Journal of Basrah Researches (Sciences) **51**(1), 195 (2025)
DOI: https://doi.org/10.56714/bjrs.51.1.17

A Deep Learning-Based Enhancement to OLSR for Robust Attack Detection and Secure Multimedia Transmission in MANETs

Maithem Mohammed Ali Abdullah *, **Hamid Ali Abed AL-Asadi**

Department of Computer Science College of Education for Pure Sciences University of Basrah Basrah, Iraq.

ARTICLE INFO

Received 6 April 2025
Revised 18 May 2025
Accepted 26 May 2025
Published 30 June 2025

Keywords:

OLSRP, Selective Packet Drop, MANET, Deep Learning, Densenet, Intrusion Detection.

Citation: M. M. A. Abdullah, H. A. A. AL-Asadi. , J.Basrah Res. (Sci.) **51**(1),195 (2025). DOI:https://doi.org/10.56714/bjrs.51.1.17

ABSTRACT

Wireless Multimedia Sensor Networks (WMSNs) and Mobile Ad Hoc Networks (MANETs) share important features, such as their decentralized topology and multimedia transmission without infrastructure. However, their dynamic nature subjects them to internal routing attacks, including but not limited to, selective packet drop attacks in which the malicious nodes block data flows without detections. This paper presents SA-DCBiGNet which is a hybrid deep learning model that implemented a combination of Dense Convolutional Neural Networks (DCNN), Bidirectional GRUs (Bi-GRU), and Channel Attention as a defense approach in the Optimized Link State Routing Protocol (OLSRP). Using behavioral logs and network metrics, the model identifies adversarial nodes with high precision. The model was evaluated using Python/NS-3 and the WSN-DS dataset and it identified adversarial nodes with high level of accuracy of 99.75% accuracy, 99.30% precision, 99.02% F1-Score, and 98.8% recall, which is better than traditional methods.

1. Introduction

Mobile Ad Hoc Networks (MANETs) are essential for wireless multimedia communication in infrastructure-less environments, such as military, rescue, and remote situations. MANETs are decentralized and self-configurable, which allows for quick deployment in urgent cases. These attributes support time critical real-time applications such as video transmission. However, reliable multimedia delivery faces challenges such as limited bandwidth availability, changes in topology, and energy constraints [1,2].

To counter bandwidth fluctuations, proactive routing protocols such as the Optimized Link State Routing Protocol (OLSRP) manage routing efficiency through constantly communicating routing information among devices. Unfortunately, the use of proactive protocols raises the potential for attacks. For example, Gray Hole attacks occur when one or more malicious nodes advertise the best path but selectively drop packets, which promotes efficiency, but ultimately degrades Quality of Service (QoS) for the user. Due to the dynamically structured and decentralized environment of MANETs, identifying Gray Hole attacks is complex [٣,4].

*Corresponding author email: pgs.maithem.muhammad@uobasrah.edu.iq

ISSN: 1817-2695 (Print); 2411-524X (Online)
Online at: https://jou.jobrs.edu.iq

Deep Learning, or (DL), tools have been shown to identify when anomalous activity occurs and detect malicious behavior. DL models can learn traffic patterns and identify anomalous traffic in real-time. As a result, using DL tools support securing a MANET against stealthy threats[5,6].
To address Gray Hole attacks, this study outlines the implementation of a deep learning-based model. The SA-DCBiGNet model will integrate into OLSRP for monitoring routing performance, identifying, and mitigating Gray Hole attacks before any protocol performance degradation can occur[7,8]. The proposed model aims to both improve the security factors towards an assuring routing layer while retaining reliable multimedia transmission capabilities[9]. The proposed model adds resiliency and intelligence to MANET communication frameworks through SIM-based monitoring protection factors against Gray Hole attacks.The proposed solution primary objectives can be summarized in the following points:

- As a means of identifying adversarial nodes, for example, an instance of a Gray hole attack, with the aim of offering compelling video stream routing in a MANET environment, a novel hybrid deep learning architecture is proposed.
- To enhance this attack detection ability and improve accuracy, the deep learning model has fused the existing intrusion detection systems by supervision learning.
- Developing an automated response system for hostile node isolation and building additional security measures as required based on what was detected[10,11].

2. Related Study

Several researchers have suggested detection systems for MANETs, for example, some have trained supervised classifiers on routing features to classify the behavior of nodes. While these methods do improve detection accuracy, they may not generalize or be adaptable to scenarios containing temporal dynamics or evolutionary attack patterns.
Rani et al. [12] suggested a defense strategy against dual attacks, such as Black Hole Attack (BHA) and Gray Hole Attack (GHA), by implementing Artificial Neural Networks (ANN) with Artificial Bee Colony (ABC) optimization. This hybrid system of deep learning and swarm intelligence was meant for better detection accuracy and better routing based on the most trusted nodes for packet forwarding. The system was implemented and tested using MATLAB, showing better performance when compared to ordinary systems under simulated black hole and gray hole attacks.
Vatambeti et al. [13] proposed an algorithm called Gray wolf optimization (GWO), based on trust-based data aggregation, namely, gray wolf optimization trust accumulation, to enhance routing security in MANETs. The primary goal of this algorithm is to continuously update trust values without compromising path stability for packet delivery even during data transmission. The proposed system achieves a 98.5% detection rate and increases the packet delivery ratio to 98.2% at 10 m/s node mobility. The performance of their method demonstrates advantages for ensuring secure and stable routes, as long as continuous monitoring of node behavior and trust levels is performed.
Shamim et al [14] presented a neural network-based classification scheme intended to provide detection for hasty Black and Gray Hole attacks. Due to the safety-critical perspective associated with autonomous and connected vehicles (ACVs), they stressed the necessity of supporting consistent packet delivery. Their proposed approach intended to detect attacks while implementing organized reaction mechanisms to mitigate malicious behavior on behalf of the vehicles. Overall, the experimental results showed a better detection rate than current schemes, thus demonstrating its value in securing communication in a VANET environment.
The research conducted by Malik et al [15] proposed a new approach, Detection and Prevention of Gray Hole Attacks (DPGHA), for AODV-based VANETs. DPGHA suggested a scheme based on dynamic threshold values from anomalies in packet behavior in terms of the differences in both the number of packets received, forwarded, and generated, as well as between their relative sequence numbers, in determining malicious nodes. After being developed and tested with SUMO and NS-2, DPGHA provided significant improvements over existing benchmark techniques: DPGHA reduced routing overhead by a factor of 10.85%, delay by 3.85% while increasing the packet delivery ratio by 4.67%, the throughput by 6.58%, while also achieving a maximum detection rate of 2.3%.

Saad M. Hassan et al [16] applied a structured analysis of the characteristics of MANET and focused on detection and mitigation of black and gray hole attacks, noting the novel use of ML and optimization approaches. FL, reinforcement learning, and metaheuristic algorithms, were noted. The outcomes suggested that LSTM networks and FL improved detection accuracy and tightened system resiliency. Moreover, they also mentioned the role of game theory and reinforcement learning in optimizing routing protocols, thus displaying the need for detectors that are adaptive and intelligent in order to create a secure and resilient MANET.

S. Vimalnath et al [17], introduced a new detection and mitigation approach against both categories of gray hole attacks in AODV-based VANETs starting with a novel method called Detection and Prevention of GHA (DPGHA). The approach utilizes dynamic thresholds from abnormalities in received, forwarded, and generated packets and their sequence numbers. The use of dynamic monitoring improves detection accuracy and reliability; however, resource-constrained nodes may encounter higher computational cost and resource usage. The algorithm supports cooperative detection and vehicle endurance. The simulation results showed that the integrated algorithm ARBD, enhanced the accuracy and efficiency of gray hole detection, ultimately improving the performance and security of the VANET.

M. Alshebani et al [18] conducted research on the detection of anomalies in networks using the WSN-DS dataset utilizing artificial neural networks focusing on the CNN-LSTM model. They performed experiments involving five distinct attack labels obtaining promising outcomes with anomaly detection accuracy of 98% and precision and recall rates of 99%. Their results suggest that CNN-LSTM is an effective and suitable deep learning algorithm for performing real-time anomaly detection in wireless sensor networks (WSNs) and confirms its potential for improving network security against a variety of intrusions.

K. P. Sharma et al [19], proposed an avant-garde Enhanced Black Widow Optimization (EBWO) algorithm together with a Bidirectional Gated Recurrent Unit (BiGRU) and Attention Mechanism (ATTN model). The EBWO was employed to perform optimization of all parameters of the BiGRU-ATTN model which in turn enhanced detection performance. Experimental evaluations using the WSN-DS dataset, demonstrated that the propose method exceeded the performance of traditional deep learning models to improve accuracy and robustness in detecting cyber threats within wireless sensor networks.

3. Background

This section presents a conceptual perspective of Mobile Ad Hoc Networks (MANETs), which are characterized by a decentralized network structure, and highly dependent on routing protocols, such as Optimized Link State Routing (OLSR). Additionally, the section provides a conceptual review of deep learning approaches that can improve intrusion detection related to and the overall security of dynamic networks.

3.1. Mobile Ad Hoc Network (MANET)

Mobile Ad Hoc Networks (MANETs) are decentralized self-configuring wireless mobile nodes with no fixed infrastructure. All nodes act as a forwarder and buffer, replacing a centralized authority. The mobility of nodes causes constant topological changes to the network, making it difficult to deliver multimedia traffic reliably, with video traffic being the most difficult to maintain. Although MANETs provide a form of flexibility, it introduces an enormous number of security vulnerabilities. A definitive example is the gray hole attack, where malicious nodes drop packets selectively after luring the network node. This unexpected event needs an “immediate” response, which is even more catastrophic for real-time applications [20]. Figure 1 shows the basic architecture of a typical MANET.

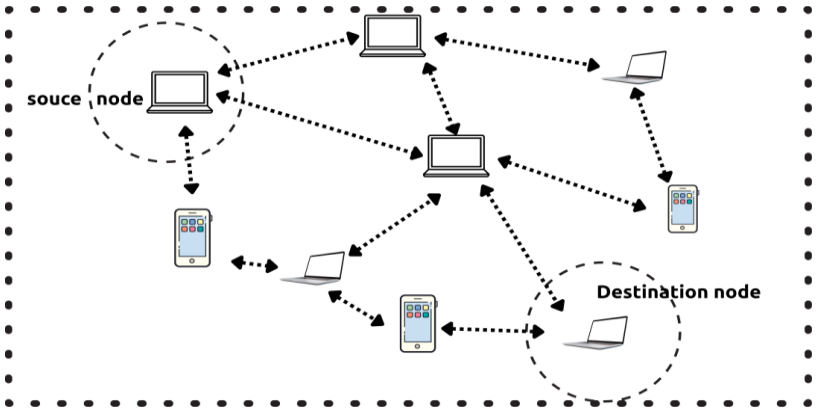

Fig. 1. Basic MANET architecture.

3.2. Gray Hole Attack

Gray Hole Attack is one of the threats in wireless ad hoc networks, in which a malicious node drops packets selectively after pretending to send a packet as a legitimate forwarding node. In contrast to Black Hole Attack, where the malicious node drops all data packets, a Gray Hole node has a random and unpredictable behavior forwarding some packets, and dropping the rest. This is an important advantage, because it makes the detection of Gray Hole behavior much more difficult, and could lead to such significant interruptions to data deliveries, even increasing the degradation of the network performance, especially with networks that are dynamic and indoctrinated like MANETs or WMSNs. Figure 12 show a high-level taxonomy of gray hole attacks in MANETs which identifies three general types of gray hole behavior: Selective Packet Dropping, Node Specific Behavior, Path Establishment and Targeted Dropping [21,22]. Figure 2 represent the gray hole attack.

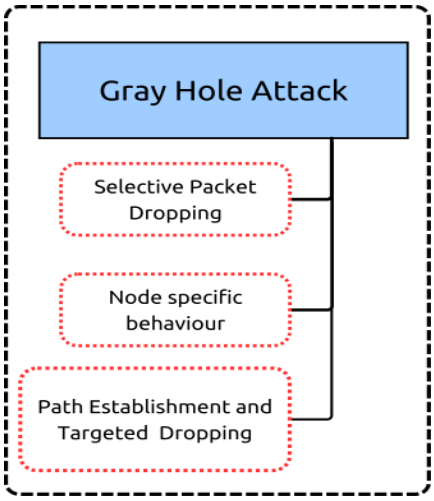

Fig. 2. Details of the gray hole attack.

- The Selective Packet Dropping branch explains how a potential intruder selectively takes part in routing and randomly drops packets to disrupt specific communications. This will lead towards selective disruption. It will always be important for detection, in order to identify and stop any and all disruptions.
- The Node-Specific Behavior branch explains how the attacker biases based upon packet origin selectively. This creates different experiences in the network with the latter creating split network reliability and performance outcomes. The last two behaviors are another reminder that routing protocols must be improved by incorporating cryptographic methods to secure the network.
- The Path Establishment and Targeted Dropping branch describes how the attacker only takes a part in path establishment to drop packets, and in essence, impair network communications.

The systematic attack should address adequate security with respect to preventing the integrity of the network [23]. Figure 3 describe the gray hole node in MANET.

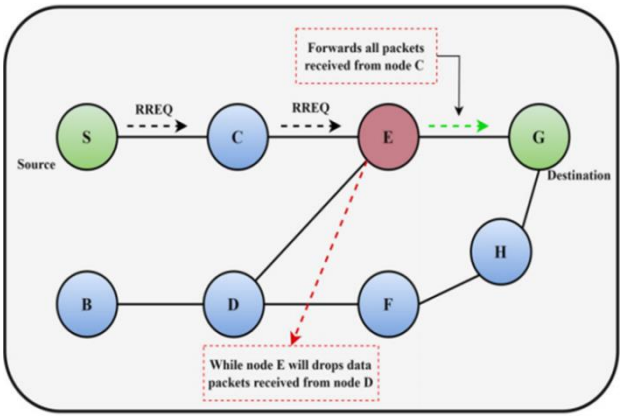

Fig. 3. Representation of the gray hole node.

3.3. MANET Routing Protocols

Mobile ad hoc network (MANETs) routing protocols can be categorized into types according to different aspects of the network environment, multimedia traffic handling, QoS, routing type, used technology, and computing techniques, into three major types based on the operation behavior: proactive, reactive, and hybrid[24]. Figure 4 gives an overview of the different types of routing protocols.

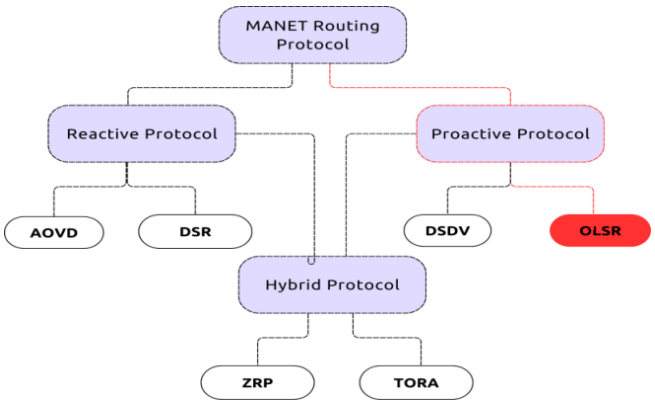

Fig. 4. Categorization of MANET Routing Protocols.

- Proactive routing protocols are constantly updating routing information by sending periodic control messages. This behavior ensures a route is ready when needed and therefore, minimizes transmission delays. One of the most popular Proactive routing protocols is the Optimized Link State Routing Protocol (OLSR); it focuses on optimizing by reducing the volume of control traffic through optimization methods.
- Reactive routing protocols only create routes by requiring enough communication to start some data on the link. After the source nodes or endpoints create data on their start, it causes a route discovery process to take place so a path to correct the destination can be found. while the intense latency that existed for the initiation of route discovery during the time of no proper data is less overhead in addressing the communication, it adds latency in that the route detection duration does add latency against responsiveness.
- Hybrid routing protocols are methods of routing that allow for both reactive and proactive schemes. Their intention leaks the discovery latency of some reactive approaches and the

constant and voluntary process of routing proactive techniques while improving the flexibility and adaptability for scalability[25,26].

3.3.1. Optimized Link State Routing (OLSR) Protocol

The Optimized Link State Routing Protocol (OLSR) is a proactive routing protocol created for Mobile Ad Hoc Networks (MANET). It is widely accepted and a standardization for dynamic and infrastructure-less communication. Many other routing protocols cannot match OLSR routing, especially for multimedia content across highly mobile networks. OLSR uses Multipoint Relays (MPR) to minimize transmissions required by flooding, resulting in control overhead. The optimized structure of OLSR makes it a suitable routing solution for MANETs using real-time and multimedia applications [27]. The protocol architecture protocol architecture is shown in Figure 5.

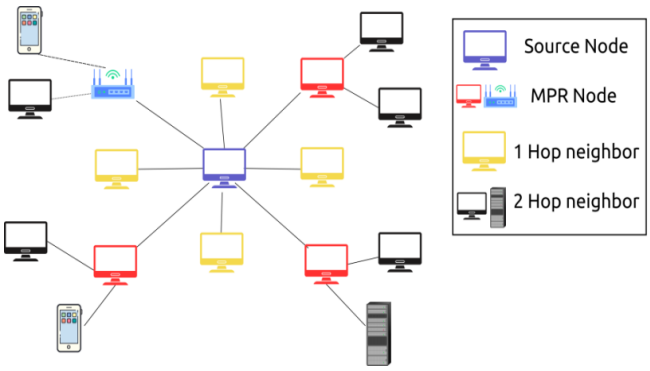

Fig. 5. architecture of the OLSR protocol.

3.4 Deep Learning For Network Protection

Given the dynamic, flexible, and limited resources of Wireless Multimedia Sensor Networks (WMSNs), traditional security methods typically cannot efficiently identify black hole or gray hole attacks. These attacks rely on the unique decentralized structure and unlimited data dimensions of WMSNs for exploitation. The deep-layered structure of DL enables the model to detect behavior changes that can be used to classify and describe attacks automatically. Because of deep learning (DL) capacities, the DL methods described in this paper offer classification, prediction, and real-time response against advanced intrusions and other threats, along with critical measures to enhance data integrity, scalability, and security for WMSNs. The multiple layers in DL models allow inputs to be abstracted and detailed representations enhance the modeling techniques' capacities for understanding complex, temporal, and dynamic threat behavior [28, 29]. Figure 6 shows the overall structure of a deep learning-based intrusion detection system.

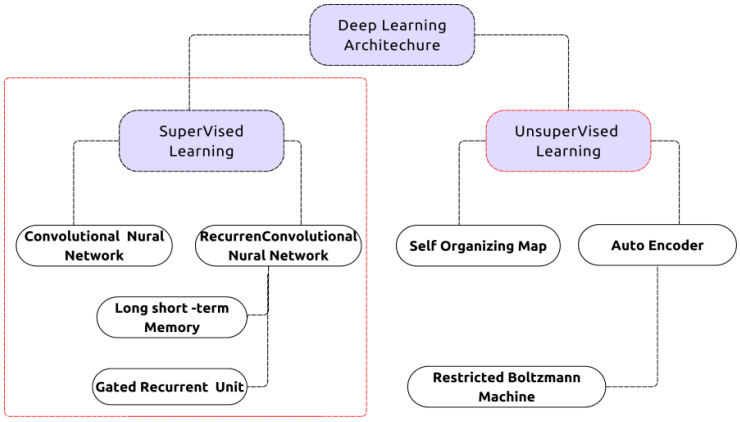

Fig. 6. Deep learning algorithms.

3.5. The proposed system

The proposed system incorporates a deep learning-based detection method SA-DCBiGNet (Spatial-Attentive Dense Convolutional Bidirectional Gated Network) that uses channel attention mechanism directly into the OLSRP (Optimized Link State Routing Protocol) stack for the detection and mitigation of Gray Hole attacks in real-time. figure 7 shows the block diagram of the proposed model.

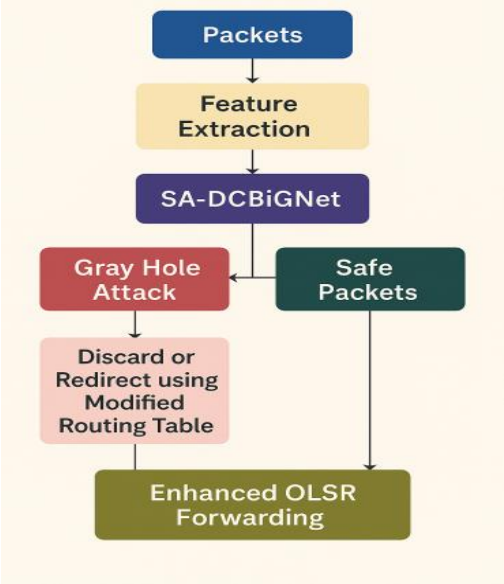

Fig. 7. block diagram of the proposed model.

The proposed system improves upon traditional OLSR (Optimized Link State Routing) protocol by integrating a deep learning-based detection module, SA-DCBiGNet to detect and remediate Gray Hole attacks in real-time. The data flow chart shows the data exchange that typifies usage when routing control packets (HELLO messages, TC messages, etc.) enter the OLSR stack. The packets are preprocessed where relevant features are extracted in order to identify behaviors associated with nodes or node groups based on metrics related to: forwarding rate, reception consistency, anomaly features, and so on. These features are then returned to the detection step, utilizing the SA-DCBiGNet, which consists of convolutional layers for spatial features, Bidirectional GRU layers for temporal sequence modeling, as well as a Channel Attention mechanism that identified which behavioral features were most important for classification. Based upon the prediction of the SA-DCBiGNet model each node is classified as Good or Bad. This classification is returned into the corresponding modified OLSR routing logic where the forwarding table can be updated on the fly to remove or deprioritize routes that included detected malicious nodes. As a result the data packets can be redirected based on trustworthy delivery routes and thereby dramatically lessening the impact of a Gray Hole attacks, as well as unifying malicious and non malicous routes from the routing table before delivery.

3.5.1 Detection Procedure Of Gray Hole Attack

Identifying gray hole attacks is conducted by the OLSRP stack with the SA-DCBiGNet model. The primary design features of the SA-DCBiGNet model are to preserve the temporal, spatial, and behavioral characteristics of network traffic in order to display non-disquieting node behaviours (e.g., an abnormal node behaviour). This will be seen in the detection process layer-by-layer discrepancy. Figure 8 represent the internal layers of the system.

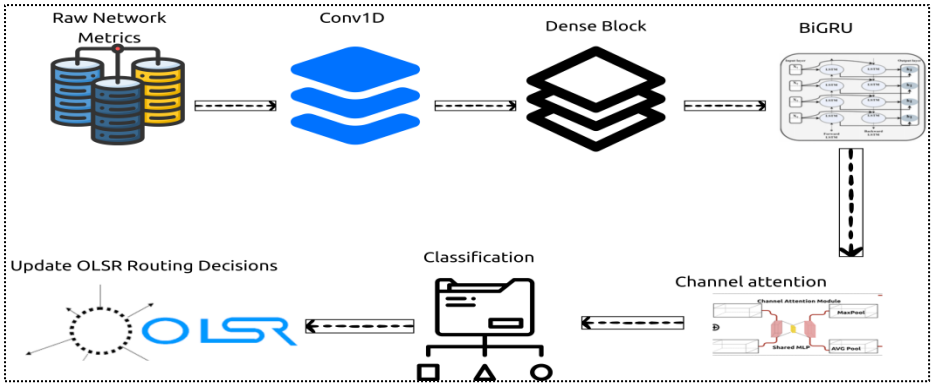

Fig. 8. represent the layers of the system.

A deep learning-based framework aimed at securing OLSR routing in MANETs against gray hole attacks. It starts by collecting raw network metrics, which are then processed using a Conv1D layer to extract local spatial features. These features pass through dense blocks for enhanced representation and are then analyzed by a Bidirectional Gated Recurrent Unit (Bi-GRU) to capture temporal dependencies. A channel attention mechanism follows, emphasizing the most informative features. The output is classified to detect potential malicious behavior. Finally, the results are used to dynamically update OLSR routing decisions, ensuring more secure, adaptive, and efficient multimedia communication within highly dynamic and decentralized MANET environments.

3.5.2 Experimental Setup

In order to assess the effectiveness of our introduced model, the SA-DCBiGNet, regarding detecting gray hole attacks in an OLSRP-based Wireless Sensor Network (WSN), a set of experimental trials were conducted using the WSN-DS dataset. The experimental preconditions, the preprocessing methods carried out, and the performance metrics used are detailed below::

3.5.3 Data Pre-processing

Prior to training, the dataset underwent several pre-processing steps. Table 1 shows the explanation of data pre-processing

Table 1. Data pre-processing concept.

Caption	Purpose
Missing Values Handling	Entries with missing or incomplete data were removed.
Normalization	Continuous features, such as Delay, Hop_Count, and Energy_Level, underwent normalization via min-max scaling to ensure consistency in the ranges of values during input into predictive models.
Encoding	Categorical fields including Routing_Type and Node_ID were converted into dummy variables or one-hot form, enabling compatibility with ML algorithms.
Label Mapping	The binary column for labels created a distinction between normal behavior (0) and instances of gray hole attack (1).

3.6 Model Evaluation

After training, evaluating the model is one of the core aspects of deep learning to assess the model performance based on standard evaluation metrics such as Precision (P), Accuracy, F1-Score (F1), and Recall (R). To guarantee reliability and robustness in real-world contexts, models are evaluated

on validation and testing datasets corresponding to the datasets used in training the model. The above metrics are defined as:**Accuracy**: The percentage of correctly classified instances

$$\text{Accuracy} = \frac{number\ of\ correct\ predictions}{total\ number\ of\ correctio} * 100 \quad (1)$$

- **Precision**: How many of the detected attacks were actual attacks.

$$\text{Precision} = \frac{TP}{TP+FP} \quad (2)$$

- **Recall:** The ability of the model to detect actual attacks.

$$Recall = 1 + \frac{TP}{TP+FN} \quad (3)$$

- **F1-Score**: The harmonic mean of precision and recall

$$F1\ Score = 2 * \frac{Precision*recall}{Precision+recall} \quad (4)$$

Let TP denote the number of assaults that have been recognized to be assaults; TN denotes the number of normals that have been recognized to be normal (not an assault); FP denotes the number of normals that were incorrectly classified as an assault; and FN denotes the number of assaults that were incorrectly classified as normal (Stevens, 2023). In the identification of black holes, precision and recall are important, where a high recall means that most assaults were detected, and a high precision indicates there were very few false positives.

3.7 Simulation Results

In this section, we employed Python and NS-3 to conduct an exploratory study. This model was simulated across various network scenarios that the existing literature had not previously explored in relation to the performance of the proposed approach. Therefore, the measurement results demonstrate the innovative strengths and weaknesses securely. The simulations consist of five videos, where it is anticipated that 80 percent of the videos will be used for instruction and 20 percent for assessing the performance of the model. Table 2 shows the real hyperparameters used for the model.

Table 2. Hyperparameters and values of the model.

parameters	values	parameters	values
No. of Layers	4	Early stopping	10
No. of Units per Layer	32	Epochs	100
Activation function	ReLU / Sigmoi	Loss	Binary cross entropy
Learning rate	0.001	Optimization algorithm	Adam
Dropout layer	2	Batch size	32
Simulator	Ns-3.30	Routing protocol	OLSR

The WSN-DS dataset was utilized to evaluate the performance of our proposed SA-DCBiGNet model for the detection of black hole attacks in WMSNs. The evaluation results were promising, as our algorithm achieved an accuracy of 99.79%, precision of 99.00%- demonstrating high precision capability, recall of 98.3%, and an F1-score of 99.02% indicating a high level of reliability and performance of our proposed method to detect multiple DOS attacks, such as black-hole attacks. The evaluation also indicated there was accuracy for both the test and training in Figure 10..

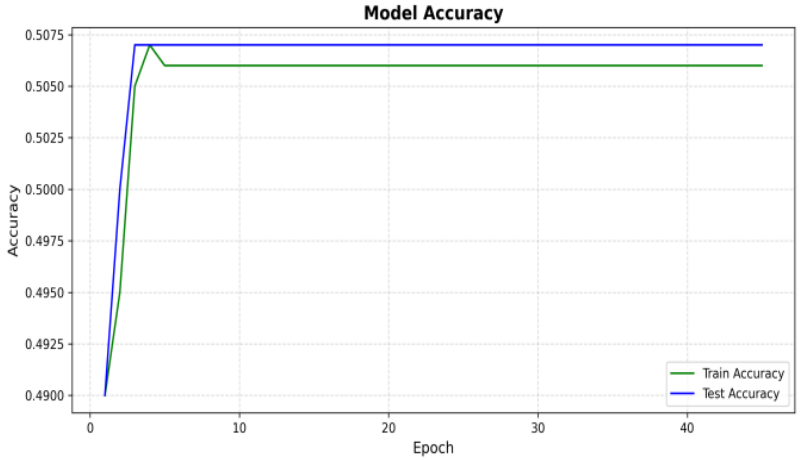

Fig. 9. Model Accuracy: Train vs. Test.

The accuracy of the model throughout a selected number of epochs is displayed in Figure 9. Although we set the epochs at 100, the training was stopped prematurely because of a patience parameter of 5, which is a hyperparameter specified in TensorBoard that prevents the model from being trained to the point of overfitting by stopping the training process when there is no change in accuracy over 5 epochs after each epoch. Both accuracies converge roughly around 0.51 which suggests to us that the model is getting reasonable classification accuracy. Again, this suggests we need to either tune hyperparameters further or change the architecture of the model to make it more effective in generalizing to unseen data and overall performance.

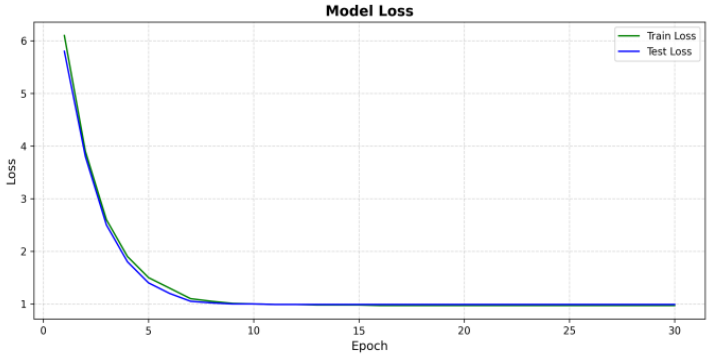

Fig. 10. Model loss: Train vs. Test.

Figure 10 shows the loss curves from the model for the respective epochs and both losses decrease very quickly, indicating that the model is effective and appropriate for training. By the 30th epoch, training loss approaches the value of 1, while test loss marginally higher, confirming that the model has high-level classification capability. This close loss value demonstrates the model has learned and generalized well, and it can appropriately process new unseen data without much risk of over -fitting. The new proposed model demonstrates consistently improved specifications, value, and performance in comparing testing and training loss values.

3.7.1 Comparison of the performance metrics

The demonstrated performance of the suggested model reflects the superior levels of accuracy and detection maintaining the same dataset which indicates excellent model performance in this aspect as depicted in Figure 11. We also compared the performance of our suggested technique to other methods retrieved through literature review.

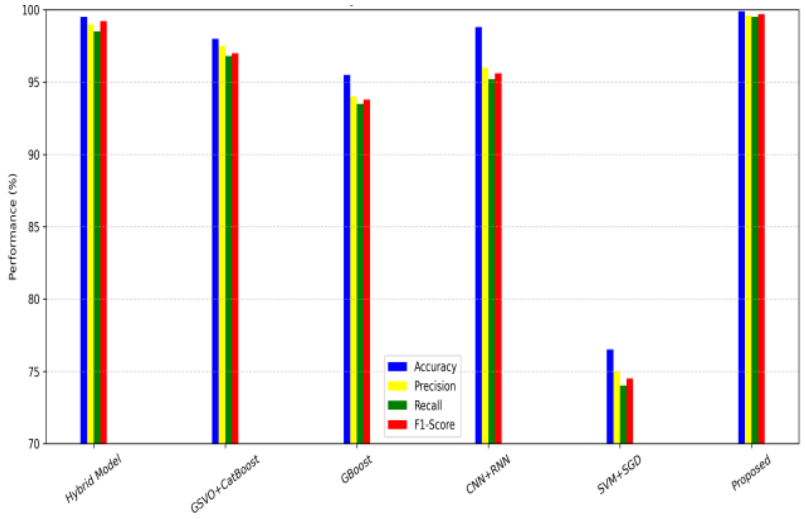

Fig. 11. Comparison of performance metrics with other algorithms.

The model displayed optimal classification performance, succeeding high levels of 99.70%, a precision of 99.٣0%, a recall of 98.٦٠%, and an F1-score of 99.02%. Each reflects the system's ability to detect harmful behavior while minimizing false alarms. These metrics collectively confirm the model's robustness and its capacity to maintain consistent detection performance. These outstanding results validate the model's robustness and its ability to generalize well across unseen data. Compared to conventional approaches such as CNN+RNN, SVM+(SGD),GSVO+ CatBoost and GBoost, the proposed model exhibits a notable improvement in both detection performance and stability, mainly due to the integration of sequential and spatial learning components combined with the attention mechanism. Table 3 demonstrates Comparison of performance metrics.

Table 3. Comparison of performance metrics of existing ML and DL techniques

Year Ref	Algorithm	method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
2022/ [15]	Gboost	Machine learning	99.6	98.8	-	-
2023/ [16]	CNN+RNN (Combination of CNN and RNN)	Deep learning	98.79	94.86	92.97	93.72
2024/ [17]	1.Support Vector Machine (SVM) 2.Stochastic Gradient Descent (SGD)	Machine learning	96.00	98.00	96.00	79.00
2024/ [18]	GSWO-CatBoost	Machine learning	99.62	97.27	97.78	97.47
2025/ [19]	Hybrid model CNN ,LSTM ,GRU	Deep learning	95.00	-	-	98.8
Our proposed	**SA-DCBiGNet with Twin Attention Mechanism**	**Deep learning**	**99.70**	**99.30**	**98.60**	**99.02**

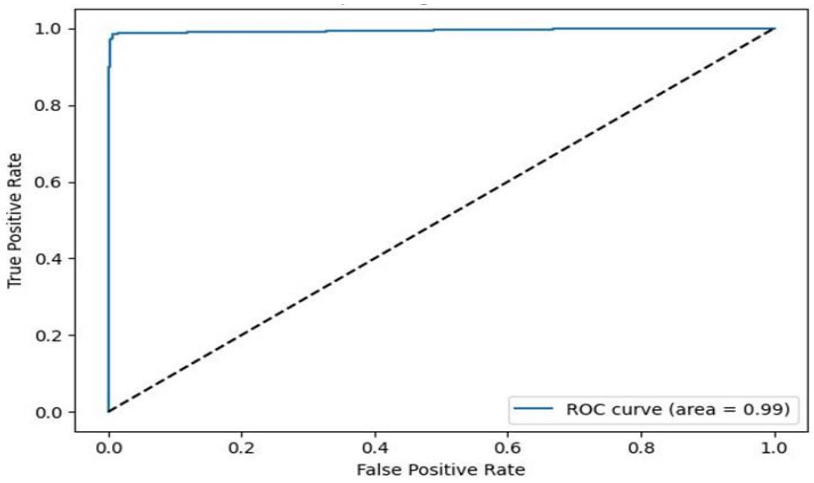

Fig. 12. Analysing ROC Curves for Model Performance.

Figure 12 demonstrates the ROC curve factor of the performance of the model graphically, by contrast, the true positive rates (TPR) are displayed against the false positive rates (FPR). The higher the area under the curve (AUC) value reflects quality of performance with higher values indicating better discrimination between positive class and negative class.

3.8 Discussion

This section emphasizes the exceptional performance of the SA-DCBiGNet (Dense Convolutional Bidirectional Gated Network) model for detecting gray hole attacks in Mobile Ad-Hoc Networks (MANETs). This model was implemented with NS-3 and Python, and achieved impressive results with an accuracy of 99.70%, precision of 99.00%, recall of 98.30%, and F1 score of 99.02%.
When compared to existing studies with the same dataset type, our model outperforms other similar studies, with Gboost (accuracy, 99.6%, precision, 98.8%), with CNN+RNN (accuracy, 98.79%, precision, 94.86%, recall, 92.97%, F1 Score, 93.72%), with SVM with SGD (accuracy, 96.00% F1 Score, 79.00%), with GSWO-CatBoost (accuracy, 99.62% F1 Score, 97.47%)and Hybrid CNN-LSTM-GRU (accuracy, 95.00%, F1 Score, 98.8%).
SA-DCBiGNet uses advanced deep learning components like convolutional layers and GRUs crucial for capturing dynamic behaviors of networks and the ever-changing behavior of nodes that are commonplace in the rapidly changing environment of MANETs. The attention mechanism it was also equipped with allows the model to focus on relevant features without focusing on others features which allows the relevant features to be intensified yielding improved detection rate from the model while minimizing false positives on the other hand.
Whereas most detection models fail with temporal data, SA-DCBiGNet excels with sequential patterns and effectively learns to distinguish between them ensuring exceptionally accurate detection of attacks in a timely manner. It is light weight enough to be used in a resource limited environment while not experiencing degradation in its performance. In addition, it uses a substantial number of training samples, which enables the model to be robust to misclassification and generalizes well to attack types other than gray hole attacks.incorporation of these deep learning techniques build it as a leading solution for improving security in MANET.

3.9 Conclusion

The detection process begins by analyzing multimedia traffic using the SA-DCBiGNet model, which extracts nodes behavior based on delivery metrics to classify them as benign and malicious nodes. This detection ensures a comprehensive security enhancement designed for Wireless Multimedia Sensor Networks (WMSNs), focusing on ensuring data integrity, reducing packet duplication.

MANET comprises a number of mobile nodes that do not have a centralized control. Due to this, it is vulnerable to several attacks, such as gray hole attacks. This paper focuses on security issues concerning MANETs stands for mobile ad hoc networks with an emphasis on black hole attacks. Unfortunately, mobile ad hoc network features will not permit unauthorized terminals to connect to the networkof the attacker. Then, we designed situationally appropriate strategies for MANETs which are specific security measures that can adapt to different network conditions and attack scenarios. The characteristics of deep learning-based security detection techniques have been studied. Then, after gathering the input videos, the suggested study looks for black hole nodes that behave differently from other nodes under particular environments. Consequently, the SA-DCBIGNet model exhibits significant improvements in deep learning algorithms and achieves the best results in the detection process. The outcomes generated by Deep Learning algorithms are significantly better than those of other learning approaches. Overall, our proposal helps strengthen security protocols and lays the groundwork for further studies on robust network defense systems.

References

[1] A. M. Eltahlawy, H. K. Aslan, E. G. Abdallah, M. S. Elsayed, A. D. Jurcut, and M. A. Azer, "A survey on parameters affecting Manet Performance," Electronics, vol. 12, p. 1956, 2023.

[2] H. A. Abed AL-Asadi, "An optimal algorithm for better efficiency in WMSN for multimedia applications," IET Wireless Sensor Systems, vol. 11, pp. 248-258, 2021.

[3] N. Schweitzer, L. Cohen, T. Hirst, A. Dvir, and A. Stulman, "Achieving manet protection without the use of superfluous fictitious nodes," Computer Communications, vol. 229, p. 107978, 2025.

[4] S. M. Hassan, M. M. Mohamad, and F. B. Muchtar, "Advanced intrusion detection in MANETs: A survey of machine learning and optimization techniques for mitigating black/gray hole attacks," IEEE Access, 2024.

[5] S. Remya, M. J. Pillai, A. Sha, G. Rajan, S. R. Subbareddy, and Y. yun Cho, "Saltus-"A Sudden Transition" Empowered by Federated Learning for Efficient Big Data Handling in Multimedia Sensor Networks," IEEE Access, 2024.

[6] K. Y. Cett, N. A. Mahiddin, F. F. M. Affandi, R. H. R. Bongsu, and A. Hayati, "Performance analysis of OLSR protocol in manet considering different mobility speed and network density," International Journal of Wireless & Mobile Networks, vol. 13, pp. 21-32, 2021.

[7] G. Arulselvan and A. Rajaram, "Routing attacks detection in MANET using trust management enabled hybrid machine learning," Wireless Networks, pp. 1-15, 2024.

[8] H. Hicham, N. Mehallegue, and M. Benssalah, "Optimized MPR Selection in OLSR routing protocol for UAV Communications in Public Safety applications," 2025.

[9] J. Ryu and S. Kim, "Trust system-and multiple verification technique-based method for detecting wormhole attacks in MANETs," IEEE Access, 2024.

[10] R. Reka, R. Karthick, R. S. Ram, and G. Singh, "Multi head self-attention gated graph convolutional network based multi-attack

[11] P. Rani, S. Verma, and G. N. Nguyen, "Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network," IEEE access, vol. 8, pp. 121755-121764, 2020.

[12] R. Vatambeti, K. S. Supriya, and S. Sanshi, "Identifying and detecting black hole and gray hole attack in MANET using gray wolf optimization," International Journal of Communication Systems, vol. 33, p. e4610, 2020.

[13] S. Younas, F. Rehman, T. Maqsood, S. Mustafa, A. Akhunzada, and A. Gani, "Collaborative detection of black hole and gray hole attacks for secure data communication in VANETs," Applied Sciences, vol. 12, p. 12448, 2022.
[14] A. Malik, M. Z. Khan, S. M. Qaisar, M. Faisal, and G. Mehmood, "An efficient approach for the detection and prevention of gray-hole attacks in VANETs," IEEE Access, vol. 11, pp. 46691-46706, 2023.
[15] M. Yazdanypoor, S. Cirillo, and G. Solimando, "Developing a Hybrid Detection Approach to Mitigating Black Hole and Gray Hole Attacks in Mobile Ad Hoc Networks," Applied Sciences, vol. 14, p. 7982, 2024.
[16] S. M. Hassan, M. M. Mohamad, and F. B. Muchtar, "Advanced intrusion detection in MANETs: A survey of machine learning and optimization techniques for mitigating black/gray hole attacks," IEEE Access, 2024.
[17] S. Vimalnath, R. Midhun, A. Kavinesh, P. Karvendan, and K. Kishore, "Enhanced Security Framework for Gray-Hole Attack Prevention in Vehicular Networks," in 2025 International Conference on Visual Analytics and Data Visualization (ICVADV), 2025, pp. 296-301.
[18] M. Alshebani, K. Jazayeri, B. Arman, K. Alpan, and K. Dimililer, "CNN-LSTM Based Network Anomaly Detection in WSN-DS," in The Proceedings of the International Conference on Smart City Applications, 2025, pp. 63-72.
[19] K. P. Sharma, R. Hussain, A. A. Jaharadak, A. A. Trawnih, D. Verma, S. Dasi, et al., "Hybrid Convolutional Neural Network for Robust Attack Detection in Wireless Sensor Networks," Internet Technology Letters, p. e650, 2025.
[٢٠] S. P. Dongare and R. Mangrulkar, "Optimal cluster head selection based energy efficient technique for defending against gray hole and black hole attacks in wireless sensor networks," Procedia Computer Science, vol. 78, pp. 423-430, 2016.
[21] G. Liu, H. Zhao, F. Fan, G. Liu, Q. Xu, and S. Nazir, "An enhanced intrusion detection model based on improved kNN in WSNs," Sensors, vol. 22, p. 1407, 2022.
[22] S. Gurung and V. Mankotia, "ABGF-AODV protocol to prevent black-hole, gray-hole and flooding attacks in MANET," Telecommunication Systems, pp. 1-17, 2024.
[23] A. Abdelhamid, M. S. Elsayed, A. D. Jurcut, and M. A. Azer, "A lightweight anomaly detection system for black hole attack," Electronics, vol. 12, p. 1294, 2023.
[24] M. Baumgartner, J. Papaj, N. Kurkina, L. Dobos, and A. Cizmar, "Resilient enhancements of routing protocols in MANET," Peer-to-Peer Networking and Applications, vol. 17, pp. 3200-3221, 2024.
[25] M. Bhonsle et al., "Enhancing Security in Wireless Mesh Networks: A Deep Learning Approach to Black Hole Attack Detection," Advance Sustainable Science Engineering and Technology, vol. 7, no. 1, pp. 02501010–02501010, 2025.
[26] D. A. Rashid and M. B. Mohammed, "Black Hole Attack Detection in Wireless Sensor Networks Using Hybrid Optimization Algorithm," UHD Journal of Science and Technology, vol. 8, no. 1, pp. 142–150, 2024.
[27] A. Manhar and D. Dembla, "Routing Optimizing Decisions in MANET: The Enhanced Hybrid Routing Protocol (EHRP) with Adaptive Routing based on Network Situation."
[28] R. Jain, "Ant colony inspired energy efficient OLSR (AC-OLSR) routing protocol in MANETS," Wireless Personal Communications, vol. 124, pp. 3307-3320, 2022.
[29] M. S. U. Suseela, V. Praveena, N. Lakshmi, M. Hemalatha, and V. S. Kumar, "Advanced Cross-Layer Protocol Architecture through Modified Ideal Link State Routing (MOLSR)," in 2024 7th International Conference on Contemporary Computing and Informatics (IC3I), 2024, pp. 1186-1190.

Journal of Basrah Researches (Sciences) **51**(1), 195 (2025)
DOI: https://doi.org/10.56714/bjrs.51.1.17

تحسين قائم على التعلم العميق ل OLSR للكشف القوي عن الهجمات ونقل الوسائط المتعددة الآمن في MANETs

ميثم محمد علي عبد الله *، حامد علي عابد الأسدي.

قسم علوم الحاسب ، كلية التربية للعلوم البحتة، جامعة البصرة، البصرة ، العراق.

معلومات البحث

الاستلام 6 نيسان 2025
االمراجعة 18 أيار 2025
القبول 26 أيار 2025
النشر 30 حزيران 2025

الكلمات المفتاحية

OLSRP ، إسقاط الحزمة الانتقائي ، MANET ، التعلم العميق ، الشبكة المكثفة ، اكتشاف التسلل.

الملخص

تشترك شبكات استشعار الوسائط المتعددة اللاسلكية (WMSNs) والشبكات المخصصة المتنقلة (MANETs) في ميزات مهمة ، مثل طوبولوجيا اللامركزية ونقل الوسائط المتعددة بدون بنية تحتية. ومع ذلك ، فإن طبيعتها الديناميكية تعرضها لهجمات التوجيه الداخلية ، بما في ذلك على سبيل المثال لا الحصر ، هجمات إسقاط الحزم الانتقائية التي تحظر فيها العقد الضارة تدفق البيانات دون اكتشافات. تقدم هذه الورقة DCBiGNet-SA وهو نموذج هجين للتعلم العميق ينفذ مزيجا من الشبكات العصبية التلافيفية الكثيفة (DCNN) ، و GRUs ثنائية الاتجاه (GRU-Bi) ، وانتباه القناة كنهج دفاعي في بروتوكول توجيه حالة الارتباط المحسن (OLSRP). باستخدام السجلات السلوكية ومقاييس الشبكة ، يحدد النموذج العقد الخصومة بدقة عالية. تم تقييم النموذج باستخدام ٣-NS / Python ومجموعة بيانات DS-WSN وحدد العقد العدائية بمستوى عال من الدقة بنسبة ٩٩,٧٥٪ ، ودقة ٩٩,٣٠٪ ، و Score-F1 ٩٩,٠٢٪ ، و ٩٨,٨٪ استدعاء ، وهو أفضل من الطرق التقليدية.

Citation: M. M. A. Abdullah, H. A. A. AL-Asadi., J.Basrah Res. (Sci.) **51**(1),195 (2025). DOI:https://doi.org/10.56714/bjrs.51.1.17

***Corresponding author email:** pgs.maithem.muhammad@uobasrah.edu.iq

ISSN: 1817-2695 (Print); 2411-524X (Online)
Online at: https://jou.jobrs.edu.iq