ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 11, Issue 4, pp: (20-28), Month: October - December 2023, Available at: www.researchpublish.com

# Attention Based Gated Recurrent Neural Network for Wormhole Attack Detection in MANETs

Balkisu Musa Hari[1], Ali Ahmad Aminu[2]

[1,2] Department of Computer Science Gombe State University

DOI: https://doi.org/10.5281/zenodo.8424623

Published Date: 10-October-2023

*Abstract:* **The wormhole attack is a type of attack on the network layer that affects the routing protocols. In this study, we investigate the use of Gated Recurrent Unit (GRU) with an attention mechanism and Decision Tree, for detecting wormhole attacks in mobile ad hoc networks (MANETs). This study is divided into three main tasks. Firstly, simulating wormhole attacks in a mobile ad hoc networks (MANETs) environment with a finite number of nodes Secondly, describe the network characteristics that contribute to feature selection. Consequently, we perform data generation and data gathering operations that produce a large volume of datasets. Finally, we applied the proposed model to detect wormhole attacks in mobile ad hoc networks (MANETs). The model was evaluated and tested with the simulated datasets consisting of eight selected features and an instance using Accuracy, Precision, Recall, and F1-Score as performance metrics. Experimental results demonstrate that the proposed method outperformed other related methods from the literature in terms of the aforementioned evaluation criteria.**

*Keywords:* **Manets, Wormhole, Attention mechanism, DT, Feature Selection.**

## I. INTRODUCTION

Mobile ad hoc networks (MANETs) are self-organizing, distributed networks made up of portable nodes that talk to one another over radio waves without the need for a centralized infrastructure. Because of their adaptability and toughness, MANETs have many uses in both military and civilian environments, including emergency response. A decentralized type of wireless network, known as mobile ad hoc network (MANET) or wireless ad hoc network, is one that moves autonomously and is not dependent on any pre-existing infrastructure or system, such as access points and routers in wireless and wired networks, respectively. Instead, every node participates in routing by sending data to other nodes or destinations. As a result, the position of which nodes send data is continually changing based on the network connectivity and also the algorithm (i.e., the routing method in use), according to M. Zanjireh et al. [1]. However, due to the use of open medium access and dynamically changing topologies, MANETs are susceptible to different types of attacks, such as black hole attacks, grayhole attacks, Sybil attacks, and Wormhole attacks. The wormhole attack is the most common and fatal attack among these attacks that substantially disrupt the routing protocols of the network, thus, making the entire network unsafe. When an attacker captures and retransmits packets from one location to another through a faster wired or wireless link, they are able to bypass intermediate nodes and create a virtual tunnel between the two distant locations in the network. This is known as a wormhole attack. By Eavesdropping on network traffic, unauthorized access to network resources, and disruption of network services are all possible outcomes of this. To overcome the problem of wormhole attack in MANETs, several studies have proposed different methods for detecting and mitigating the damage caused by wormhole attack in MANETs. Among them are machine learning methods for intrusive detection by Abdan, M., and S. A. H. Seno (2022) [2]; A wormhole attack in mobile ad-hoc networks: detection and prevention by Shastri, A., and

J. Joshi (2016)[3]; feature selection based on cross-correlation for the intrusion detection system by Farahani, G. (2020) [4]; and wormhole attack detection in ad hoc networks using machine learning techniques by Prasad, M., et al. (2019)[5]. And other work that related to the wormhole attack. While most of these studies have improved on the state of the arts, the problem of wormhole attacks in MANETs still remains a challenge due to the evolving nature of the attackers and the challenging nature of the problem. Hence, this study proposes the use of attention-based gated recurrent unit (GRU) and decision tree (DT) networks to improve the performance a prediction model can achieve in the task of wormhole detection in MANETs. An attention mechanism is used by AG-RNNs, a subclass of recurrent neural networks, to concentrate on important elements of the input sequence, improving the network's capacity to recognize patterns and long-term relationships. DTs, on the other hand, are decision support systems that classify data in accordance with a preset set of rules by using a model that resembles a tree of decisions and their potential outcomes. To assess the performance of the proposed model, its performance was evaluated with a simulated dataset using accuracy, precision, recall, F1-score, and ROC_AUC_Score as performance metrics. Experimental results show that the proposed method outperforms some of the existing methods from the literature and could be potentially employed to enhance wormhole attack detection and mitigation in MANETS. The suggested model was tested based on the aforementioned dataset, and the findings demonstrated that it performed better than previous techniques for wormhole attack detection in mobile ad hoc networks, with better accuracy than the others. Overall, the suggested model offers a practical and time-saving method for identifying wormhole attacks in MANETs, which makes a substantial contribution to the field of network security research.

## II. REVIEW OF RELATED WORKS

A number of papers have proposed various approaches to identify and counteract wormhole attacks in MANETs, which have garnered substantial research interest over the years. This study of the literature gives an overview of the most recent studies on wormhole attacks in MANETs and shows the many techniques used to detect and mitigate the wormhole attack in MANETs. M. Prasad et al. [5] proposed the machine learning approach and the algorithms used to categorize normal and malicious test samples in the supervised mode of training. The result shows a 93.12% detection rate and 5.3% false alarm, which is higher than compared to other approaches. However, it has some limitations, such as manual feature selection and data collection, which need to be extended for further research. H.U. Johnson et al. [6] present a packet leash for detecting and thus defending against wormhole attacks by designing an efficient authentication protocol called TIK for use with temporal leashes. The two types of leashes were presented: temporal and geographic leashes. This geographic and temporal leash can limit the maximum packet transmission distance. A leash is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. Zardari Z.A. et al. [7] proposed a lightweight technique wormhole node detection based on calculating the average sequence number with a significant delay in the network. The method lengthens the network life and saves the battery power of the wireless nodes. The parameters used are packet delivery ratio, throughput, and average delay. Nevertheless, the method is only to detect attacks in the wormhole. Murty & L. Rajami [8] suggest a simple and effective Intrusion Detection System (IDS) to categorize various attacks in MANETs. According to the research, four features Traffic patterns were used for extraction, and support vector machine (SVM) classification algorithms were used for classification. They also analyze the viability of using machine learning methods to find security breaches in MANETs. The uniqueness of the study is the self-created dataset acquired from a data packet passing through the mobile ad hoc network. Pre-processing, feature extraction, and classification are the three processes that make up the system. For the validation of the suggested models, they employed mathematical techniques. However, a system trained with a consistent set of characteristics cannot produce an encouraging detection result since the mobile nodes are dynamic and attacks are entirely random in nature. According to Farahani G. [4], a cross-correlation-based feature selection (CCFS) method was suggested. It was compared with the cuttlefish algorithm (CFA) and mutual information-based feature selection (MIFS). In their research, they used four distinct datasets and four different classifiers based on four separate features. For better performance of the proposed CCFS method, consider the correlation between features, which helps to better distinguish the attack from normal instances on datasets. Consideration of feature correlation improves the efficacy of the suggested CCFS-technique, aiding in better distinguishing attacks from regular occurrences on the dataset. However, the value of FPR is not determined during the simulation by either of the datasets. Patel A. et al. [9] proposed a hash-based compression function (HCF). The HCF can use any hash function to compute the value of the hash field for the RREQ packet. However, the result is not benchmarking. Panwar A. et al. [10] suggest a trust-based routing technique that computes the threshold trust values based on the ideal network conditions. The technique is acceptable for different areas of applications and utilities. Nevertheless, in the near future, other network features will be examined for strengthening

MANET security. The suggested study only entails the computation of a small number of network parameters. Table 1 provides a summary of the proposed approach for wormhole detection in MANETs from the literature.

In conclusion, wormhole attacks are a significant security threat in MANETs, and various techniques have been proposed to detect and prevent these attacks. The different approaches used include cryptographic techniques, hop-count signatures, packet-pair approaches, neighbour coverage ratios, and others. Each technique has its own strengths and weaknesses, and future research should focus on developing more robust and effective techniques to counter this threat.

**Table 1: The summaries of the different wormhole attack detection approaches from the literature.**

| Author | Year | Method | Results |
|---|---|---|---|
| Prasad et al. | 2019 | Stochastic Gradient Descent (SGD)<br>Naïve Bayes (NB) | The accuracy obtained is 93.12% for the detection of an attack |
| Abdan.et al. | 2022 | K-Nearest Neighbour(KNN)<br>Support Vector Machine (SVM)<br>Decision-Tree (DT)<br>Latent Dirichlet Allocation (LDA)<br>Naïve Bayes (NB)<br>Convolutional Neural Network (CNN) | The results obtained are based on feature extraction, classification, and several methods of machine learning. |
| Panwar, et al. | 2020 | Stochastic Gradient Descent (SGD)<br>Naïve Bayes (NB) | It computes the threshold trust values based on the ideal network conditions; the technique is acceptable for different areas of applications and utilities. |
| Singh et. al. | 2020 | Support Vector Machine(SVM)<br>K- Nearest Neighbour(KNN) | Detection of wormhole attacks in Wireless Sensor Network. |
| Shastri and J.Joshi et al. | 2016 | Hop-based analysis. | It can detect both concealed and revealed attacks. |
| Singh et al. | 2019 | Support Vector Machine<br>K-Nearest Neighbour. | Developing a multi-hop communication scenario utilizing the AODV routing technology to detect wormhole attacks in VANETs. |

## III. METHODOLOGY

### *A. Data Collection and Pre-processing*

We simulated wormhole attacks in MATLAB 2019b using a finite number of nodes. This creates a network topology that consists of nodes, devices, channels, and networks. There are various network applications that send packets over networks, either creating, accepting, or processing packets. Packets are generated, approved, and processed as the simulation model execution progresses to the main role and continues processing until termination. The simulation was conducted in an ad hoc network environment with regular nodes and malicious nodes. The simulation environment includes the topology room, which is measured in square meters, spontaneous node activity, and the 250-meter radio range of a node. Feature selection is one of the fundamental ideas in machine learning, and it directly affects the system's performance. Features that are irrelevant or only partially relevant can adversely affect the system's performance. The output file contains extensive node information, but only the data specific to a given application is informative. When unimportant or less informative features that do not support categorization are ignored, similar features may be chosen for the dataset. Abdan M. et al. [2] Feature selection has several benefits, including reducing over fitting, decreasing

training time, and increasing accuracy, among others. We have selected eight key characteristics that significantly improve the system's performance. We have collected over thirty thousand distinct samples, both normal and malicious, during the simulation. We are building a dataset compiled from eight selected features and labelled. It is a large dataset for wormhole attack detection, created in the context of a mobile ad hoc network.

### *B. Dataset Description*

We conducted our study to examine the effectiveness and efficiency of detecting wormhole attacks in mobile ad hoc networks. We have simulated wormhole attacks in the MATLAB 2019b set with a finite number of nodes. It creates a topology with the node, computer, channel, and protocol as its components. It has focused on the base eight selected features for the diagnosis of wormhole attacks in mobile ad hoc, which is a benchmark with the selected features. In order to overcome the problem of wormhole attacks, a decision tree classifier was used, and it has a higher AUC than the other approaches. The classification is performed based on two classes' normal and malicious nodes.

### *C. Proposed Model*

An attention-based gated recurrent neural network (AG-RNN) in conjunction with a decision tree (DT) is the model that is put forth in this study as a method of wormhole attack detection in a mobile ad hoc network. The decision tree is a classification technique that divides the data into more manageable categories based on chosen features, whereas the attention-based gated recurrent neural network is a sort of neural network that permits the selection of certain input sequence segments. The suggested approach first takes network traffic data and uses a feature extractor to take out the features. The attention-based gated recurrent neural network then receives the features and uses attention mechanisms to choose the key features before sending them to the decision tree for classification. The input data is then divided into wormhole and non-wormhole traffic by the decision tree.

**Attention-Based Gated RNN Model:** A mobile device communication network that self-configures and operates devoid of a fixed infrastructure is known as a mobile ad hoc network (MANET). However, wormhole attacks are just one of the security risks that MANETs are susceptible to. In a wormhole attack, suspicious nodes build a tunnel between two remote network locations, breaking off the regular communication channels. This may seriously impair the network's ability to function and jeopardize its security. An attention-based gated recurrent neural network model has been suggested as a means of detecting wormhole attacks in MANETs.

**Decision Tree Model:** This study focuses on identifying wormhole attacks, a specific kind of security concern, in mobile ad hoc networks (MANETs). The proposed approach to detecting this attack involves using a decision tree model in conjunction with an attention-based recurrent neural network (RNN). The DT algorithm uses trees to solve classification and regression problems. To get the outcome, an inverted tree is built, with branches branching off from a homogeneously dispersed root node to wildly disparate leaf nodes. The fact that data does not require pre-processing or distribution is one of the major advantages. Furthermore, DTs can offer a clear rationale for the prediction. Abdan M. et al. [2] a decision tree is a supervised machine learning algorithm that learns a series of if-then-else decision rules from the training data. Based on the values of the input features, it divides the feature space into various areas and gives each region a class label. The decision tree model is used in the context of the research topic to categorize network traffic as either normal or suspicious of a wormhole attack. The attention-based RNN is used in this study to process the network traffic data's sequential character. The attention mechanism is used by the model to give each feature a distinct weight after receiving a list of network traffic features as input. The RNN layers are then used to process the weighted features, capturing the temporal dependencies in the data. The decision tree model for classification uses the RNN's output. The suggested method seeks to increase the detection precision of wormhole attacks in MANETs by merging the attention-based RNN and decision tree model. The decision tree uses the learned patterns to categorize the traffic as normal or suggestive of a wormhole assault, while the attention mechanism aids in the model's focus on key aspects and temporal correlations. In order to detect wormhole attacks in MANETs, the study topic combines a decision tree model with an attention-based RNN, thereby improving the security and dependability of such networks. Figure 1 provide an overview of the proposed approach.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 11, Issue 4, pp: (20-28), Month: October - December 2023, Available at: www.researchpublish.com

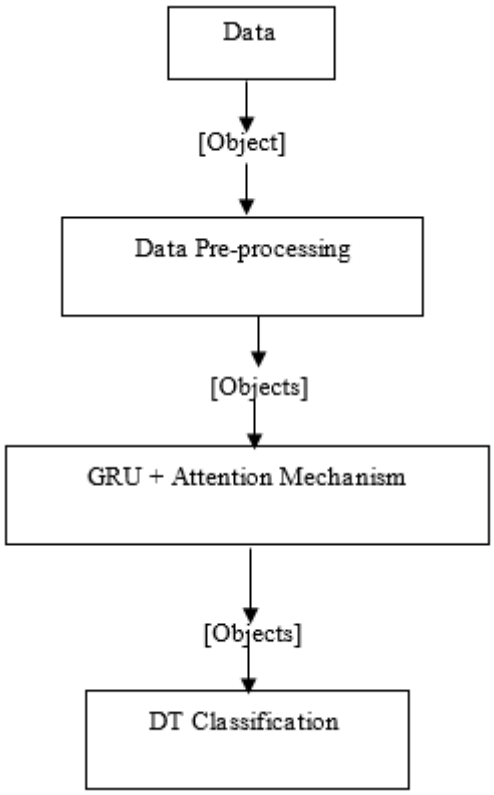


**Fig 1: A flow diagram of the proposed Approach.**

## IV. IMPLEMENTATION DETAILS

### *A. Implementation Details:*

The proposed approach was implemented and trained using Python and TenserFlow programming. The MATLAB 2019b program was used for simulating and generating the datasets. The network topology design and gathering the datasets needed to test the effectiveness of the proposed approach. Data preparation is a crucial stage in the data-gathering process. Realistic data might be noisy, redundant, partial, and inconsistent and is often derived from heterogeneous platforms. Wang et al. [11]. Therefore, converting raw data into an appropriate format for analysis is necessary for better outcomes. Farahani G. [4]. The proposed method creates a sequential RNN model with a binary cross-entropy loss function and particular optimizer parameters (Adam with a specified learning rate). These decisions attempt to efficiently optimize the model's weights during training while also teaching the model to produce accurate binary classification predictions. The convergence and performance of the model are influenced by the learning rate, which also defines the step size for weight updates during training. The optimizer used in the method is the Adam optimizer, i.e., the popular one for training deep neural networks. This specific use combines the ideas from both the Adagrad (Adaptive Gradient Descent) and RMSprop (Root Mean Square Propagation) optimizers and is known for its efficiency and ability to handle noise. The optimizer is configured with a learning rate value of 0.003. This learning rate controls the step size at which the optimizer updates the model's weights during training. It plays a crucial role in determining the convergence and stability of the training process. Also, it determines how quickly or slowly it adjusts its weights in response to the calculations made during each training iteration. On the other hand, the choice of loss function depends on the problem being solved. In this work, the loss function is 'binary cross entropy' which is usually used for binary classification problems. Binary cross-entropy loss measures the dissimilarity between the true binary labels "0s and 1s" and the predicted probabilities generated by the model. It quantifies how well the model's predictions match the actual target values.

### *B. Performance Evaluation Metrics:*

The proposed approach is evaluated using a variety of performance metrics, such as accuracy, precision, recall, and F1-score. The explanations are based on these parameters. True positive (TP), true negative (TN), false positive (FP), and false negative (FN).

Accuracy is used to determine how many occurrences are accurately classified as attacks and normal instances. The following equation's definition of the accuracy criterion.

Accuracy = TP + TN / TP + FP + FN + TN…….. (I)

Precision: precision is used for evaluating true-positive instances against false-positive ones. The following equation illustrates the instances.

Precision = TP / (TP + FP)……..… (II)

Recall: Recall is used to compare occurrences of actual positivity to those of fake negativity. Recall can be stated mathematically using the following equation.

Recall = TP / (TP + FN)…….. (III)

F1 Score: The recall and precision averages are used to determine an F1 score. The following equation can be used to compute it.

F1 Score = $\frac{2 * \text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}}$ …..... (IV)

At times, accuracy and recall in performance evaluations may not be enough. A different criterion is required if a particular algorithm has high precision but low recall. So, this issue can be resolved by F1-score.

### *C. Experimental Results*

- Experimental Setup:

We've simulated wormhole attacks in MATLAB 2019b using a finite number of nodes. This creates a network topology that consists of node, device, channel, and network. There are many different network applications that send packets over networks, either creating or accepting and processing packets. Packets are generated, approved, and processed as the simulation model execution moves to the major role and continues processing until termination. The simulation was done in an ad hoc network environment with a number of regular nodes and malicious nodes. The topology room used in square meters, spontaneous node activity, and the 250-meter radio range of a node are the simulation environments described by Abdan M. et al. [2]. The dataset obtained was split into training and testing sets. The train set split function from scikit-learn divides the data into X_train, X_test, y_train, and y_test. The model is a GRU (gated recurrent unit) together with an attention layer. The model was trained using the training data (X_train and y_train) and evaluated's performance using the testing data (X_test and y_test) and calculated metrics such as accuracy, precision, recall, F1 score, and ROC-AUC score to assess the model's performance. We used an attention-based mechanism as the model for detecting wormholes in mobile ad hoc networks. An attention-based mechanism enables the network to concentrate on specific types of data sequences while making predictions. We conducted our research by employing the DT method. We evaluate the performance using accuracy, recall, and the F-score.

The evaluation and comparison are carried out by applying the recent techniques of earlier research work and the proposed method. The primary metrics considered in the current research work are accuracy (Acc), precision, sensitivity, and F1 score. The results are shown in the tables below.

**TABLE 2: RESULT OF THE PROPOSED MODEL**

| METRICS | DT | Attention GRU | DT + Attention GRU |
|---|---|---|---|
| Accuracy | 96.17% | 98.05% | 98.18% |
| Precision | 92.67% | 96.13% | 96.39% |
| Sensitivity | 100% | 100% | 100% |
| F1_Score | 96.19% | 98.03% | 98.16% |
| ROC_AUC_Score | 96.28% | 98.11% | 98.24% |

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 11, Issue 4, pp: (20-28), Month: October - December 2023, Available at: www.researchpublish.com

**TABLE 3: COMPARISON OF RESULTS ACHIEVED BY THE PROPOSED METHOD AND OTHER METHODS**

| METRICS | Prasad, M., et al. (2019) | Farahani,G.(2020) . | Bhosale,S.A.andS.Sonavane (2022) | DT + Attention GRU |
|---|---|---|---|---|
| Accuracy | 93.1% | 93.47% | 94.51% | **98.18%** |
| Precision | 94.0% | 94.87% | NA | **96.39%** |
| Sensitivity | N.A | 95.79% | NA | **100%** |
| F1_Score | 93.4% | 95.33% | 91.19% | **98.16%** |
| ROC_AUC_Score | N.A | N.A | NA | **98.24%** |

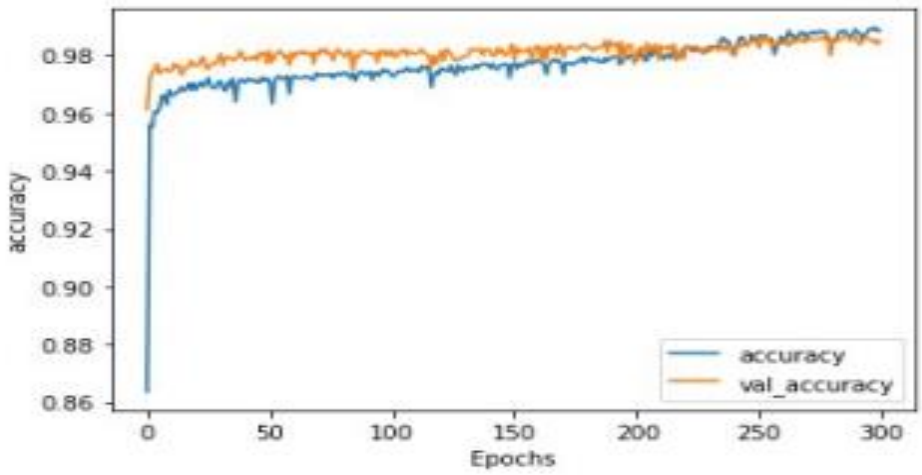


**Fig. 3: The accuracy value of the proposed model**

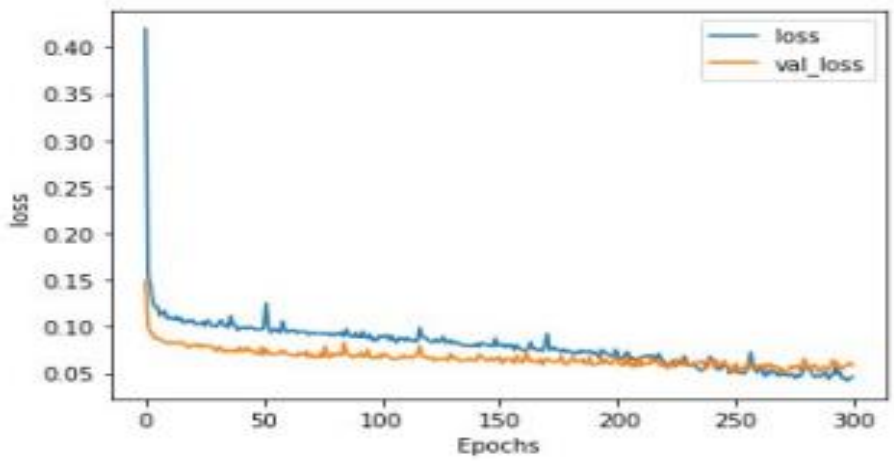


**Fig. 4: The Loss value of the proposed model**

### *D. Analysis of Results*

Table 2 summarizes the experimental results of the proposed model on the simulated datasets in terms of accuracy, recall, precision, F1 score, and ROC_AUC_Score. From the results, it can be seen that the proposed method achieved high detection rates with accuracy, precision, recall, f1score, and ROC_AUC_Score of 98.18%, 96.39%, 100%, 98.16%, and 98.24%, respectively. In addition, figures 3 and 4 show the training/validation accuracy and training/validation loss, respectively, of the proposed method, which further illustrates the performance of the proposed model during training and validation. To further assess the performance of the proposed model, the results obtained by the proposed model are compared with those of other methods from the literature. The results of the proposed model in comparison with other methods from the literature are presented in Table 3. The best results obtained by each method

are bolded for emphasis. As shown in Table 3, it can be observed that the proposed method significantly improved on the existing methods in terms of accuracy, precision, and f1 score, respectively. In contrast to the results reported by Bhosale, S.A, and S.Sonavane (2022), the proposed method demonstrated notable improvements in accuracy (3.67% improvement) and f1score (6.97%). While the work of Bhosale, S.A, and S.Sonavane (2022) did not evaluate their model using precision, recall, and ROC_AUC_Score, the proposed method achieved precision, recall, and ROC_AUC_Score of 96.39%, 100%, and 98.24%, respectively. Similarly, in the work of Farahani G. (2020), the authors reported an accuracy of 93.47%, a precision of 94.87%, a sensitivity of 95.79%, and an F1-Score of 95.33%. In comparison, the proposed method excelled in accuracy with 98.18% (4.71% enhancement) and precision at 96.38% (1.52% better). Additionally, the proposed approach achieved a sensitivity of 100%, indicating (4.21% improvement), and F1-Score of 98.16% (2.83% increase). Although Farahani's research did not provide a ROC_AUC_Score, the proposed method yielded an impressive ROC_AUC_Score of 98.24%. Finally, we assessed the findings of Prasad et al. (2019), who reported an accuracy of 93.1%, a precision of 94.0%, and an F1-Score of 93.4%. In contrast, our proposed method surpassed these metrics, achieving an accuracy of 98.2% (5.1% improvement), a precision of 96.4% (2.4% enhancement), and an F1-Score of 98.16% (4.8% increase). Additionally, our approach exhibited a sensitivity of 100% and a ROC_AUC_Score of 98.2%, which were not provided in Prasad et al.'s work. The comparative analysis reveals that the proposed method outperforms previous approaches significantly. The comparative analysis clearly demonstrates that the proposed method outperforms earlier research methodologies across various critical metrics. The substantial improvements observed in accuracy, precision, sensitivity, F1-Score, and ROC_AUC_Score underscore the effectiveness of the attention mechanism embedded in the proposed approach. Consequently, this work establishes itself as a robust and advanced solution in wormhole attack detection in MANET, offering superior performance and security-based metrics when compared to existing methods. These findings solidify the significance of our contribution to the field, highlighting the potential for practical applications and advancements in related research areas.

***E. Discussion of Findings:***

In this study, the performance of wormhole detection is evaluated based on the capability of different methods for their respective types. The proposed attention mechanism method, together with the decision tree classifier, has been evaluated using the simulated data obtained from the Matlab 2019b training and test subsets. More specifically, for the dataset, the features with a strong connection to the subject matter are chosen. With the proposed approach to determining the reliability of the restricted feature set during the feature selection process, the primary features are first determined. The performance of the proposed approach has been enhanced by implementing the Attention mechanism, removing irrelevant characteristics from the dataset, and applying a decision tree classifier. The proposed method has been compared with some well-known previous techniques, particularly the one that doesn't use the ML approach. In order to assess the proposed model, accuracy, precision, recall, and F1-score measurements are utilized for comparison. The outcomes indicate that the suggested method exceeds the previous methods in every information requirement.

The comparison between the models concludes that the results of the proposed method obtained are more accurate than the aforementioned models using the DT classifiers. The findings show the usefulness of the suggested approach in identifying attacks. Additionally, it is shown in the table above, and the accuracy and loss value for the proposed model are also shown in Fig. The models employing eight features produced better results for the acquired dataset than using all of the data.

## V. CONCLUSION

A wormhole attack is a type of attack on the network layer that reflects routing protocols. A training dataset is necessary to train models in any training mode. In order to identify wormhole attacks using attention mechanisms, real-time conditions or tests 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. We've obtained more than thirty thousand distinct samples in total, both normal and malicious, for this study. It creates a dataset with eight chosen features, and the last column indicates their labels. Decision-tree classification is used to classify data. To conclude, the results show that the accuracy, precision, sensitivity, and F1-score for both classification methods are better than the previous ones. Finally, In the future work, simulation will be done by increasing the number of wormhole tunnels to check the effectiveness of the proposed technique for different performance parameters and for a larger topological area for more flexibility and accurate results, which is one of the issues encountered, that is, a small amount of the dataset generated.

## REFERENCES

[1] M. Zanjireh, H. Zangeneh, and H. A. Jalab, "A new clustering algorithm for wireless sensor networks," in 27th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2013, pp. 1537-1542.

[2] Abdan, M. and S. A. H. Seno. "Machine learning methods for intrusive detection of wormhole attack in mobile ad hoc network (MANET)." Wireless Communications and Mobile Computing 2022: 1-12.

[3] Shastri, A. and J. Joshi (2016). "A wormhole attack in mobile ad-hoc network: detection and prevention". Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies.

[4] Farahani, G."Feature selection based on cross-correlation for the intrusion detection system."2020. Security and Communication Networks 2020: 1-17.

[5] M. Prasad, S. Tripathi, and S. K. Pandey, "Wormhole attack detection in ad hoc network using machine learning techniques," in 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-5.

[6] H.U., Y.C & Johnson, D.B Packet Leashes: "A defense against wormhole attacks in wireless ad hoc network". In INFOCOM 2004. Twenty-Third AnnualJoint Conference of the IEEE Computer and Communications Societies 2004 (Vol.4, pp. 1976-1986). IEEE

[7] Zardari, Z. A., et al. "A lightweight technique for detection and prevention of wormhole attack in MANET." 2021 EAI Endorsed Transactions on Scalable Information Systems **8**(29): e2-e2.

[8] Murty, M. K. and L. Rajamani "A Simple and Effective Intrusion Detection System for Manets." 2023.

[9] Patel, A., et al."Defending against wormhole attack in MANET". 2015 fifth international conference on communication systems and network technologies, IEEE.

[10] Panwar, A., et al. "A trust based approach for avoidance of wormhole attack in manet." (2020). International Journal of Computer Science and Mobile Computing **9**: 47-

[11] J. Li, K. Cheng, S. Wang et al., "Feature selection: a data perspective," *ACM Computing Surveys*, vol. 50, p. 94, 2017.