A MACHINE LEARNING-BASED APPROACH FOR DETECTING BLACK HOLE ATTACKS IN WIRELESS SENSOR NETWORK

Manisha Kumari[1], **Prof.(Dr) Jagdev Singh Rana**[2]
[1]**Research Scholar, Indus International University, Bathu Una, &** [2]**Professor Computer Science , Indus International University, Bathu Una**

ABSTRACT

Wireless Sensor Networks (WSNs) play an important role in modern communication systems and are widely used in environmental monitoring, healthcare, military surveillance, industrial automation, and smart applications. However, due to their distributed architecture, limited computational resources, and wireless communication characteristics, WSNs are vulnerable to several security attacks. One of the major security threats is the Black Hole Attack, in which a malicious node falsely advertises itself as the most suitable route and drops the data packets received from neighbouring nodes.

Traditional security mechanisms often face difficulties in identifying such malicious activities, particularly in dynamic network environments. This research proposes a Machine Learning-Based Approach for detecting Black Hole Attacks in Wireless Sensor Networks. The proposed approach analyses network traffic and routing behaviour using machine learning algorithms to distinguish between normal and malicious nodes.

Different classification techniques, including Decision Tree, Random Forest, Support Vector Machine (SVM), K-Nearest Neighbour (KNN), and Artificial Neural Network (ANN), are considered for comparative evaluation.

The proposed framework aims to improve attack detection accuracy, reduce false positive rates, and maintain efficient network performance. The study considers important network parameters such as packet delivery ratio, packet loss, energy consumption, detection rate, and end-to-end delay.

Keywords: Wireless Sensor Networks, Black Hole Attack, Machine Learning, Intrusion Detection System, Random Forest, Decision Tree, Network Security.

INTRODUCTION

Wireless Sensor Networks have become an important component of modern communication infrastructure. These networks consist of multiple sensor nodes that communicate wirelessly to collect, process, and transmit information to a central base station or sink node.

WSNs are widely implemented in applications such as smart agriculture, healthcare monitoring, military surveillance, industrial automation, and environmental monitoring.

Despite their advantages, Wireless Sensor Networks face several security challenges because sensor nodes generally operate with limited battery power, processing capabilities, and memory resources.One of the significant security threats in WSNs is the Black Hole Attack.In a Black Hole Attack, a malicious node advertises a false routing message to convince neighbouring nodes that it provides the shortest or most efficient path to the destination. Once the malicious node receives data packets, it drops them instead of forwarding them to the intended destination.

This behaviour results in packet loss, reduced network performance, communication disruption, and decreased reliability.

Traditional security mechanisms may not effectively identify malicious nodes in dynamic network environments. Therefore, machine learning techniques can provide an alternative approach by analysing network behaviour and identifying unusual traffic patterns.

This research focuses on developing a machine learning-based detection framework capable of identifying Black Hole Attacks in Wireless Sensor Networks.

PROBLEM STATEMENT

The increasing use of Wireless Sensor Networks has created a requirement for efficient and intelligent security mechanisms. Black Hole Attacks significantly affect network communication by preventing the successful delivery of data packets.

Existing detection approaches may face the following challenges:

Difficulty in identifying malicious nodes at an early stage.

High false positive detection rates.

Increased packet loss during malicious activities.

Limited computational and energy resources of sensor nodes.

Reduced network performance in the presence of malicious nodes.

Difficulty in maintaining detection efficiency under changing network conditions.

Therefore, there is a need to develop an intelligent detection mechanism using machine learning techniques that can identify Black Hole Attacks while maintaining network efficiency.

RESEARCH OBJECTIVES

The main objectives of this research are:

To investigate the security challenges associated with Black Hole Attacks in Wireless Sensor Networks.

To analyse existing machine learning techniques used for detecting malicious activities in WSNs.

To develop a machine learning-based framework for detecting Black Hole Attacks.

To evaluate the performance of different machine learning algorithms in terms of detection accuracy, precision, recall, and F1-score.

To analyse the impact of Black Hole Attacks on network performance.

To identify an efficient machine learning algorithm for improving the security and reliability of Wireless Sensor Networks.

LITERATURE REVIEW

Machine learning has gained considerable attention in Wireless Sensor Network security because of its ability to identify abnormal network behaviour.

Several researchers have investigated machine learning techniques for detecting different types of attacks in WSNs.

WSN-DS Dataset-Based Intrusion Detection

Almomani et al. (2016) introduced the WSN-DS dataset for intrusion detection in Wireless Sensor Networks. The dataset contains normal network activities and different denial-of-service attacks, including Black Hole, Gray Hole, Flooding, and Scheduling attacks.

The dataset was generated using Network Simulator 2 (NS-2) and contains 23 features. Artificial Neural Networks were used to classify malicious activities.

Machine Learning-Based Intrusion Detection

Gite et al. (2023) investigated machine learning-based intrusion detection techniques for identifying different attacks in Wireless Sensor Networks. Their research considered C4.5 and CART classifiers for identifying malicious network behaviour.

Deep Learning-Based Detection

Salmi and Oughdir (2023) investigated deep learning techniques for detecting denial-of-service attacks in Wireless Sensor Networks using the WSN-DS dataset. Their study considered different deep learning architectures, including CNN, RNN, and DNN.

Existing Security Mechanisms

Recent research has also explored reputation-based approaches for detecting and avoiding Black Hole Attacks. Such approaches analyse node behaviour and routing reliability to identify potentially malicious nodes.

However, computational overhead, energy efficiency, false detection, and adaptability remain important research considerations.

RESEARCH GAP

Based on the reviewed literature, the following research gaps can be investigated:

Many existing studies focus primarily on classification accuracy rather than overall network performance.

The computational and energy requirements of machine learning algorithms need further investigation in resource-constrained WSN environments.

The effectiveness of different machine learning algorithms under varying network conditions requires comparative evaluation.

False positive and false negative detection rates remain important considerations.

The ability of detection frameworks to identify malicious nodes under changing network conditions requires further investigation.

The present study addresses these research concerns through a comparative machine learning-based detection framework.

DATASET DESCRIPTION

The WSN-DS dataset can be used for the proposed research.

It contains 374,661 records and five traffic categories:

Normal

Blackhole

Grayhole

Flooding

Scheduling

The dataset was generated using NS-2 simulation and the LEACH routing protocol.

Table 1: Dataset Distribution

Traffic Class	Records
Normal	3,40,066
Blackhole	10,049
Grayhole	14,596
Flooding	3,312
Scheduling	6,638

For the main experiment, only Normal and Blackhole records will be selected.

Table 2: Selected Dataset

Class	Records
Normal	3,40,066
Blackhole	10,049
Total	3,50,115

PROPOSED METHODOLOGY

The proposed research adopts an experimental approach to detect Black Hole Attacks using machine learning algorithms.

The methodology consists of the following stages:

Dataset Collection

The WSN-DS dataset will be considered for model development and evaluation.

It contains network traffic records representing normal and malicious activities.

Additional simulation data can be generated using NS-2 or NS-3 to evaluate Black Hole Attack behaviour under different network conditions.

Data Preprocessing

The collected dataset will undergo preprocessing to improve data quality.

The preprocessing activities include:

Removal of duplicate records.

Handling missing values.

Feature selection.

Data normalization.

Encoding categorical variables.

Training and testing data separation.

Feature Selection

Important network parameters will be selected for identifying malicious behaviour.

These may include:

Packet delivery ratio.

Packet drop rate.

Forwarding behaviour.

Packet transmission rate.

Routing information.

Energy consumption.

Network delay.

Node communication behaviour.

Machine Learning Algorithms

The proposed framework considers five algorithms.

Decision Tree

Decision Tree is a supervised machine learning algorithm that classifies network activities through decision rules. It can identify suspicious routing behaviour using selected network features.

Random Forest

Random Forest uses multiple decision trees to improve classification performance. It can provide better generalization and reduce overfitting compared with a single decision tree.

Support Vector Machine (SVM)

SVM identifies an optimal decision boundary between normal and malicious network activities.

K-Nearest Neighbour (KNN)

KNN classifies network activities according to the similarity between observations. It assigns a class based on the majority class among the nearest neighbouring observations.

Artificial Neural Network (ANN)

ANN uses interconnected computational units to identify complex patterns in network traffic and classify suspicious activities.

Model Training and Testing

The dataset will be divided into training, validation, and testing subsets.

The machine learning models will be trained using labelled network traffic records.

After training, their performance will be evaluated using unseen testing data.

Stratified data splitting and cross-validation will be considered to ensure reliable evaluation.

PROPOSED SYSTEM ARCHITECTURE

The proposed framework consists of the following components:

Wireless Sensor Network Environment.

Network Traffic Collection.

Dataset Preprocessing.

Feature Extraction and Selection.

Machine Learning Classification.

Malicious Node Identification.

Detection and Alert Mechanism.

The system will monitor network activities and analyse node behaviour.

When the machine learning model identifies suspicious activity, the system will classify the corresponding node as potentially malicious.

An alert mechanism can subsequently inform the network administrator or base station.

MATHEMATICAL MODELLING

The performance of the proposed framework will be evaluated using mathematical parameters.

Let:TP = True Positive

TN = True Negative

FP = False Positive

FN = False Negative

Accuracy

Accuracy measures the proportion of correctly classified instances.

Accuracy = (TP + TN) / (TP + TN + FP + FN)

Precision

Precision measures the proportion of correctly identified malicious instances among all instances predicted as malicious.

Precision = TP / (TP + FP)

Recall

Recall measures the proportion of actual malicious instances correctly detected.

Recall = TP / (TP + FN)

F1-Score

F1-score represents the harmonic mean of precision and recall.

F1-Score = 2 × (Precision × Recall) / (Precision + Recall)

False Positive Rate

FPR measures the proportion of normal network activities incorrectly cl`assified as malicious.

FPR = FP / (FP + TN)

Table 3: Performance Evaluation Parameters

Parameter	Purpose
Accuracy	Overall classification performance
Precision	Correct attack identification
Recall	Detection capability
F1-Score	Balance between precision and recall
False Positive Rate	Incorrect attack identification
ROC-AUC	Classification capability
Execution Time	Processing efficiency

MATLAB IMPLEMENTATION

MATLAB will be used to implement and evaluate the proposed machine learning models.

The implementation will involve the following steps:

Importing the WSN-DS dataset into MATLAB.

Removing irrelevant and duplicate records.

Selecting Normal and Blackhole traffic records.

Performing data preprocessing.

Dividing the dataset into training and testing subsets.

Implementing Decision Tree, Random Forest, SVM, KNN, and ANN.

Training the classification models.

Testing the models using unseen observations.

Generating confusion matrices.

Comparing the performance of all classifiers.

Table 4: Proposed Algorithm Comparison

1.	**Classification Technique**	**Evaluation**
Decision Tree	Tree-based	Accuracy, Recall
Random Forest	Ensemble Learning	Accuracy, F1
SVM	Margin-based	Precision, Recall
KNN	Distance-based	Accuracy, F1
ANN	Neural Network	Accuracy, AUC

EXPERIMENTAL RESULTS AND DISCUSSION

The experimental evaluation will compare five machine learning algorithms using the selected WSN-DS dataset.

The following performance metrics will be calculated after MATLAB execution.

Table 5: Comparative Performance Analysis

Algorithm	Accuracy	Precision	Recall	F1-Score
Decision Tree	To be calculated	To be calculated	To be calculated	To be calculated
Random Forest	To be calculated	To be calculated	To be calculated	To be calculated
SVM	To be calculated	To be calculated	To be calculated	To be calculated
KNN	To be calculated	To be calculated	To be calculated	To be calculated
ANN	To be calculated	To be calculated	To be calculated	To be calculated

Confusion Matrix

A confusion matrix will be generated for each machine learning algorithm.

It will contain four major components:

True Positive

True Negative

False Positive

False Negative

These values will help evaluate the ability of each model to identify Blackhole attacks.

ROC Curve

The Receiver Operating Characteristic (ROC) curve will be used to evaluate the relationship between True Positive Rate and False Positive Rate.

The Area Under the Curve (AUC) will be calculated to compare the classification performance of different algorithms.

Execution Time

The execution time of each algorithm will also be measured to understand its computational requirements.

EXPECTED OUTCOMES

The proposed research is expected to provide the following outcomes:

Development of an intelligent machine learning-based framework for detecting Black Hole Attacks.

Comparative evaluation of five machine learning algorithms.

Identification of important network features associated with malicious node behaviour.

Improvement in the identification of malicious nodes.

Reduction in false positive detection rates.

Better understanding of the relationship between attack detection and network performance.

Identification of an appropriate machine learning model for WSN security applications.

LIMITATIONS OF THE STUDY

The proposed study has certain limitations.

The WSN-DS dataset is simulation-based and may not represent all real-world network environments.

The dataset is based on a particular routing protocol.

Class imbalance may influence classification performance.

Machine learning models may require additional computational resources.

The proposed binary classification experiment focuses on Normal and Blackhole traffic rather than all attack categories.

CONCLUSION

Black Hole Attacks represent a significant security challenge for Wireless Sensor Networks because malicious nodes can disrupt communication by dropping data packets.

This research proposes a machine learning-based framework for detecting Black Hole Attacks through the analysis of network traffic and routing behaviour.

Different supervised machine learning algorithms, including Decision Tree, Random Forest, SVM, KNN, and ANN, are considered for comparative evaluation.

The proposed framework focuses not only on classification performance but also on network-related parameters such as packet delivery ratio, energy consumption, packet loss, and end-to-end delay.

The final selection of the most effective algorithm will depend on the actual experimental results obtained through MATLAB implementation.

Future research can investigate adaptive detection techniques, deep learning, and reinforcement learning to improve detection capabilities under dynamic network conditions.

REFERENCES

Almomani, I., Al-Kasasbeh, M., & Al-Akhras, M. (2016). WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks. International Journal of Advanced Computer Science and Applications, 7(3). https://doi.org/10.14569/IJACSA.2016.070351

Gite, P., Chouhan, K., Krishna, K. M., Nayak, C. K., Soni, M., & Shrivastava, A. (2023). ML Based Intrusion Detection Scheme for various types of attacks in a WSN using C4.5 and CART classifiers. Materials Today: Proceedings. https://doi.org/10.1016/j.matpr.2021.07.378

Salmi, S., & Oughdir, L. (2023). Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network. Journal of Big Data, 10, 17. https://doi.org/10.1186/s40537-023-00692-w

Hanif, M., Ashraf, H., Jalil, Z., Jhanjhi, N. Z., Humayun, M., Saeed, S., & Almuhaideb, A. M. (2022). AI-Based Wormhole Attack Detection Techniques in Wireless Sensor Networks. Electronics, 11(15), 2324. https://doi.org/10.3390/electronics11152324

An Enhanced Intrusion Detection Model Based on Improved kNN in WSNs. (2022). Sensors, 22(4), 1407. https://doi.org/10.3390/s22041407

Copyright & License:
© Authors retain the copyright of this article. This work is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.