Grenze International Journal of Engineering and Technology, June Issue

Machine Learning Based Intrusion Detection of Wormhole Attack in Mobile Ad-Hoc Networks

K. Kaleeswari[1] and Dr.P.Ranjith kumar[2]
[1]II - M.E., Applied Electronics, P.S.R. Engineering College, Sivakasi, Tamilnadu, India
[2]Professor – ECE, P.S.R. Engineering College, Sivakasi, Tamilnadu, India
Email: kaleeswari251299@gmail.com, ranjithkumar@psr.edu.in

***Abstract*— Mobile Ad hoc networks are transient, infrastructure-free networks that self-organize. A group of peer nodes that interact with one another without the aid of any infrastructure make up an ad hoc network. The most serious security risk to an ad hoc network is a wormhole attack, which is not resistant to standard security measures. A simulation of a wormhole attack in an environment of an ad hoc network with numerous wormhole tunnels is one of our objectives. The characterization of packet attributes that influence feature selection is the following job. In order to produce a large volume of dataset, we conduct data generation and data collection operations. The final job involves using machine learning to detect wormhole attacks. Previously, a wormhole assault was discovered using conventional methods. The most serious security risk to an ad hoc network is a wormhole attack, which is not resistant to standard security measures. A network layer attack that mimics routing methods is known as a wormhole attack. Several machine learning techniques, including the support vector machine (SVM), decision tree (DT), and convolutional neural network, are used to accomplish the classification. (CNN). Additionally, we used the MANET's node's speed as well as other node characteristics for feature extraction. We have gathered 3997 unique examples that include both benign and malicious nodes (normal 3781 and malicious 216). The classification findings demonstrate that the SVM, DT, and CNN methods, respectively, have accuracy rates of 98.2%, 98.9%, and 96.4%. According to our research, the DT method's accuracy is better than other methods at 98.9%. SVM and CNN both show high accuracy for the following priority.**

***Index Terms*— Intrusion Detection System, Mobile Ad-hoc Network, Machine learning, Wormhole attack, Normal and Malicious Node, Accuracy, Precision and Sensitivity.**

I. INTRODUCTION

Significant progress has been made in the area of wireless networks over the past few years, including the emergence of numerous new mobile handheld devices like laptops, smartphones, and Internet of Things IOT-based devices. Ad-hoc networks allow wireless devices to speak with one another and share data via networks without any infrastructure [1].To build a dynamic network for the transmission of data from source to destination, the nodes in an ad-hoc network are responsible for finding Neighbours. Since the nodes move about the network and interact with one another arbitrarily, the network topology changes in a way that is unpredictable and random. Ad-hoc network nodes have the ability to gather, store, process, and transmit data. In an ad hoc network, mobile nodes self-organize their operations and build a dynamic topology. The network is dependable and capable of securely sharing information to nodes' ability to recognize the existence of other nodes. The most significant security threat

Grenze ID: 01.GIJET.9.2.9_1

to an ad-hoc network is a wormhole attack, which is susceptible to standard security measures. It enables the intrusive party to drop packets, tunnel them across points, and broadcast into the network.
There are numerous methods for building tunnels, including inbound and outbound communication channels between malicious nodes. Such nodes fetch packets using erroneous route information or, more commonly, erroneous hop counts. The attackers can communicate more quickly than the other nodes in the sensor network because they are directly connected to one another through a tunnel in a worm hole attack. A worm hole attack is discovered by at least two hostile nodes via a tunnel, a private channel. At this point, data packets will start to accumulate and be sent to a separate location through the wormhole tunnel. A malicious node receives a control packet and one side of the tunnel. The packets are retransmitted locally if they are sent across a private channel from the opposite end to another interesting node. Machine learning (ML) techniques are explored for WHA detection in this article because they can be used to apply anomaly detection to ad-hoc networks and have a significant impact on the future. For exceptional performance, researchers frequently use the SVM approach. It has lastly, we have determined the areas that require more research can be targeted, allowing us to employ the Same detection techniques for a bigger topological area for more adaptability and precise results. The term "supervised training" indicates that a trainer may act as an administrator during the course of the training process. The information that is labelled with the statistics tag in this case needs to be trained. Via the prompt and accurate reaction, the information was previously evident. One of the most common supervised learning techniques include Support Vector Machines (SVM), Artificial Neural Networks (ANN), Decision Trees, K-Nearest- Neighbors (KNN), and Linear / Ensemble classifiers.

II. Related Work

IDS was recently implemented in ad hoc networks with a unique set of attacks. Mahendra Prasad, Amit Tripathi, and others [1] investigated this method to replicate wormhole attacks in ad hoc networks and traced the transmission of packet data at each node as output files that contain whole information of network topology. Machine learning algorithms use this high volume labelled dataset to categorized normal and malicious test samples in the supervised mode of training by two popular machine learning classifier NB and SGD to detect the attack and also show their performance. Khalid Alissa, Tahir Alyas et al [2], Proposed a EDA (Exploratory Data Analysis) technique. This is the statistical analysis phase through which the whole dataset is analyzed.The model will be able to be trained on a big data set. Machine learning classifiers such as Random Forest and SVM can also be tested. Quan Sun, Xinyu Miao et al [3] proposed a machine learning-based method to detect spoofing attacks for heterogeneous wireless networks by using physical-layer information. Popli, Rubi Dr Rashmi et al [4] to identify the forecast of malicious nodes and attacks on MANET and take into account node features in the system, a machine learning technique based on the SVM-GA classifier is suggested. It may be possible to foresee path attacks by recognizing healthy and destructive nodes. The results of the simulation demonstrate that the suggested method is highly accurate in predicting and ordering dangerous nodes in the system.
Rahma Meddeb et al [5] developed an anomaly-based technique to track traffic trends. The author simulated four attacks from three categories, including attacks that disrupt routing, drop packets, and use resources. In order to maximize the performance of our dataset, we applied data preparation techniques to increase the quality of the obtained data. Using the Support Vector Machine (SVM) classifier. Based on the results, it can be concluded that the suggested IDS has a high detection rate for all three types of assaults. Safaa Laqtib, Khalid El Yassini et al [6] discusses the ad hoc network security attacks and machine learning-based intrusion detection approaches to counter these attacks. To make it easier to identify attacks and give networks the ability to decide whether to allow intrusion while also learning more about their mobile environment, machine learning-based intrusion detection technologies must be implemented and developed.
A black-box attack strategy against machine-learning-based anomaly network flow detection systems was put forth by Sensen Guo et al. [7].As part of our assault strategy, a replacement machine learning model for the target model will be trained.To identify and isolate the malicious nodes in the network. Qing Ren, Ngoc T, and colleagues [9] introduced the flooding attack detection algorithm based on our suggested route discovery frequency history feature vector and the KNN data mining algorithm.. In order to demonstrate that access pattern leakage will result in security concerns in VANET, Feng Tian et al. [11] implemented a reconstruction attack on a secure outsourced geographical dataset. Our approach can support the attack for optional spatial granularity thanks to spatial discretization. Junejo, Muhammad Haleem, and others [12] In the MiTM attack scenario, a privacy-preserving attack-resistant lightweight trust model is proposed to enhance Internet of Vehicles (IoV) security by quickly identifying dishonest nodes and revoke their credentials. For the intrusion classification challenge, S. Sumathi, et al. [14] used a recurrent neural network and deep learning neural network model. The LSTM network is used, and

the effectiveness of its intrusion detection capabilities is examined. The performance of the model is enhanced using the hybrid HHO-PSO method. The technique suggested by S. Gnanavel et al. [20] provides both a system defense and a potent deterrent against cross-VM side-channel attacks. With the suggested method, cloud data is successfully shielded from cross-VM channel assault detection. The linear classification method is used in Block-Level Double Encryption (SBLDE).

The hybrid NID-Shield NIDS proposed by Thomas Rincy et al [17] was used to classify the UNSW-NB15 and NSL-KDD 20% dataset. Various assaults might have strange connections since some, like R2L and U2R, might have few N/W connections while others, like Probe and DoS, might have a lot of N/W connections or might combine any of them. The method developed by S. Gnanavel et al.[20] is used to prevent system crashes caused by attacks and is effective against cross-VM side-channel attacks. The suggested approach efficiently protects cloud data compared to other existing solutions, and it also gets rid of cross-VM channel attack detection.

III. Proposed Process

The topology of the network is not fixed because mobile nodes in MANETs have a dynamic nature, which makes it extremely difficult to implement any security measures. The network is self-configured and self-deployed; there is no central authority available for communication. The network is more vulnerable to errors and security threats because nodes communicate with each other wirelessly.

In MANETs, an IDS (Intrusion Detection System) is used as a defense mechanism to track and look into ominous activity. It provides a variety of tools for spotting various network anomalies. Because of its open structure, MANETs render the network more susceptible to many types of assaults because nodes can join and depart at any time. The main goal of IDS is to detect any malicious activity before it might damage the network. So every node in MANETs is equipped with IDS to filter the unauthorized access. Implementing IDS in real-world applications is quite difficult due to the resource limitations faced by nodes in MANETs. In order to recognize various fresh threats and vulnerabilities, machine learning techniques are used. IDS can be configured based upon various machine learning techniques Various classification approaches in ML can be applied to classify normal and intruder nodes and also compare its accuracies for better performances.

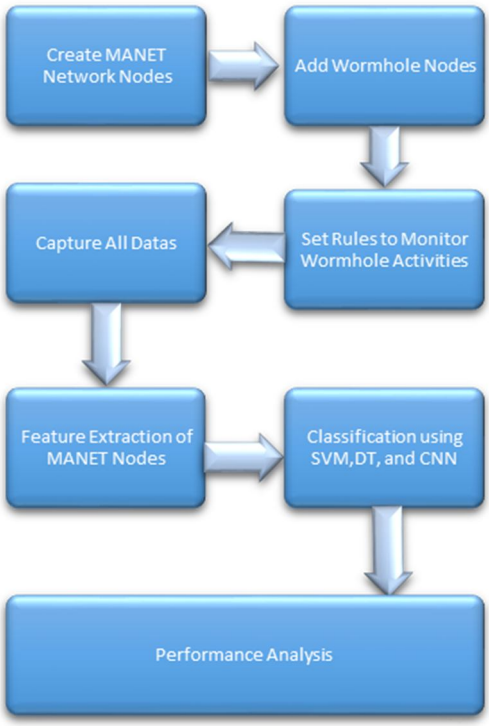


Fig.1. Architecture of IDS

A. Support Vector Machine (Svm)

SVM aims to find a balance between the complexity of the model and its learning ability. To predict the malicious nodes in MANETs, SVM is an effective method for problem-solving with a large number of samples, and

predicting intrusions in the mobile networks in our case, Hence, theoretically, SVM may determine the problem's global optimal point. The kernel function of SVM determines its learning ability with two commonly used kernels. Network nodes are split into two classes, -1 and +1, by the SVM class.
The nodes are then assigned to classes and the boundary between the two classes is specified based on how they behave. When a package is sent to a path node that must not be reached before it is sent to the path at all, the node is classified as a class -1 node and the type of attack is predicted. By using these class attributes and labels, the SVM class can identify malicious nodes in the network. These nodes are recognized based on predetermined traits and anomalous behaviour in relation to other nodes.

B. Decision Tree

A machine learning method called a decision tree algorithm makes predictions by using a decision tree. It follows a decision-tree-like model of choices and potential outcomes. The algorithm divides the data recursively into subsets according to the most important attribute at each node of the tree. Trees are supervised learning approaches that can be used to solve classification and regression problems, but they are most typically used to solve classification problems. It is a tree-structured classifier, with each leaf node denoting the classification result and inner nodes denoting the dataset's features.
A decision tree is used to learn simple decision rules that are inferred from training data in order to build a training model that can be used to predict the class or value of the target variable. The CART algorithm, which stands for Classification and Regression Tree algorithm, is used to construct a tree. A decision tree only poses a question and divides the tree into subtrees according to the response (Yes/No).

C. Convolutional Neural Network

The CNN is most frequently utilized for deep learning and neural networks with massive datasets, including pictures and videos (Convolutional Neural Network). We've built a multi-level neural network using cortical neurobiology. This structure consists of a completely connected layer and a convolution. It is possible that subsampling layers exist between these two levels. They get the best DNNs by combining the complexity of DNNs with well-scaled, multi-dimensionally localized input data. As a result, CNN is applied right away to datasets that need training a sizable number of nodes and components. convolutional neural network (CNN) can significantly improve the accuracy of classification. It is a multilayer Neural Network architecture caused by cortex neurobiology. It consists of convolutional layers and fully connected layers. Between these two layers, subsampling layers can exist. Therefore, the immediate use of CNN occurs in databases where relatively many nodes and parameters need to be learned.

IV. Results And Discussion

The following performance measures are employed for evaluation: accuracy (ACC), precision (P), and sensitivity or recall (R). True Positive (TP), True Negative (TN), False Positive (FP), and False-Negative (FN) (FN) are four different parameters used to measure these metrics. The percentage of documents that have been successfully categorized over the whole amount of data is called accuracy. Precision refers to the performance's pertinent proportion. Recall, on the other hand, is the proportion of correct classifications made by the algorithm for total functional outcomes. The terms "Detection Rate" (DR) and "True Positive Rate" are both used to describe the proportion of anomalous records that are correctly identified as anomalies to all anomaly data (TPR). The False Positive Rate (FPR), which represents the proportion of the total number that incorrectly flags an ordinary record as abnormal when it does so, is as follows.

$$ACC = \frac{TP + TN}{TP + FP + FN + TN}$$

$$P = \frac{TP}{TP + FP}$$

$$DR = TPR = R = \frac{TP}{TP + FN}$$

$$FPR = \frac{FP}{FP + TN}$$

Based on the TP, TN, FP and FN are referred as,

- True Positive (TP): Total number of malicious node that have been correctly classified as Malicious
- False Negative (FN): Total number of malicious nodes that have been misclassified as benign nodes.
- False Positive (FP): Number of benign nodes that have been misclassified as malicious.
- True Negative (TN): Number of benign nodes that have been correctly classified as benign.

A. Experimental Setup

The ad hoc network, where M are malicious nodes and N-M are benign nodes, consists of N bidirectional communication nodes that share messages and packets across a shared wireless medium. A tunnel is built by malicious nodes, who then carry out their defined wormhole attack operations. We also suppose that every node keeps an eye on its surrounding nodes.

We have simulated wormhole assaults on the Python platform using a finite number of nodes. It creates a network topology that includes the network, channel, node, and computer protocols. In this simulation procedure, different network applications send and receive packets across a network. The simulation model execution reaches the principal role and is processed through to the termination stage as packets are either generated or approved and processed the original position of nodes and their points of communication with nearby nodes.

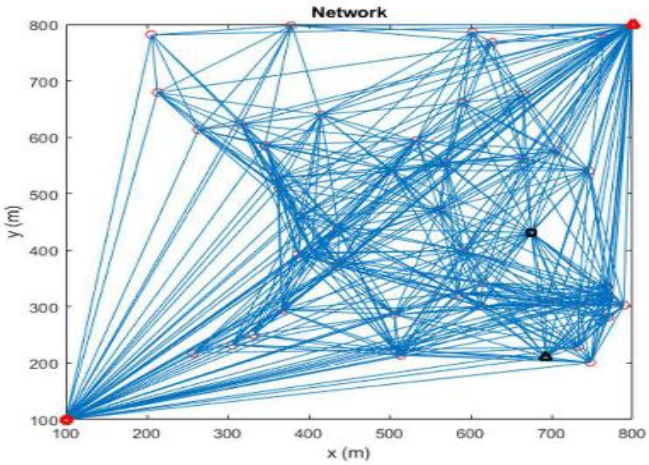


Fig.4. The Initial Position of MANET Node

An ad hoc network setup with 48 legitimate nodes and two malicious nodes was used for this simulation. The experimental conditions of the simulation environment include the topology room 1000x1000 m2, the spontaneous node activity, and the node's radio range of 250 meters (1000 for wormhole nodes). In Fig. 4, normal nodes are shown as red circles, while wormhole nodes are shown as black triangles. Also, blue lines connecting the nodes represent the initial connection.

B. Feature Extraction Result

We identify samples using the individual node address and assume that malicious nodes frequently produce malicious samples. A total of 3997 unique samples, both benign and malignant, have been collected (normal 3781 and malicious 216). It compiles a dataset and tags it with the eight selected qualities. It is a large dataset for wormhole attack detection that was produced in an ad hoc network setting.

C. Classification Result

Illustrations show the classification outcomes using the Support Vector Machine (SVM), Decision Tree (DT), and Convolutional Neural Network (CNN) machine learning techniques. Considering the confusion matrix, red elements denote erroneous values while green arrays display true values.

a) SVM Classification

For instance, 158 (or 73.1%) of 216 wormhole nodes are accurately detected using the SVM approach. However 58 (24.9%) of them were incorrectly identified as normal nodes. Or to put it another way, the SVM method's sensitivity is 73.1%. The normal node, however, may be identified with 99.6% specificity using the SVM approach. Only 15 (0.4%) of the 3781 normal nodes were misdiagnosed, which is what it says.

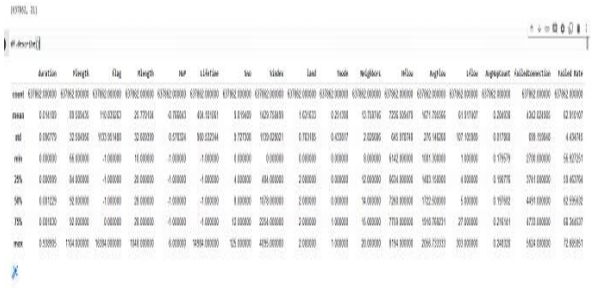
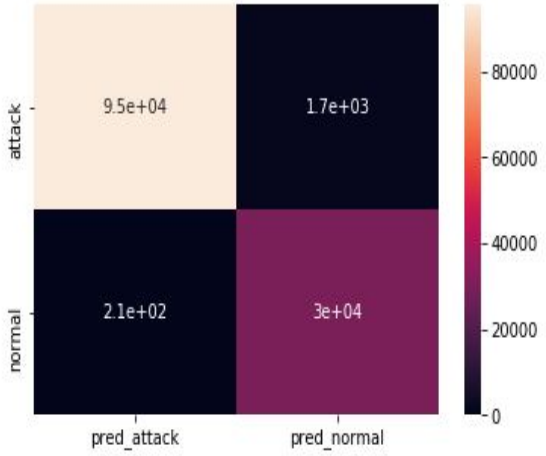


Fig.5. SVM Data Set

According to the perplexing true values matrix, the higher cell displays the true negative, and the bottom one displays the true positive. From red cells, the upper one is a false negative class, and the bottom one is a false positive class, respectively. On the basis of two categories—harmful and normal nodes—classification is carried out. Vertical cells demonstrate precision and negative predictive values, whereas horizontal grey cells represent sensitivity and specificity.



The outcomes of classifying data using a variety of machine learning techniques, including Support Vector Machine (SVM), Decision Tree (DT), and Convolutional Neural Network (CNN), are shown. In the confusion matrix, the green arrays represent real values, while the red elements represent false values. Often, the target class is regarded as a positive class in binary evaluation.

Fig.6. SVM Node Classification

b) Decision Tree Classification

Furthermore, 87.7% (precision) of the detected wormhole nodes using the DT classifier are in a genuine condition. The DT classifier, on the other hand, has a precision rate of 87.7%. The overall accuracy value that makes up DT is the value in the confusion matrix's lower-right corner cell. This number is 98.9%.

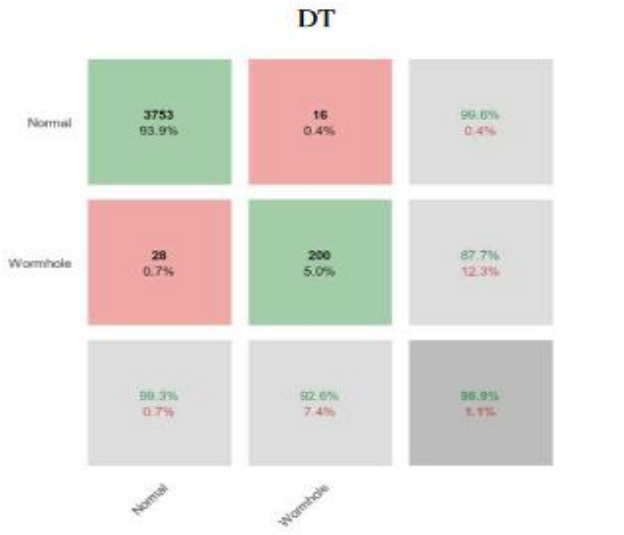


Fig.7. DT Node Classification

As a result, the accuracy of the SVM, DT, and CNN approaches is 98.2%, 98.9%, and 96.4%, respectively, according to the results. Moreover, the classifier's overall error value is highlighted in red lettering in the lower-right corner. We calculated that DT outperforms all conventional classifiers in terms of accuracy.

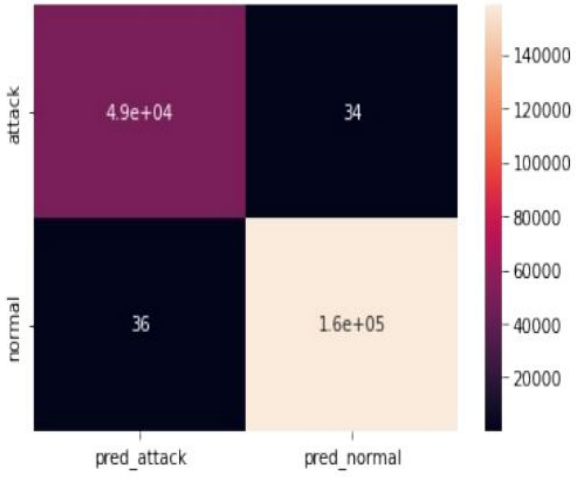


Fig.8. Attack Classification

c) CNN Classification

In Fig 9, the CNN architecture node classification is displayed. For every 3997 nodes in the input layer, there are 8 features. As a result, the input matrix is 8x1. Also, we employed two convolutional layers with ten 2x2 size, stride, and padding-free filters. Also, we utilized the Tanh and ReLU routines to activate the layers. Thereafter, 384 and 2 cells, respectively, are employed in each of two fully connected layers. To find probability 15 and activate the last layers, the Soft Max layer is used last. Finally, taking into account mutually exclusive classes, the classification layer based on cross-entropy is applied. The area under the ROC curve, often known as Accuracy, is a criterion for performance analysis of the classifier.

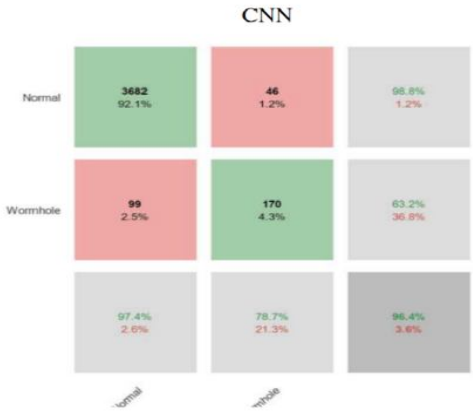


Fig.9. CNN Node Classification

The graph below illustrates CNN Architecture's accuracy and value.

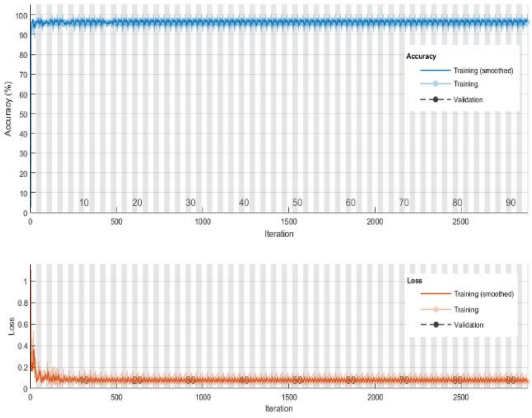


Fig: 10. Graph for Accuracy and Loss value in CNN

D.Accuracy Comparision

The results of the machine learning method comparison are displayed in the Table.1. Results show that the sensitivity of the DT method works better than other methods. The sensitivity represents the capability of the technique to find wormhole nodes in MANET. As a result, its magnitude signified the classifiers' potential. In other words, the DT classifier is more sensitive than previous techniques. The accuracy also demonstrates the method's dependability or potential for results. For instance, the SVM approach has a 91.3% accuracy rate. This indicates that 91.3% of the nodes that the SVM identified as wormhole nodes are in fact the genuine thing. The specificity also demonstrates how the classifier recognizes a typical node. The SVM technique has a high specificity.

TABLE. I. PERFORMANCE OF DIFFERENT CLASSIFICATION METHODS

PARAMETER	SVM	DT	CNN
Sensitivity	73.1%	92.6%	78.7%
Specificity	99.6%	99.3%	97.4%
Precision	91.3%	87.7%	63.2%
Accuracy	98.2%	98.9%	96.4%

Eventually, the DT technique is what led to the higher Accuracy value. The accuracy of the DT approach is 98.9%, which is higher than that of other methods, according to the results. SVM and CNN both indicate great accuracy for the following priority.

V. Conclusion

A network layer exploit that mimics routing protocols is known as a wormhole attack. A training dataset is necessary to train models in any training mode in order to identify wormhole assaults using machine learning. Due to abundant or evaluations for classification can serve as training datasets. The experimental data can be defined as a function that has a target value and a descriptive function. In this research, we present 3997 unique examples, including both benign and malignant ones (normal 3781 and malicious 216). It generates a dataset with eight selected features that is labelled. Many machine learning techniques, including the Support Vector Machine (SVM), Decision Tree (DT), and Convolutional Neural Network, are used to do the categorization (CNN). As a result, the accuracy of the SVM, DT, and CNN approaches is 98.2%, 98.9%, and 96.4%, respectively, according to the results. The sensitivity of the DT method works better than other methods, according to the results. The higher specificity is belonging to SVM approach. The accuracy of the DT approach is 98.9%, which is higher than that of other methods, according to the results. Both SVM and CNN show excellent accuracy for the next priority. The success of our technique motivates us to extend this work to tackle the constraints and simulation mentioned in a 3D ad hoc network.

References

[1] Mahendra Prasad , Tripathi, Wormhole attack detection in ad hoc network using machine learning technique "Communication and Networking Technologies 10.1109/ICCCNT45670.2019.8944634.

[2] Khalid Alissa, Tahir Alyas, Kashif Zafar, Qaiser Abbas, Nadia Tabassum, Shadman Sakib, "Botnet Attack Detection in IoT Using Machine Learning", Computational Intelligence and Neuroscience, vol. 2022, Article ID 4515642, 14 pages, 2022. Doi:10.1155/2022/4515642

[3] Quan Sun, Xinyu Miao, Zhihao Guan, Jin Wang, Demin Gao, "Spoofing Attack Detection Using Machine Learning in Cross-Technology Communication", Security and Communication Networks, vol. 2021, Article ID 3314595, 12 pages, 2021. Doi:10.1155/2021/3314595

[4] Popli, Rubi Dr Rashmi. "A worm hole attack detection in mobile ad-hoc network using GA and SVM." International Journal of Engineering Applied Sciences and Technology 5.3 (2020): 582-588.

[5] Meddeb, R., Jemili, F., Triki, B., & Korbaa, O. (2019). Anomaly-based behavioral detection in mobile Ad-Hoc networks. Procedia Computer Science, 159, 77-86.

[6] Laqtib, Safaa, Khalid El Yassini, and Moulay Lahcen Hasnaoui. "A deep learning methods for intrusion detection systems based machine learning in manet." Proceedings of the 4th International Conference on Smart City Applications. 2019.

[7] Sensen Guo, Jinxiong Zhao, Xiaoyu Li, Junhong Duan, Dejun Mu, Xiao Jing, "A Black-Box Attack Method against Machine-Learning-Based Anomaly Network Flow Detection Models", Security and Communication Networks, vol. 2021, Article ID 5578335, 13 pages, 2021. Doi:10.1155/2021/5578335

[8] Saswati Mukherjee, Matangini Chattopadhyay, Samiran Chattopadhyay, Pragma Kar, "Wormhole Detection Based on Ordinal MDS Using RTT in Wireless Sensor Network", Journal of Computer Networks and Communications, vol. 2016, Article ID 3405264, 15 pages, 2016. Doi:10.1155/2016/3405264

[9] Ngoc T. Luong, Tu T. Vo, Doan Hoang, "FAPRP: A Machine Learning Approach to Flooding Attacks Prevention Routing Protocol in Mobile Ad Hoc Networks", Wireless Communications and Mobile Computing, vol. 2019, Article ID 6869307, 17 pages, 2019. Doi:10.1155/2019/6869307

[10] Mohammed S. Alzaidi, Chatti Subbalakshmi, T. V. Roshini, Piyush Kumar Shukla, Surendra Kumar Shukla, Papiya Dutta, Musah Alhassan, "5G-Telecommunication Allocation Network Using IoT Enabled Improved Machine Learning Technique", Wireless Communications and Mobile Computing, vol. 2022, Article ID 6229356, 10 pages, 2022. Doi:10.1155/2022/6229356

[11] Qing Ren, Feng Tian, Xiangyi Lu, Yumeng Shen, Zhenqiang Wu, Xiaolin Gui, "A Reconstruction Attack Scheme on Secure Outsourced Spatial Dataset in Vehicular Ad-Hoc Networks", Security and Communication Networks, vol. 2021, Article ID 5317062, 12 pages, 2021. Doi:10.1155/2021/5317062

[12] Muhammad Haleem Junejo, Ab Al-Hadi Ab Rahman, Riaz Ahmed Shaikh, Kamaludin Mohamad Yusof, Imran Memon, Hadiqua Fazal, Dileep Kumar, "A Privacy-Preserving Attack-Resistant Trust Model for Internet of Vehicles Ad Hoc Networks", Scientific Programming, vol. 2020, Article ID 8831611, 21 pages, 2020. Doi:10.1155/2020/8831611

[13] Muhammad Shafiq, Shah Nazir, Xiangzhan Yu, "Identification of Attack Traffic Using Machine Learning in Smart IoT Networks", Security and Communication Networks, vol. 2022, Article ID 9804596, 4 pages, 2022. Doi:10.1155/2022/9804596

[14] S. Sumathi, R. Rajesh, Sangsoon Lim, "Recurrent and Deep Learning Neural Network Models for DDoS Attack Detection", Journal of Sensors, vol. 2022, Article ID 8530312, 21 pages, 2022. Doi:10.1155/2022/8530312

[15] Xiaoya Xu, Yunpeng Wang, Pengcheng Wang, "Comprehensive Review on Misbehavior Detection for Vehicular Ad Hoc Networks", Journal of Advanced Transportation, vol. 2022, Article ID 4725805, 27 pages, 2022. Doi:10.1155/2022/4725805
[16] Murtadha M. A. Alkadhmi, Osman N. Uçan, Muhammad Ilyas, "An Efficient and Reliable Routing Method for Hybrid Mobile Ad Hoc Networks Using Deep Reinforcement Learning", Applied Bionics and Biomechanics, vol. 2020, Article ID 8888904, 13 pages, 2020. Doi:10.1155/2020/8888904
[17] Thomas Rincy N, Roopam Gupta, "Design and Development of an Efficient Network Intrusion Detection System Using Machine Learning Techniques", Wireless Communications and Mobile Computing, vol. 2021, Article ID 9974270, 35 pages, 2021. Doi:10.1155/2021/9974270
[18] Nitika Phull, Parminder Singh, Mohammad Shabaz, F. Sammy, "Performance Enhancement of Cluster-Based Ad Hoc On-Demand Distance Vector Routing in Vehicular Ad Hoc Networks", Scientific Programming, vol. 2022, Article ID 7423989, 15 pages, 2022. Doi:10.1155/2022/7423989
[19] Zhifei Wang, Gang Xu, Na Zhang, Zhihan Qi, Fengqi Wei, Liqiang He, "Ferry Node Identification Model for the Security of Mobile Ad Hoc Network", Security and Communication Networks, vol. 2021, Article ID 6682311, 13 pages, 2021. Doi:10.1155/2021/6682311
[20] S. Gnanavel, K. E. Narayana, K. Jayashree, P. Nancy, Dawit Mamiru Teressa, "Implementation of Block-Level Double Encryption Based on Machine Learning Techniques for Attack Detection and Prevention", Wireless Communications and Mobile Computing, vol. 2022, Article ID 4255220, 9 pages, 2022. Doi:10.1155/2022/4255220
[21] Muhammad Sameer Sheikh, Jun Liang, Wensong Wang, "Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey", Wireless Communications and Mobile Computing, vol. 2020, Article ID 5129620, 25 pages, 2020. Doi:10.1155/2020/5129620
[22] Iftikhar Ahmad, Muhammad Yousaf, Suhail Yousaf, Muhammad Ovais Ahmad, "Fake News Detection Using Machine Learning Ensemble Methods", Complexity, vol. 2020, Article ID 8885861, 11 pages, 2020. Doi:10.1155/2020/8885861
[23] Seunghyun Park, Jin-Young Choi, "Malware Detection in Self-Driving Vehicles Using Machine Learning Algorithms", Journal of Advanced Transportation, vol. 2020, Article ID 3035741, 9 pages, 2020. Doi:10.1155/2020/3035741
[24] Shujuan Wang, Qian Zhang, Shuguang Lu, "NCaAC: Network Coding-Aware Admission Control for Prioritized Data Dissemination in Vehicular Ad Hoc Networks", Wireless Communications and Mobile Computing, vol. 2020, Article ID 6758536, 14 pages, 2020. Doi:10.1155/2020/6758536
[25] Mohammad Sirajuddin, Ch. Rupa, Surbhi Bhatia, R. N. Thakur, Arwa Mashat, "Hybrid Cryptographic Scheme for Secure Communication in Mobile Ad Hoc Network-Based E-Healthcare System", Wireless Communications and Mobile Computing, vol. 2022, Article ID 9134036, 8 pages, 2022. Doi:10.1155/2022/9134036