IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Mathematical Modelling of Engineering Problems
Vol. 12, No. 11, November, 2025, pp. 4041-4048
Journal homepage: http://iieta.org/journals/mmep

A Deep Learning Framework for Black Hole Attack Detection in SDN-Integrated MANET-IoT Environments

Hassan Hadi Saleh[1], Abd Ali Hussein[2], Saja Salim Mohammed[3], Mayssam Saad Kadhum[4*], Kilan M. Hussein[3], Mustafa Nadhim Ghazal[4]

[1] Department of Computer Science, College of Education for Pure Science, University of Diyala, Diyala 32001, Iraq
[2] Department of Computer Engineering, College of Engineering, University of Diyala, Diyala 32001, Iraq
[3] Department of Computer Science, College of Science, University of Diyala, Diyala 32001, Iraq
[4] Department of Communications Engineering, College of Engineering, University of Diyala, Diyala 32001, Iraq

Corresponding Author Email: mayssam.saad.eng.elctron@uodiyala.edu.iq

https://doi.org/10.18280/mmep.121130

Received: 18 July 2025
Revised: 16 September 2025
Accepted: 25 September 2025
Available online: 30 November 2025

Keywords:
mobile Ad-hoc, software defined networking, IoT, BiLSTM, MANET

ABSTRACT

Mobile Ad-hoc Networks (MANETs) are networks of wireless devices formed from mobile nodes that might self-configure and self-healing. They offer scalability and independence from fixed infrastructure, making them compatible with a variety of applications, including duties in the military, disaster recovery, healthcare, sensor networks, and the Internet of Things (IoT). To enhance the effectiveness of software-defined networking (SDN) and address the challenges of MANETs, SDNs have been developed to integrate centralized control with flexible governance. Notwithstanding this advancement, MANETs continue to be susceptible to blackhole attacks, where malicious nodes sever packet flow to and from them, thus disrupting network connectivity. This research proposes a deep learning-based detection approach tailored for SDN integrated with MANET-IoT ecosystems. A hybrid DL network architecture is proposed in this work, which integrates several one-dimensional convolutional layers with Bidirectional LSTM (BiLSTM) and LSTM units, capturing both spatial and sequential dependencies from the network traffic data. This was supported by constructing a reasonable dataset through blackhole condition simulations with 16 nodes on the IoT-Lab testbed with varying packet sizes. Critical parameters such as round-trip time (RTT), packet loss, and routing anomalies were incorporated into the dataset. Experimental findings indicated that the proposed approach surpassed comparable state-of-the-art algorithms, achieving an impressive 99.5% detection accuracy. This paper illustrates the potential of deep learning in enhancing threat detection within SDN-enabled MANET-IoT networks.

1. INTRODUCTION

An ad hoc wireless network is the name given to a wireless communication network made up of mobile devices like smartphones. In the absence of fixed infrastructure, these nodes are capable of creating a network that is decentralized in nature and can dynamically configure itself. A collection of mobile nodes that are capturing and sharing information is known as “mesh”. Each node acts autonomously as a router. Within a network, membership have the ability to move and change their places of residence, which makes it easier for them to share resources. Due to its restricted resources, Mobile Ad-hoc Network (MANET) has a number of difficulties, including power limitations, reduced bandwidth, range, and security [1]. One of the primary problems with MANET is its shortage of a centralized control and command architecture. MANET comprises two phases for mobile node communication across multi-hop wireless channels: link layer protocol, which ensures one hop connectivity across multiple hops, and the protocol of network layer, which extends the connectivity to multiple hops [2]. Two of the most significant tasks of the network layer are forwarding data packets and performing ad hoc routing. They communicate with one another for the purpose of carrying packets from where they came from to the destination. The ad hoc routing protocol may maintain the route configurations of every node up to date by transmitting messages regarding routing between them [3]. However, each packet forwarding as well as routing activities are vulnerable to malicious attacks, which can lead to a variety of disruptions in the network layer. These interruptions can be caused by a number of different factors. Attackers have the ability to bring traffic to certain locations within the network by using various routing protocols [4].

These networks suffer from two main issues: energy conservation and security breaches brought on by attackers. The advanced communication system that separates the control plane from the system informational plane is called software-defined networking (SDN) [5]. It is thought to be a dynamic, layered, scalable, and energy-efficient method of managing and controlling network topologies, both wired and

wireless. In SDN-based MANETs, a logically centralized SDN controller is responsible for managing flow rules, monitoring network traffic, and updating routing paths in real time. The SDN controller and MANET were combined to address security-related issues [2]. SDN MANET indicates that the structure has been customized to a certain operational requirement, ecosystem conditions, and equipment performance. Some of the primary benefits of SDN MANET are network administration, bandwidth control, improved security, and managing energy while routing. This centralized control also allows for dynamic mitigation of malicious behavior and anomaly detection based on global network state [6].

In MANET, there are two different types of attacks [7], both passive and active. Passive attacks [8] do not change the data delivered over the networking; rather, they attempt to harvest sensitive data from network communications. A passive attacked node might act selfishly in order to steal the information that was sent. Passive attacks are challenging for detection because they are not disrupting network functionality [9]. Typically, encryption is used to defend against passive attacks. Active attacks [10] hinder the passage of messages between nodes. Intruders inject false information into the network. These attacks can occur at any protocol layer, including network, transport, application, and others. Active attacks are more severe and can be either internal or external in nature [11]. Black Hole Attack is one type of active attack [12]. The performance of a MANET can be significantly affected by a black hole attack, which can be executed by either a one independent node or as a collective of malicious nodes. In a black hole attack, a node that is malicious uses it is routing protocol to advertise itself as the node with the shortest path to the target [13]. They present a novel detection scheme for active and passive black-hole attacks in MANETs. Furthermore, the system is concerned with evaluating a set of selected characteristics for every node-based on AdaBoost SVM technique. These characteristics are gathered from cluster member nodes using Ad hoc On-demand Multi Path Distance Vector (OMDV) and Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol for routing and clustering methods. Since SVM appears to be a stable classifier, the AdaBoost weight adaptation technique significantly impacts the classification process by enhancing the weights of the extracted features. This hybrid approach is essential for detecting both passive and active black hole threats in MANETs [13]. This aggressive node announces the availability of new routes without examining its routing table. In this attack, the perpetrator node is always able to respond to the route request, so it modifies the data packet and discards it [14]. In a protocol dependent on flooding, the requesting node will receive the malevolent node's response before receiving a response from an actual node; thus, a malicious and bogus route will be created. When this route is configured, it is up to the node to decide whether to delete packets or forward them toward an unknown destination [15]. Mitigates identified security threats [16]. Effect of mobility variation to determine the accuracy of the detection process, including the routing overhead protocol [17]. Implements Dynamic Spectrum Resource Control (DSRC) as a mechanism to perform real-time threat mitigation after threat detection for network recovery purposes [18]. Spike neural networks have also been shown to classify SDN traffic efficiently [19].

To address this issue, we propose a DL-based detection model tailored for SDN-based MANET-IoT networks. The architecture combines multiple 1D convolutional layers with BiLSTM and LSTM units to learn both temporal and spatial behavior of network traffic. The second contribution is the simulation strategy and dataset generation, performed using the IoT-Lab testbed with controlled black hole attack scenarios and multiple packet sizes across 16 nodes. In along with providing high-accuracy detection, this dataset replicates actual IoT traffic behavior.

2. MACHINE LEARNING TECHNIQUES FOR DETECTION OF BLACK HOLE ATTACKS IN MANET-IOT NETWORKS

It is noted that additional research is needed on the implementation of machine learning for security purposes in MANETs. Attacks within MANET can be effectively managed with the help of machine learning resources, which are capable of automated attack detection and information on specific attack patterns. More recent publications about blackhole attack detection on MANETs include. Mahin et al. performed a blackhole attack with two infected nodes in 2019. They managed through QualNet 7.4v emulator, which was building control DYMO routing protocol on the network. Some of the metrics in analyzing QualNet statistics data include packet delivery ratio (PDR), packet loss rate, throughput, and average transmission latency.

To monitor the system, average transmission latency, as well as packet drop rate, are defined. In this study, the authors use different machine learning classifiers and compare their accuracy for the selected metrics. The DT, KNN, SVV, and neural network classifiers were tested in MATLAB. The authors believe that SVM is the most accurate classifier when compared to other algorithms.

Effectively diagnosing the black hole attack and mitigating it by deactivating the malicious nodes at the appropriate moment, the proposed mechanism enables the network to achieve peak performance. Later, the work is evaluated against a variety of speeds, pause times, and terrain types to validate our proposal. After applying the proposed strategy, it is perceived that the network's performance has improved, resulting in an increase in PDR and throughput and a decrease in packet drop rate along with transmission latency. Through this endeavor the weaknesses of DYMO routing protocol have been successfully bridled. Research results indicated that the SVM achieves the highest possible detection accuracy, which is 97.5%, while NN gain second best detection value which is 95%, DT and KNN gain the lower results which are 92.5% and 85% respectively.

However, practical deployments of SDN-MANETs face real-world limitations. DL-based intrusion detection models can be computationally intensive and may not be optimal for energy-constrained IoT devices [20]. In addition, our experiment is limited to 16 nodes, and further validation is needed to ensure scalability. This limitation, while representative for controlled testbeds, may affect scalability when transitioning to real-world, large-scale deployments Finally, adversarial evasion techniques that manipulate input data could potentially deceive detection models, posing another challenge that future implementations must address.

Jayakrishna and Prasanth [20] presented an effective intrusion identification and prevention model for MANET using a hybrid KNN-LSTM classifier with COOT optimization for increasing network security. The suggested intrusion prevention and detection approach is divided into

four phases: separating attack nodes from normal nodes, forecasting different sorts of assaults, determining the frequency of attacks, and implementing an intrusion prevention mechanism. For achieving the highest trust value, the attack nodes are differentiated from the normal nodes using COOT optimization in the first instance. In the second phase, a hybrid LSTM-KNN model for detection of any kind of network threat is demonstrated. Preprocessing, feature extraction, and classification of different types of attacks are all done in the second phase.

The proposed methodology will be assessed with respect to mobility volatility to measure the precision of the detection process, including the expenses related to the routing protocol. According to the evaluation outcomes, the MANET successfully identified both passive and active black hole attacks with a 97% accuracy rate and a reasonable time complexity across different mobility scenarios. Additionally, the strategy proposed accurately differentiates between malicious and benign node dropout behavior by using a tunable threshold. Different machine learning algorithms were applied by Abdan and Seno et al. [21], such as KNN, DT, SVM, CNN, NB, and LDA. Moreover, as far as feature extraction in the context of MANETs is concerned, we added node attributes, especially the node speed, to our extraction features. A total of 3997 samples have been gathered, consisting of 3781 normal samples and 216 attack samples, encompassing both normal and malevolent models. The classification results show that the SVM achieves 97.1%, KNN achieves 98.2%, DT achieves 98.9%, LDA achieves 94.7%, Naive Bayes (NB) achieves 95.2%, and CNN techniques achieve 96.4% in accuracies. According to the results of their study, the accuracy of the DT method achieved 98.9%, which surpasses the accuracy of alternative approaches. In the subsequent order, LDA, CNN, NB, KNN and SVM show a good level of accuracy.

The third phase carries out assault classification, determining if the attack is abnormal or normal. DNA encryption algorithm is applied for security, and the final phase tries to limit the attack nodes detected in the network using a two-stage authentication scheme. More satisfactory results were obtained when the suggested hybrid KNN-LSTM classification model was compared with a set of measures, including 96% inaccuracy, 93% precision, 82% recall, 0.04 error rate, and 85% F1-score. This proves that the proposed security solution successfully reduces severe MANET attacks.

To further improve attack detection in MANET and SDN-IoT settings, various recent research works investigated hybrid DL and ensemble learning methods in addition to the aforementioned works. For example, Altunay and Albayrak [22] analyzed machine learning for wireless sensor network applications, and Alsheikh et al. [23] suggested a hybrid CNN-LSTM model for IoT-based intrusion detection. Primarily for MANETs, Alsoufi et al. [24] used anomaly-based deep learning methods. Pandey and Singh [25] and Rui et al. [26] have also shown ensemble approaches to carry out black hole detection, which provide valuable frameworks for malicious node detection. Other efforts, like made by Abdallah et al. [27] and Webber et al. [28], are based on trust-aware classification models and SDN-based secure routing. Additionally, an integrated DL intrusion detection model designed for SDN systems was described by Ataa et al. [29]. These approaches collectively underscore the growing significance of intelligent, adaptive models for securing next-generation ad hoc networks.

3. METHODOLOGY

3.1 Dataset generation

To simulate an attack, the first step is to collect data from a network. In this experiment, we put up an accessible IPv6 Wireless Personal Area Network (WPAN) net in Grenoble on 16 nodes from IOT-Lab with different packets sizes 10, 20, 50, 100 and 200. The data that we analyze is derived from a series of tests on IoT devices, which we performed in a simulator. We want to know if we can recognize network attacks inside the IoT environment using data from Internet Control Message Protocol (ICMP), a particular network layer protocol packet. The experiment set includes scenarios involving Black Hole attacks, along with typical behavior. To emulate black hole attacks, selected nodes were configured to drop all incoming packets while falsely advertising optimal routing paths through manipulated RPL control messages. This ensured the attacker could attract traffic while preventing successful delivery. Each experiment is run in a period of 200 ICMP pings for each node. This value was chosen as a compromise between ensuring sufficient statistical diversity and maintaining a manageable experiment runtime on the constrained IoT-Lab testbed. The resulting dataset includes key features such as round-trip time (RTT), packet loss, hop count, and routing anomalies. Outliers were identified by applying the Interquartile Range (IQR) method to the RTT values, where any RTT below $Q1 - 1.5 \times IQR$ or above $Q3 + 1.5 \times IQR$ was labeled as anomalous behavior. These outliers are critical in signaling delay-based disruptions caused by attack scenarios. The dataset generated involves several relevant features that include:

- Node ID (node id): The ID of each of the 16 nodes.
- Packet Count (pckt_count): Number of packets received during certain packet time.
- Total RTT (tr_time): The summation of RTT of each node during test with a specific packet size. RTT represents the time measured in milliseconds (ms), required for a connection request to go from its starting point to its destination and back.
- Hops: The number of routers through which a packet (a portion of data) travels from the source to its destination.
- Outliers: Number of anomalies during a specific time.
- Loss: The number of packets lost during a specific time.
- Var: The RTT Variance, which indicates path jitter.
- Mean: The mean (average) RTT.
- Max: The maximum RTT.
- Min: The minimum RTT.

Table 1. Sample of the generated dataset

Node	Tr_time	Pckt_count	Mean	Var	Hop	Min	Max	Loss	Outliers	Label
aaaa::212:740°:0:0:8	1020.473	181	5.63922	0.13841	4	5.01728	6.67236	19	11	1
aaaa::212:740°:0:0:4	908.424	195	4.65568	0.17689	2	4.05263	6.81404	5	11	0
aaaa::212:7407:0:0:7	908.0212	181	5.34815	0.16515	3	4.59145	7.24356	19	10	1
aaaa::212:7406:0:0:6	703.2819	148	4.75217	0.20704	2	4.13676	6.57697	52	7	0
aaaa::212:740e:0:0:e	851.6833	127	6.70272	0.13688	5	5.97886	7.62168	73	7	0

In addition, it includes a label indicating whether the node is part of a black hole attack. Table 1 shows the sample of the dataset.

3.2 Proposed model structure

Four 1D layers based on convolution, two BiLSTM layers, two LSTM layers, an input layer, a permute layer, a concatenate layer, a dropout layer, and a dense layer are all incorporated in the proposed model. This CNN layout combines several types of different functional layers, including rectified linear units (ReLU), pooling, and convolution. Data from time series provides sequential substances that are necessary for interpretation and are adequately retrieved by the convolutional layer. In CNNs, pooling layers make down sampling less difficult. The CNN employs the band combinations generated by the permutation layer to create strong classifying features. By combining the outputs of multiple disparate layers into a single tensor, the pooling layer is essential for multi-task learning. By leveraging common features across tasks, this fusion improves performance and is best suited for combining features learned from different activities. Furthermore, pooling layers improve the training efficiency of multi-task models by reducing training time and parameters. This efficiency results from the application of shared layers, which enables the model to learn from more than one task simultaneously. Furthermore, by aggregating similar features across tasks, pooling layers improve the model's ability to generalize across new data points. The model becomes better able to handle new cases that are similar to cases learned by transferring knowledge from various processes. Below is a representation of the presented model, a three-level stacked CNN-BiLSTM-LSTM model with an autoencoder architecture:

- **Layer 1**: Input layer.
- **Layer 2** (permute layer): The dimensions for the input are modified employing this type of layer.
- **Layer 3**, or its convolutional 1D layer: This layer is composed of up to 128 filters, each with a padding of 1 and a kernel size of 3. This layer transports results to the convolutional layer (Layer 5), resulting from the collection of input data from the input layer (Layer 1).
- **Layer 4** (convolutional 1D layer): This layer, containing 128 filters with a kernel dimension of 3 and padding of 1, accepts the data input from Layer 2 (permutes layer) and passes its outcome to Layer 6 (convolutional layer).
- **Layer 5**: This convolutional 1D layer has 64 filters with a kernel size of 1 and a padding of 1. For the purpose of transmitting outputs to the Layer 7 (BiLSTM layer), this layer receives input data from Layer 3 (convolutional layer), mirroring Layer 5.
- **Layer 6** (convolutional 1D layer): This layer comprises 64 filters with a kernel dimension of 1 and padding of 1. Furthermore, it collects information from input from the convolutional layer (Layer 3) and transfers it towards the BiLSTM layer (Layer 8).
- **Layer 7**: Convolutional Layer 5's incorporated layer, the BiLSTM layer, has 128 filters. It transfers outputs to the Layer 9 (LSTM layer) while collecting input data from the Layer 5 (convolutional layer).
- **Layer 8** (BiLSTM layer): The combined layer for convolutional Layer 6 has 128 filters. It transfers results to the Layer 9 (LSTM layer) after collecting input data from the Layer 6 (convolutional layer).
- **Layer 9** (LSTM layer): This layer, which is the integrated layer for BiLSTM Layer 7, consists of 128 filters. It transfers output to the layer 11 (concatenate layer) after reading input data from the layer 7 (BiLSTM layer).
- **Layer 10** (LSTM layer): This layer connects to BiLSTM layer 7 and has 128 filters. It transfers results to the layer 11 (concatenate layer) after reading input data from the Layer 8 (BiLSTM layer).
- **Layer 11** (encoded columns): A concatenate layer that produces a map with several features. It passes the feature maps to Layer 12 (dropout layer) after concatenating them from the Layers 9 and 10 (LSTM layers).
- **Layer 12** (dropout layer): Randomly sets 20% of the input units to 0 during training in order to apply a 20% dropout rate to Layer 11 (encoded columns) and avoid overfitting.

The overall framework of the proposed model is shown in Figure 1.

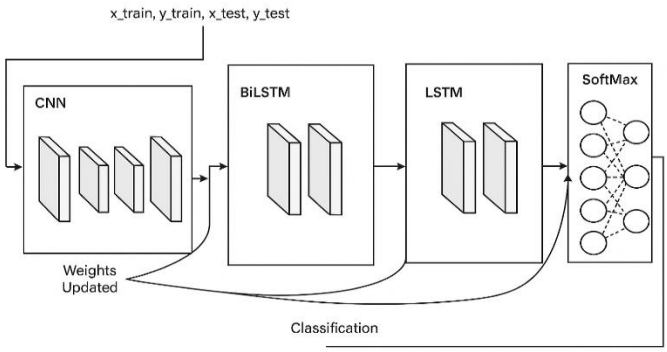

Figure 1. Structure of 3-layer stacked CNN-BiLSTM-LSTM model

4. RESULTS AND DISCUSSION

4.1 Dataset preparation and analysis

Data resulting from networks could have different meanings and variance due to their different network topologies. This could reduce the learning rate of DL algorithms and ML. Thus, we apply features normalization, the results are shown in Table 2.

Table 2. Dataset after normalization process

Node	Tr_time	Pckt_count	Mean	Var	Hop	Min	Max	Loss	Outliers	Label
aaaa::212:7408:8:808	0.885857	0.903553	0.551169	0.096433	0.75	0.584472	0.446894	0.096447	0.6875	1
aaaa::212:740a:4:404	0.979108	0.974619	0.25959	0.131021	0.25	0.27682	0.332001	0.025381	0.6875	0
aaaa::212:7407:7:707	0.873129	0.903553	0.454029	0.121016	0.5	0.560327	0.623121	0.096447	0.625	0
aaaa::212:7406:6:606	0.599682	0.736041	0.286272	0.159708	0.25	0.303937	0.325619	0.263959	0.5625	1
aaaa::212:740e:ee:0e	0.729583	0.629442	0.836614	0.094571	1	0.891438	0.669655	0.370558	0.4375	0

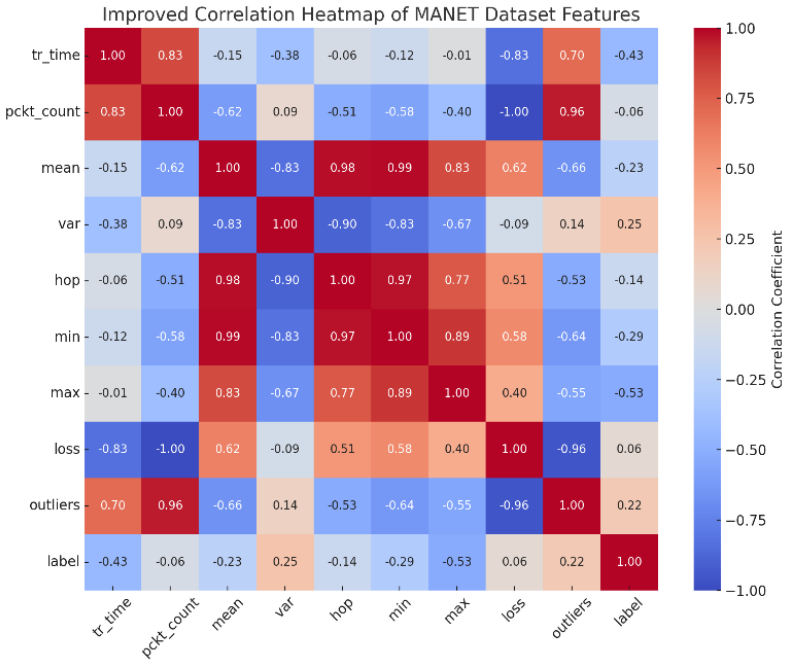

Figure 2. Data correlation results

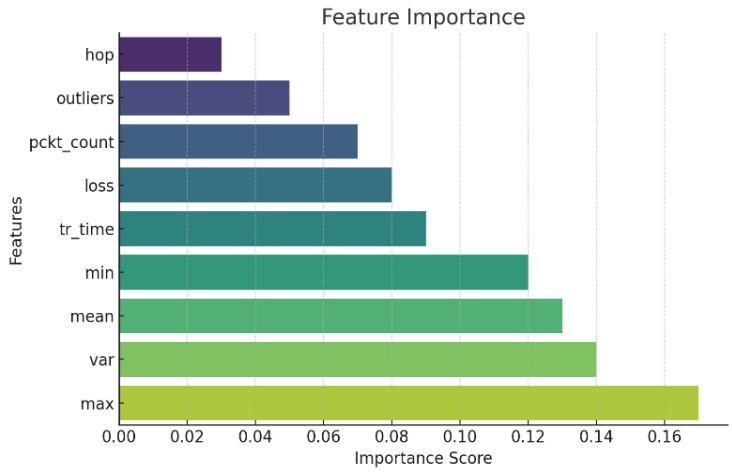

Figure 3. Features importance analysis results

4.2 Selection of features

Certain features may be more significant than others; therefore, selecting a suitable set of features will assist in improving the results provided by a learning classifier. Hence, we amylase dataset for correlation of features. In this step, the data has been analyzed to find the correlated variables. By removing highly correlated features, the dimensionality of the dataset is decreased, resulting in increased processing efficiency. The importance of achieving faster training times becomes particularly pronounced in situations that require real-time processing or extensive datasets. The Seaborn correlation technique is used to investigate data correlation. Making a correlation matrix and correlogram is a breeze with Seaborn. Because the Seaborn correlograms immediately illustrate the relationship between each variable in your matrix, they are helpful for exploratory investigation. To find a correlation between features, the threshold value of 0.8 is used, where the feature is correlated if it is above the threshold value. Figure 2 shows the correlation analysis results for each code smell dataset.

From Figure 2, the correlation matrix shows that, with the exception of outliers, every feature has a roughly negative correlation with the class. This shows that a model may be trained to distinguish between networks that are under attack and those that are not. Additionally, we choose the most important features iteratively using the Random Forest Classifier. Hence, the feature with a high importance distorts the influence of other features and may lead to overfitting, whereas a characteristic with a low importance may cause the learning process to slow down or even diverge. Figure 3 shows the feature importance analysis results.

Table 3. Training and validation results for proposed models

Accuracy (%)	N Precision (%)	A Precision (%)	N Recall (%)	A Recall (%)	N F1-score (%)	A F1-score (%)
99.557	99.4569	99.4569	99.6525	99.4078	99.6368	99.4323

*N: normal; ** A: black hole attack

Table 4. Summarizing the k-fold results

Fold	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
1	99.08	99.01	99.12	99.06
2	99.14	99.07	99.18	99.12
3	99.09	98.98	99.15	99.06
4	99.19	99.10	99.25	99.17
5	99.11	99.04	99.08	99.06
Avg	99.12 ± 0.21	99.04	99.16	99.09

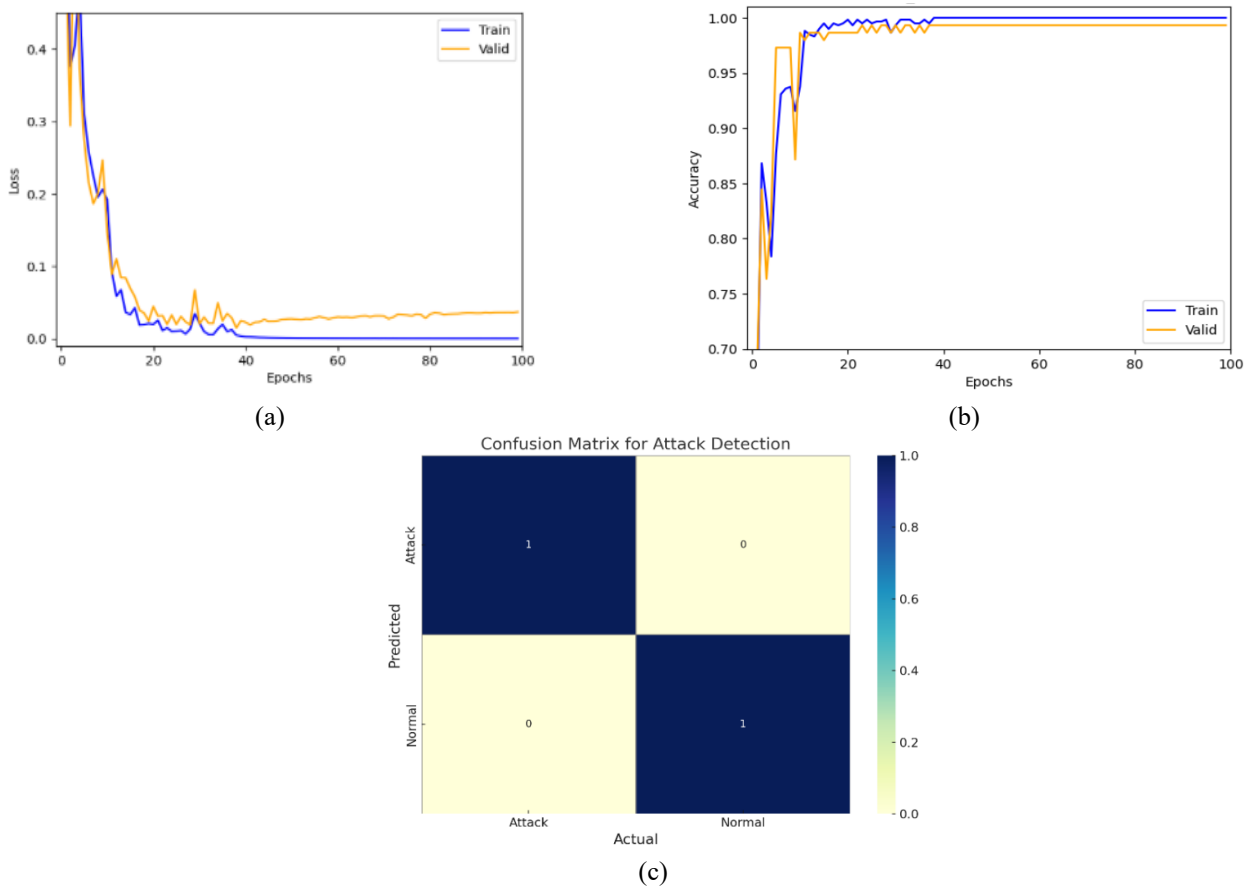

Figure 4. Classification results of the proposed model (a) train/validate loss per epoch, (b) train/validate accuracy results per epoch, and (c) the confusion matrix

Table 5. Comparative summary of recent black hole attack detection models in MANET environments

Recent Works	Method	Results
[2]	Decision Tree (DT), KNN, SVM, and NN	The SVM gains the highest detection accuracy, which is 97.5%, while neural network gains second-best detection value, which is 95%. DT and KNN gain the lower results which are 92.5% and 85% respectively.
[12]	AdaBoost SVM	The model achieves 97% in detecting accuracy of both passive and active black-hole attacks in MANET.
[13]	K-Nearest Neighbor (KNN) method for clustering and fuzzy modeling for choosing the cluster head	The result shows that the proposed method has an improvement over other methods in detection of black hole attacks, reaching up to 192.54%. In addition, it can be modified or combined with other techniques to identify additional assaults. In addition, other decision-making methods, which include SVM, NN, DT, and naïve Bayes methods, can be utilized in the nodes clustering section.
[17]	Various ML techniques, including KNN, SVM, DT, Linear Discriminant Analysis (LDA), Naive Bayes (NB), and Convolutional Neural Network (CNN)	The classification results show that the SVM achieved 97.1%, KNN achieved 98.2%, DT achieved 98.9%, LDA achieved 94.7%, NB achieved 95.2%, and CNN techniques achieved 96.4% in accuracies. According to the results of their study, the accuracy of the DT method is 98.9%, which surpasses the accuracy of alternative approaches.
[20]	Hybrid KNN and LSTM classifier using COOT optimization	The tested with several metrics that yielded better results, including accuracy of 96%, precision of 93%, recall of 82%, error value of 0.04, specificity of 98%, F1-score of 85%, Negative Predictive Value (NPV) of 98%.
Proposed Model	Hybrid deep stacked CNN-BiLSTM-LSTM	Achieved higher validation accuracy reach up to 99.557%. The model is also achieving higher results in other metrics which are 99.4569% in precision, 99.6525% in recall and 99.6368% in F1-score for detect normal behavior and 99.456% in precision, 999.4078% in recall and 99.4323% in F1-score for detecting black hole attacks.

The results of both the correlation matrix and important features show that the most important elements are the maximum and minimum RTTs values, as well as the mean and variance. Furthermore, the count of hops and anomalous values for a node does not appear to provide significant indications about the class to which it is related. Although the feature importance analysis in Figure 3 indicates that RTT-based features max, min, mean, and variance are most significant, we initially retained all features, including hops and outliers, to evaluate their combined contribution to model performance. This decision was based on the possibility that even low-importance features may carry complementary information when used in DL architectures. We also performed a reduced-feature test excluding the lowest-ranked features, which showed minimal impact on accuracy. Therefore, the final model prioritizes detection performance while maintaining feature generality.

4.3 Training and validation results

In this part, we test the proposed model for detecting black hole attacks in SDN-based MANET-IoT Networks. The data has been split into 80% train and 20% validate. The model has been trained for 500 epochs, and we use the traditional metrics to evaluate the proposed model performance, which are accuracy, precision, recall and F1-score. Table 3, Table 4, and Figure 4 show the training/validation results. To ensure the robustness of the proposed model and reduce the risk of overfitting due to the limited dataset size, we also performed a 5-fold cross-validation. In each fold, the model was trained on 80% of the data and validated on the remaining 20%, with folds rotated accordingly. The average detection accuracy across folds was 99.12%, with a standard deviation of ±0.21. Precision, recall, and F1-score values remained consistently high across folds, indicating strong generalization ability. These results support the stability and reliability of the model's performance beyond a single train-test split.

Table 3 and Figures 4 demonstrate that the model achieved higher results, which gained above 99% over all metrics. The model validation and training losses, as shown in Figure 4(a), are extremely small, at 0.0153 with training and 0.0061 with validation. As seen in Figures 4(b) and Table 3, the models achieved higher training and validation accuracy which reaching up to 99.56%. The model also achieves higher results in other metrics, which are 99.47% in precision, 99.65% in recall and 99.6368% in F1-score for detecting normal behavior and 99.46% in precision, 99.41% in recall and 99.43% in F1-score for detecting black hole attacks.

In the next part, we compared the results with some recent related works. The results are shown in Table 5. The results presented in Table 5 are for indicative comparison only. The referenced studies were conducted using different datasets, experimental setups, or simulation environments (e.g., QualNet), and therefore, direct performance comparison may not be fully equivalent.

5. CONCLUSION

In MANET, the most significant challenges are on security side, the dynamic architecture of MANETs makes implementing network security very challenging. There are several types of attacks that can affect MANETs, where black hole attack is one of the most significant attacks that can affect the network performance. Several security methods have been proposed to detect such threats; however, defense mechanisms were beyond the scope of this study. several types of security methods are proposed to detect and defense against this type of threats. As macML and DL techniques have the potential to detect unknown threats, they have become a popular option among researchers. This paper reviews various ML-based security approaches for MANETs, which can be categorized into three main types: ML-based intrusion detection systems, attack detection models, and trust-based models. In this work, we proposed a DL model designed to detect black hole attacks using a hybrid neural network architecture. The results show that the model achieved high performance, exceeding 99% across all evaluation metrics. Future work will focus on expanding the dataset, exploring adversarial robustness, and real-world deployment scenarios for hybrid MANET-SDN environments.

REFERENCES

[1] Agrawal, R., Faujdar, N., Romero, C.A.T., Sharma, O., Abdulsahib, G.M., Khalaf, O.I., Mansoor, R.F., Ghoneim, O.A. (2023). Classification and comparison of ad hoc networks: A review. Egyptian Informatics Journal, 24(1): 1-25. https://doi.org/10.1016/j.eij.2022.10.004

[2] Srilakshmi, U., Veeraiah, N., Alotaibi, Y., Alghamdi, S.A., Khalaf, O.I., Subbayamma, B.V. (2021). An improved hybrid secure multipath routing protocol for MANET. IEEE Access, 9: 163043-163053. https://doi.org/10.1109/ACCESS.2021.3133882

[3] Bouhorma, M., Bentaouit, H., Boudhir, A. (2009). Performance comparison of ad-hoc routing protocols AODV and DSR. In 2009 International Conference on Multimedia Computing and Systems, Ouarzazate, Morocco, pp. 511-514. https://doi.org/10.1109/MMCS.2009.5256641

[4] Aouad, S., El Meghrouni, I., Sabri, Y., Hilmani, A., Maizate, A. (2023). Security of software defined networks: Evolution and challenges. International Journal of Reconfigurable and Embedded Systems (IJRES), 12(3): 384-391. https://doi.org/10.11591/ijres.v12.i3.pp384-391

[5] Abu Zant, M., Yasin, A. (2019). Avoiding and isolating flooding attack by enhancing AODV MANET protocol (AIF_AODV). Security and Communication Networks, 2019(1): 8249108. https://doi.org/10.1155/2019/8249108

[6] Kadhim, H., Hatem, M.A. (2019). Secure data packet in MANET based chaos-modified AES algorithm. In 2019 2nd International Conference on Engineering Technology and its Applications (IICETA), Al-Najef, Iraq, pp. 208-213. https://doi.org/10.1109/IICETA47481.2019.9012982

[7] Nazir, M.K., Rehman, R.U., Nazir, A. (2016). A novel review on security and routing protocols in MANET. Communications and Network, 8(4): 205-218. https://doi.org/10.4236/cn.2016.84020

[8] Nadeem, A., Howarth, M.P. (2014). An intrusion detection & adaptive response mechanism for MANETs. Ad Hoc Networks, 13: 368-380. https://doi.org/10.1016/j.adhoc.2013.08.017

[9] Abdelhamid, A., Elsayed, M.S., Jurcut, A.D., Azer, M.A.

(2023). A lightweight anomaly detection system for black hole attack. Electronics, 12(6): 1294. https://doi.org/10.3390/electronics12061294

[10] Malik, A., Khan, M.Z., Faisal, M., Khan, F., Seo, J.T. (2022). An efficient dynamic solution for the detection and prevention of black hole attack in VANETs. Sensors, 22(5): 1897. https://doi.org/10.3390/s22051897

[11] Popli, R., Sethi, M., Kansal, I., Garg, A., Goyal, N. (2021). Machine learning based security solutions in MANETs: State of the art approaches. Journal of Physics: Conference Series, 1950(1): 012070. https://doi.org/10.1088/1742-6596/1950/1/012070

[12] Mahin, S.H., Taranum, F., Fatima, L.N., Ur Rahman Khan, K. (2019) Detection and Interception of Black Hole Attack in MANETs. International Journal of Recent Technology and Engineering (IJRTE), 8(2S11): 2392-2398. https://doi.org/10.35940/ijrte.b1274.0982s1119

[13] Hikal, N.A., Shams, M.Y., Salem, H., Eid, M.M. (2021). Detection of black-hole attacks in MANET using adaboost support vector machine. Journal of Intelligent & Fuzzy Systems, 41(1): 669-682. https://doi.org/10.3233/JIFS-202471

[14] Khan, B.U.I., Anwar, F., Rahman, F.D.B.A., Olanrewaju, R.F., Kiah, M.L.B.M., Rahman, M.A., Janin, Z. (2022). Exploring MANET security aspects: Analysis of attacks and node misbehaviour issues. Malaysian Journal of Computer Science, 35(4): 307-338. https://doi.org/10.22452/mjcs.vol35no4.2

[15] Zilberman, A., Stulman, A., Dvir, A. (2024). Identifying a malicious node in a UAV network. IEEE Transactions on Network and Service Management, 21(1): 1226-1240. https://doi.org/10.1109/TNSM.2023.3300809

[16] Abd Alhasan, A.Q., Rohani, M.F., Hamad, O.N. (2024). An enhanced ultra-lightweight mutual authentication protocol for RFID. Mathematical Modelling of Engineering Problems, 11(12): 3465-3477. https://doi.org/10.18280/mmep.111225

[17] Farahani, G. (2021). Black hole attack detection using K-nearest neighbor algorithm and reputation calculation in mobile ad hoc networks. Security and Communication Networks, 2021: 8814141. https://doi.org/10.1155/2021/8814141

[18] Salunke, K., Kurumbanshi, S. (2024). Towards secure and resilient MANETs: A SHIELD-based strategy for application-layer DDoS prevention and QoS optimization. SSRN, Paper No. 5337943. https://doi.org/10.2139/ssrn.5337943

[19] Al-Azawee, S.J., Al-Jamali, N.A.S. (2025). Heterogeneous traffic management in SDN-enabled data center network using machine-learning SPIKE model. Mathematical Modelling of Engineering Problems, 12(10): 3531-3544. https://doi.org/10.18280/mmep.121019

[20] Jayakrishna, N., Prasanth, N.N. (2025). A hybrid deep learning model for detection and mitigation of DDoS attacks in VANETs. Scientific Reports, 15: 34170. https://doi.org/10.1038/s41598-025-15215-1

[21] Abdan, M., Seno, S.A.H. (2022). Machine learning methods for intrusive detection of wormhole attack in mobile ad hoc network (MANET). Wireless Communications and Mobile Computing, 2022(1): 2375702. https://doi.org/10.1155/2022/2375702

[22] Altunay, H.C., Albayrak, Z. (2023). A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks. Engineering Science and Technology, an International Journal, 38: 101322. https://doi.org/10.1016/j.jestch.2022.101322

[23] Alsheikh, M.A., Lin, S., Niyato, D., Tan, H.P. (2014). Machine learning in wireless sensor networks: Algorithms, strategies, and applications. IEEE Communications Surveys & Tutorials, 16(4): 1996-2018. https://doi.org/10.1109/COMST.2014.2320099

[24] Alsoufi, M.A., Razak, S., Siraj, M.M., Nafea, I., Ghaleb, F.A., Saeed, F., Nasser, M. (2021). Anomaly-based intrusion detection systems in IoT using deep learning: A systematic literature review. Applied Sciences, 11(18): 8383. https://doi.org/10.3390/app11188383

[25] Pandey, S., Singh, V. (2020). Blackhole attack detection using machine learning approach on MANET. In International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, pp. 797-802. https://doi.org/10.1109/ICESC48915.2020.9155770

[26] Rui, K., Pan, H., Shu, S. (2023). Secure routing in the Internet of Things (IoT) with intrusion detection capability based on software-defined networking and machine learning techniques. Scientific Reports, 13(1): 18003. https://doi.org/10.1038/s41598-023-44764-6

[27] Abdallah, A.A., El Sayed Abdallah, M.S., Aslan, H., Azer, M.A., Cho, Y.I., Abdallah, M.S. (2024). Enhancing mobile ad hoc network security: An anomaly detection approach using support vector machine for black-hole attack detection. International Journal of Safety and Security Engineering, 14(4): 1015-1028. https://doi.org/10.18280/ijsse.140401

[28] Webber, J.L., Arafa, A., Mehbodniya, A., Karupusamy, S., Shah, B., Dahiya, A.K., Kanani, P. (2023). An efficient intrusion detection framework for mitigating blackhole and sinkhole attacks in healthcare wireless sensor networks. Computers and Electrical Engineering, 111(Part B): 108964. https://doi.org/10.1016/j.compeleceng.2023.108964

[29] Ataa, M.S., Sanad, E.E., El-khoribi, R.A. (2024). Intrusion detection in software defined network using deep learning approaches. Scientific Reports, 14(1): 29159. https://doi.org/10.1038/s41598-024-79001-1