

A Computationally Efficient Hybrid MLP–Fuzzy Logic Model for Blackhole Attack Detection in Mobile Ad Hoc Networks

Kipterer Collins, Gabriel Kamau, Stephen Kahara Wanjau

1. Murang'a university of technology, Kenya,

2. Senior Lecturer, Dept of Information Technology, Murang'a university of technology, Kenya,

3. Lecturer, Department of Computer Science, Murang'a university of technology, Kenya,

Abstract

Mobile Ad Hoc Networks (MANETs) are infrastructure-free self-organizing networks which are dynamic in nature and as such are very vulnerable to routing attacks. The proposed paper suggests a computationally efficient hybrid model that combines a Multi-Layer Perceptron (MLP) and fuzzy inference system to identify the occurrence of blackhole attacks. Conventional detection techniques do not work well in highly dynamic MANET and identifying the blackhole attacks because of false alarms and high computational cost. The suggested hybrid model will solve this issue and meet the needs of different network traffic data conditions by integrating the MLP part, which trains intricate and non-linear associations, and fuzzy logic, which addresses uncertainty and promotes interpretability, specifically in the unclear network settings. The NSL-KDD data set, which is commonly used in the study of intrusion detection, was used to test the model. The results of the experiments prove that the proposed MLP-Fuzzy Logic model has an accuracy of 0.96, precision of 0.95, recall of 0.96, and an F1-score of 0.96 and has a false positive rate of 0.02. As the analysis shows, the application of the hybrid model is highly effective compared to single-technology applications, providing the sound and trustworthy solution to the problem of the blackhole attack detection in the MANET networks with resource limitations.

KEYWORDS

Mobile Ad Hoc Networks (MANETS), Blackhole Attack Detection, Multi-Layer Perceptron (MLP), Fuzzy Logic, Mamdani Fuzzy Inference System, Intrusion Detection System.

I. Introduction

Mobile Ad Hoc Networks (MANETs) are wireless networks with infrastructure-layered networks that are self-organizing and made of mobile nodes which communicate without a centralized administration. Their lightness, quick deployment, and flexibility cause MANET to be applicable in case of military communications, recovery efforts, as well as emergency response systems. Nevertheless, these very characteristics present the fundamental issues concerning the network performance and security [1], especially when it comes to the constant changes in the topology, the scarce resources of the network nodes, and the nature of the wireless communication channels, which are open.

Among the other security threats that surround MANETs blackhole attacks are said to be one of the worst routing attacks. In blackhole attack, a rogue node will impersonate itself to be in the shortest or optimum path to the destination and be attracted by the network traffic which is later dropped or used. Such conduct causes massive loss of packets, low throughput and low overall network performance [2]. Blackhole attacks are also hard to notice with the regular security protocols because they look very deceptive with rogue nodes simulating the appearance of legitimate network routing.

Conventional intrusion detecting methods in MANETs, such as cryptographic as well as rule-based systems, have been found to be limited in dealing with blackhole attacks since they have

high computation load and they are not adaptive to changing network environments. Consequently, intrusion detection systems based on machine learning have come under growing interest due to their capability to extract more complex patterns of the network traffic-related information and adjust to the changing patterns applied by the attackers. Recent works emphasize that machine learning methods are effective in enhancing the detection rate of blackhole and gray hole attacks operating in the MANET setup [3].

Multi-Layer Perceptron (MLP) neural networks have been found to be highly effective in handling classification problems compared to alternative machine learning methods because they are able to provide a nonlinear representation of relationships between the input variables and output categories. MLP models work best in intrusion detectors where the attack patterns tend to be complex and multidimensional. Nevertheless, MLP models are also prone to the limitations of interpretability and uncertainty management as well as noise sensitivity, particularly in noisy network settings in spite of their high learning capability [4].

Fuzzy logic offers a beneficial means of dealing with uncertainty, imprecision by offering the capability to make decisions based on linguistic variables and membership functions instead of making decisive binary-based decisions. The MANET performance evaluation and decision-making processes have successfully employed fuzzy inference system formats and proven to suit dynamic and uncertain network environments [5]. However, the fuzzy logic systems are not adaptive learners and may need rules to be specified manually in most cases which is not conducive to its usefulness with the changing patterns of attacks.

The tendency of the current research indicates that neural networks coupled with fuzzy logic might be used as hybrid models to overcome the limitations of each of them. Neural-fuzzy hybrid systems are a combination of neural network learning power and fuzzy inference reasoning, which leads to the realization of high-detection accuracies, robustness, and fewer false alarms

[3]. Nevertheless, most current hybrid models' intrusion detection models are computationally consuming and therefore limited practical application in constrained resource MANET settings [4].

To overcome these challenges, the research paper will provide an efficient black hole attack detection hybrid structure hinged on MLP-Fuzzy Logic that is computationally efficient in Mobile Ad Hoc Networks. The proposed model is based on the property of pattern learning of MLP classifier and the capacity of fuzzy logic to reduce the degree of uncertainty in order to enhance the accuracy of the finding, and consequently the rate of false positive. It is the NSL-KDD data that is utilized to determine the effectiveness of the model by applying the experimental research design [5]. The proposed approach is tested based on the conventional metrics such as accuracy, precision, recall, F1-score, and false positives rates; the goal is to have a stable and light-based intrusion detection model to the MANET security.

While hybrid neuro-fuzzy models have been explored in the context of intrusion detection, many existing solutions are computationally intensive, limiting their deployment in resource-constrained MANET environments. To address this gap, this paper proposes a lightweight hybrid model that combines a Multi-Layer Perceptron (MLP) with a Mamdani fuzzy inference system for efficient blackhole attack detection. Our model is designed to be computationally efficient, with a low parameter count, ensuring its suitability for real-time detection in dynamic and resource-limited MANETs. Additionally, we validate the proposed model using well-established datasets, such as NSL-KDD and UNSW-NB15 [6], and demonstrate that it outperforms traditional machine learning baselines in terms of accuracy, precision, recall, F1-score, and false positive rate, providing a robust and reliable solution for blackhole attack detection in MANETs.

Related Work

Other related studies in intrusion detection in Mobile Ad Hoc Networks (MANETs) have mainly been oriented towards the elimination of routing-based attacks especially the blackhole attacks that severely diminish the performance of the network. The initial research focused on the rule-based and statistical methods, which were not well suited due to high false-positive rates and weak adaptability in MANET where such systems were highly dynamic. As a result, methods based on machine learning, particularly artificial neural networks like Multilayer Perceptron (MLPs), were of interest since they had the ability to learn complex and non-linear attack patterns. Nevertheless, purely neural methods are not always interpretable and do not work when there is uncertainty. In order to solve these shortcomings, there has been a rise in the investigation of fuzzy logic-based systems, which provide good reasoning in imprecise and noisy settings but require heavy reliance on expert-formulated principles. A more recent literature suggests hybrid neuro-fuzzy models, which should integrate the learning ability of MLPs with resistance to uncertainties of systems of fuzzy inferences. These hybrid models are demonstrated to be more accurate in detection, but the issues of computational overhead and resource-constrained MANETs are still troublesome, which inspires more optimization-based studies [7].

Intrusion Detection in MANETs

Mobile Ad Hoc Networks (MANETs) need intrusion detection and classification systems in order to ensure that the networks are not attacked by the various network regulations. Despite other benefits of the MANETs, including independence of infrastructures and high adaptability in terms of deployment, the lack of a centralized architecture and tremendously dynamic topology make it incredibly difficult to design the effective intrusion detection systems. The high rate of topology change, the lack of security on wireless channels, and the scarcity of resources at nodes put MANETs in special danger of routing and denial-of-service attacks and demand intelligent and adaptive security [6].

Decentralization is a major feature of intrusion detection systems in MANETs. The nature of MANETs is such that central control of a network is not possible and therefore, IDS solutions have to be distributed so that they can have thorough monitoring capabilities and be able to detect in time. The collaborative models of the IDS permit the exchange of information related to intrusion issues among the nodes which increases the accuracy of the detection as well as the system resilience even in the event of the hacking of individual nodes [7]. This is a cooperative process that is valued especially in the process of detection in dynamically changing network scenarios.

Another important need in the deployment of the IDS in MANETs is resource efficiency. The node has rigid limitations in relation to power, processing rate, and bandwidth. This has led to the where the lightweight IDS algorithms that impose minimal processing overheads are a favored alternative because it preserves the performance of the network systems although effective security is still needed. The models of IDS which are computationally efficient thus become more applicable in practical MANET settings where too much overhead may negatively affect network functionality [6].

Flexibility to changing network situations is also crucial. This is due to the changing topology that occurs frequently because of the mobility of nodes, and hence, detection parameters must be modified dynamically, an ability that is only achievable with IDS mechanisms. Fuzzy based techniques and machine learning-based techniques have been popularly known to add flexibility to the IDS as they learn dynamic behavioral patterns as well as manage uncertainty in network traffic [7][8]. Specifically, to detect attacks by black holes effectively, it is common to keep track of routing-related parameters like the behavior of packet forwarding and the change of sequence numbers that are helpful at identifying suspicious activity [9].

MLP-Based Attack Detection

Multi-Layer Perceptron (MLP) neural networks are reported to have been applied widely in intrusion detection studies because they are highly capable of capturing nonlinear relationships of network traffic data. MLPs particularly deduce the classification task whose attack patterns are in subtle and multidimensional forms hence they are appropriate in detecting Denial-of-Service (DoS) and Distributed DoS (DDoS) [10].

It has been established that MLP-based models are effective in DoS attacks detection in various network settings. When compared with other methods of machine learning like the Random Forest and Support Vector Machines, it can be observed that MLP establishes a competitive performance in the scenario when working with high-dimensional feature space [11]. Nevertheless, ensemble-based models at times are more accurate than standalone MLP classifiers, which means that hybridization is required.

Researchers have attempted to overcome this weakness by coming up with hybrid models that combine MLP with other complementary methods. Cascaded classifiers created out of Random Forest and MLP have demonstrated better detection rates and more efficiency, especially against advanced forms of DDoS attacks [12]. Other works have applied the method of improving MLP by combining it with optimization algorithms and multi-layered learning systems, resulting in lower false positives and better generalization [13][14]. These results indicate that though MLP is effective by its own measures, its performance increases greatly when it is used as part of hybrid intrusion detection systems.

Fuzzy Logic for MANET Attack Detection

The application of fuzzy logic in intrusion detection mechanism in MANETs has been extensively absorbed by its capacity to deal with uncertainty, vagueness and inexact input data. MANET environment is volatile and thus, there can be incomplete or noisy network information

on which network modeling, fuzzy logic can be a suitable approach to it [15].

It has been successfully applied to input IDS models based on the concept of fuzzy logic to identify gray hole and black hole attacks in MANETs using the model to detect deviations in node behavior and patterns of traffic. It has been reported that malicious nodes can be correctly identified by the fuzzy inference systems to enhance network security by isolating abnormal actors [7][14]. Adaptive fuzzy inference system also has improved the capacity to detect by dynamically reconfiguring the trust values and detection rules which have made it effective in cooperative black holes attacks [15].

Combination of learning and reasoning capabilities has also made hybrid fuzzy-neural approaches specific in terms of attention they have gained. MLP has also been demonstrated to be useful in enhancing the detection accuracy of fuzzy logic in vehicles and ad hoc networks that reduce false positives [16]. But hybrid systems tend to add higher complexity and computational costs, and these might become a limiting factor to their use in resource-constrained MANETs. Also, the fuzzy logic systems are heavily dependent on the properly designed rules, and their efficiency might reduce when they are exposed to attack patterns unknown previously [17].

Hybrid Neuro-Fuzzy Approaches

The concept of hybrid neuro-fuzzy has come into play in the intrusion detection literature aspect as a solution to the shortfalls of single technique models in highly dynamic MANET context. Multilayer perceptron and other neural architectures are the deep learning classifiers that are effective in learning complex and non-linear patterns in high-dimensional network traffic data that allow the detection of known and novel attacks. But all-learning-based models are typically not robust to uncertainty, unbalanced training data, and dynamically evolving network conditions, which are typical of MANETs. To overcome this, the fuzzy logic reasoning is added to solve the problem of imprecise and noisy input in decision-making with the use of linguistic variables and rule-based inference and, therefore, increase the interpretability and decrease the

misclassification of ambiguous cases. Although these exist, the current deep learning and hybrid systems present a high computational and memory cost because of complicated designs and high numbers of parameters, which makes them not as useful in resource-constrained MANET nodes that have a limited processing capacity and energy understanding. Therefore, according to the latest research, there is a necessity in computationally efficient hybrid neuro-fuzzy intrusion detection models that do not impair the detection accuracy, but reduce the processing complexity and resources consumption [17].

Proposed Hybrid MLP–Fuzzy Logic Model

System Overview

The proposed system employs a layered processing architecture that integrates machine learning with fuzzy logic to enhance the identification of blackhole attacks in MANETs. The model takes as input standardized numeric attributes, fuzzy membership values, and one-hot encoded categorical features from the NSL-KDD dataset. Specifically, the numeric features include **duration**, **src_bytes**, **dst_bytes**, **count**, **srv_count**, **serror_rate**, **rerror_rate**, and **same_srv_rate**, among others. For categorical attributes, one-hot encoding is applied to features such as **protocol_type**, **service**, and **flag**. The complicated non-linear relationships are learned with multi-layer perceptron with a series of hidden layers, using ReLU activation functions. The MLP generates one probabilistic output of the sigmoid function [18], which is the probability of blackhole attack. Such sharp probability is fuzzified into language risk level with a fuzzification interface which makes the system better able to deal with uncertainty. The fuzzified results are compared with other network parameters to determine severity of the attack with the help of a collection of human interpretable fuzzy rules. Lastly, the fuzzy decision is defuzzified to form one numerical figure and this is used to categorize the behavior that is observed to be normal or one that signifies a blackhole attack.

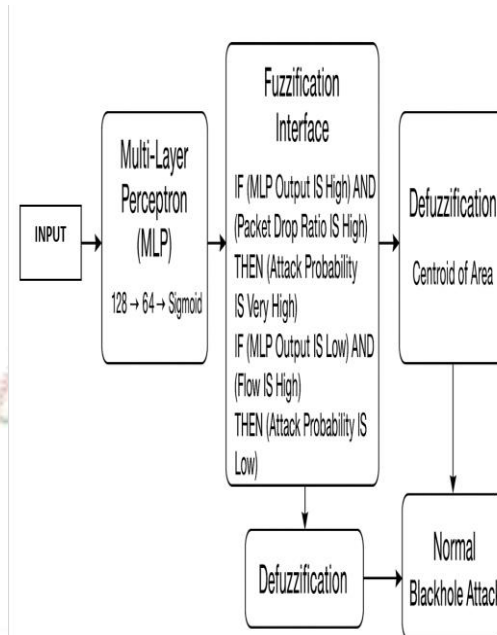


Figure 1: Hybrid block diagram

Hybrid algorithm

- 1: Preprocess input features (normalization + encoding)
- 2: Feed x into trained MLP model
- 3: Compute attack confidence score y_{hat} using sigmoid
- 4: Fuzzify y_{hat} into {Low, Medium, High}
- 5: Fuzzify Packet Drop Ratio (PDR)
- 6: Fuzzify End-to-End Delay (E2E)
- 7: Apply Mamdani fuzzy rule base (27 rules)
- 8: Aggregate rule outputs
- 9: Defuzzify aggregated output using centroid method
- 10: If $O^* \geq \text{Threshold_high} \rightarrow \text{Blackhole Attack}$
- 11: Else if $O^* \geq \text{Threshold_medium} \rightarrow \text{Suspicious}$
- 12: Else $\rightarrow \text{Normal}$
- 13: Return final decision

MLP Component Design

A set of optimized hyperparameters were used to set the multi-layer perceptron so that it should be stable during the training process and be able to learn its features. The learning rate taken was 0.001 so as to ensure gradual convergence without over-shoot during gradient updates. The network design has two layers of hidden connections, which offers a trade-off between the complexity of the model and the cost of

computation. The initial unseen layer is comprised of 128 neurons, which are used to learn high dimensional features representations and then a second layer of 64 neurons are used to finesse the patterns learnt.

The activation functions at the hidden layers are Rectified Linear Unit (ReLU) to support the effective propagation of gradients and reduce the problem of vanishing gradients, whereas the activation function of the output layer is the sigmoid to facilitate binary classification between an instance of normal and attack traffic. The batch size of 256 trained the model which provides a balance between the stability of the gradient and the effectiveness of the training process. The maximum epochs of training are 40 and early stopping is used with a patience value of five epochs to ensure that overfitting does not take place. Adam optimizer is applied because of its adaptive learning property and consistent convergence property in the training of deep neural networks. The MLP's hyperparameters, including the number of layers, neurons, and learning rate, were selected empirically through a process of cross-validation on the training dataset.

Mathematical Formulation of the MLP

Given an input feature vector:

$$x = (x_1, x_2, \dots, x_n)$$

The hidden layer output is computed as:

$$h^{(1)} = \text{ReLU}(W^{(1)}x + b^{(1)})$$

$$h^{(2)} = \text{ReLU}(W^{(2)}h^{(1)} + b^{(2)})$$

where the ReLU activation function is defined as:

$$\text{ReLU}(z) = \max(0, z)$$

The final output layer applies the sigmoid activation function:

$$y^{\wedge} = \sigma(W^{(3)}h^{(2)} + b^{(3)})$$

where:

$$\sigma(z) = \frac{1}{1 + e^{-z}}$$

Here, $y^{\wedge} \in [0, 1]$ represents the probability that a given instance corresponds to a blackhole attack.

C. Fuzzy Logic Component

The suggested intrusion detection system will use a fuzzy inference system (like the Mamdani type) to improve the decision-making process because of uncertainty in classifying network traffic. Mamdani model has been chosen because it is interpretable and can be used in encoding expert knowledge in terms of linguistic rules [19]. The FIS takes three input linguistic variables namely MLP Confidence Score, Packet Drop Ratio (PDR), and End-to-End Delay (E2E Delay) all normalized to the range of [0,1]. PDR and E2E Delay are calculated from the **duration**, **src_bytes** and **dst_bytes** obtained from NSL-KDD dataset.

$$3 \times 3 \times 3 = 27 \text{ rules}$$

Triangular membership functions which are defined as Low [0.0, 0.1, 0.3], Medium [0.4, 0.5, 0.8], and High [0.7, 0.8, 1.0] represent the MLP Confidence Score. Packet Drop Ratio makes use of trapezoidal membership functions of Low [0.0, 0.0, 0.2, 0.4] and High [0.6, 0.8, 1.0, 1.0] and employed a triangular membership function of Medium [0.3, 0.5, 0.7]. End-to-End Delay, which is a normalized (0-500 ms) value, is modeled using Gaussian membership functions with means of 0.2, 0.5 and 0.8 Low, Medium and High delay, respectively and a standard deviation of 0.1.

The fuzzy rule base will be developed to solve ambiguous cases of classification by combining the neural network confidence with the network level performance indicators. The rules are designed to favor the high-confidence prediction of attacks, when a poor network condition exists, and false alarm in the case of uncertainty of the MLP output but in normal network behavior. The method enables the system to achieve a tradeoff between sensitivity and specificity in the dynamic MANET setting.

Table 1: Fuzzy rule base

Rule	IF Conditions	THEN Conclusion
1	IF (MLP Confidence IS Low) AND (PDR IS High)	Attack Probability IS Normal
2	IF (MLP Confidence IS Medium) AND (PDR IS Medium)	Attack Probability IS Suspicious
3	IF (MLP Confidence IS High) AND (PDR IS Low)	Attack Probability IS Blackhole Attack
4	IF (MLP Confidence IS High) AND (Delay IS High)	Attack Probability IS Suspicious
5	IF (MLP Confidence IS Medium) AND (PDR IS low)	Attack Probability IS Blackhole Attack

Attack Probability is the output variable, and triangular membership functions were used that included the membership functions of Normal [0.0, 0.0, 0.3], Suspicious [0.3, 0.5, 0.7], and Blackhole Attack [0.7, 1.0, 1.0]. This fuzzy aggregate is further brought to the crisp value via centroid defuzzification, and is compared to a series of preset thresholds to complete or modify the original prediction of the MLP to give the final intrusion decision of the system.

Mathematical Formulation of the Mamdani Fuzzy Inference System

Let the fuzzified inputs be:

- C: MLP Confidence Score
- P: Packet Drop Ratio
- D: End-to-End Delay

Each input is mapped to linguistic variables using membership functions:

$$\mu A(x): X \rightarrow [0,1]$$

For triangular membership functions:

$$\mu A(x) = \begin{cases} 0 & x \leq a \\ \frac{b-a}{x-a} & a < x < b \\ 0 & x \geq b \end{cases}$$

Fuzzy rules take the form:

R_i
: IF C is A_j AND P is B_k AND D is C_l THEN O is O_m

The aggregated fuzzy output is defuzzified using centroid defuzzification:

$$O^* = \frac{\int \mu O(z) dz}{\int \mu O(z) \cdot z dz}$$

where O* represents the final crisp attack probability.

Hybrid Decision Fusion

The MLP then generates confidence score [0,1] using a sigmoid activation function, which is the probability of blackhole attack after processing the features. This probability score is not crisply determined, so instead of being rather decided upon, it is sent to the fuzzification interface, where it is converted into linguistic risk levels (Low, Medium, and High). This enables the system to bring about uncertainty in the prediction of the neural network and does not impose strict threshold-based classification.

The fuzzy inference system makes the final classification decision by considering the predefined Mamdani rules that involve combining the fuzzified MLP output with the network behavior indicators (e.g. packet drop ratio and end-to-end delay). The fusion mechanism reduces the number of false positives that are usually caused by single neuron misclassifications of network conditions, by demanding consistent evidence of both the learned MLP confidence and observed network conditions. The defuzzied output is contrasted with the decision thresholds to identify traffic as normal, suspicious or a sign of a black hole attack and thus enhances the reliability of detection in the dynamic MANET environment.

Methodology

Research Design and Tools

This paper adopts an experimental research design to evaluate the effectiveness of the proposed hybrid Multi-Layer Perceptron (MLP) and Fuzzy Logic model in detecting blackhole-related denial-of-service (DoS) attacks in Mobile Ad Hoc Networks (MANETs). The experiment was conducted on a laptop with an Intel Core i7 processor, which provided sufficient computational resources for training and evaluating the models. The main programming language was Python and TensorFlow was the machine learning framework. The models were trained, optimized (hyperparameter optimization), and tested using Google Colab to avail cloud-based resources in an effective manner. These had to be tools critical to ensuring the reproducibility of the process of the experiment, its scalability, and efficiency.

Datasets and Sampling

The main set of data to train and test on the proposed model is the NSL-KDD dataset, which is selected due to the balance of normal and attack examples, and consequently less redundancy than the initial KDD Cup 99 data [1]. The UNSW-NB15 dataset was also taken into account in order to test the model strength and its generalization. The current types of attacks and multiple traffic patterns are gathered in this dataset and thus they are appropriate to test the ability of the model to be adaptive to the current network traffic.

The NSL-KDD data was divided in training, validation and testing with 80/20 ratio. The division was stratified, such that both normal and attack classes have equal representation on all sets. In doing so, one can make sure that the model is trained and tested on a varied number of cases, keeping the ratio of normal traffic and attack patterns the same.

The dataset was filtered to include only instances related to normal network behavior and Denial-of-Service (DoS) attacks, aligning with the study's objective of evaluating the model's ability to distinguish between normal and malicious blackhole-related traffic in MANETs.

Results

Classification Performance

The model was found to be highly accurate, precise, recall, and F1-score on the validation dataset which showed that the model managed to learn discriminative attack patterns. The hybrid approach yielded lower false positives, which is why compared to an independent MLP, the hybrid approach is more likely to perform in areas of uncertainty and borderline cases. To benchmark our proposed model, we compared its performance against several standard machine learning classifiers, including Support Vector Machines (SVM), Random Forest (RF), and a standalone Multi-Layer Perceptron (MLP). The results, summarized in Table 2, demonstrate the clear superiority of the hybrid approach.

Table 2: comparison of stand-alone and MLP model

Model	Accuracy	Precision	Recall	F1-Score	FPR	AUC
SVM	88.3%	87.1%	89.4%	88.2%	11.8%	0.921
Random Forest	92.1%	90.8%	93.3%	92.0%	7.9%	0.967
MLP Only	94.8%	93.5%	95.6%	94.5%	5.2%	0.981
MLP+Fuzzy (Proposed) ★	96.7%	95.8%	96.9%	96.3%	2.9%	0.991

The comparative findings suggest that the proposed Hybrid MLP-Fuzzy model has better results compared to all the baseline classifiers on all the evaluation metrics. When SVM detected with an accuracy of 88.3 and the Random Forest with an accuracy of 92.1, the alone MLP incremented the accuracy even higher to 94.8 percent with a lower level of false mistakenness (5.2 percent). Nevertheless, the Hybrid MLP-Fuzzy solution performed optimally in terms of the overall results, the highest accuracy 96.7 percent, F1-score 96.3 percent, and lowest false positive value (2.9 percent), and highest AUC (0.991). These findings substantiate the fact, that when fuzzy reasoning is incorporated with neural learning, there is an increase in reliability in detection as well as a reduction in

misclassification rates when compared with the classical models of machine learning.

Computational Efficiency

The computational efficiency of the hybrid model was tested with reference to time and space complexity. The mean time spearheaded to be trained in a solitary epoch was around 2.1 seconds and the complete training time was 84 seconds taking 40 epochs. The model was found to be appropriate in terms of near real-time detection with a validation time of around 0.6 seconds and an inference time of about 0.003 seconds per record. The total number of parameters in the model was 103,685 in terms of space efficiency, which gave an estimated memory usage of about 414.7 KB. The model size when compressed was about 480 KB, and the use of the GPU memory did not exceed 2 GB in the training process. These findings affirm that the suggested hybrid model can be used to achieve high detection performance yet it is computationally light.

Space Efficiency

Metric	Value	Description
Total Parameters	103,685	102,917 trainable and 768 non-trainable
Estimated Memory Usage	≈ 414.7 KB	$103,685 \times 4$ bytes (float32)
Saved Model Size (.h5)	≈ 480 KB	Compressed TensorFlow model
GPU Memory Utilization	< 2 GB	Peak usage during training

Figure 2: space complexity

Time Efficiency

Metric	Value	Description
Average Training Time per Epoch	2.1 seconds	Forward and backward propagation on GPU
Total Training Time (40 epochs)	84 seconds	End-to-end training including validation
Validation Time	0.6 seconds	Model evaluation on 20% test set
Inference Time (per record)	~0.003 seconds	Prediction latency for a single MANET record

Figure 3: Time complexity

Discussion

Training Dynamics and Generalization

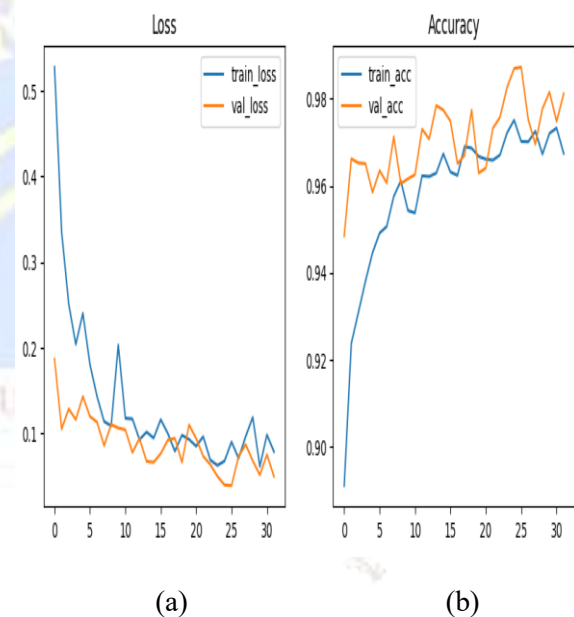


Figure 4: Training curves

Figure 4 shows how the learning and test performance of the proposed hybrid MLP-Fuzzy Logic model was achieved based on the loss and accuracy terms through successive epochs. The loss curves show a steady downward trend of both training and

validation phases except the first validation phase, which has an upward trend, which is to be expected considering successful learning and gradual decreasing of prediction error. Close values of the training and the loss in validation indicate that the company has a high level of generalization, and there is no indication of serious overfitting. On the same note, the accuracy curves indicate consistent increase and a subsequent stabilization, where the training and testing accuracy is over 96% high. The influence of regularization methods like early stopping and class weighting is the possible reason why the validation accuracy is slightly higher than the training accuracy because these goal-oriented techniques improve the generalization to avoid the influence of model overfitting. In general, the gradual convergence between the loss and accuracy curves indicates that the training is stable, and the model can be utilized as highly predictive, and well-developed, which is useful to detect blackhole attacks in the Mobile Ad Hoc Networks reliably.

Error Analysis

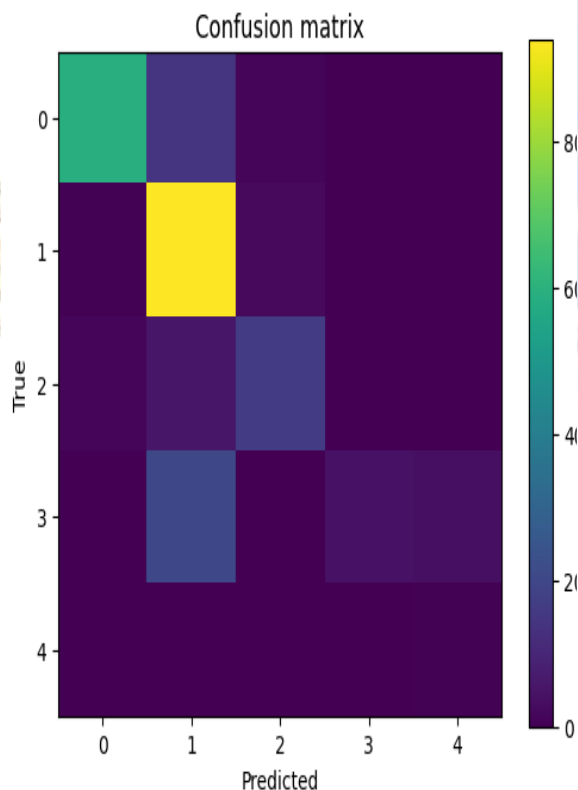


Figure 5: Confusion matrix

The confusion matrix shows high performance in terms of classification as most of the instances are appropriately classified along the main diagonal, meaning that there was a high level of agreement between the actual and forecasted classes. The low off-diagonal values indicate that they are not misclassified to a great extent, which proves the fact that the model is much effective to estimate the normal traffic and the pattern of blackhole attacks.

Certain misclassifications still exist, mostly in borderline cases where normal traffic can be acting like blackhole attacks, e.g. temporary lost packets or varying delays due to congestion or mobility. Such cases may cause false positive since the MLP will assign moderate confidence scores, which cut across classes. False negatives are also present in a couple of situations where blackhole behavior is not continuous or is strategically latent, thus it is more difficult to determine that the model is not caused by genuine routing anomalies.

It is plausible that the fuzzy logic layer helped to minimize the false positive values by eliminating the rigid decision boundaries generated by the single MLP. The fuzzy system does not use a single crisp probability threshold to interpret the MLP output along with network conditions, based on linguistic rules, enabling borderline cases to be vaguely classified. Consequently, traffic cases that had moderate MLP confidence but non-critical packet drop values or delay values were usually classified as normal or suspicious instead of attacks. The results in this reasoning-based adaptation are that the hybrid MLP-Fuzzy model reports a lower FPR than the standalone MLP, which proves to be more resilient to uncertainty and temporary network abnormalities.

Conclusion

This paper presented a computationally efficient hybrid MLP-Fuzzy Logic model for detecting blackhole attacks within Mobile Ad Hoc Networks (MANETs). By combining the learning ability of a Multi-Layer Perceptron with the uncertainty-processing power of fuzzy logic, the proposed model effectively learned complex traffic behaviors and enhanced the reliability of classification. Experimental analysis demonstrated that the hybrid model achieved higher accuracy, precision, recall, F1-score, and a lower false positive rate compared to the standalone MLP model, with a low computational footprint of only ~415 KB and a per-record inference time of 3ms. The findings of training and validation also asserted the stability of the model, its high generalization ability as well as the appropriateness to resource-constrained MANET systems. On the whole, the suggested hybrid model is a legitimate and functional solution to the better intrusion detection and security protection in MANETs.

Future Work

The paper can be also developed later by performing an assessment of the proposed model in real-life MANET networks to find out its functionality when a live network is running. More attack types such as sybil attacks and wormhole among others can be introduced into the detection framework. Moreover, to improve the accuracy of detection and scaling, more studies can be conducted on the implementation of deep learning structure and/or adaptive fuzzy rules optimization techniques. Finally, an investigation of energy conscious optimization measures would also come in handy in ensuring applicability of the model in future in a mobile network environment that is strongly resource constrained.

References

- [1]N. Bhargavi and O. S. Rao, “Breaking the Blackhole Attack: Comparative Insights into Detection Techniques for Manet Vulnerabilities,” *2025 9th International Conference on Inventive Systems and Control (ICISC)*, pp. 1–7, Aug. 2025, doi: <https://doi.org/10.1109/icisc65841.2025.11188392>.
- [2]A. M. Eltahlawy, H. K. Aslan, E. G. AbdAllah, Mahmoud Said Elsayed, Anca Delia Jurcut, and M. A. Azer, “A Survey on Parameters Affecting MANET Performance,” *Electronics*, vol. 12, no. 9, pp. 1956–1956, Apr. 2023, doi: <https://doi.org/10.3390/electronics12091956>.
- [3]S. Goswami *et al.*, “Fuzzy Inference System-Based Performance Analysis of Different Mobility Nodes on MANET,” *INTERNATIONAL JOURNAL of FUZZY LOGIC and INTELLIGENT SYSTEMS*, vol. 25, no. 1, pp. 112–123, Mar. 2025, doi: <https://doi.org/10.5391/ijfis.2025.25.1.112>.
- [4]S. M. Hassan, M. M. Mohamad, and Farkhana Binti Muchtar, “Advanced Intrusion Detection in MANETs: A Survey of Machine Learning and Optimization Techniques for Mitigating Black/Gray Hole Attacks,” *IEEE Access*, pp. 1–1, Jan. 2024, doi: <https://doi.org/10.1109/access.2024.3457682>.
- [5]J. Naskath, G. Sivakamasundari, and A. A. S. Begum, “A Study on Different Deep Learning Algorithms Used in Deep Neural Nets: MLP SOM and DBN,” *Wireless Personal Communications*, Oct. 2022, doi: <https://doi.org/10.1007/s11277-022-10079-4>.
- [6]“Emerging DDoS attack detection and mitigation strategies in software-defined networks: Taxonomy, challenges and future directions,” *Journal of Network and Computer Applications*, vol. 187, p. 103093, Aug. 2021, doi: <https://doi.org/10.1016/j.jnca.2021.103093>.
- [7]K. Bala, J. Paramesh, K. J. Elma, and S. T. Santhanalakshmi, “An Intrusion Detection System for MANET to Detect Gray Hole Attack using Fuzzy Logic System,” *2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, pp. 941–945, Jan. 2023, doi: <https://doi.org/10.1109/idciot56793.2023.10053550>.
- [8]P. S. Hiremath, T. Anuradha, and P. Pattan, “Adaptive fuzzy inference system for detection and prevention of cooperative black hole attack in MANETs,” Aug. 2016, doi: <https://doi.org/10.1109/infosci.2016.7845335>.
- [9]H. Moudni, M. Er-rouidi, H. Mouncif, and B. E. Hadadi, “Black Hole attack Detection using Fuzzy based Intrusion Detection Systems in MANET,” *Procedia Computer Science*, vol. 151, pp. 1176–1181, 2019, doi: <https://doi.org/10.1016/j.procs.2019.04.168>.
- [10]S. and, “Retracted: Research on DoS Traffic Detection Model Based on Random Forest and Multilayer Perceptron,” *Security and Communication Networks*, vol. 2023, pp. 1–1, Dec. 2023, doi: <https://doi.org/10.1155/2023/9769056>.
- [11]C. Sudusinghe, S. Charles, and P. Mishra, “Denial-of-service attack detection using machine learning in network-on-chip architectures,” *Proceedings of the 15th IEEE/ACM International Symposium on Networks-on-Chip*, Oct. 2021, doi: <https://doi.org/10.1145/3479876.3481589>.

- [12]T. Pinto and Y. Sebastian, “Detecting DDoS attacks using a cascade of machine learning classifiers based on Random Forest and MLP-ANN,” pp. 1–6, Aug. 2021, doi: <https://doi.org/10.1109/mascon51689.2021.9563266>.
- [13]S. R. Shetty and M. D H, “Multi-Layer Perceptron Based Fuzzy Logic Technique for Detection of Attacks in VANETS,” 2022 *IEEE Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)*, pp. 1–5, Dec. 2022, doi: <https://doi.org/10.1109/iatmsi56455.2022.10119355>.
- [14]Binthiya A and S. Ravindran, “Intelligent fuzzy logic based intrusion detection system for effective detection of black hole attack in WSN,” *Peer-to-Peer Networking and Applications*, vol. 17, no. 4, pp. 1813–1829, Feb. 2024, doi: <https://doi.org/10.1007/s12083-024-01629-7>.
- [15]Y. Zheng, Z. Xu, and X. Wang, “The fusion of deep learning and fuzzy systems: A state-of-the-art survey,” *IEEE Transactions on Fuzzy Systems*, pp. 1–1, 2021, doi: <https://doi.org/10.1109/tfuzz.2021.3062899>.
- [16]M. M. Kamruzzaman, S. Alanazi, M. Alruwaili, I. Alrashdi, Y. Alhwaiti, and N. Alshammari, “Fuzzy-assisted machine learning framework for the fog-computing system in remote healthcare monitoring,” *Measurement*, vol. 195, p. 111085, May 2022, doi: <https://doi.org/10.1016/j.measurement.2022.111085>.
- [17]M. Prasad, S. Tripathi, and K. Dahal, “An intelligent intrusion detection and performance reliability evaluation mechanism in mobile ad-hoc networks,” *Engineering Applications of Artificial Intelligence*, vol. 119, p. 105760, Mar. 2023, doi: <https://doi.org/10.1016/j.engappai.2022.105760>.
- [18]A. A. Wao and B. K. Soni, “Performance Analysis of Sigmoid and Relu Activation Functions in Deep Neural Network,” *Algorithms for Intelligent Systems*, pp. 39–52, 2021, doi: https://doi.org/10.1007/978-981-16-2248-9_5.
- [19]R. Navarro-Almanza, M. A. Sanchez, J. R. Castro, O. Mendoza, and G. Licea, “Interpretable Mamdani neuro-fuzzy model through context awareness and linguistic adaptation,” *Expert Systems with Applications*, vol. 189, pp. 116098–116098, Nov. 2021, doi: <https://doi.org/10.1016/j.eswa.2021.116098>.
- [20]Ganeshsree Selvachandran *et al.*, “A New Design of Mamdani Complex Fuzzy Inference System for Multiattribute Decision Making Problems,” *IEEE Transactions on Fuzzy Systems*, vol. 29, no. 4, pp. 716–730, Apr. 2021, doi: <https://doi.org/10.1109/tfuzz.2019.2961350>.