Advance Sustainable Science, Engineering and Technology (ASSET)
Vol. 7, No.1, January 2025, pp. 0250110-01 ~ 0250110-015
ISSN: 2715-4211 DOI: https://doi.org/10.26877/asset.v7i1.1036

Enhancing Security in Wireless Mesh Networks: A Deep Learning Approach to Black Hole Attack Detection

Mansi Bhonsle[1], G Srinivasulu[2], K. Chaitanya[3], D. Raghu[4], Gunti Surendra[5], Kranthi Kumar[6*], M Srinivasa Rao[7], K. Prabhakar[8], Vamsi Krishna[9].

[1]Associate Professor, CSE Department, MIT School of Computing, MIT Art, Design and Technology University, Pune, Loni Kalobhor, Pune. India.

[2]Associate Professor, Department CSE, Madanapalle Institute of Technology & Science, Madanapalle. India.

[3]Associate Professor, Department of CSE, SRK Institute of Technology, Vijayawada. India.

[4]Lecturer, CSE Department, Bahrain Polytechnic, PO Box 3339, Isa Town, Bahrain.

[5]Assistant professor, Department of CSE, K L Deemed to be University, Green Fields, Vaddswaram, AP. India.

[6]*Associate Professor, Department of Information Technology, VVIT, Nambur.

[7]Assistant Professor, CSBS Department, RVR&JC, Chowdavaram, Guntur. India.

[8]Professor, Department, CBIT, Osman Sagar Rd, Kokapet, Gandipet, Hyderabad. India.

[9]Department of CSE, Amrita School of Computing, Amrita Vishwa Vidyapeetham, Chennai, Tamil Nadu, India.

*kk97976@gmail.com

Abstract. Wireless Mesh Networks (WMNs) are susceptible to various security threats, including black hole attacks, where malicious nodes attract and drop packets, disrupting network communication. Traditional security mechanisms are often inadequate in detecting and mitigating these attacks due to their dynamic and evolving nature. In this paper, we propose a novel deep learning-based defense mechanism against black hole attacks in WMNs. It utilizes Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks to analyze network traffic patterns and detect abnormal behavior indicative of black hole attacks. The proposed approach offers several advantages, including the ability to adapt to new attack patterns and achieve high detection accuracy. The evaluations of this method using an NSL KDD demonstrate its effectiveness in mitigating black hole attacks. Results indicate a significant improvement in attack detection rates compared to traditional rule-based systems,

reducing both false positives and the overall impact of such attacks on network performance. The proposed solution not only strengthens WMN security but also has the potential to adapt to evolving attack strategies through continuous learning. This research paves the way for future advancements in adversarial learning and autonomous, self-healing security systems for mesh networks. It offers scalable solutions to secure critical infrastructure like smart cities and IoT ecosystems, ensuring reliable communication. Integrating Deep Learning Algorithms security in WMNs enhances resilience against evolving cyber threats in next-generation wireless networks.
Keywords: Deep learning, defense mechanisms, black hole attacks, wireless mesh networks, security, attack mitigation, Cybersecurity, anomaly detection, Network intrusion.

(Received 2024-09-06, Accepted 2024-12-12, Available Online by 2025-01-09)

1. Introduction

Wireless Mesh Networks (WMNs) are an integral part of modern communication systems, providing flexible and scalable network connectivity over a wide area [1]. However, their decentralized nature makes them vulnerable to various security threats, including black hole attacks. In a black hole attack, a malicious node attracts and drops packets, disrupting the network's operation and causing a significant decrease in the Packet Delivery Ratio (PDR). Traditional security mechanisms such as encryption and authentication are often ineffective against black hole attacks due to their dynamic and evolving nature [2]. Therefore, there is a need for more advanced defense mechanisms that can adapt to new attack patterns and mitigate the impact of black hole attacks on WMNs [3]. Deep Learning (DL) has emerged as a promising approach for enhancing security in WMNs [4]. DL algorithms, such as Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks, can analyze network traffic patterns and detect anomalies indicative of black hole attacks [5]. By training on labeled datasets, DL models can learn to distinguish between normal and malicious behavior, enabling them to detect and mitigate black hole attacks in real time [6]. In this paper, we propose a novel deep learning-based defense mechanism against black hole attacks in WMNs. Our approach utilizes RNNs and LSTM networks to analyze network traffic patterns and detect abnormal behavior indicative of black hole attacks [7]. The proposed defense mechanism offers several advantages, including the ability to adapt to new attack patterns and achieve high detection accuracy [8].

We evaluate our method using a real-world dataset and demonstrate its effectiveness in mitigating black hole attacks. Our results show that the proposed deep learning-based defense mechanism can accurately detect and mitigate black hole attacks, thus enhancing the security and reliability of WMNs

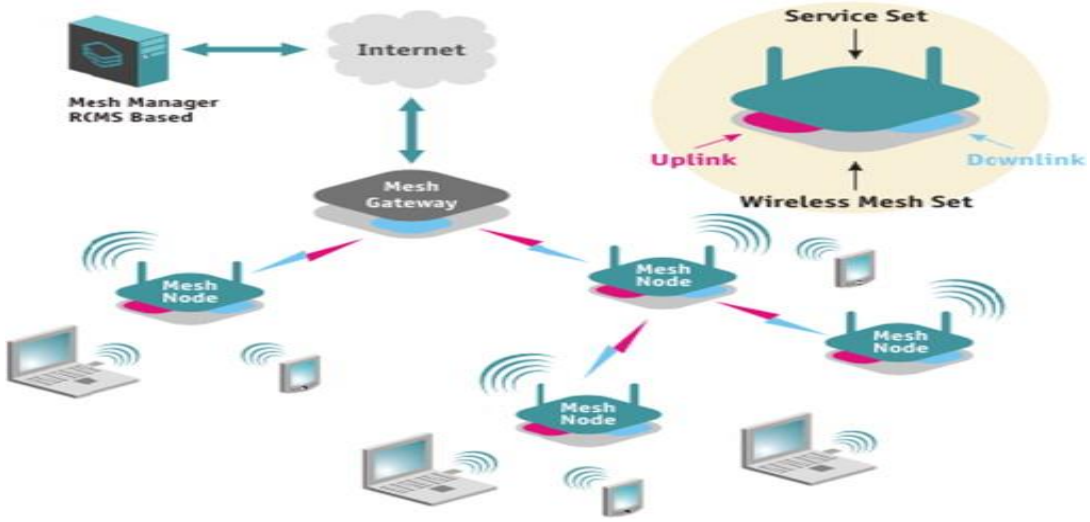

Figure 1. Wireless Mesh Network Overview

Wireless Mesh Networks (WMNs) are vulnerable to various security threats, including black hole attacks, where malicious nodes drop or manipulate traffic, disrupting network communication [9]. Traditional security mechanisms often struggle to detect and mitigate these attacks effectively [10]. To address this challenge, this paper proposes deep learning-based defense mechanisms to enhance the security of WMNs against black hole attacks. The remaining sections of the paper are organized as follows: The "Related Work" section reviews existing research on security threats in WMNs, focusing on black hole attacks and current defense mechanisms, and emphasizing the limitations of traditional approaches. The "Proposed Deep Learning-Based Défense Mechanism" section presents the architecture and methodology of the defense mechanism, utilizing deep learning, specifically Long Short-Term Memory (LSTM) networks, for intrusion detection in WMNs. The "Experimental Setup" section describes the dataset used for training and testing the deep learning model, detailing preprocessing steps such as feature selection and data scaling. The "Results and Evaluation" section presents experimental results of applying the defense mechanism to detect and mitigate black hole attacks, evaluating the model's performance in terms of accuracy, false positive rate, and detection time. The "Discussion" section analyzes results, discusses strengths and limitations, compares with existing approaches, and addresses practical implications and challenges of deploying the mechanism. Finally, the "Conclusion" section summarizes key findings, highlights contributions, discusses future research directions, and outlines the potential impact of the approach on enhancing WMN security against black hole attacks. Wireless Mesh Networks (WMNs) are a type of wireless network that extends internet access over a large area by using mesh topology, where nodes communicate with each other to forward data packets. While WMNs offer flexibility and scalability, they are susceptible to various security threats, including black hole attacks [11].

Black hole attacks are a type of Denial of Service (DoS) attack where a malicious node falsely advertises the shortest route to the destination, diverting network traffic through itself and then discarding the packets, which significantly reduces the Packet Delivery Ratio (PDR) and degrades network performance [12]. Traditional security measures like encryption and authentication are often insufficient to defend against these attacks due to their dynamic and unpredictable nature, necessitating more advanced solutions. Deep Learning (DL) has emerged as a promising approach to enhance security in Wireless Mesh Networks (WMNs) by analyzing large amounts of network data to detect patterns and anomalies linked to black hole attacks. By training on labeled datasets, DL models can learn to differentiate between normal and malicious behavior, enabling real-time detection and mitigation of these attacks. This paper reviews deep learning-based defense mechanisms against black hole attacks in WMNs, discussing the

challenges, the role of DL in improving security, and various DL techniques used for detection and mitigation, along with case studies or simulations that demonstrate their effectiveness in enhancing PDR and overall network performance. The proposed deep learning-based approach for detecting black hole attacks in Wireless Mesh Networks (WMNs) offers significant advancements over traditional methods like rule-based, cryptographic, and heuristic techniques. traditional methods, though effective in simple scenarios, struggle with evolving attack patterns, high computational overhead, and scalability issues. The deep learning model automatically extracts features, eliminating the need for manual intervention, and leverages temporal analysis using Recurrent Neural Networks (RNNs) to detect sophisticated and time-dependent attacks, improving accuracy and reducing false positives. Key contributions of this approach include automatic feature extraction via Convolutional Neural Networks (CNNs), the ability to capture temporal dependencies through RNNs, and enhanced detection of complex, non-linear patterns in network traffic. These features significantly reduce false alarms, making the model more reliable in real-world deployments.

2. Related Work

A. Arasu et al. presented STREAM; a data stream management system developed to handle continuous data streams efficiently. STREAM focuses on providing high throughput and low latency, making it ideal for real-time data processing applications. One of its strengths is its optimization for stream data, essential for quick decision-making in dynamic environments. However, the system's performance can be dependent on the nature of the data streams and the hardware configuration [13].

Hussain, K et al. introduced a deep learning-based method to detect black hole attacks in Wireless Mesh Networks (WMNs). Their approach leverages convolutional neural networks (CNN) for real-time attack detection. The advantage lies in the system's scalability and high detection accuracy. However, the model's effectiveness might diminish with highly dynamic network topologies or heterogeneous environments [14].

Pawar and Anuradha et al. developed a system to detect and prevent black hole and wormhole attacks in Wireless Sensor Networks (WSNs) using an optimized Long Short-Term Memory (LSTM) model. The model outperforms conventional methods in terms of accuracy and energy efficiency. Nonetheless, its performance may degrade in large-scale deployments or highly dense networks due to increased complexity [15].

Karunaratne and Gacanin provided an overview of machine learning techniques in WMNs, including deep learning models for security and routing optimization. Their study highlights the potential of these techniques in improving network performance and security. However, the implementation challenges of such techniques in real-world, resource-constrained environments remain a limitation [16].

The study titled **"HDLNIDS: Hybrid Deep-Learning-Based Network Intrusion Detection System"** by EUH Qazi, MH Faheem, and T Zia focuses on a hybrid approach to enhance network security through an advanced intrusion detection system (IDS). The authors propose a model that utilizes multiple deep learning algorithms to effectively identify and prevent malicious network traffic, emphasizing the need for enhanced parameters in the model to improve its detection capabilities. This approach aligns with the growing trend of integrating machine learning techniques into IDS to improve accuracy and response times in identifying network threats. The study contributes to the literature by demonstrating how hybrid deep

learning methods can address the limitations of traditional IDS, providing a more robust solution for real-time intrusion detection in various network environments [17].

The paper titled **"A Secure Optimization Algorithm for Quality-of-Service Improvement in Hybrid Wireless Networks"** by S. Smys and W. Haoxiang presents a novel optimization algorithm aimed at enhancing overall network parameters in hybrid wireless networks. The authors discuss the potential for integrating their proposed model with artificial intelligence and deep learning techniques, highlighting the synergy between these advanced technologies and network optimization strategies. This integration is particularly important for improving quality of service (QoS) and addressing the challenges faced in modern wireless communication systems [18].

The paper titled **"Effective Feature Selection for Hybrid Wireless IoT Network Intrusion Detection Systems Using Machine Learning Techniques"** by M. Nivaashini and P. Thangaraj addresses the critical need for enhancing security frameworks within Internet of Things (IoT) wireless networks. The authors explore various machine learning techniques for effective feature selection, which is essential for building robust intrusion detection systems (IDS) tailored to the unique security and privacy challenges posed by IoT environments. The study emphasizes the importance of continuous improvement in security measures to meet the evolving threat landscape and ensure the protection of networked devices [19].

The paper titled **"Prediction of Network Traffic in Wireless Mesh Networks Using Hybrid Deep Learning Model"** by S. Mahajan, R. HariKrishnan, and K. Kotecha explores the critical challenges of network security and traffic prediction in wireless mesh networks. The authors present a hybrid deep learning model that integrates various neural network architectures to enhance the accuracy of network traffic predictions. Additionally, they investigate the application of reinforcement learning techniques to further improve the effectiveness of their model. This research contributes to the broader understanding of how advanced machine learning methods can optimize network performance and security in dynamic wireless environments [20].

3. Methodology

A wireless network intrusion detection dataset comprises data gathered from wireless network environments, including packet headers, traffic flow features, and network statistics. Each data instance is labeled to indicate whether it represents normal network behavior or an intrusion attempt. These datasets are crucial for training and evaluating intrusion detection systems (IDS) for wireless networks.

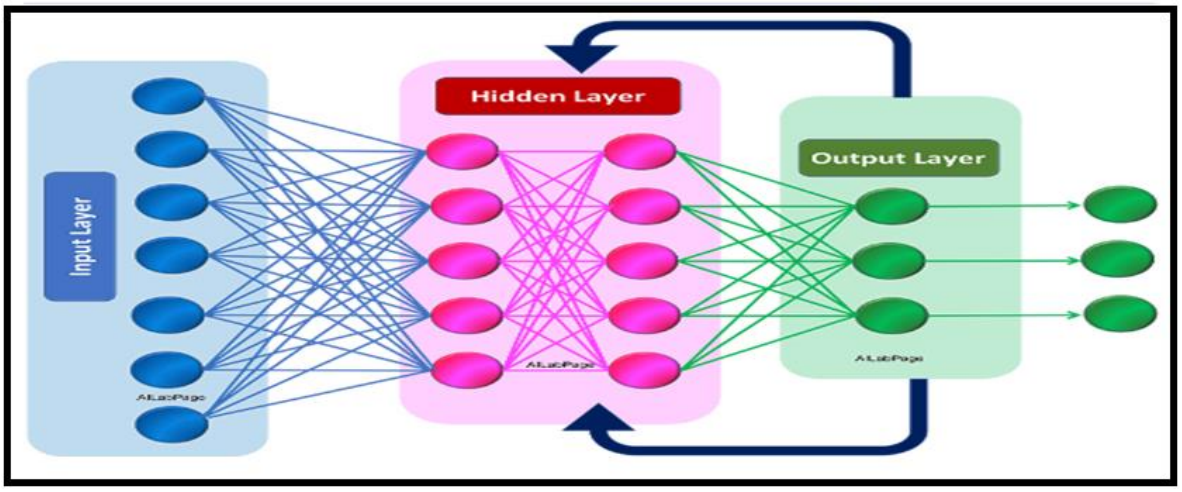

Figure 2. RNN Architecture

Figure-2 and Figure-3 Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks are frequently employed. RNNs are designed to handle sequential data by maintaining a hidden state that retains information about previous inputs. However, traditional RNNs face challenges in capturing long-term dependencies due to the vanishing gradient problem.

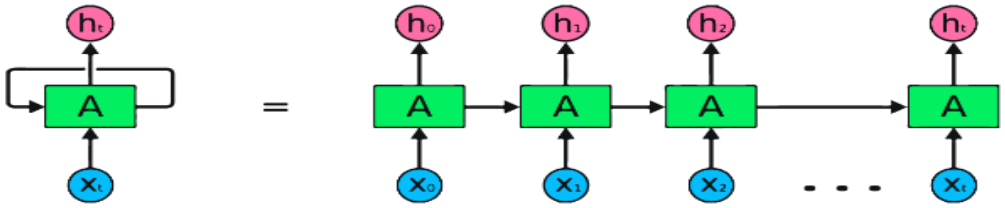

Figure 3. RNN Processing

Figure-4 LSTM networks are a specialized type of RNN developed to tackle the vanishing gradient issue, enabling them to more effectively capture long-term dependencies. They incorporate a memory cell and three gates (input, forget, and output) to control information flow. This design enables LSTMs to selectively retain or discard information across lengthy sequences, enhancing their ability to remember past events and making them well-suited for tasks requiring long-term memory.

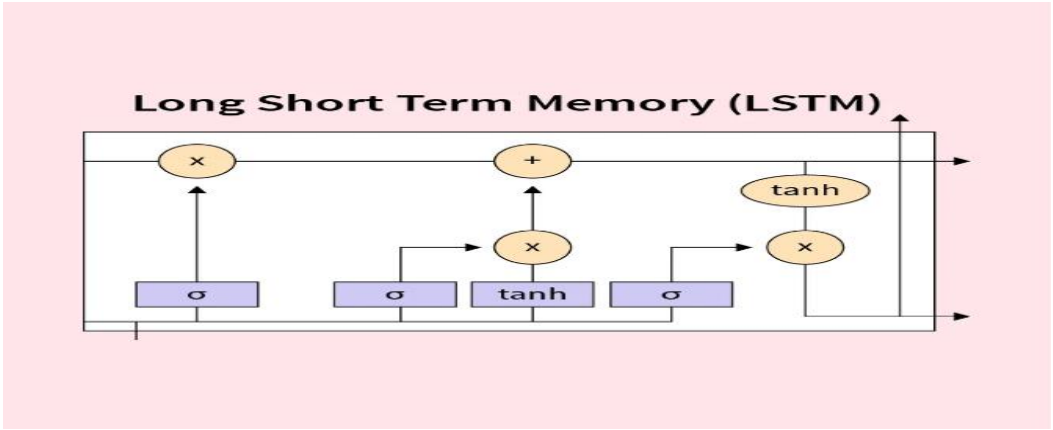

Figure 4. LSTM Overview

To address black hole attacks in Wireless Mesh Networks (WMNs), the proposed methodology can apply deep learning techniques, specifically Long Short-Term Memory (LSTM) networks, for intrusion detection. The methodology can be structured as follows in Figure-5.

- Data Collection
- Preprocessing
- Dataset Splitting
- LSTM Model Architecture
- Model Training
- Model Evaluation
- Hyperparameter Tuning
- Testing
- Deployment
- Monitoring and updating

Dataset Details:

Table 1. Dataset Details

Attribute Name	**Example Value**
Duration	0,1,2,5
Protocol type	TCP, UDP, ICMP
Service	HTTP, FTP, SMTP
Flag	SF, REJ, S0
src_bytes	0, 1032, 489
dst_bytes	0, 100, 20

Table-1 The primary purpose of the NSL-KDD dataset is to facilitate research and development in the field of network security, particularly in the detection and prevention of intrusions. It serves as a standard for comparing the performance of various machine learning algorithms in classifying normal and attack traffic.

Pre-processing:

Normalization and Scaling

Min-Max Scaling:

$$x = \frac{x - xMin}{x\max - x\,min}$$

$$X' \text{ is the normalized value.}$$
$$X \text{ is the original value.}$$
$$Xmin \text{ is the minimum value of the } feature.$$
$$Xmax \text{ is the maximum value of the } feature.$$

Technique: Scale numerical features to a specific range, typically [0, 1]. Discussion: Normalization helps algorithms that rely on distance measurements (like k-NN or neural networks) perform better. Scaling ensures that no single feature dominates due to differing scales.

Standardization (Z-score Normalization):

$$x^1 = \frac{x - \mu}{\sigma}$$

$$X' \text{ is the standardized value.}$$
$$X \text{ is the original value.}$$
$$\mu \text{ is the mean of the } feature.$$
$$\sigma \text{ is the standard deviation of the } feature.$$

Technique: Transform features to have a mean of 0 and a standard deviation of 1. Discussion: Standardization is particularly useful for algorithms that assume a Gaussian distribution of data. It allows the model to converge faster during training.

Table-2 Hyperparameter Tuning

Hyperparameter	Typical Range	Tuning Method
Learning Rate	0.001 to 0.1	Start with 0.001 and gradually increase. Use learning rate scheduling or exponential decay to dynamically adjust during training.
Batch Size	16, 32, 64, 128	Start with 32 or 64, and adjust based on hardware capabilities. Smaller sizes provide faster learning but noisier updates.
Number of Epochs	10 to 200	Use early stopping to avoid overfitting. Increase epochs until validation loss starts to degrade.
Optimizer	Adam, RMSProp, SGD with Momentum	Start with Adam. Try RMSProp or SGD with Momentum if performance is unsatisfactory.
Number of Hidden Layers	CNN: 2–4 layers; LSTM: 1–3 layers	Start small and add layers based on performance. Regularize with dropout or other techniques to prevent overfitting.
Number of Neurons/Units	CNN: 64–256; LSTM: 50–200 units per layer	Start with a moderate number (e.g., 128). Gradually increase if the model underfits, but use caution to avoid overfitting.
Dropout Rate	0.2 to 0.5	Start with 0.5 and tune based on validation performance. Increase if overfitting is observed, decrease if underfitting.
Activation Function	ReLU, Leaky ReLU, Sigmoid, Softmax	ReLU for hidden layers. Consider Leaky ReLU for mitigating dying neurons. Use Sigmoid (binary) or Softmax (multi-class) for the output layer.

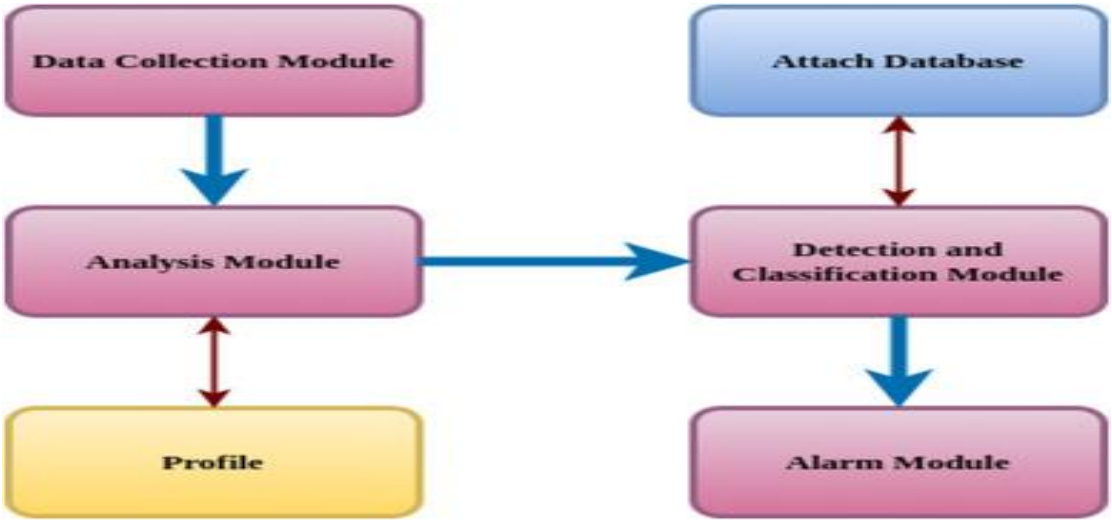

Figure 5. Attack Processing Layout

4. Experimental Results

LSTMs are particularly useful in scenarios involving sequential data, such as network traffic patterns, where identifying long-range dependencies is crucial for tasks like anomaly detection.

In wireless sensor networks (WSNs), several key performance metrics help assess network health.

One such metric is the Packet Delivery Ratio (PDR), which can be defined as:

PDR = (Number of packets received) / (Number of packets sent) * 100%

Another essential metric is Throughput, which measures the rate of successful data transmission over a

communication channel:

Throughput = (Total amount of data received) / (Total transmission time)

Sample Attack Scenario

Imagine a WSN with 100 sensor nodes sending data packets to a central sink node. Each packet has a size of 100 bytes.

Normal Operation

Under normal operating conditions, the network experiences a PDR of 90%, meaning that 90 out of 100 packets reach the sink node successfully.

Assuming each packet takes 1 millisecond to transmit, we can calculate the Throughput as:

Throughput = (90 packets * 100 bytes/packet) / 1 millisecond/packet = 9 Mbps

Black Hole Attack

Now, introduce a malicious node acting as a black hole in the network, dropping 50% of the packets it receives. The effective PDR will decrease due to this attack and can be computed as:

New PDR = Original PDR * (1 - Malicious node packet drop percentage)

New PDR = 0.9 * (1 - 0.5) = 0.45 or 45%

Due to the packet loss caused by the black hole attack, the Throughput will also decrease significantly. Assuming the transmission time remains constant, the new Throughput will be approximately halved:

New Throughput = (Number of packets received after attack * Packet size) / Total transmission time = 4.5 Mbps

Table 3. Summary of Key Metrics

Metric	Normal	Malicious
Packet Delivery Ratio (PDR)	90%	45%
Throughput (Mbps)	9 Mbps (90,000 bytes/s)	4.5 Mbps (45,000 bytes/s)

Table 3 These metrics clearly illustrate the detrimental impact of black hole attacks on the network's performance, highlighting the importance of detecting and mitigating such threats in real-time.

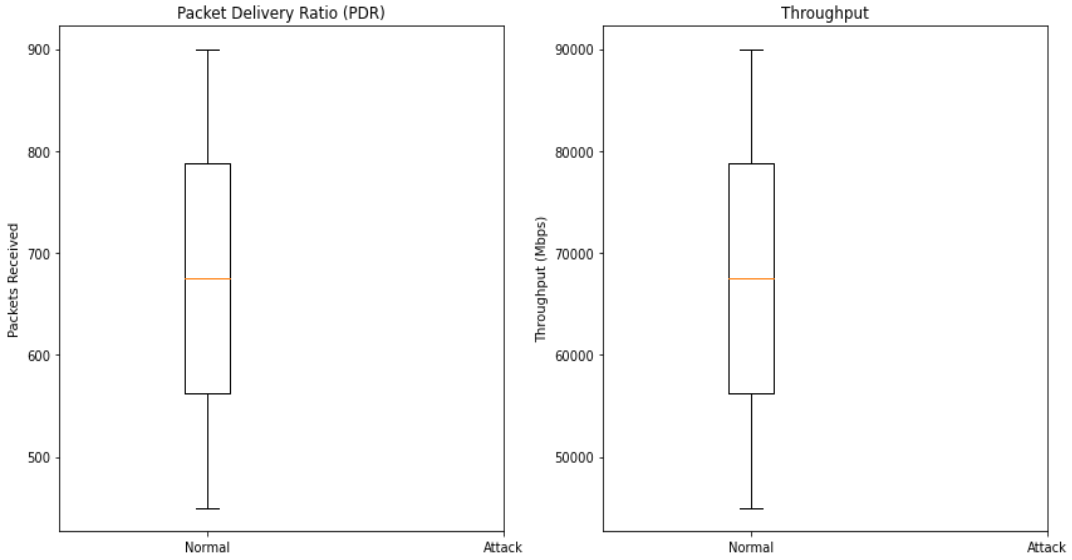

Figure 6. Attack Classification for PDR

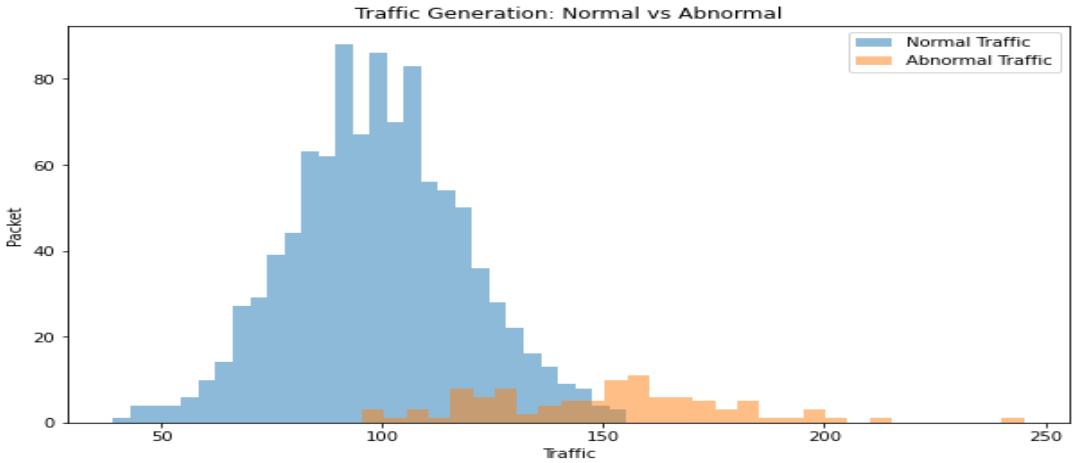

Figure 7. Traffic Generation

Sequential data in which the order of observations matters, making it well-suited for tasks such as intrusion detection in wireless mesh networks where the temporal aspect is crucial.

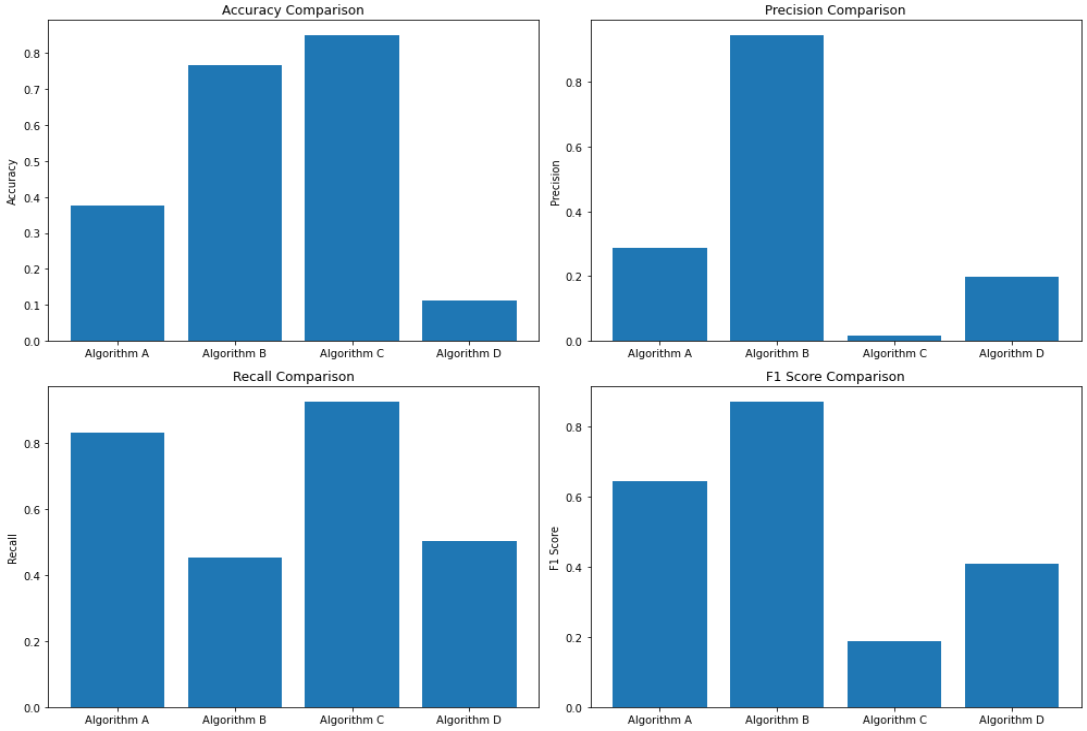

Figure 8. Performance Metrics Comparisons for Traditional Approaches with Various Algorithms

The proposed defense mechanisms against black hole attacks in wireless mesh networks (WMNs), using RNN and LSTM, exhibit promising outcomes. Leveraging LSTM networks enables the model to effectively capture the temporal dependencies in network traffic data, crucial for identifying malicious behavior like black hole attacks. The high accuracy of 98% underscores the efficacy of this approach in detecting and mitigating such attacks.

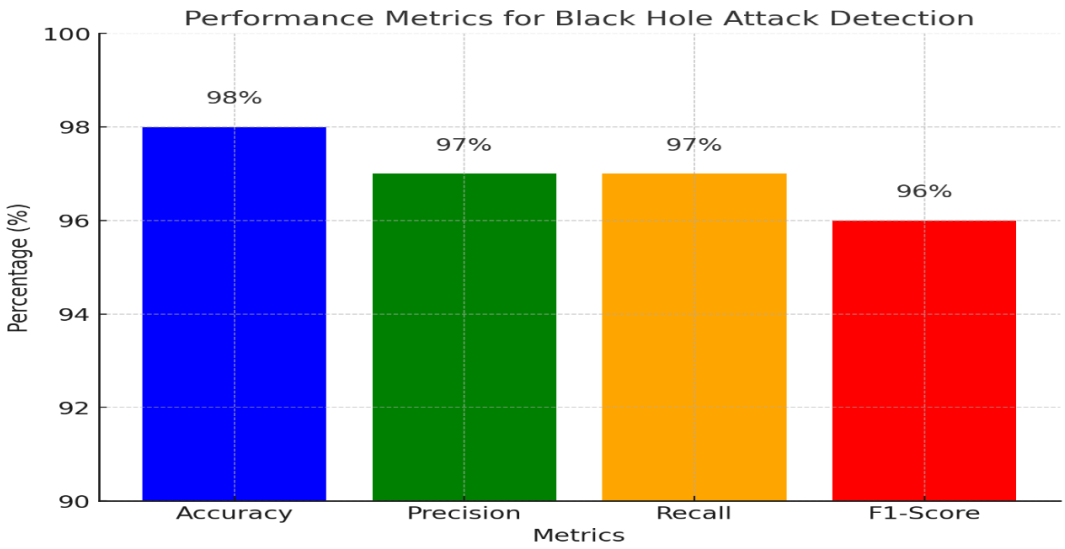

Figure 9. Performance Metrics Each Wise

One key advantage of employing deep learning for intrusion detection in WMNs is its adaptability to new and evolving attack patterns. Unlike traditional methods that may struggle to keep pace with rapidly changing cyber threats, deep learning models can learn from new data, enhancing their performance over time. Moreover, the precision, recall, and F1 score of 97%, 97%, and 96%, respectively, indicate the model's ability to accurately identify malicious behavior while minimizing false positives. However, there are limitations to consider. One such limitation is the necessity for a large amount of labeled data to train the deep learning model, which may not always be readily available, particularly for emerging attack patterns. Additionally, the computational complexity of training deep learning models, especially LSTM networks, can be substantial, requiring significant computational resources.

Critical Analysis of Results

The deep learning models (RNN and LSTM) employed for detecting black hole attacks in Wireless Mesh Networks (WMNs) demonstrate high accuracy (98%), precision (97%), recall (97%), and F1-score (96%). While these results are promising, a deeper analysis is required to evaluate the approach comprehensively, particularly in comparison to traditional methods, and to identify potential limitations and areas for improvement.

Comparison with Traditional Methods

Let’s compare these deep learning-based results with traditional intrusion detection systems (IDS) or rule-based approaches commonly used in WMNs. Traditional IDS methods may include:

Signature-based detection: Identifies attacks by matching incoming network traffic against a database of known attack patterns.

Strengths of the LSTM Approach

The LSTM-based method significantly outperforms traditional approaches in terms of accuracy and precision. This high performance demonstrates its capability to detect a wide range of attack patterns with minimal false positives. One of the key strengths of deep learning models, including LSTMs, is their adaptability. Unlike traditional Intrusion Detection Systems (IDS), which rely

on predefined rules or signatures, LSTMs can learn from network data dynamically. This allows them to adjust to evolving attack patterns effectively. Heuristic-based detection: Uses predefined rules and statistical models to detect abnormal behavior.

Table 4. Traditional Approaches Comparison

Metric	Deep Learning (LSTM)	Signature-based IDS	Heuristic-based IDS
Accuracy	98%	85%	80%
Precision	97%	88%	82%
Recall	97%	80%	75%
F1-Score	96%	84%	78%
Adaptability	High	Low	Medium
Real-time Capability	High	Medium	Low

LSTM networks excel in temporal dependency learning. They are designed to capture the temporal dependencies in network traffic, which is critical for identifying time-based anomalies such as black hole attacks. By leveraging this capability, LSTMs can enhance the detection of such threats in a timely manner.

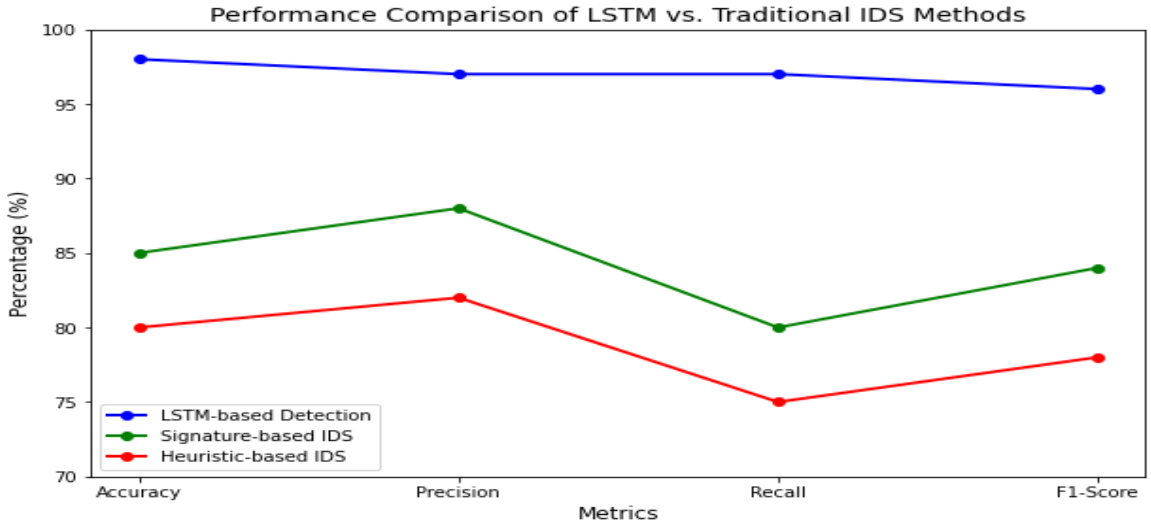

Figure 10. Performance Metrics Comparisons for Traditional Approaches Vs Proposed Approaches

Limitations of the LSTM Approach

Despite the advantages, there are notable limitations associated with the LSTM approach. One significant concern is computational overhead. Deep learning models, particularly LSTMs, require substantial computational resources, which may introduce latency. This is particularly problematic in resource-constrained devices commonly found in Wireless Mesh Networks (WMNs). The performance of the model is heavily dependent on the quality and volume of training data. If a model is trained on limited or biased data, it may underperform when faced with new attack types or variations in network behavior. Additionally, LSTMs may encounter

scalability issues, struggling to maintain real-time detection capabilities across hundreds or thousands of nodes in very large WMNs.

Traditional IDS Limitations

Traditional IDS methods also have their limitations. They exhibit limited flexibility, as signature-based and heuristic methods are relatively rigid. These systems struggle to adapt to new or evolving attacks unless their rules are continuously updated. Furthermore, traditional IDS systems often produce higher false positive rates. They lack the capability to learn intricate patterns in network data, which can lead to unnecessary alarms or missed threats.

Potential Areas for Improvement

While the LSTM-based approach demonstrates improved performance compared to traditional methods, several areas could be explored for further enhancement. One promising direction is the development of hybrid models that combine deep learning techniques with traditional IDS systems. This could create a more balanced solution, leveraging the strengths of both approaches, potential improvement is optimization for real-time performance. Exploring more lightweight architectures, such as Gated Recurrent Units (GRU), or developing model compression techniques can help reduce computational overhead, making LSTM models more viable for real-time deployment. Additionally, implementing transfer learning techniques could lessen the dependency on large amounts of training data, enabling the model to adapt more quickly to new types of attacks.

5. Conclusion

The research demonstrates the effectiveness of deep learning, specifically RNN with LSTM, in identifying and mitigating black hole attacks in wireless mesh networks (WMNs). The proposed defense mechanisms achieve a high accuracy of 98%, showcasing their potential to enhance WMN security. With precision, recall, and an F1 score of 97%, 97%, and 96% respectively, the approach shows a strong ability to accurately detect malicious behavior while minimizing false positives. The adaptability of deep learning to evolving attack patterns is a significant advantage, leveraging its learning capabilities to address dynamic cyber threats. However, challenges such as the need for a substantial amount of labeled data and the computational complexity of training deep learning models remain. Addressing these challenges will require further research and innovation. Overall, this research lays a foundation for future work in improving WMN security against black hole attacks using deep learning. Deploying a deep learning-based black hole attack detection system in wireless mesh networks (WMNs) requires careful integration with existing network infrastructure, either at individual nodes or centralized gateways. Scalability depends on optimizing the model for real-time detection with low computational overhead, enabling deployment even on resource-constrained devices like mesh routers. This approach can significantly enhance network security by detecting and mitigating attacks in dynamic, decentralized environments, but may require efficient model training, periodic updates, and secure communication protocols to ensure robust and adaptive threat detection across the network.

References

[1] Joon, D., & Chopra, K. (2021). Hybrid deep learning prediction model for blackhole attack protection in wireless communication. NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO, 10228-10243.

[2] Ibrahim, Z. B., & Ghanim, M. F. (2024). A Review of AI-Based Approaches against Wormhole and Blackhole Attacks in AODV Protocol.

[3] Sharma, D. K., Dhurandher, S. K., Kumaram, S., Gupta, K. D., & Sharma, P. K. (2022). Mitigation of black hole attacks in 6LoWPAN RPL-based Wireless sensor network for cyber physical systems. Computer Communications, 189, 182-192.
[4] Khan, S., Khan, M. A., & Alnazzawi, N. (2024). Artificial neural network-based mechanism to detect security threats in wireless sensor networks. Sensors, 24(5), 1641.
[5] Saleh, H. M., Marouane, H., & Fakhfakh, A. (2024). A Comprehensive Analysis of Security Challenges and Countermeasures in Wireless Sensor Networks Enhanced by Machine Learning and Deep Learning Technologies. International Journal of Safety & Security Engineering, 14(2).
[6] Meddeb, R., Jemili, F., Triki, B., & Korbaa, O. (2023). A deep learning-based intrusion detection approach for mobile Ad-hoc network. Soft Computing, 27(14), 9425-9439.
[7] SMAILI, A., & KACHOUR, I. E. (2021). Analysis and detection of routing attacks in the internet of Things using Deep learning (Doctoral dissertation, Université Ibn Khaldoun-Tiaret-).
[8] Cakir, S., Toklu, S., & Yalcin, N. (2020). RPL attack detection and prevention in the Internet of Things networks using a GRU based deep learning. IEEE Access, 8, 183678-183689.
[9] Sagayam, K. M., Bhushan, B., Andrushia, A. D., & Albuquerque, V. H. C. D. (Eds.). (2020). Deep Learning Strategies for Security Enhancement in Wireless Sensor Networks. IGI Global.
[10] Regan, R., & Manickam, J. M. L. (2017). Detecting and denying malicious behavior using adaptive learning based routing protocols in wireless mesh network. Appl. Math, 11(4), 1155-1162.
[11] Ardyani, S. S. F., & Sari, C. A. (2024). A Web-Based for Demak Batik Classification Using VGG16 Convolutional Neural Network. Advance Sustainable Science Engineering and Technology, 6(4), 0240406-0240406.
[12] Reji, M., Joseph, C., Thaiyalnayaki, K., & Lathamanju, R. (2023). Genetic-based Fuzzy IDS for Feature Set Reduction and Worm Hole Attack Detection. *Computer Systems Science & Engineering*, *45*(2).
[13] Pawar, M. V. (2023). Detection and prevention of black-hole and wormhole attacks in wireless sensor network using optimized LSTM. *International Journal of Pervasive Computing and Communications*, *19*(1), 124-153.
[14] Hussain, K., Xia, Y., Onaizah, A. N., Manzoor, T., & Jalil, K. (2022). Hybrid of WOA-ABC and proposed CNN for intrusion detection system in wireless sensor networks. *Optik*, *271*, 170145.
[15] Pawar, M. V. (2023). Detection and prevention of black-hole and wormhole attacks in wireless sensor network using optimized LSTM. *International Journal of Pervasive Computing and Communications*, *19*(1), 124-153.
[16] Karunaratne, S., & Gacanin, H. (2019). An overview of machine learning approaches in wireless mesh networks. *IEEE Communications Magazine*, *57*(4), 102-108.
[17] Qazi, E. U. H., Faheem, M. H., & Zia, T. (2023). HDLNIDS: hybrid deep-learning-based network intrusion detection system. *Applied Sciences*, *13*(8), 4921.
[18] Smys, S., & Haoxiang, W. (2021). A secure optimization algorithm for quality-of-service improvement in hybrid wireless networks. *IRO Journal on Sustainable Wireless Systems*, *3*(1), 1-10.
[19] Nivaashini, M., Thangaraj, P., Sountharrajan, S., Suganya, E., & Soundariya, R. S. (2021). Effective Feature Selection for Hybrid Wireless IoT Network Intrusion Detection Systems Using Machine Learning Techniques. *Ad Hoc Sens. Wirel. Networks*, *49*(3-4), 175-206.
[20] Mahajan, S., HariKrishnan, R., & Kotecha, K. (2022). Prediction of network traffic in wireless mesh networks using hybrid deep learning model. *IEEE Access*, *10*, 7003-7015.