Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Detecting Wormhole Attack in Environmental Monitoring System for Agriculture using Deep Learning

Azizol Abdullah[1,*], Ali Nasser Ahmed Albaihani[1], Baharudin Osman[2], Yahya Omar[3]

[1] Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Jalan Universiti 1, 43400 Serdang, Selangor, Malaysia
[2] School of Computing, Univeristi Utara Malaysia, Sintok, 06010 Bukit Kayu Hitam, Kedah, Malaysia
[3] Faculty of Chemical and Petroleum Engineering, UCSI University, UCSI Heights, Jalan Puncak Menara Gading, Taman Connaught, 56000 Cheras, Kuala Lumpur, Malaysia

ARTICLE INFO

Article history:
Received 17 June 2023
Received in revised form 4 July 2024
Accepted 21 August 2024
Available online 19 September 2024

Keywords:
Security; IoT; wormhole attack; IDS; deep learning; routing attacks

ABSTRACT

The Internet of Things (IoT) is a rapidly growing field that connects various devices and systems to the internet, enabling them to communicate and share data. However, this increased connectivity also makes IoT networks vulnerable to various types of attacks, one of which is the wormhole attack. A wormhole attack is a type of security threat in which an attacker creates a tunnel between two or more nodes in an IoT network, allowing the attacker to intercept, modify or inject malicious packets into the network. This can lead to serious security issues such as unauthorized access, data leakage and network disruption. The problem of wormhole attack detection in IoT networks is a crucial issue that must be addressed. Traditional security methods, such as firewalls and intrusion detection systems, may not be effective in detecting and preventing wormhole attacks, as these attacks are difficult to detect due to the stealthy nature of the attacker. Therefore, there is a need for new and more advanced methods for wormhole attack detection in IoT networks, such as deep learning approaches. The goal of this paper is to use a deep learning approach to detect wormhole attacks in IoT networks and to compare the performance of this approach with traditional machine learning methods. This research paper presents a deep learning approach for wormhole attack detection in Internet of Things (IoT) networks using Long Short-Term Memory (LSTM) model. The proposed method is compared with traditional machine learning techniques which are Decision Tree, and Naive Bayes. The performance of the proposed approach is evaluated using a malware dataset for predicting the type of wormhole attack (WHR). The evaluation metrics used in this study include accuracy, F1 score, precision, recall and confusion matrix. The implementation of the proposed approach is performed using Python programming and the Anaconda Navigator (Spyder notebook) tool. The results show that the proposed LSTM-based approach outperforms traditional machine learning techniques in terms of accuracy and F1 score which is 99% while Decision Tree Model accuracy is 94% and Naïve Bayes Model scores 93%, the output results of this paper demonstrating the effectiveness of deep learning in wormhole attack detection in IoT networks.

* *Corresponding author.*
E-mail address: azizol@upm.edu.my

https://doi.org/10.37934/araset.51.2.153176

1. Introduction

The Internet of Things (IoT) refers to the growing network of interconnected devices, sensors, and systems that are able to collect and share data. These devices can range from simple sensors to complex systems such as self-driving cars and industrial control systems. As the number of connected devices continues to grow, the security of IoT networks has become a critical concern (Paudel & Neupane) [1]. IoT networks are vulnerable to a variety of security threats, including unauthorized access, data breaches, and denial of service attacks. One particularly dangerous type of attack is the wormhole attack, in which an attacker creates a virtual tunnel through the network to intercept and manipulate data. This can have serious consequences, such as causing equipment failure or exposing sensitive information.

To protect IoT networks from these types of attacks, various security methods have been developed, including intrusion detection systems (IDS), firewalls, and encryption. However, many of these solutions are designed for traditional internet applications and may not be suitable for resource constrained IoT networks. Furthermore, as IoT technology continues to evolve and new types of attacks emerge, it is important to continue researching and developing new security solutions to keep IoT networks safe (www.oracle.com/internet-of-things). AODV (Ad hoc On-Demand Distance Vector) and TCP (Transmission Control Protocol) are both networking protocols that are used in different types of networks. AODV is a routing protocol used in mobile ad hoc networks (MANETs) while TCP is a transport protocol used in traditional internet networks.

In terms of security, both AODV and TCP have their own vulnerabilities and potential attack vectors (Sobral *et al.,*) [2]. A wormhole attack is one such attack that can be launched against both AODV and TCP. A wormhole attack in AODV networks involves creating a tunnel between two malicious nodes, through which the attacker can intercept and manipulate network traffic. This can allow the attacker to control the routing of data packets and disrupt the normal operation of the network (Ma *et al.,*) [3].

In TCP networks, a wormhole attack can be used to intercept and delay or reorder packets, disrupting the normal flow of data and potentially causing connection timeouts or other issues (Violettas *et al.,*) [4]. In fact, both AODV and TCP protocols have some vulnerabilities to wormhole attacks, and it is important to be aware of these threats and take steps to mitigate them in order to maintain the security of the network.

Wormhole attacks in Internet of Things (IoT) networks are a serious security concern that can greatly impact the functionality and reliability of IoT systems. In a wormhole attack, an attacker creates a virtual tunnel, or wormhole, between two or more nodes in an IoT network. This tunnel allows the attacker to intercept and redirect network traffic, potentially allowing them to gain unauthorized access to sensitive information or disrupt communication within the network. This type of attack is particularly concerning in IoT networks due to the large number of connected devices and the lack of security measures in many IoT devices. As a result, it is essential to develop effective methods for detecting and mitigating wormhole attacks in IoT networks to ensure the security and reliability of these systems.

Wormhole attacks in wireless networks can be classified based on the number of hidden and participating nodes.

i. Single-hop wormhole attack: In this type of attack, the wormhole link is established between two directly visible nodes. The attacker creates a tunnel between these nodes, and all the packets that are transmitted through this tunnel are captured, modified, or dropped.

ii. Multi-hop wormhole attack: In this type of attack, the wormhole link is established between two or more hidden nodes. The attacker creates a tunnel between these nodes, and all the packets that are transmitted through this tunnel are captured, modified, or dropped.

iii. Participating wormhole attack: In this type of attack, a hidden node participates in the normal communication of the network and establishes a wormhole link with another hidden node. The attacker can capture, modify, or drop the packets that are transmitted through this tunnel.

Wormhole attacks involve the creation of a fake, shorter path within a network that disrupts the normal routing topology by manipulating the distance between nodes (Singh *et al.,*) [5]. The attack is carried out by two malicious nodes that establish a tunnel between them. The first node captures data packets from one location and sends them to the second node, which is located at a distant location. The second node then sends the data packets locally, allowing the attacker to intercept and manipulate network traffic. This type of attack can be easily launched by an attacker without any prior knowledge of the network and without disturbing any legitimate nodes. There are different modes of wormhole attacks, such as hidden and participation modes. Figure 1 illustrates the types of wormhole attacks.

Figure 2 shows an example of a wormhole attack in a wireless sensor network (Hanif *et al.,*) [6]. In hidden modes, packet encapsulation and packet relay are included. In packet encapsulation, each data packet is sent through legal paths only. When one wormhole node receives a data packet, it encapsulates the packet to stop the increasing hop count. In packet relay mode, a wormhole attack can be launched using one node only. This malicious node relays packets of far-located nodes to make them neighbours. In participation modes, high-power transmission and out-of-band are included. In high-power transmission, a single malicious node with a high transmission capability attracts the data packets to follow its path. In the out-of-band mode, two malicious nodes make an out-of-band channel with high bandwidth to create a wormhole tunnel between them.

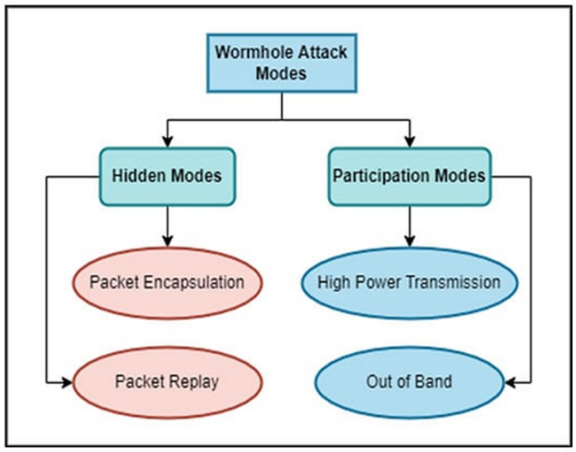

Fig. 1. Types of Wormhole Attacks

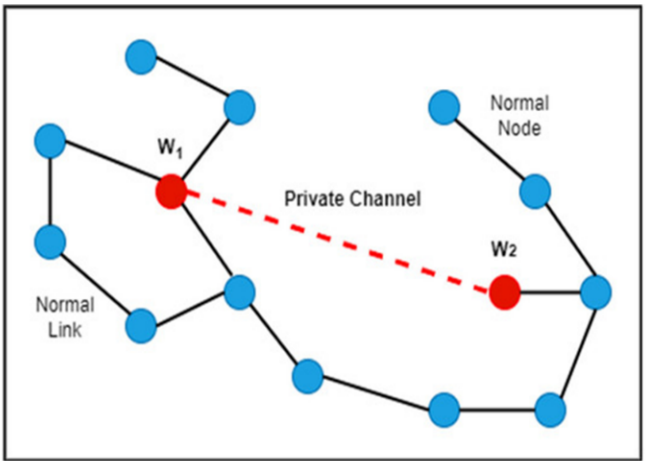

Fig. 2. An example of a wormhole attack in a wireless sensor network

An intrusion detection system (IDS) that can detect wormhole attacks at an early stage has been designed in previous studies [7,8]. However, there is little evidence that intrusion detection systems (IDS) can effectively address the security needs of resource-constrained IoT networks at this time. Existing IDSs are used for either WSN (Wireless Sensor Network) or traditional internet applications.

Security in the Internet of Things and various security attacks on RPL and 6LoWPAN were covered in few research articles [9,10].

It's a challenging task to design a security solution for IoT networks due to many new protocols like DTLS (Choudhury *et al.,*) [11], IPsec (Raza *et al.,*) [12], 6LoWPAN (Verma & Ranga) [13], etc. involved in IoT communication. Wormhole attacks, sinkhole attacks, black hole attacks, selective forwarding attacks and other attacks have an adverse effect on the performance of the Internet of Things network [14-16]. Due to the introduction of many threats in the Internet of Things (IoT) networks, data communication in the Internet of Things is affected. Routing errors are an important factor that affects the security of data communication at the network layer of the IoT protocol stack. Wormhole attacks can cause routing errors, which in turn affect data communication in the Internet of Things.

The Internet of Things (IoT) has witnessed several studies focusing on the use of deep learning techniques to detect wormhole attacks. For example, [17-19] have explored the application of deep learning in intrusion detection and wormhole attack detection in cyber-security networks, IoT networks, and RPL-based IoT, respectively. These studies have made valuable contributions to the field by leveraging deep learning methods to enhance the detection of wormhole attacks. However, despite these advancements, there remain challenges and opportunities for further research. This paper aims to address these challenges and present novel contributions to the detection of wormhole attacks in IoT networks, specifically in the context of environmental monitoring systems for agriculture.

While existing studies have explored deep learning techniques, this research differentiates itself in several key aspects. Firstly, it focuses on the unique domain of environmental monitoring systems for agriculture, which requires tailored security solutions to protect critical agricultural infrastructure. The specific requirements and constraints of such systems, including limited resources and the need for high detection accuracy, present distinct challenges that need to be addressed.

Secondly, this research aims to extend the current state-of-the-art by not only leveraging deep learning approaches but also comparing their performance with traditional machine learning techniques. By conducting a comprehensive evaluation and comparison, including Decision Tree and Naive Bayes models, this study aims to provide insights into the effectiveness of deep learning in detecting wormhole attacks compared to traditional machine learning methods. By conducting a thorough comparative analysis, we aim to demonstrate the superiority of deep learning approach, specifically the Long Short-Term Memory (LSTM) model in detecting wormhole attacks in IoT networks, particularly within the context of environmental monitoring systems for agriculture.

Moreover, this research aims to address the limitations identified in previous studies. While the existing literature has demonstrated promising results, such as high accuracy rates achieved by machine learning algorithms, these studies have often been conducted on limited numbers of nodes or smaller datasets. This research seeks to overcome these limitations by working with larger numbers of nodes and datasets, thereby providing a more realistic evaluation of the proposed approach's effectiveness.

By incorporating insights from the state-of-the-art studies while emphasizing the unique contributions and differentiating factors of this research, we lay the foundation for further exploration of wormhole attack detection in IoT networks, specifically in the domain of environmental monitoring systems for agriculture. The subsequent sections of this paper will delve into the methodology, experimental setup, and evaluation results to showcase the effectiveness and superiority of the proposed approach over existing methods.

To conclude, this research makes a significant contribution to the field by tackling the unique challenges faced by environmental monitoring systems in agriculture. It offers a thorough evaluation

and comparison of deep learning and traditional machine learning methods for detecting wormhole attacks. By doing this, the study aims to enhance the accuracy and positive detection rate, particularly when dealing with larger datasets and a greater number of nodes.

2. Literature Review

The increasing use of the Internet of Things (IoT) has also led to an increase in malicious attacks, with the wormhole attack being a significant threat to the security of IoT networks. Intrusion Detection Systems (IDS) play a crucial role in detecting such attacks at an early stage. Existing IDSs have limitations, particularly when applied to resource-constrained IoT networks. As a result, researchers have explored various approaches, including deep learning techniques, to enhance the detection of wormhole attacks in IoT networks. This literature review aims to summarize and critically analyse the research papers related to detecting wormhole attacks using deep learning in environmental monitoring systems for agriculture.

A comparison of the impacts of black-hole and wormhole attacks in Cloud MANET-enabled IoT for agricultural field monitoring, using the AODV routing protocol was conducted by Safdar Malik *et al.,* [20]. The authors used the NS-3 simulator to measure performance metrics such as throughput, packet delivery ratio, end-to-end delay, and jitter. Their findings indicated that wormhole attacks have a more significant impact on network performance than black-hole attacks.

Another study conducted by Azman *et al.,* [21], evaluated three wireless sensor network routing protocols (AODV, OLSR, and OEG) for agriculture applications. They proposed a novel OEG routing protocol that uses an odd-even criterion to distribute traffic load and reduce congestion. The comparison based on metrics like packet delivery ratio, throughput, energy consumption, routing overhead, fairness index, and passive nodes showed that OEG outperforms AODV and OLSR, especially in large-sized networks. However, OEG has limitations regarding network fairness, which suggests opportunities for future improvements.

Meddeb *et al.,* [22] presented an anomaly-based approach to network traffic patterns, simulating three types of attacks, including packet loss attacks, route interruption attacks, and resource depletion attacks. They used a Support Vector Machine (SVM) classifier to transform their dataset into rules, achieving a high detection rate and efficient identification of Denial of Service (DoS) attacks. However, this study has room for improvement in identifying other types of attacks.

The research by Geethapriya & Chawla [23] developed an IDS using deep learning techniques to detect malicious traffic in IoT networks. They found that using deep learning algorithms for detecting various types of attacks, including wormhole attacks, in IoT networks is both feasible and practical, achieving high precision and recall rates for different attack types.

Another study conducted by Thiyagu *et al.,* [24] proposed a Recurrent Neural Network (RNN) based on LSTM to detect wormhole attacks in IoT networks. The RNN was tested in the Cooja simulator and achieved high accuracy and F1 score of 96%, indicating its effectiveness in detecting wormhole attacks.

Thamilarasu & Chawla [25] proposed an IDS based on Deep Belief Network to identify malicious routing traffic in IoT networks. The proposed IDS demonstrated efficient performance in both real and simulated data scenarios.

Singh *et al.,* [26] proposed a framework for detecting wormhole attacks in Wireless Sensor Networks using artificial intelligence techniques. However, the framework did not fully consider the computation and processing limitations of heterogeneous IoT networks.

A machine learning approach for identifying wormhole attacks in ad hoc networks introduced by Prasad *et al.,* [27]. Their method showed promise in identifying wormhole attacks using critical features and a limited number of nodes in a network simulator.

Bhosale *et al.,* [28] presented a hybrid wormhole mitigation technique called RHE2WADI, which utilized hop count and Received Signal Strength Indicator (RSSI) data to detect malicious nodes in IoT networks. The proposed method achieved a high detection accuracy of up to 95%.

Gulganwa & Jain [29] proposed an unsupervised learning-based method for detecting wormhole attacks using a weighted clustering algorithm. The proposed system collected data from the base station and formed network clusters without disrupting network operations, achieving an accuracy rate of 90%.

Abdan & Seno [30] proposed several machines learning algorithms, including K-Nearest Neighbour (KNN), Support Vector Machine (SVM), Decision Tree (DT), Naive Bayes (NB), and Convolutional Neural Network (CNN) for classification of wormhole attacks in mobile ad-hoc networks (MANET). The results showed varied accuracy for different methods, indicating the potential of different techniques for detecting wormhole attacks.

The literature review highlights the efforts made by researchers to develop effective intrusion detection systems for detecting wormhole attacks in IoT networks, particularly in the context of environmental monitoring systems for agriculture. The use of deep learning techniques and other machine learning algorithms has shown promising results, achieving high detection rates and accuracy. However, there is still room for improvement, especially regarding the adaptability of these methods to resource-constrained IoT networks. Future research should focus on refining the existing techniques to address the unique security challenges posed by IoT environments in agriculture.

3. Methodology

3.1 Research Framework

This research paper focuses on detecting wormhole attacks in IoT network. It consists of three phases:

i. analysis of wormhole attack in the AODV and TCP routing protocols
ii. design and development of detection models using dataset selection, pre-processing, and coding
iii. implementation and analysis of the accuracy of the Decision tree model, Naive Bayes model, and LSTM model. The results are used to evaluate the performance of the models. The research framework is shown in Figure 3.

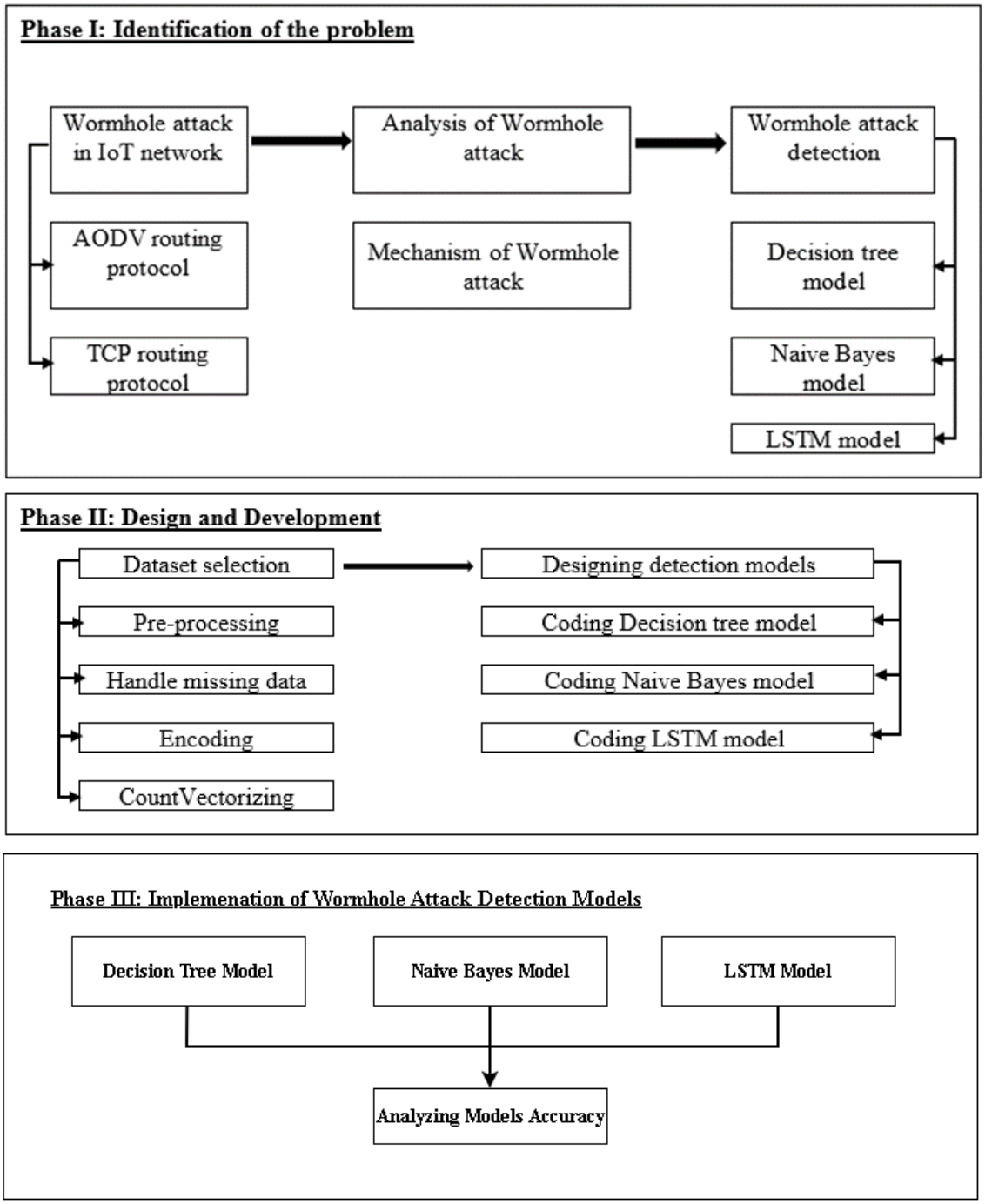

Fig. 3. Research Framework

3.2 Dataset

Malware Dataset were used to achieve the objective of this study which is available online at (https://github.com/anchal27sri/Intrusion-Detection-with-machine-Learning/find/master). It contains 6,37,862 different samples including normal and malicious (normal 1,52,144 and malicious 4,85,718). Moreover, the dataset compiled on 21 selected features and labelled. Indeed, an incomplete field of the dataset is filled with -1. This large dataset introduced into IOT wireless network (AODV, TCP and UDP protocols) to detect the wormhole attacks.

3.3 Data Selection

Data selection is the process of determining the appropriate data type and source, as well as suitable instruments to collect data. It precedes the actual practice of data collection, then this data goes through filtration were the only data that is relevant to the purpose of this study were selected. Therefore, the data selected contains Attack and Normal in the network nodes specifically in AODV and TCP protocols.

3.4 Data Pre-Processing

The dataset can have many irrelevant and missing data. To handle this issue, data pre-processing was done to ensure the dataset is clear for training and obtaining significant accuracy of the wormhole attack detection.

3.5 Missing Data

This situation arises when some data is missing. It can be handled in various ways.

i. Ignore the tuples: This approach is suitable only when the dataset we have is quite large and multiple values are missing within a tuple.
ii. Fill the Missing values: There are various ways to do this task. You can choose to fill the missing values manually, by attribute mean or the most probable value.

In this step, the missing values is replaced by “0”.

3.6 Encoding Categorical Data

That categorical data is defined as variables with a finite set of label values. That most machine learning algorithms require numerical input and output variables. An integer and one hot encoding are used to convert categorical data to integer data. In this step, “0” and “1” are assigned to represent the wormhole attack in the IOT network as “Normal” and “Attack” respectively.

3.7 K-Means Clustering

K-means is an unsupervised learning method for clustering data points. The algorithm iteratively divides data points into K clusters by minimizing the variance in each cluster. Each data point is assigned to one of the K clusters at random. Then, for each cluster, we compute the centroid (functionally the centre) and reassign each data point to the cluster with the closest centroid. This process is repeated until the cluster assignments for each data point no longer change. Figure 4 illustrate the K-means cluster for 175341 network samples.

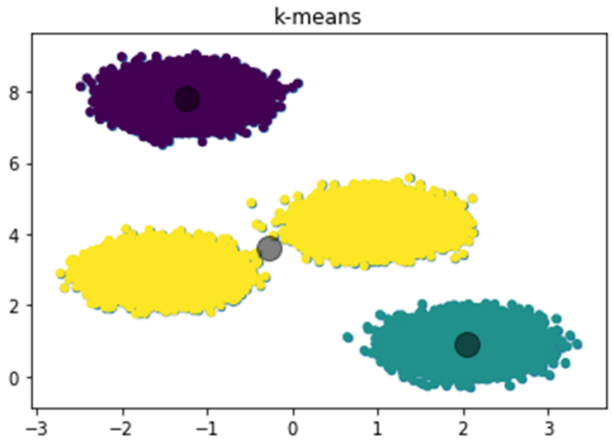

Fig. 4. Illustration K-Means of The Network Samples

Data splitting is the act of partitioning available data into two portions, usually for cross-validator purposes. One Portion of the data is used to develop a predictive model and the other to evaluate the model's performance. Separating data into training and testing sets is an important part of evaluating data mining models. Typically, when you separate a data set into a training set and testing set, most of the data is used for training, and a smaller portion of the data is used for testing. To train any machine learning or Deep learning model irrespective what type of dataset is being used, you have to split the dataset into training data and testing data. In this step, the data splitting details presented in Table 1.

Table 1
Data Splitting Details

x_train shape	574075 samples
y_train shape	574075 samples
x_test shape	63787 samples
y_test shape	63787 samples

4. Results and Discussion

The results generated by Naïve bayes, Decision Tree, and LSTM models of true positive rave, false positive rate, confusion Matrices, and the classification accuracy are discussed in the flowing sections.

4.1 Naive Bayes Model

The performance of a Naive Bayes model in detecting wormhole attacks can vary depending on the specific implementation, the quality of the training data, and the complexity of the wormhole attack. Naive Bayes models are based on the Bayes' theorem and make assumptions about the independence of the features, which may not hold in the case of wormhole attack detection. There have been several studies that have reported the performance of Naive Bayes models in detecting wormhole attacks. However, the performance of Naive Bayes alone is generally not as good as other AI models, such as LSTM which has been studied in this research.

Furthermore, this research conducted an algorithm experiment using Naive Bayes wormhole detection model on the data proposed in the previous chapter. However, the average true and false

positive rate recorded in this model is 36% and 64% respectively. Figure 5 illustrates the graphical result of the true and false positive rate using Naive Bayes.

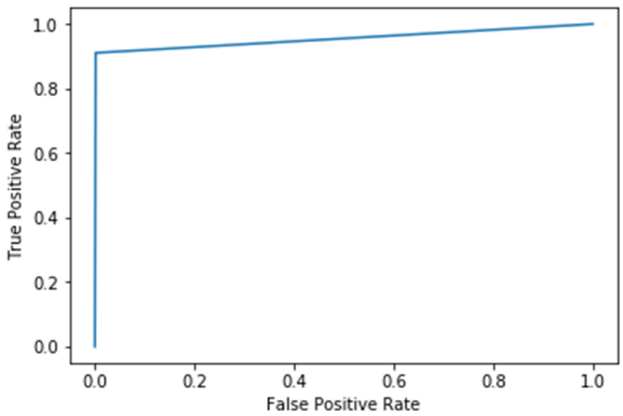

Fig. 5. The output of True Positive Rate Vs False Positive Rate generated by Naive Bayes Model

In the context of a wormhole attack, the true label would refer to the actual presence or absence of a wormhole in the network, while the predicted label would be the output of a detection model that attempts to identify the presence or absence of a wormhole based on the analysis of network data. Figure 6 illustrated the true label vs predicted label using Naive Bayes. Based on the confusion matrix below the predicted absence of wormhole attack by the model and the actual attacked networks are 4342 nodes. Moreover, the predicted wormhole attacks, and it is true these networks got attacked are 44220 nodes. Furthermore, the predicted absence of wormhole attack and the actual absence of wormhole attacks are 15203 nodes. Naive Bayes model predicted wormhole attack, but it did not attack 22 nodes.

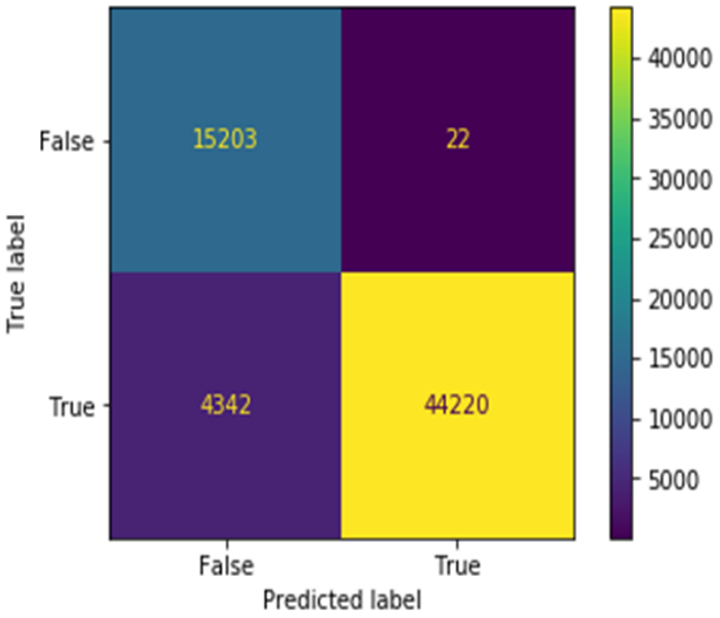

Fig. 6. Confusion Matrices Generated by Naive Bayes Model

Naive Bayes model performance for detecting the wormhole attack through the data is given in Table 2 as well illustrated in Figure 7. The weighted average for F1-score has a value of 93% which

means the balance between precision and recall has a very high percentage in this model. Moreover, the precision of detecting wormhole attack or not utilizing Naive Bayes model has scored 95%.

Table 2
Accuracy Detection Generated by Naive Bayes

Class Name	F1-Score	Precision	Recall
Weighted average (Naive Bayes)	0.93	0.95	0.93

Referring to confusion Matrices above, predicting the number of nodes that has been or has not been attacked by wormhole are significant compared to false predicted. Furthermore, predicting the wormhole attack only using Naive Bayes model as illustrated in Figure 7, has achieved 93%.

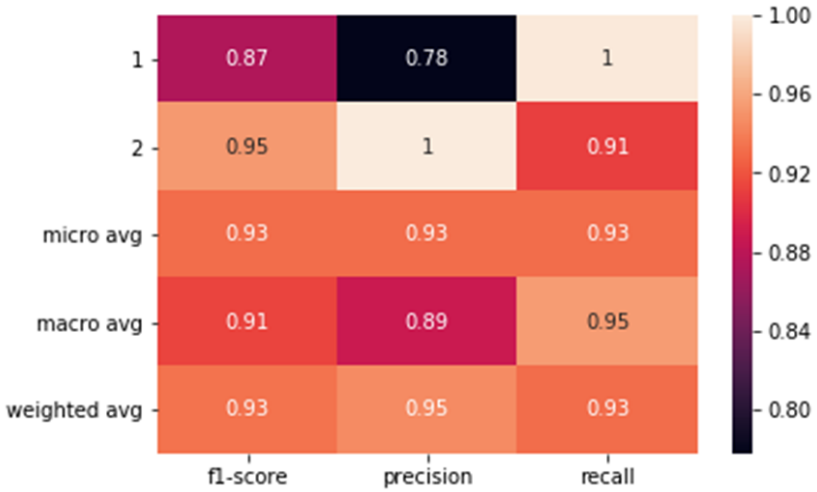

Fig. 7. Accuracy Detection Generated by Naive Bayes

4.2 Decision Tree Model

Detecting the wormhole attack through Decision Tree Model as illustrated in Figure 8 which presented by the true positive rate. The positive rate in this model increased slightly compared to the previous model. However, the TPR in this model recorded 39% which means 39% of the nodes in the given data that is actually attacked by wormhole is predicted or identified by the model. Moreover, identifying the normal nodes or these nodes that were not attacked by wormhole can be presented by the false positive rate (TFR). Decision Tree Model recorded 65% in the given data. Indeed, TPR and TFR enhanced using Decision Tree Model which reflect on increasing the classification accuracy.

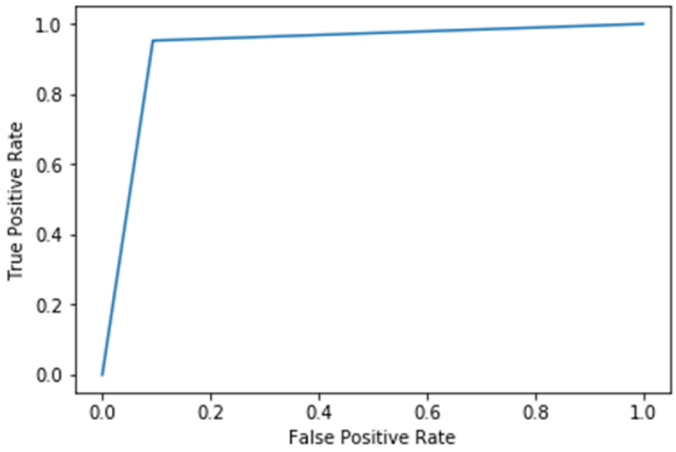

Fig. 8. The Output of True Positive Rate Vs False Positive Rate Generated by Decision Tree Model

Predicting the non-attacked nodes as well the attacked nodes by wormhole are illustrated in Figure 9. The confusion Matrices below presents the true label and the predicted label by Decision Tree Model. The number of nodes that were predicted to be attacked by wormhole 46181 nodes which is correct prediction. Moreover, the prediction of the absence of wormhole attack which is true recorded in 2205 nodes. Furthermore, the prediction of the absence of wormhole attack while it is true there is wormhole attacked are 13950 nodes. total of prediction of the absence of wormhole attack which is true recorded in 1451 nodes.

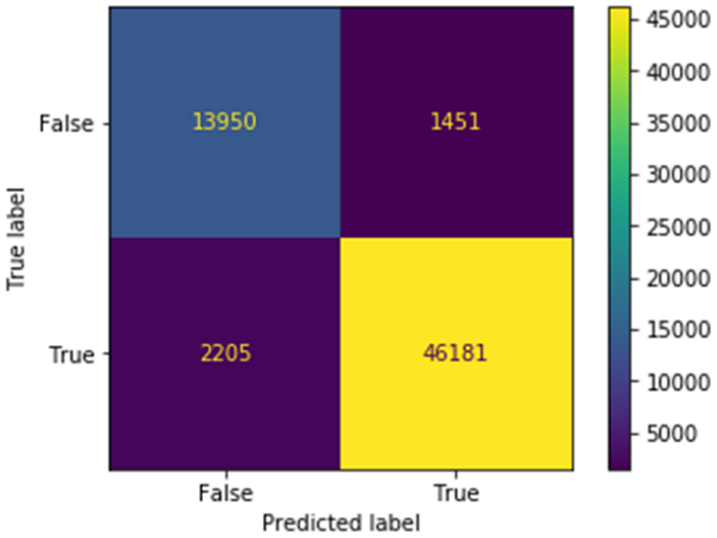

Fig. 9. Confusion Matrices Generated by Decision Tree Model

Figure 10 and Table 3 illustrate the performance accuracy of decision tree model. However, F1-score is the harmonic mean of precision and recall and is a commonly used metric to evaluate the performance of a classification model. An F1-score of 94% means that the model has a good balance between precision and recall. Moreover, Precision is the proportion of true positive predictions out of all positive predictions made by the model. A precision of 94% means that the model correctly identified 94% of wormhole attacks that were predicted by the model. Furthermore, Recall is the proportion of true positive predictions out of all actual positive cases. A recall of 94% means that the model was able to correctly identify 94% of all the wormhole attacks in the dataset.

Table 3
Accuracy Detection Generated by Decision Tree Model

Class Name	F1-Score	Precision	Recall
Weighted average (Decision Tree)	0.94	0.94	0.94

In summary, the decision tree model is doing well in terms of accuracy, as it's able to correctly identify a high proportion of positive and negative cases, and also in terms of balance between precision and recall.

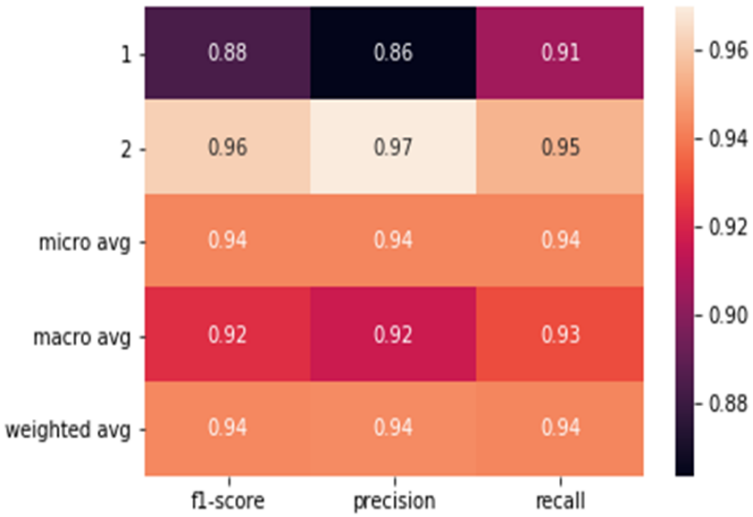

Fig. 10. Accuracy Detection Generated by Decision Tree Model

4.3 LSTM Model

True Positive Rate is a measure of the proportion of wormhole attacks that were correctly identified by LSTM model. Figure 11 illustrates the true positive rate vs false positive rate generated by the model. However, the average true positive rate is 43% which means that the model correctly identified 43% of all wormhole attacks in the dataset IoT networks. Moreover, false positive rate indicates the predicted non-attack wormhole by the model, where the average false positive rate is 79%. Using LSTM model enhanced the detection of wormhole attacks compared to the other models proposed by this study. Furthermore, detailed analysis will be discussed in the coming sections.

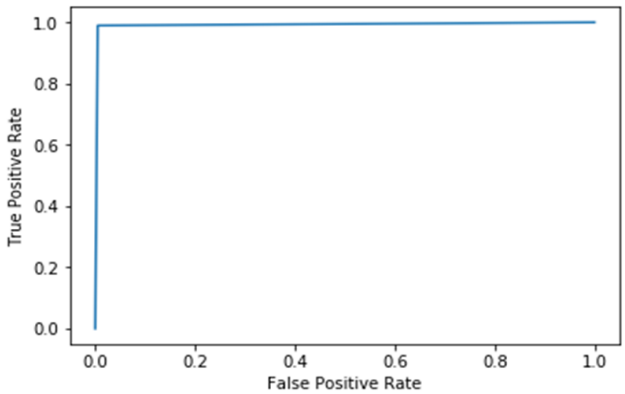

Fig. 11. The Output of True Positive Rate Vs False Positive Rate Generated by LSTM Model

Figure 12 illustrates the confusion Matrices of LSTM model. The predicted wormhole attacks by the model are 47955 nodes, where these nodes submitted to wormhole attacks. Moreover, the predicted non-wormhole attack by LSTM model is 607 nodes but it is true these nodes have been attacked by wormholes. Furthermore, the model predicted there are 15213 nodes that have not been attacked by wormhole while it is true these nodes did not attack by wormhole. Indeed, only 12 nodes from the dataset were not predicted by the model as wormhole attack while it is true these nodes submitted to the type of attack.

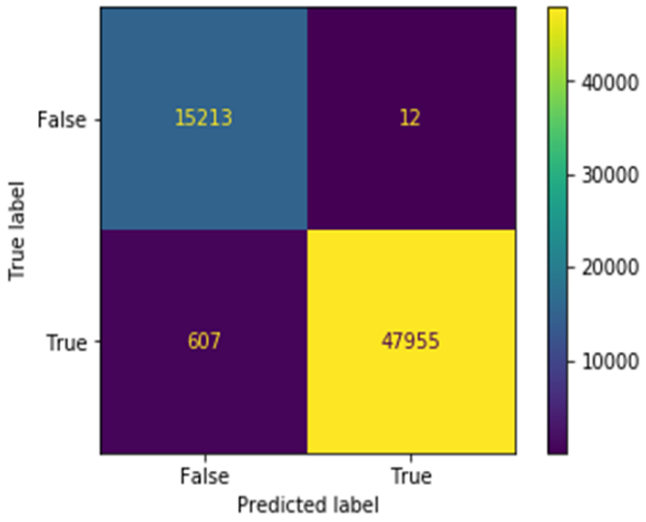

Fig. 12. Confusion Matrices Generated by LSTM Model

Figure 13 illustrates the distribution nodes in the dataset, where the red coloured dots present the detected wormhole attacks, while the dark blue dots represent the non-wormhole attack.

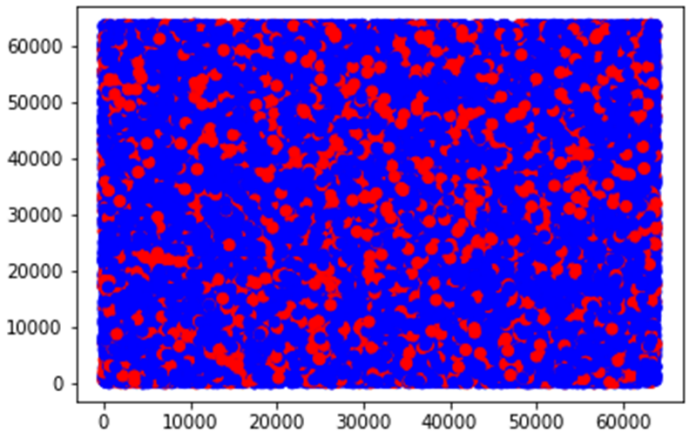

Fig. 13. Distribution Nodes Generated By LSTM Model

F1-score, is a measure of a model's accuracy that balances precision and recall. It is calculated as the harmonic mean of precision and recall, where the best value is 1.0 and the worst value is 0.0. An F1-score of 0.99 indicates that the model has a very high accuracy, as it is close to 1. Moreover, precision is a measure of how many nodes classified as wormhole attack by the model are actually true. A precision of 0.99 means that 99% of the nodes classified as wormhole attack are actually correct these nodes exposed to the type of attack.

Table 4
Accuracy Detection Generated by LSTM Model

Class Name	F1-Score	Precision	Recall
Weighted average (LSTM)	0.99	0.99	0.99

Furthermore, Recall is a measure of how many nodes identified by the models and these identifications are correct . A recall of 0.99 means that the model correctly identifies 99% of the actual attack and unattacked by the wormhole. A F1-score, precision, and recall of 0.99 for an LSTM model indicate that the model is very accurate and perform well on the task it was trained for. Table 4 and Figure 14 presenting the result generated by the algorithm using LSTM model.

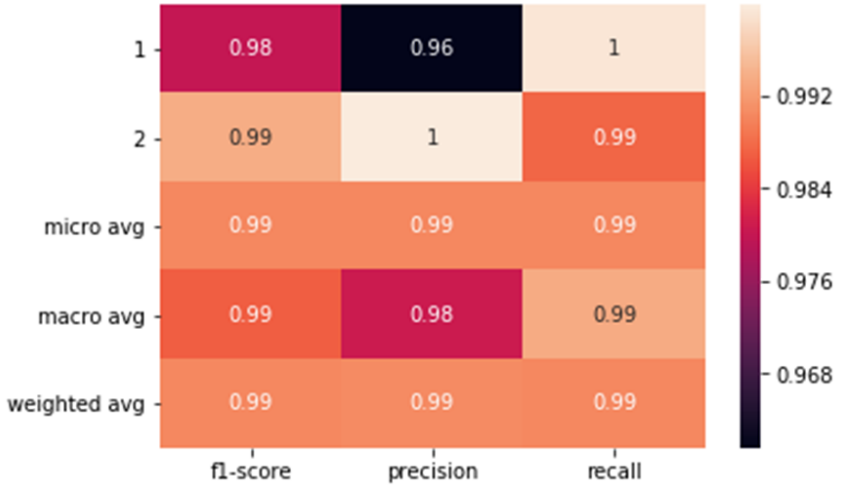

Fig. 14. Accuracy Detection Generated by LSTM Model

4.4 Models Comparison (TPR and TFR)

True Positive Rate (TPR) and false positive rate are a measure of the correct proportion of detection of wormhole attack or non-wormhole attack by the models. In the context of wormhole attack detection, a TPR of 1.0 would mean that the model is able to correctly identify all wormhole attacks, while a TPR of 0.0 would mean that the model is not able to identify any wormhole attacks which means the network is not attacked by the wormhole (TFR). Figure 15 illustrates the true positive rate vs false positive rate generated by the three models. However, the LSTM model has the highest true positive rate among these models. LSTM models gave better results in True Positive Rate (TPR) is their ability to handle long-term dependencies. In the case of wormhole attack detection, for example, an attack may be spread out over a period of time, and an LSTM model can learn to identify patterns that indicate an attack is taking place. Additionally, LSTMs have an internal memory that can store information from previous steps and make decisions based on that information. This can help the model to distinguish between normal and abnormal behaviour.

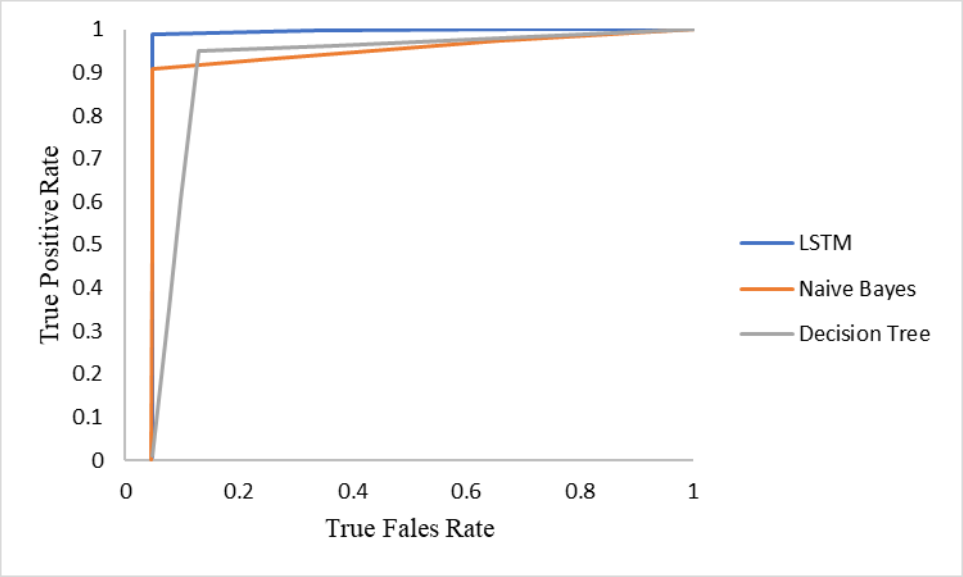

Fig. 15. True Positive Rate Vs False Positive Rate for LSTM, Naive Bayes, and Decision Tree Models

Furthermore, Figure 16 and Figure 17 illustrate the average true positive rate and false positive rate in all models respectively.

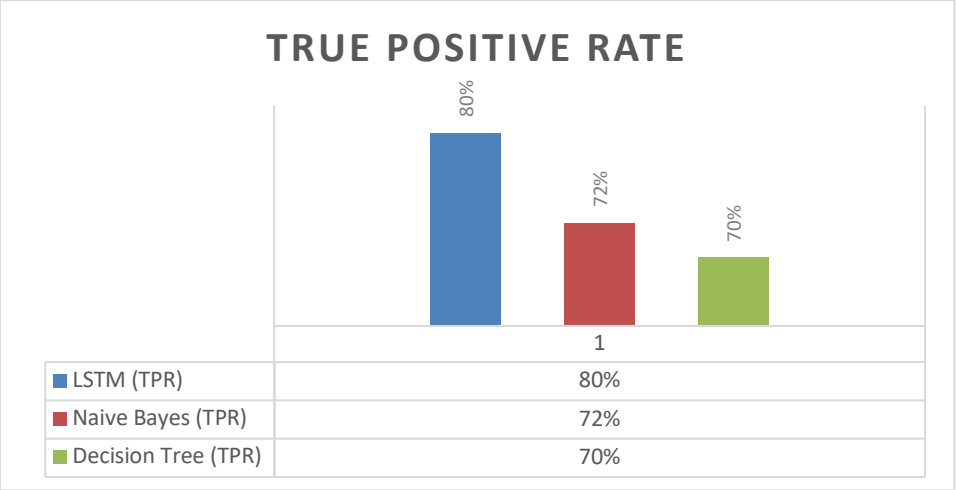

Fig. 16. The Average True Positive Rate LSTM, Naive Bayes, and Decision Tree Models

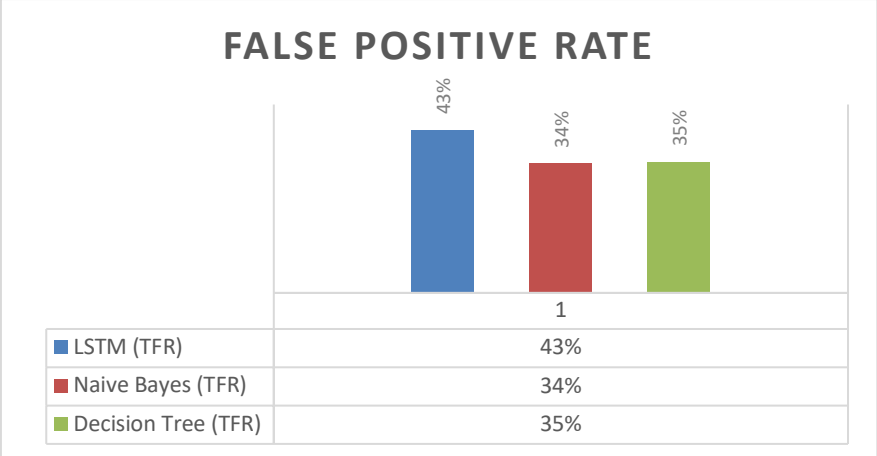

Fig. 17. The Average False Positive Rate for LSTM, Naive Bayes, and Decision Tree Models

4.4.1 Confusion matrices

Table 5 and Figure 18 presenting the number of nodes that are predicted to have wormhole attack on them which is true prediction. However, LSTM model predicted the highest number of nodes that were exposed to wormhole attack with 47955 nodes followed by Decision Tree model with 46181 then lastly Naïve Bayes model with 44220 nodes.

Table 5
The Corrected Prediction of Wormhole Attack on the Total Number of Nodes that Actually attacked by Wormhole

Models	Nodes NO
LSTM (Predicted wormhole attack = presence of wormhole attack)	47955
Naive Bayes (Predicted wormhole attack = presence of wormhole attack)	44220
Decision Tree (Predicted wormhole attack = presence of wormhole attack)	46181

LSTM model is recurrent neural network that is well-suited for processing sequential data, such as network traffic data, and can learn to identify patterns that indicate a wormhole attack.

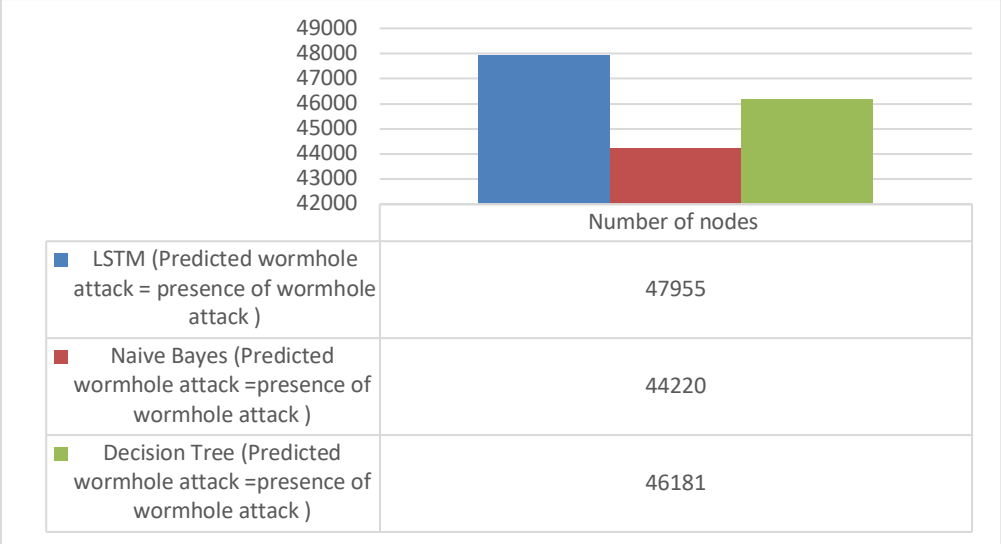

Fig. 18. The Corrected Prediction of Wormhole Attack on the Total Number of Nodes that is Actually Attacked by Wormhole

Table 6 and Figure 19 present the result generated by each model in this study of the total nodes that has been predicted the absence of wormhole attack which is true in the given dataset.

Table 6
The Corrected Prediction of the Absence of Wormhole Attack on the Total Number of Nodes that is Actually Not Attacked by Wormhole

Model	Nodes NO
LSTM (Predicted NO wormhole attack = absence of wormhole attack)	15213
Naive Bayes (Predicted NO wormhole attack = absence of wormhole attack)	15203
Decision Tree (Predicted No wormhole attack = absence of wormhole attack)	13950

Due to the advance mechanism of LSTM model compared to the rest of the models, LSTM model records the highest correct prediction of the absence of wormhole attack with 15213 nodes followed by Naïve Bayes model then Decision Tree model by 15203 and 13950 nodes respectively.

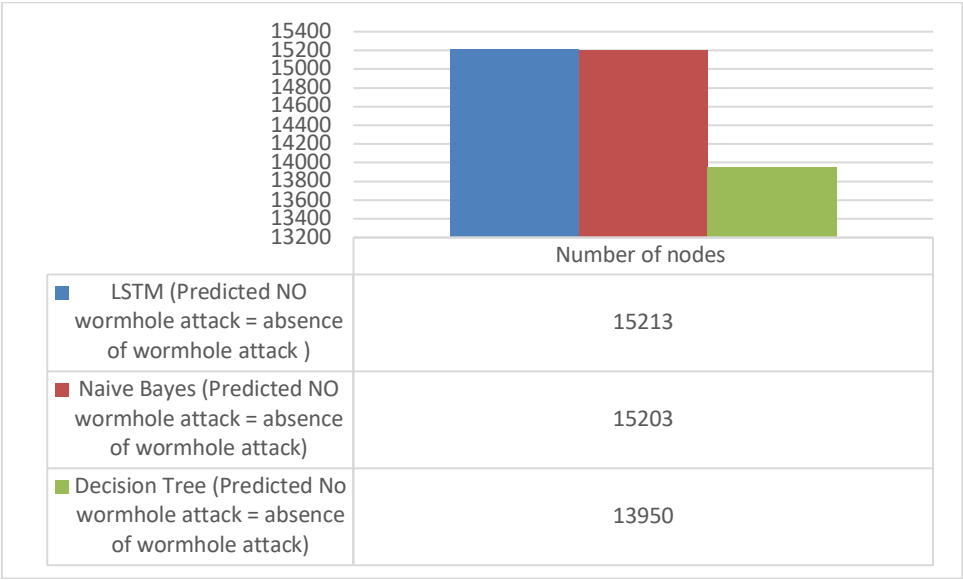

Fig. 19. The Corrected Prediction of the Absence of Wormhole Attack on the Total Number of Nodes that is Actually Not Attacked by Wormhole

Table 7 and Figure 20 present the incorrect prediction of wormhole attack by the models in this study while it is not true where there is no wormhole exposed to the networking nodes. However, slight differences between LSTM model and Naïve Bayes model identify the presence of wormhole attack, where LSTM model misidentifies 12 nodes while Naïve Bayes misidentifies 22 nodes.

Table 1
The Incorrected Prediction of the presence of Wormhole Attack on the Total Number of Nodes that Actually Not Attacked by Wormhole

Models	Nodes NO
LSTM (Predicted wormhole attack = absence of wormhole attack)	12
Naive Bayes (Predicted wormhole attack = absence of wormhole attack)	22
Decision Tree (Predicted wormhole attack = absence of wormhole attack)	1451

Moreover, the Decision Tree model recorded the highest number of nodes that were misidentified as wormhole attack while they are not attacked by wormhole. The number of nodes that was incorrectly predicted is 1451 nodes.

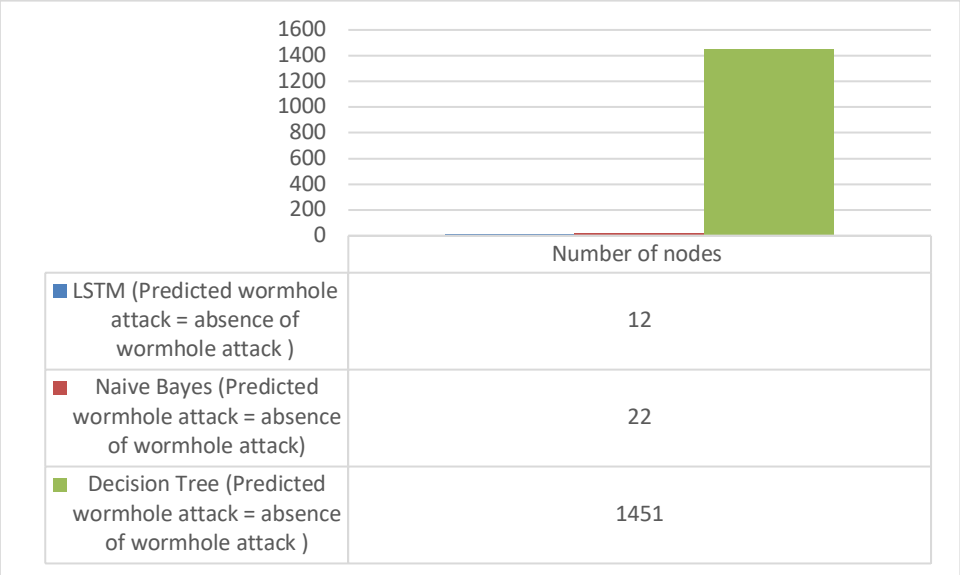

Fig. 20. The Incorrected Prediction of the presence of Wormhole Attack on the Total Number of Nodes that is Actually Not Attacked by Wormhole

Table 8 and Figure 21 illustrate the results generated by LSTM, Naïve Bayes, and Decision Tree models of predicting the absence of wormhole attack while these nodes have been exposed to the attack.

Table 8
The Incorrected Prediction of the absence of Wormhole Attack on the Total Number of Nodes that are Actually Attacked by Wormhole

Models	Nodes No
LSTM (Predicted NO wormhole attack = presence of wormhole attack)	607
Naive Bayes (Predicted NO wormhole attack = presence of wormhole attack)	4342
Decision Tree (Predicted No wormhole attack = presence of wormhole attack)	2205

However, the lowest number of nodes that have been misidentified in this case is recorded by LSTM model with 607 nodes. Decision Tree model has lower number of nodes that incorrectly predicted with 2205 nodes than that was recorded in Naïve bayes model (4342 node).

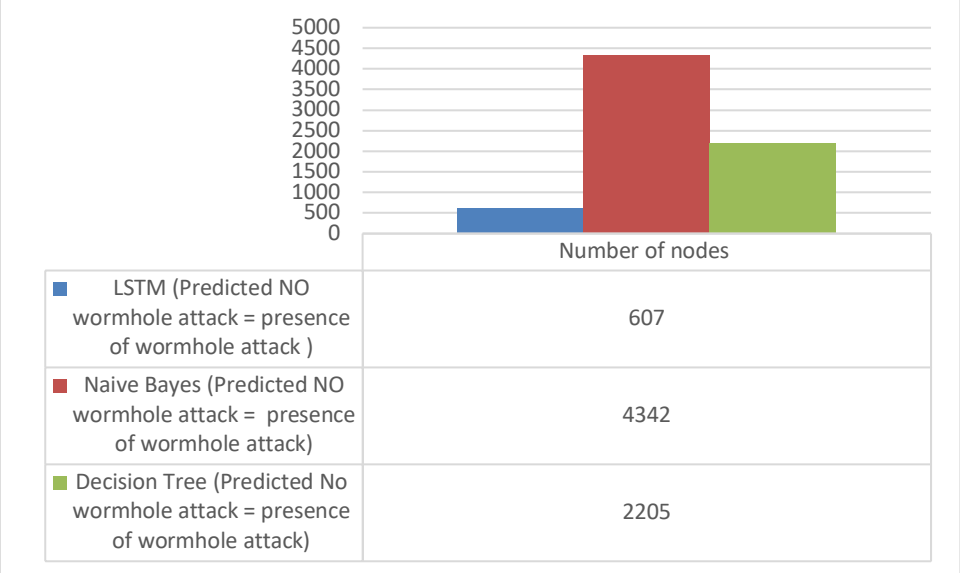

Fig. 21. The Incorrected Prediction of the absence of Wormhole Attack on the Total Number of Nodes that are Actually Attacked by Wormhole

4.4.2 Classification accuracy

The classification accuracy of LSTM, Naive Bayes, and Decision Tree models for wormhole attack detection will depend on several factors, including the quality and quantity of the data used to train and evaluate the models, the specific implementation and configuration of the models, and the characteristics of the wormhole attack being detected. In general, LSTMs are well-suited for processing sequential data, such as network traffic data, and can learn to identify patterns that indicate a wormhole attack. They are often used in wireless sensor networks and other similar applications where the data is time-series in nature. Naive Bayes is a probabilistic classifier based on Bayes' theorem, which is often used for text classification and spam filtering. It can be less accurate than other models for wormhole attack detection, as it makes the "naive" assumption that features are conditionally independent given the class, which may not hold true for network traffic data.

Table 9 and Figure 22 presenting the Classification accuracy of the models have been studied by this paper. However, the best model that scores the highest accuracy in the dataset proposed in this paper is LSTM model with 99% followed by Decision Tree model with 94% and lastly Naïve Bayes model with 93%. LSTM models are a type of Recurrent Neural Network (RNN) that are specifically designed to handle sequential data and maintain information from previous time steps. This makes LSTM well suited for tasks such as time series prediction, language translation, and speech recognition.

Table 2
Classification Accuracy of All the Models

	LSTM Deep Learning	Decision Tree	Naïve Bayes
F1-Score	99%	94%	93%

In the context of wormhole attack detection in IOT network, LSTM models are able to analyse the patterns and trends in the data over time, which allows them to detect the presence of a wormhole attack more effectively than Naive Bayes and decision tree models. Additionally, LSTM models can handle high-dimensional and complex data, which makes them well suited for the analysis of the large datasets typically used in IOT network.

In contrast, Naive Bayes and decision tree models are not designed to handle sequential data. They are based on simple probability calculations and decision-making algorithms, respectively, and do not have the ability to maintain information from previous time steps.

In summary, LSTM models are able to handle sequential data, maintain information from previous time steps, and handle high-dimensional and complex data, which makes them well suited for wormhole attack detection in IOT network and thus able to outperform Naive Bayes and decision tree models.

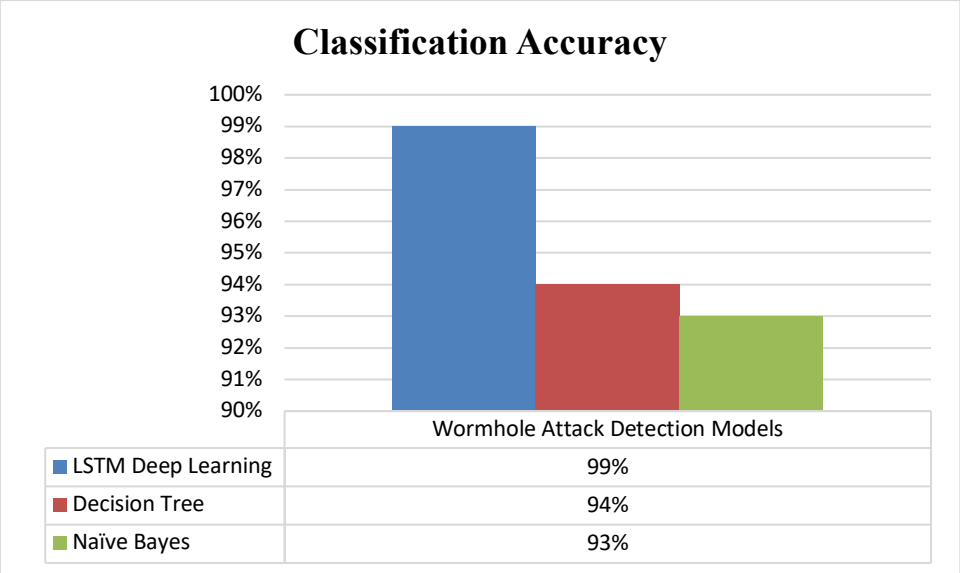

Fig. 22. Classification Accuracy of All the Models

5. Conclusion

In conclusion, this research focused on the challenging task of wormhole attack detection in wireless sensor networks. Several models, including LSTM Deep Learning, Decision Tree, and Naive Bayes, were studied and evaluated. The Naive Bayes model demonstrated a classification accuracy of 93% on the given data, while the Decision Tree model achieved a classification accuracy of 94% on the same data. However, the most promising results were obtained using the LSTM Deep Learning model, which achieved a remarkable classification accuracy of 99% for wormhole attack detection on the proposed dataset. Leveraging the strengths of LSTM in modelling time series data and sequences, the LSTM model exhibited superior performance in detecting wormhole attacks.

In summary, this research highlights the effectiveness of deep learning, particularly LSTM, in addressing the challenges of wormhole attack detection in wireless sensor networks. The findings underscore the potential of advanced machine learning techniques to enhance the security and reliability of IoT networks, especially in the context of environmental monitoring systems for agriculture. Future research may further explore the integration of deep learning models into practical IoT applications to fortify network defences and safeguard critical infrastructures.

6. Recommendation

To improve the accuracy of the AI models in detecting wormhole attacks in IoT networks, it's recommended to add more features to the model which can help it to capture more information about the network and better distinguish between normal and malicious traffic. Furthermore, it's recommended to use ensemble methods, combining multiple models can lead to better performance than using a single model alone. Combining decision tree with other techniques such as Artificial Neural Networks or Support Vector Machines may lead to better performance. Also, it's recommended to validate the test the AI models on different types of networks, and different types of wormhole attacks in order to improve its robustness and adaptability. Additionally, it is important to take into account the effect of node mobility on the detection system, as wormhole attacks are likely to be affected by node mobility.

Acknowledgement
This research received no specific grant from any funding agency in the public, commercial, or not-for profit sectors.

References
[1] Paudel, Nilakantha, and Ram C. Neupane. "A general architecture for a real-time monitoring system based on the internet of things." In *Proceedings of the 2019 3rd International Symposium on Computer Science and Intelligent Control*, pp. 1-12. 2019. https://doi.org/10.1145/3386164.3387295

[2] Sobral, José VV, Joel JPC Rodrigues, Ricardo AL Rabêlo, Jalal Al-Muhtadi, and Valery Korotaev. "Routing protocols for low power and lossy networks in internet of things applications." *Sensors* 19, no. 9 (2019): 2144. https://doi.org/10.3390/s19092144

[3] Ma, Guojun, Xing Li, Qingqi Pei, and Zi Li. "A security routing protocol for Internet of Things based on RPL." In *2017 International conference on networking and network applications (NaNA)*, pp. 209-213. IEEE, 2017. https://doi.org/10.1109/NaNA.2017.28

[4] Violettas, George, Sophia Petridou, and Lefteris Mamatas. "Routing under heterogeneity and mobility for the Internet of Things: A centralized control approach." In *2018 IEEE Global Communications Conference (GLOBECOM)*, pp. 1-7. IEEE, 2018. https://doi.org/10.1109/GLOCOM.2018.8647237

[5] Singh, Moirangthem Marjit, Nishigandha Dutta, Thounaojam Rupachandra Singh, and Utpal Nandi. "A technique to detect wormhole attack in wireless sensor network using artificial neural network." In *Evolutionary Computing and Mobile Sustainable Networks: Proceedings of ICECMSN 2020*, pp. 297-307. Springer Singapore, 2021. https://doi.org/10.1007/978-981-15-5258-8_29

[6] Hanif, Maria, Humaira Ashraf, Zakia Jalil, Noor Zaman Jhanjhi, Mamoona Humayun, Saqib Saeed, and Abdullah M. Almuhaideb. "AI-based wormhole attack detection techniques in wireless sensor networks." *Electronics* 11, no. 15 (2022): 2324. https://doi.org/10.3390/electronics11152324

[7] Kaliyar, Pallavi, Wafa Ben Jaballah, Mauro Conti, and Chhagan Lal. "LiDL: localization with early detection of sybil and wormhole attacks in IoT networks." *Computers & Security* 94 (2020): 101849. https://doi.org/10.1016/j.cose.2020.101849

[8] Sharma, Surbhi, and Baijnath Kaushik. "A survey on internet of vehicles: Applications, security issues & solutions." *Vehicular Communications* 20 (2019): 100182. https://doi.org/10.1016/j.vehcom.2019.100182

[9] Violettas, George, Sophia Petridou, and Lefteris Mamatas. "Evolutionary software defined networking-inspired routing control strategies for the internet of things." *IEEE Access* 7 (2019): 132173-132192. https://doi.org/10.1109/ACCESS.2019.2940465

[10] HaddadPajouh, Hamed, Ali Dehghantanha, Reza M. Parizi, Mohammed Aledhari, and Hadis Karimipour. "A survey on internet of things security: Requirements, challenges, and solutions." *Internet of Things* 14 (2021): 100129. https://doi.org/10.1016/j.iot.2019.100129

[11] Choudhury, Bikramjit, Amitava Nag, and Sukumar Nandi. "DTLS based secure group communication scheme for Internet of Things." In *2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, pp. 156-164. IEEE, 2020. https://doi.org/10.1109/MASS50613.2020.00029

[12] Raza, Shahid, Simon Duquennoy, Tony Chung, Dogan Yazar, Thiemo Voigt, and Utz Roedig. "Securing communication in 6LoWPAN with compressed IPsec." In *2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*, pp. 1-8. IEEE, 2011. https://doi.org/10.1109/DCOSS.2011.5982177
[13] Verma, Abhishek, and Virender Ranga. "Security of RPL based 6LoWPAN Networks in the Internet of Things: A Review." *IEEE Sensors Journal* 20, no. 11 (2020): 5666-5690. https://doi.org/10.1109/JSEN.2020.2973677
[14] Thomas, Lijo, S. Anamalamudi, and S. Anand. *Packet delivery deadline time in 6LoWPAN routing header*. IETF Secretariat, Internet-Draft draft-ietf-6lo-deadline-time-05. txt, 2019.
[15] Kaur, Mandeep, and Manminder Singh. "Internet of Things: challenges and research opportunities." In *Wireless Sensor Networks and the Internet of Things*, pp. 343-350. Apple Academic Press, 2021. https://doi.org/10.1201/9781003131229-24
[16] Karale, Ashwin. "The challenges of IoT addressing security, ethics, privacy, and laws." *Internet of Things* 15 (2021): 100420. https://doi.org/10.1016/j.iot.2021.100420
[17] Chethana, C., Piyush Kumar Pareek, Victor Hugo Costa de Albuquerque, Ashish Khanna, and Deepak Gupta. "Deep learning technique based intrusion detection in cyber-security networks." In *2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon)*, pp. 1-7. IEEE, 2022. https://doi.org/10.1109/MysuruCon55714.2022.9972350
[18] Alghamdi, Rubayyi, and Martine Bellaiche. "A cascaded federated deep learning based framework for detecting wormhole attacks in IoT networks." *Computers & Security* 125 (2023): 103014. https://doi.org/10.1016/j.cose.2022.103014
[19] Zahra, F., N. Z. Jhanjhi, Sarfraz Nawaz Brohi, Navid Ali Khan, Mehedi Masud, and Mohammed A. AlZain. "Rank and wormhole attack detection model for RPL-based internet of things using machine learning." *Sensors* 22, no. 18 (2022): 6765. https://doi.org/10.3390/s22186765
[20] Safdar Malik, Tauqeer, Muhammad Nasir Siddiqui, Muhammad Mateen, Kaleem Razzaq Malik, Song Sun, and Junhao Wen. "Comparison of blackhole and wormhole attacks in cloud MANET enabled IoT for agricultural field monitoring." *Security and Communication Networks* 2022 (2022). https://doi.org/10.1155/2022/4943218
[21] Azman, Amierul Syazrul Azril, Mohamad Yusry Lee, Siva Kumar Subramaniam, and Farah Shahnaz Feroz. "Novel wireless sensor network routing protocol performance evaluation using diverse packet size for agriculture application." *International Journal of Integrated Engineering* 13, no. 4 (2021): 16-28. https://doi.org/10.30880/ijie.2021.13.04.002
[22] Meddeb, Rahma, Farah Jemili, Bayrem Triki, and Ouajdi Korbaa. "Anomaly-based behavioral detection in mobile Ad-Hoc networks." *Procedia Computer Science* 159 (2019): 77-86. https://doi.org/10.1016/j.procs.2019.09.162
[23] Thamilarasu, Geethapriya, and Shiven Chawla. "Towards deep-learning-driven intrusion detection for the internet of things." *Sensors* 19, no. 9 (2019): 1977. https://doi.org/10.3390/s19091977
[24] Thiyagu, T., S. Krishnaveni, and R. Arthi. "Deep learning approach for RPL wormhole attack." In *Intelligent Data Communication Technologies and Internet of Things: Proceedings of ICICI 2021*, pp. 321-330. Singapore: Springer Nature Singapore, 2022. https://doi.org/10.1007/978-981-16-7610-9_23
[25] Thamilarasu, Geethapriya, and Shiven Chawla. "Towards deep-learning-driven intrusion detection for the internet of things." *Sensors* 19, no. 9 (2019): 1977. https://doi.org/10.3390/s19091977
[26] Singh, Moirangthem Marjit, Nishigandha Dutta, Thounaojam Rupachandra Singh, and Utpal Nandi. "A technique to detect wormhole attack in wireless sensor network using artificial neural network." In *Evolutionary Computing and Mobile Sustainable Networks: Proceedings of ICECMSN 2020*, pp. 297-307. Springer Singapore, 2021. https://doi.org/10.1007/978-981-15-5258-8_29
[27] Prasad, Mahendra, Sachin Tripathi, and Keshav Dahal. "Wormhole attack detection in ad hoc network using machine learning technique." In *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1-7. IEEE, 2019. https://doi.org/10.1109/ICCCNT45670.2019.8944634
[28] Deshmukh-Bhosale, Snehal, and Santosh S. Sonavane. "A real-time intrusion detection system for wormhole attack in the RPL based Internet of Things." *Procedia Manufacturing* 32 (2019): 840-847. https://doi.org/10.1016/j.promfg.2019.02.292
[29] Gulganwa, Pooja, and Saurabh Jain. "EES-WCA: energy efficient and secure weighted clustering for WSN using machine learning approach." *International Journal of Information Technology* 14, no. 1 (2022): 135-144. https://doi.org/10.1007/s41870-021-00744-5
[30] Abdan, Masoud, and Seyed Amin Hosseini Seno. "Machine learning methods for intrusive detection of wormhole attack in mobile ad hoc network (MANET)." *Wireless Communications and Mobile Computing* 2022 (2022): 1-12. https://doi.org/10.1155/2022/2375702
[31] Gite, Pratik, Kuldeep Chouhan, K. Murali Krishna, Chinmaya Kumar Nayak, Mukesh Soni, and Amit Shrivastava. "ML Based Intrusion Detection Scheme for various types of attacks in a WSN using C4. 5 and CART classifiers." *Materials Today: Proceedings* 80 (2023): 3769-3776. https://doi.org/10.1016/j.matpr.2021.07.378

[32] Akhtar, Md Amir Khusru, and Mohit Kumar. "Detection of DDoS Attack Using Naive Bayes Classifier." In *Advancements in Security and Privacy Initiatives for Multimedia Images*, pp. 214-225. IGI Global, 2021. https://doi.org/10.4018/978-1-7998-2795-5.ch009

[33] Wang, Xiaojia, Ting Huang, Keyu Zhu, and Xibin Zhao. "LSTM-Based Broad Learning System for Remaining Useful Life Prediction." *Mathematics* 10, no. 12 (2022): 2066. https://doi.org/10.3390/math10122066

[34] Patel, M. A., & Patel, M. M. (2018). "Wormhole attack detection in wireless sensor network." *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*. https://doi.org/10.1109/icirca.2018.8597366

[35] Chu, Ting-Hui, Shu-Yu Kuo, and Yao-Hsin Chou. "Using Quantum-inspired Tabu Search Algorithm with Logic Operation and Moving Average Indicator for Wormhole Attack Detection in a WSN." *Journal of Internet Technology* 20, no. 1 (2019): 167-176.

[36] Verma, Abhishek, and Virender Ranga. "ELNIDS: Ensemble learning based network intrusion detection system for RPL based Internet of Things." In *2019 4th International conference on Internet of Things: Smart innovation and usages (IoT-SIU)*, pp. 1-6. IEEE, 2019. https://doi.org/10.1109/IoT-SIU.2019.8777504

[37] Nandhini, P. S., and B. M. Mehtre. "Intrusion detection system based RPL attack detection techniques and countermeasures in IoT: a comparison." In *2019 International Conference on Communication and Electronics Systems (ICCES)*, pp. 666-672. IEEE, 2019. https://doi.org/10.1109/ICCES45898.2019.9002088

[38] Alenezi, Faheed AF, Sejun Song, and Baek-Young Choi. "WAND: wormhole attack analysis using the neighbor discovery for software-defined heterogeneous internet of things." In *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1-6. IEEE, 2021. https://doi.org/10.1109/ICCWorkshops50388.2021.9473770

[39] Shahid, Hafsa, Humaira Ashraf, Hafsa Javed, Mamoona Humayun, N. Z. Jhanjhi, and Mohammed A. AlZain. "Energy optimised security against wormhole attack in iot-based wireless sensor networks." *Comput. Mater. Contin* 68, no. 2 (2021): 1967-81. https://doi.org/10.32604/cmc.2021.015259

[40] Jhanjhi, N. Z., Sarfraz Nawaz Brohi, Nazir A. Malik, and Mamoona Humayun. "Proposing a hybrid rpl protocol for rank and wormhole attack mitigation using machine learning." In *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*, pp. 1-6. IEEE, 2020.

[41] Maleh, Yassine, Abdelkbir Sahid, and Mustapha Belaissaoui. "Optimized machine learning techniques for IoT 6LoWPAN cyber attacks detection." In *Proceedings of the 12th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2020) 12*, pp. 669-677. Springer International Publishing, 2021. https://doi.org/10.1007/978-3-030-73689-7_64

[42] Lakshmi Narayanan, K., R. Santhana Krishnan, E. Golden Julie, Y. Harold Robinson, and Vimal Shanmuganathan. "Machine learning based detection and a novel EC-BRTT algorithm based prevention of DoS attacks in wireless sensor networks." *Wireless Personal Communications* (2021): 1-25. https://doi.org/10.1007/s11277-021-08277-7

[43] Kaur, Taranpreet, and Rajeev Kumar. "Mitigation of blackhole attacks and wormhole attacks in wireless sensor networks using aodv protocol." In *2018 IEEE International Conference on Smart Energy Grid Engineering (SEGE)*, pp. 288-292. IEEE, 2018. https://doi.org/10.1109/SEGE.2018.8499473

[44] Tiruvakadu, Divya Sai Keerthi, and Venkataram Pallapa. "Confirmation of wormhole attack in MANETs using honeypot." *Computers & Security* 76 (2018): 32-49. https://doi.org/10.1016/j.cose.2018.02.004

[45] Zardari, Zulfiqar Ali, Kamran Ali Memon, Reehan Ali Shah, Sanaullah Dehraj, and Iftikhar Ahmed. "A lightweight technique for detection and prevention of wormhole attack in MANET." *EAI Endorsed Transactions on Scalable Information Systems* 8, no. 29 (2021): e2-e2.

[46] Kfoury, Elie, Julien Saab, Paul Younes, and Roger Achkar. "A self organizing map intrusion detection system for RPL protocol attacks." *International Journal of Interdisciplinary Telecommunications and Networking (IJITN)* 11, no. 1 (2019): 30-43. https://doi.org/10.4018/IJITN.2019010103