Detection of Network Layer Attacks in Wireless Sensor Network

V.Gowtami Annapurna,
Asst. Professor
Computer Science and Engineering
GVPCEW
Visakhapatnam, India
dinavahigowtami@gvpcew.ac.in

K.Anusha
Computer Science and Engineering
GVPCEW
Visakhapatnam, India
19jg1a0556.anusha@gvpcew.ac.in

CH. Kamala Varsha
Computer Science and Engineering
GVPCEW
Visakhapatnam, India
19jg1a0522.varsha@gvpcew.ac.in

M.Deepthi
Computer Science and Engineering
GVPCEW
Visakhapatnam, India
19jg1a0564.deepthi@gvpcew.ac.in

G.Keerthi
Computer Science and Engineering
GVPCEW
Visakhapatnam, India
19jg1a0544.keerthi@gvpcew.ac.in

***Abstract*— The Wireless Sensor Network (WSN) technology is being used in a huge number of monitoring applications. It consists of a large number of sensor nodes with limited battery life. These sensor devices are deployed randomly in a sensor zone to collect the data. But these are threatened and attacked by several malicious behaviors caused by some nodes, which result in security attacks. Several security attacks occur in different layers of the wireless sensor network. Due to these attacks, confidential information can be stolen by attackers or unauthorized users, which can cause several problems for authorized users. Cyber-attacks by sending large data packets that deplete computer network service resources by using multiple computers when attacking are called wormhole and Sybil attacks. It is important to identify these attacks to prevent further damage. To overcome these problems, we use a prediction module that consists of various machine learning algorithms to find the best-performing algorithm. we use XGBoost, Adaboost, Random Forest, and KNN algorithms. To train these algorithms, we have used the WHASA dataset which contains 10 different attacks of the VANET environment and benign (normal) class. By using these algorithms classification of attacks can be done which occur on the computer network service that is " normal " access or access under " attack " by Wormhole and Sybil attack as an output.**

Keywords*— Wireless Sensor Network, XGBOOST, Adaboost, Random Forest, and KNN.

I. INTRODUCTION

In engineering, communication, and networking, new sensor designs, information technologies, and wireless systems have recently been invented. Advanced sensors are used to bridge the gap between the physical and digital worlds. Wireless sensor networks are used in a variety of devices, military surveillance, industries, and machines to help avoid infrastructure failures and accidents conserve natural resources, preserve wildlife, increase productivity, and provide security, among other things. Data from nodes is highly confidential, but some unauthorized users wish to mislead this confidential data through security attacks.

A security attack is an action that jeopardizes the security of an organization's information. These attacks can be launched from any location. The attacker could be a a single person or a group of people. Security attacks are classified as either active or passive. In an active attack, the victim knows whether the attack occurs or not, and the attacker can change or modify the content of the messages, whereas in a passive attack, the victim is unaware of the occurrence of the attack, and the attacker observes or copies the content of the messages.

This paper provides a brief overview of network layer attack detection in Wireless Sensor Networks. The OSI architecture model is used for Wireless Sensor Networks. It has five layers: Application, Transport, Network, Data Link, and Physical, as well as three cross layers: Power Management Plane, Mobility Management Plane, and Task Management Plane. These three cross-layers are primarily used for network control and sensor integration to improve overall network efficiency.

Different types of attacks can occur in different layers of a Wireless Sensor Network. In Wireless Sensor Networks, the Network Layer will be the primary layer for misdirecting information or data, as data routing occurs only in this layer. Wormhole attacks, Flooding attacks, Selective Forwarding, Black Hole attacks, Sinkhole attacks, Sybil attacks, and Replay attacks are examples of network layer security attacks. These attacks and their detection have been discussed in previous studies [3]. Wormhole attack detection and Sybil attack detection are discussed in this paper because these are the two main attacks in the Network Layer of a Wireless Sensor Network.

In any network, a wormhole attack creates a virtual tunnel between two or more nodes. Through that virtual tunnel, two or more nodes can transfer data packets, whereas Sybil attacks, which consist of a malicious node illegally forming an unbounded number of identities, are harmful threats to wireless sensor networks. Because of these types of attacks, security for Wireless Sensor Networks has become a difficult task in today's modern world. As the nodes in Wireless Sensor Networks are attacked by attackers, the information traveling in the network layer nodes is stolen by unauthorized persons. Detection of these types of attacks is required to prevent data/information loss or node damage in Wireless Sensor Networks.

Previous studies [1-15] describe Wireless Sensor Networks, Applications of Wireless Sensor Networks, and different types of attacks that occur in the layers of the

Wireless Sensor Network and how to detect those attacks using various methods. Different types of methods for detecting wormhole attacks and Sybil attacks that can occur in various types of networks such as Wireless Sensor Networks and Ad hoc Networks are explained [4]. [13] describes the VANET environment and how the Bloom filter is used in VANET. VANET is a new network innovation architecture that separates the network data plane and the control plane and has network programmability, centralized management control, and interface opening capabilities.

In this paper, four Machine Learning algorithms are mentioned in the VANET environment for the detection of Wormhole and Sybil attacks: XGBoost, AdaBoost, Random Forest, and KNN. Wormhole and Sybil attacks in the Network Layer of a Wireless Sensor Network can be detected using these algorithms. These four algorithms are used to detect and classify these attacks, regardless of whether the node contains one of these two attacks or not.

II. RELATED WORK

In today's world, securing information has become a difficult problem. Many attackers steal information by employing various types of attacks. Stealing information has become a common occurrence in Wireless Sensor Networks, as attackers use various types of attacks to steal information that is difficult to detect. Wormhole and Sybil's attacks are the most common attacks used by attackers to steal information from Wireless Sensor Networks. To detect these attacks, high-performance algorithms that can detect and classify the type of attack are required. Several research papers are required to put this into action.

Nowadays Wireless Sensor Network technology became more popular as many sectors are using this technology widely. Wireless Sensor Network contains many application and many security threats [1] which are very harmful to the people and their information who are using it. Several countermeasures and defensive techniques are implemented to prevent security threats in Wireless Sensor Networks. To prevent the different types of attacks which are occurred in the Wireless Sensor Network different types of detection methods and possible countermeasures are proposed. The concept was each method and approach has its level of accurate detection. Also mentioned is that these methods are scalable and efficient in various applications of Wireless Sensor Networks [2].

Related to the Wireless Sensor Network, Mobile Ad hoc Network(MANET) is also affected by several types of security attacks [3]. Several types of techniques and measures are taken to detect these attacks. In this paper, mainly network layer attacks are explained with their countermeasures to prevent these attacks. Several security attacks are also occurred in cognitive radios & cognitive radio networks [4]. In this paper, a detailed tabulation of the possible security threats/attacks faced by cognitive radios & cognitive radio networks in the Network layer, along with the current state-of-the-art to detect the attacks and possible countermeasures is discussed. A wormhole attack is one of the major attacks that occur in network layer attacks. Several detection and prevention methods are explained. In this paper [10], some methods give outstanding performance, and some have a few shortcomings. There are several types of methods and techniques to detect the Sybil attack.

Because of the movable nature of VANETs, several issues are appearing in the actual application of this technology. Because VANET operates over a wireless channel, it is more complex to implement. As a result, a rogue node may easily introduce security threats. Such assaults have the potential to disrupt network operations. reviewed denial-of-service attacks and their severity levels in our review study. This paper [9] examines the various strategies for combating denial of service.

As the VANET environment is used for the detection of attacks in Wireless Sensor Networks, [13] proposed a model to use a Bloom filter to deal with the detection of link flooding attacks in the VANET. The model which is described contains two subsystems which are the collector and detector. The classification of the packets is sent to the Bloom filter to determine whether it is abnormal because relevant IP features are stored in the Bloom filter.

In [5] Machine learning algorithms such as the Hidden Markov Model and the XGBoost Algorithm are used for signature-based intrusion detection in intrusion detection systems. Algorithms create classifiers of signatures of specific attacks based on the CICIDS dataset. For intrusion detection, these trained classifiers are tested against user data. Based on the results of the implementation, it is concluded that the extreme gradient boosting algorithm provides higher accuracy and performance than the hidden Markov model algorithm for intrusion detection.

This study [8] proposes an intrusion detection model that is mostly based on XGBoost (Extreme Gradient Boosting) and employs the WOA (Whale Optimization Algorithm) to determine the appropriate settings for it. The experimental results are applied to the well-known KDD CUP 99 data in the computer network field, and when compared to the accuracy of the results obtained by parameter adjustment traditionally, it shows that the intrusion detection model under this method outperforms the methods based on GridSearch-XGBoost, WOA-SVM, and GridSearch-SVM.

In Wireless Sensor Network, [6] proposes a new intrusion detection system based on the K Nearest Neighbor (KNN) classification algorithm. This system can distinguish aberrant nodes from normal nodes by observing their anomalous actions and analyzing the detection system's parameter selection and error rate. By upgrading the wireless ad hoc on-demand distance vector routing protocol, this system has accomplished efficient and speedy intrusion detection (AODV). In this study [7], an AdaBoost ensemble model called Ada-IDS is designed to detect these three ICMPv6-based security exploits in the RPL-based Internet of Things. The suggested model identifies assaults with 99.6% accuracy, with no false alarms. The Ada-IDS ensemble model is used in the IoT network's Border Router to protect the IoT nodes and network.

This study [11] introduces a novel strategy for reducing DDoS traffic on TLD servers. Random Forest is used to classifying traffic on Spark with an accuracy of 99.2%, and a traffic filter based on machine learning techniques is applied to large recursive DNS servers on the Internet. The classification model is constructed on spark and performs with 0.0% FPR and 4.36% FNR, indicating that both accuracy and performance requirements are reached in practice. The results suggest that the model can handle large-

scale DNS query flows and is fast enough to be deployed in practice.

This work [12] provides a method for balancing the dataset using the synthetic minority oversampling technique (SMOTE) and then training the classifier for intrusion detection using the random forest algorithm. The simulations are run on a benchmark incursion dataset, and the random forest approach achieves an accuracy of 92.39%, which is greater than other comparable techniques. The accuracy of the random forest paired with the SMOTE has grown to 92.57% after oversampling the minority samples. This demonstrates that the suggested technique provides an effective solution to the problem of class imbalance and enhances intrusion detection performance.

A method is proposed to detect wormhole and Sybil attacks using a Support Vector Machine (SVM) classifier [14]. The SVM algorithm learns the pattern with the help of training samples, and it predicts the unknown traffic sample to be normal or attacked. To instruct the SVM algorithm 2000 DARPA intrusion detection scenario dataset is taken. Compared with the other simulations the SVM has a lower false positive and higher accuracy.

The combination of SVM and SOM is proposed in this paper [15] to classify wormhole and Sybil attacks. SVM and SOM algorithms are trained by the datasets which are ready-made before the model is used for the testing process. For the filtering of the traffic in the control plane, each protocol contains a dedicated SVM. The simulation indicates that than deploying the SVM and SOM individually, the combination of SVM and SOM has better performance.

III. PROPOSED SYSTEM

Wormhole and Sybil's attacks are widespread threats to wireless sensor networks, even when the attacker does not intend to take any data. Wormhole and Sybil attacks, in general, seek to consume system resources until the target is no longer accessible to provide services. Wormhole and Sybil's assaults are classified into three types: application layer attacks, protocol attacks, and volumetric attacks.

An attacker can use a volumetric assault to exhaust the victim's available resources or bandwidth toward the target. This type of attack might affect not just the data plane in the VANET, but also the controller and southbound interface, because a client host can initiate an inquiry from the data plane to the control plane.

Although there has been much debate regarding wormhole and sybil attacks in VANET and VANET networks, the enormous number of VANET gadgets, as well as the communication link between controllers and switches in VANET, remains a strong opportunity to launch assaults. More validations in the real network are also necessary. Furthermore, VANET's programmability and centralized control provide users with more alternatives for investigating this issue. A volumetric attack is used in this paper.

Wormhole and sybil attacks are identified in this suggested system, which enters the wireless sensor network nodes as one cannot readily detect the assaults and cannot identify which sort of attacks occurred to the network nodes. During the detection process, the nodes may include any of the attacks, such as wormhole or sybil attacks, or they may not contain any of the assaults, indicating that no attack has happened to the node. As a result, three predictions will be made in this study. The wormhole attack and sybil attack contain many types of classes that pertain to them independently.

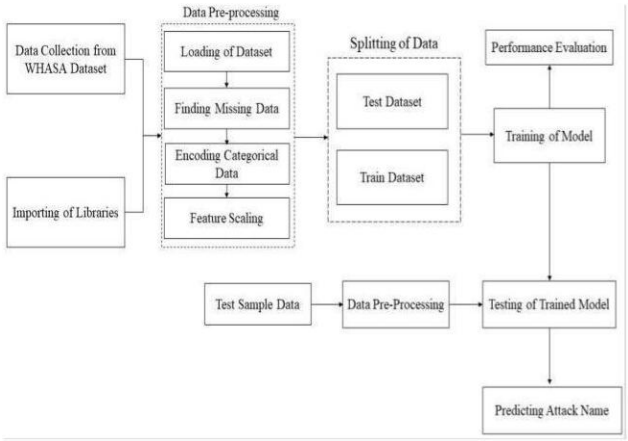

Fig. 1. Proposed System

In Fig. 1, the WHASA dataset is subjected to data preprocessing to normalize the complete dataset; this data preparation includes dataset loading, missing data detection, categorical data encoding, and feature scaling. The WHASA dataset is divided into Test and Train datasets for testing and training of the algorithms. Later, the algorithms XGBoost and KNN will be trained. The performance evaluation is carried out to demonstrate the superiority of the suggested approach. A data preparation test sample is used for the testing of an algorithm that has a high-performance assessment and forecasts the attack name. The attack may be a wormhole attack, a sybil attack, or nothing at all, which was classified as BENIGN.

IV. DATASET

In this paper, the dataset utilized is the WHASA dataset, which comprises benign and up-to-date frequent wormhole and sybil attacks, and which mimics actual real-world data (PCAPs) when compared to other datasets at assaults. It also provides the findings of a network traffic analysis performed using WHASA FlowMeter-V3 that included labeled flows based on the time stamp, source and destination IPs, source and destination ports, protocols, and attack vectors (CSV files).

The creation of realistic background traffic was a primary goal when creating this dataset. The B- Profile system is proposed in this dataset to profile the abstract behavior of human interactions and produce lifelike benign background traffic. For this dataset, the abstract behavior of 25 users was developed based on the HTTP, HTTPS, FTP, SSH, and email protocols so that the identification of the transfer between the nodes may occur to understand the transferring process in packets.

V. ALGORITHMS USED

A. XG Boost Algorithm:

XGBoost is an acronym for Extreme Gradient Boosting. It is a distributed gradient boosting library designed to be very effective, versatile, and portable. It implements machine learning methods using the Gradient Boosting framework. It provides a parallel tree boosting to handle a wide range of data science tasks rapidly and correctly. It is a kind of

gradient-boosted decision tree (GBM) designed primarily to improve speed and efficacy.

Weights are very significant in XGBoost. Before being put into the decision tree that predictions outcomes, each independent variable is assigned a weight. Variables inaccurately predicted by the tree are given greater weight before being transferred to the second decision tree. These many classifiers and predictions are then merged to produce.

Gradient Boosted decision trees are implemented using XGBoost technology. It may be used to tackle regression, classification, ranking, and custom prediction issues.

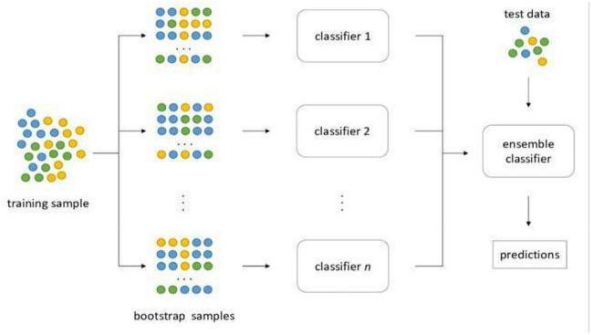

Fig. 2. XGBoost Algorithm

B. *ADABOOST Algorithm:*

AdaBoost, which stands for Adaptive Boosting utilized as an ensemble approach, is a statistical classification meta-algorithm. The most frequent AdaBoost method is one-level decision trees, which are decision trees with only one split. These trees are also known as Decision Stumps. To boost performance, it may be integrated with several different types of learning algorithms. The output of the other learning algorithms ('weak learners') is blended into a weighted sum that reflects the final output of the boosted classifier. AdaBoost is commonly used for binary classification, although it may be expanded to multiple classes or real-line bounded intervals.

Although AdaBoost is often used to combine weak base learners (such as decision stumps), it has been shown to effectively combine strong base learners (such as deep decision trees), providing a more accurate model. When AdaBoost is paired with decision tree learning, the relative 'hardness' of each training sample obtained at each stage of the AdaBoost algorithm is fed into the tree growth algorithm, enabling later trees to focus on harder-to-classify cases. The weight-assigning approach employed after each iteration separates the AdaBoost algorithm from all other boosting algorithms, and it is its most distinguishing characteristic.

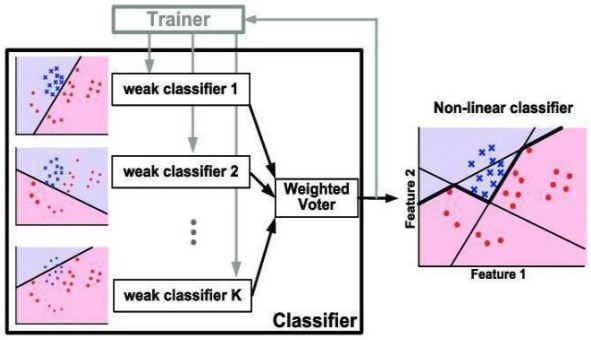

Fig. 3. Ada Boost Algorithm

C. *Random Forest Algorithm:*

Random Forest is a well-known supervised learning machine learning method. It may be used in machine learning to solve classification and regression issues. It is built on the notion of ensemble learning, which is a process in which numerous classifiers are combined to solve a complicated issue and enhance the model's performance. "Random Forest is a classifier that comprises several decision trees on different subsets of the provided dataset and takes the average to enhance the predicted accuracy of that dataset," as the name indicates. Rather than depending on a single decision tree, the random forest aggregates projections from each tree and predicts the final output based on the majority vote of predictions.

Because the random forest mixes numerous trees to forecast the class of the dataset, some decision trees maycorrectly predict the output while others may not. However, when all of the trees are joined, they correctly forecast the outcome. The dataset's feature variable should have some real values so that the classifier can predict correct outcomes rather than guesses. Two conditions for a more successful Random Forest classifier are that each tree's predictions have very low correlations. According to this method, the more trees in the forest, the higher the accuracy and the smaller the danger of over-fitting.

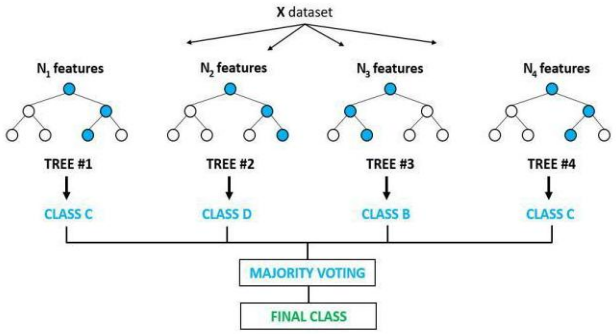

Fig. 4. Random Forest Algorithm

D. *K Nearest Neighbour Algorithm:*

K-Nearest Neighbor, one of the most basic machine learning algorithms, uses the supervised learning technique. It compares the new case's data to previous cases and assigns it to the category that most closely matches those cases. After all of the previous data has been saved, a new data point is categorized using the K-NN algorithm based on similarity. This implies that new data may be swiftly and reliably

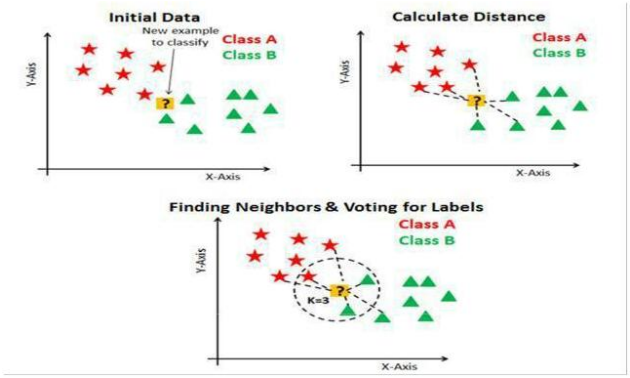

Fig. 5. KNN Algorithm

classified into an appropriate category using the K-NN approach. It may be used for both classification and regression, however, it is most commonly utilized for classification.

Because K-NN is a non-parametric approach, no assumptions about the underlying data are made. It is also known as a lazy learner algorithm since it keeps the training dataset instead of learning from it right away. When categorizing data, it instead utilizes the dataset to execute an action. The KNN method simply saves the dataset throughout the training phase, and when new data is received, it classifies it into a category that is comparable to the present data.

VI. METHODOLOGY

The primary goal of this research is to identify wormhole and sybil attacks at the network layer of a Wireless Sensor Network. Several processes are involved in this procedure, including data collection, library import, data preprocessing, handling missing data, categorical data, feature scaling, and dataset splitting.

A. Collection of Dataset

The WHASA dataset, which is a real-time dataset, is gathered in this work. The WHASA database comprises both benign and recent common wormhole and sybil attacks.

B. Importing Libraries

To use Python for data preparation, a few preset Python libraries are imported in this study. In this work, three specific libraries are used for data preparation:

Numpy:

Numpy The Python module allows you to integrate any type of mathematical operation in your code. This functionality may also be used to add large, multi-dimensional arrays and matrices. Numpy is imported as np in this publication.

Matplotlib:

The second library is the Python 2D charting package matplotlib, which requires the pyplot sub-module to be imported. In the code, this library is used to create any type of chart. Matplotlib is imported as plt in this work from matplotlib.pyplot.

Pandas:

Pandas is an open-source library designed primarily for working with relational or labeled data straightforwardly. It offers several data structures and methods for manipulating numerical data and time series. This library is based on the NumPy library. Pandas is quick, with great performance and productivity for users. This library is used to load the dataset that we gathered. It is used in algorithm modeling. It is imported as pd in this document.

C. Data Preprocessing

Data pre-processing is the process of preparing raw data for use with a machine learning model. It is the first and most critical stage in the development of a machine-learning model. It is not always necessary to clean and prepare data while constructing a machine learning project.

Furthermore, while working with data, cleaning, and formatting is essential. As a result, the data pre-processing job is employed for this. Data Preparation Requirements: Real-world data frequently contains noise, and missing values, and may be in an unfavorable format, making it impractical to directly train machine learning models on it.

1) Handling Missing Data

If the dataset has some missing data, it may pose a significant challenge to the machine learning model. As a result, handling missing values in the dataset is required. There are primarily two methods for dealing with missing data. The first is to delete the specific entry. It is widely used to deal with null values. In this manner, if any particular row or column has null values, it is destroyed. The second method is to compute the mean: In this manner, the mean of the column or row containing any missing value is computed and placed instead of the missing value. This method is appropriate for features that contain numeric data, such as age, income, year, and so on.

2) Categorical Data

Coding Categorical data is data that has categories. For example, the dataset has two numerical and non-numerical category variables. Because machine learning models are primarily reliant on mathematics and numbers, it may be challenging to develop the models if the dataset contained a categorical variable. As a result, these category variables need to be encoded as integers.

3) Feature scaling

The final stage in data preparation is feature scaling. It is a method used in machine learning to normalize the independent variables of a dataset inside a defined range. Variables in the same range and scale are maintained together in feature scaling so that neither variable dominates the other.

D. Splitting of the dataset

Throughout the machine learning data preparation step, the dataset is divided into train and test datasets. It is one of the most essential data pre-treatment steps since it allows the machine learning model's functionality to be improved. To train the machine learning model, the training dataset is used. The test dataset is used to put the machine learning model to the test.

Fig. 6. Splitting of Dataset

In this paper, the dataset is split into 80% for the training and 20% for testing the machine learning model.

E. Software Requirements:

In this paper, Windows is utilized as the operating system, Python and HTML are the coding languages used, and Spyder in Anaconda Framework is the software used to implement the code.

TABLE I. SOFTWARE REQUIREMENTS

REQUIREMENT SPECIFICATION	REQUIREMENTS
Operating System	Windows
Coding Language	Python 3.7, HTML
Software(s)	Anaconda
	Framework, Spyder

VII. RESULT AND ANALYSIS

This section demonstrates the detection of wormhole and sybil attacks in the Wireless Sensor Network's network layer, as well as how the algorithms function and their accuracy. The output of this paper includes a site with buttons for Upload Dataset, Preprocess Dataset, Run XGBoost Algorithm, Run KNN Algorithm, Run AdaBoost Algorithm, Run Random Forest, and Predict Attack from Test Data.

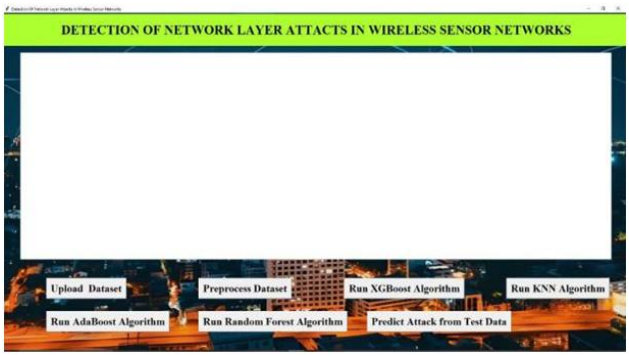

Fig. 7. User interface

Fig 7 is the user interface which contains all the buttons mentioned above with a white screen above those where all the results will be displayed.

When the buttons are pressed, the code is automatically executed, and the output is presented on the screen. The data is uploaded by clicking the Upload Dataset button, and it is then preprocessed by clicking the Preprocess Dataset button. The Run XGBoost Algorithm, Run AdaBoost Algorithm, Run Random Forest Algorithm, and Run KNN Algorithm buttons will launch the XGBoost, AdaBoost, Random Forest, and KNN algorithms, respectively. After pressing those buttons, the screen displays the Accuracy, Precision, Recall, and Fscore metrics of the individual methods.

TABLE II. METRIC VALUES IN PERCENTAGE

ALGORITHMS	XGBOOST	ADABOOST	RANDOM FOREST	KNN
ACCURACY	92.66	51.15	96.36	85.21
PRECISION	94.07	49.33	96.77	88.76
RECALL	93.79	49.78	96.69	86.64
FSCORE	93.65	47.99	96.71	86.55

By observing Table 2, Random Forest is the algorithm that has the highest accuracy with 96.36% and next is XGBoost with 92.66% followed by KNN and AdaBoost respectively with 85.21% and 51.15%.

Finally, after pressing the Predict Attack from Test Data button, the attack name will be predicted. This procedure will take place as the test dataset used for prediction is preprocessed and then delivered to the trained model for prediction of the attack name.

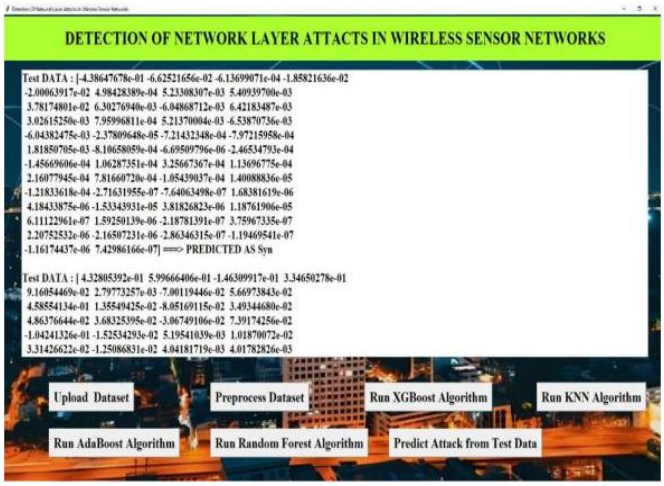

Fig. 8. Predict attack from Test Data

The prediction findings are seen in Fig 8 above. Each test data set is anticipated to have or not contain the attack. It is expected which assault it includes if it contains the attack. The above-mentioned Test data contains a wormhole attack.

The confusion matrix for the XGBoost method, AdaBoost Algorithm, Random Forest Algorithm, and KNN algorithm is produced in this work which shows the performance of the

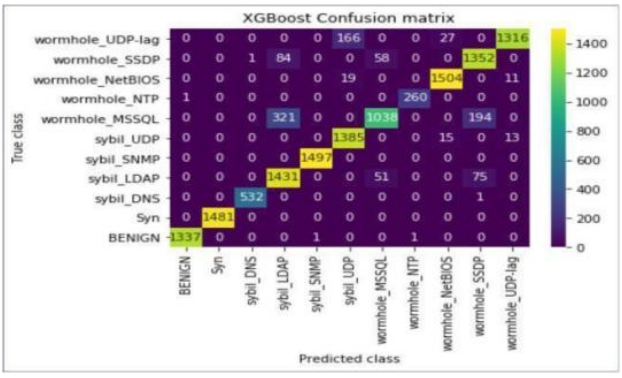

Fig. 9. XGBoost Confusion Matrix

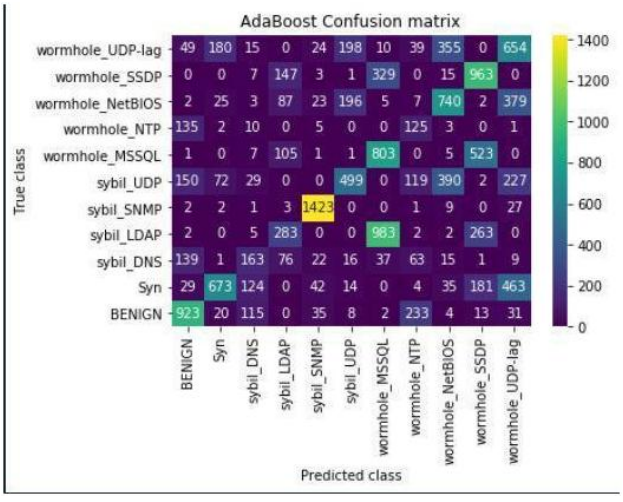

Fig. 10. AdaBoost Confusion Matrix

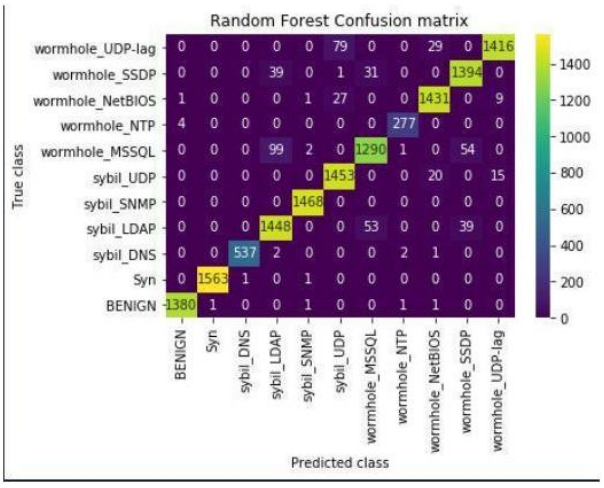

Fig. 11. Random Forest Confusion Matrix

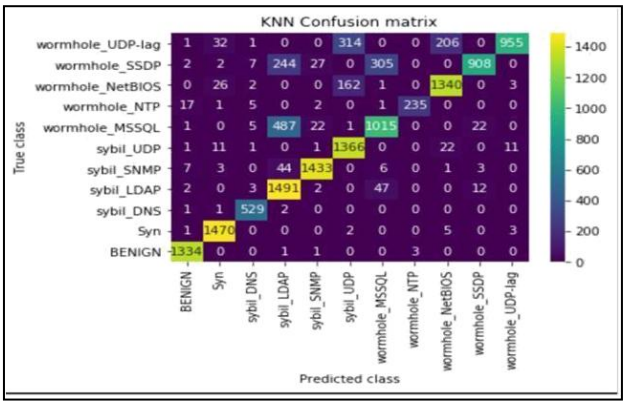

Fig. 12. KNN Confusion Matrix

algorithms. It demonstrates the relationship between the real and anticipated classes.

VIII. CONCLUSION

Wormhole and sybil attack detection may be modeled as a classification issue that distinguishes between "rational" and "irrational" network flow states based on the concept of rational thinking. This article examines in-depth common TCP flood attacks, UDP flood attacks, and ICMP flood attacks. So, in this study, we discussed machine learning strategies including the XGBoost method, the AdaBoost Algorithm, the Random Forest Algorithm, and the K Nearest Neighbor algorithm to identify attacks with high precision and accuracy. Random Forest Algorithm is with the highest accuracy of 96.3%. This study describes the creation of classification models for the three types of typical assault tactics mentioned above. It is eventually anticipated that the network traffic is normal through training and learning. If it contains an attack, it determines the type of assault.

IX. FUTURE WORK

In the current system, four Machine Learning algorithms are considered: XGBoost, AdaBoost, Random Forest, and KNN to determine which approach provides the highest level of accuracy in attack detection. Future enhancements to the present system include developing algorithms that are more accurate than the considered methods and detecting other network layer threats. So, we create the algorithms and their confusion matrix so that we can compare all of them and present the algorithm with the highest accuracy to determine which algorithm is the best among the ones studied.

REFERENCES.

[1] Pinar, Yasaroglu, et al. "Wireless sensor networks (WSNs)." 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT). IEEE, 2016 DOI:

10.1109/LISAT.2016.7494144.

[2] Vikhyath, K. B., and S. H. Brahmanand. "Wireless sensor networks security issues and challenges: A survey." Int. J. Eng. Technol 7.2 (2018): 89-94 DOI:10.14419/ijet.v7i2.33.13861.

[3] Panicker, Athira V., and G. Jisha. "Network layer attacks and protection in MANETA survey." International Journal of Computer Science and Information Technologies 5.3 (2014): 3437-3443.

[4] Shruthi, N., and C. K. Vinay. "Network layer attack: Analysis & solutions a survey." IOSR Journal of Computer Engineering 18.2 (2016): 67-80 DOI:10.9790/0661-18020.

[5] Gawali, Sanjana et al. "Intrusion Detection Using Hidden Markov Model and XGBoost Algorithm." International Journal of Scientific Research in Computer Science, Engineering and Information Technology (2020): n. pag 2456-3307 DOI:10.32628/CSEIT206287.

[6] Li, Wenchao, et al. "A new intrusion detection system based on KNN classification algorithm in wireless sensor network." Journal of Electrical and Computer Engineering 2014 (2014) https://doi.org/10.1155/2014/240217.

[7] Anitha, A. Arul, and L. Arockiam. "Ada-IDS: AdaBoost Intrusion Detection System for ICMPv6 based Attacks in Internet of Things." International Journal of Advanced Computer Science and Applications 12.11 (2021) (DOI) : 10.14569/IJACSA.2021.0121156.

[8] Song, Yan, et al. "A method of intrusion detection based on woa-xgboost algorithm." Discrete Dynamics in Nature and Society 2022 (2022) https://doi.org/10.1155/2022/5245622.

[9] Rampaul, Deepak, Rajeev Kumar Patial, and Dilip Kumar. "Detection of DoS attack in VANETs." Indian Journal of Science and Technology 9.47 (2016): 1-6 DOI: 10.17485/ijst/2016/v9i47/106865.

[10] Dwivedi, Rajendra Kumar, Prachi Sharma, and Rakesh Kumar. "Detection and prevention analysis of wormhole attack in wireless sensor network." 2018 8th international conference on cloud computing, data science & engineering (confluence). IEEE, 2018 DOI:10.1109/CONFLUENCE.2018.8442601.

[11] Chen, Liguo, et al. "Detection of dns ddos attacks with random forest algorithm on spark." Procedia computer science 134 (2018): 310-315 https://doi.org/10.1016/j.procs.2018.07.177.

[12] Ren, Qiong, Hui Cheng, and Hai Han. "Research on machine learning framework based on random forest algorithm." AIP conference proceedings. Vol. 1820. No. 1. AIP Publishing LLC, 2017 https://doi.org/10.1063/1.4977376.

[13] Xiao, P.; Li, Z.; Qi, H.; Qu, W.; Yu, H. "An Efficient wormhole and sybil Detection with Bloom Filter in VANET". IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, 23–26 August 2016; pp. 1–6. doi:10.1109/TrustCom.2016.0038.

[14] RT, K.; Selvi, S.T.; Govindarajan, K. "wormhole and sybil detection and analysis in VANET-based environment using support vector machine classifier". 2014 Sixth International Conference on Advanced Computing (ICoAC), Chennai, India, 17–19 December 2014; pp. 205–210.

[15] T. Phan.; Bao, N.; Park, M. "A Novel Hybrid Flow-Based Handler with wormhole and sybil Attacks in Software-Defined Networking".IEEE conference on UIC/ ATC/ScalComs/ CBDCom/IoP/SmartWorld, Toulouse, France, 18-21 July 2016; pp. 350-357.