., Yao, Z., & Atiquzzaman, M. (2019). Data collection for security measurement in wireless sensor networks: A survey. IEEE Internet of Things Journal, 6(2), 2205-2224. https://doi.org/10.1109/JIOT.2018.2883403.

[36] Manish M Patel, Dr. Akshai Aggarwal, Dr. Nirbhay Chaubey; "Detection of Wormhole Attack in Static Wireless Sensor Networks" International Conference on Computer Communication and Computational Sciences, October 11-12, 2017.

[37] Alghamdi, R., & Bellaiche, M. (2023). A cascaded federated deep learning-based framework for detecting wormhole attacks in IoT networks. Computers & Security, 125, 103014. https://doi.org/10.1016/j.cose.2022.103014.