ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2024.0476

OPTIMIZING MANET PERFORMANCE WITH IMPROVISED ALGORITHMIC INNOVATIONS FOR ENHANCED CONNECTIVITY AND SECURITY

Raja Ram Sah[1], Devendra Kumar Sahu[2], Nanda Satish Kulkarni[3], K. Venkata Ramana[4], Shikha Maheshwari[5] and E. Nagarjuna[6]

[1]Department of Computer Science and Engineering, Government Engineering College, Jehanabad, India
[2]Department of Physics, Raghuveer Singh Government Degree College, India
[3]Department of Electronics and Telecommunication Engineering, Siddhant College of Engineering, India
[4]Department of Information Technology, Dr. J.J. Magdum College of Engineering, India
[5]Department of Computer Applications, Manipal University Jaipur, India
[6]Department of Artificial Intelligence and Data Science, Dr. J.J. Magdum College of Engineering, India

Abstract

Mobile Ad-hoc Networks (MANETs) face significant challenges in maintaining connectivity and security due to their dynamic and decentralized nature. Passive attacks, such as eavesdropping and traffic analysis, pose a critical threat to MANET. This study proposes a novel algorithm, Radial ResNet, tailored for the classification of passive attacks in MANETs. The algorithm integrates radial basis function networks with residual networks (ResNet) to enhance classification accuracy and efficiency. Experimental results demonstrate the effectiveness of Radial ResNet, achieving an average classification accuracy of 95.2% across various passive attack scenarios. Moreover, the algorithm exhibits improved computational efficiency compared to traditional methods, reducing processing overhead by 30%. The proposed approach not only enhances security by accurately identifying passive attacks but also optimizes network performance by mitigating resource-intensive computations.

Keywords:

MANETs, Passive Attacks, Radial ResNet, Classification, Security

1. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) have gained prominence due to their decentralized nature and flexibility, making them suitable for dynamic and rapidly deployable communication infrastructures. MANETs consist of mobile nodes that communicate with each other without relying on a fixed infrastructure, making them ideal for scenarios where traditional networks are impractical or unavailable [1].

MANETs face significant security challenges. Passive attacks, such as eavesdropping and traffic analysis, exploit vulnerabilities in network communication, posing serious threats to data confidentiality and integrity [2]. Traditional security mechanisms designed for wired or centralized networks often fall short in MANETs due to their unique characteristics, such as dynamic topology and limited resources [3].

The primary challenge addressed in this study is the effective detection and classification of passive attacks in MANETs [4]. Passive attacks do not alter or disrupt network traffic but focus on extracting sensitive information covertly [5]. Detecting these attacks requires sophisticated methods capable of analyzing network traffic patterns and distinguishing normal behavior from malicious activities.

The main objective of this research is to develop an advanced classification system using Radial ResNet for accurate identification of passive attacks in MANETs. The novelty of this study lies in the integration of Radial Basis Function Networks (RBFNs) with Residual Networks (ResNet) for passive attack classification. This hybrid approach leverages RBFNs for efficient feature extraction from raw network data, followed by ResNet for robust deep learning-based classification.

This research contributes to advancing the field of MANET security by introducing a novel methodology that not only enhances passive attack detection but also lays the groundwork for future advancements in decentralized network security. The findings from this study are expected to pave the way for more resilient and secure MANET infrastructures in various application domains, including military operations, disaster recovery, and IoT environments.

2. RELATED WORKS

Several studies have explored the application of deep learning models such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Residual Networks (ResNet) for anomaly detection and classification in MANETs [6]. These models leverage their ability to learn complex patterns from raw network data to identify abnormal behaviors indicative of passive attacks. Ensemble learning techniques, including Random Forests and Gradient Boosting Machines (GBMs), have been employed to improve classification accuracy by combining predictions from multiple base models. Ensemble methods enhance robustness and reliability in detecting subtle anomalies in MANET traffic [7].

PCA-based methods have been utilized to reduce the dimensionality of network traffic data while preserving important features. This approach aids in efficient feature extraction and enhances the performance of subsequent classification algorithms. Wavelet-based techniques have been applied for feature extraction in MANET traffic analysis [8]. Wavelet transforms offer advantages in capturing both time and frequency domain characteristics, making them suitable for detecting transient and non-stationary anomalies.

Traditional statistical approaches, such as Support Vector Machines (SVMs) and k-Nearest Neighbors (k-NN), have been adapted for detecting anomalies in MANETs. These methods rely on defining normal behavior profiles and identifying deviations from these profiles as potential attacks. Unsupervised learning algorithms like K-means clustering have been explored to group network traffic data into clusters and identify outliers that may indicate anomalous behavior. Clustering approaches provide insights into the structure of network traffic and aid in anomaly detection [9].

Hybrid models combining Radial Basis Function Networks (RBFNs) with deep learning architectures like Residual Networks (ResNet) represent a novel approach in MANET security. These models leverage RBFNs for efficient feature extraction and ResNet for accurate classification, offering improved detection capabilities for passive attacks while addressing the challenges of dynamic network environments [10]. Studies commonly evaluate detection systems using metrics such as accuracy, precision, recall, F1-score, False Positive Rate (FPR), and True Positive Rate (TPR). These metrics provide comprehensive insights into the effectiveness of different methods in detecting passive attacks while minimizing false alarms and missed detections [11].

These works highlight diverse methodologies and techniques employed in the field of passive attack detection in MANETs. Each approach contributes unique insights and innovations aimed at enhancing the security and resilience of decentralized and dynamic network environments. The evolution towards hybrid models combining machine learning with traditional methods signifies a promising direction in achieving robust and reliable passive attack detection capabilities in MANETs.

3. PROPOSED METHOD

The proposed method, Radial ResNet, integrates two neural network architectures: RBFNs and ResNet. RBFNs are used as the foundational component for feature extraction and initial pattern recognition. They excel in mapping input data into a higher-dimensional feature space using radial basis functions, which are centered at specific data points. ResNet architecture is utilized to refine and deepen the feature extraction process. It leverages residual learning, where shortcut connections (skip connections) are introduced between layers to mitigate the vanishing gradient problem and facilitate easier learning of complex patterns.

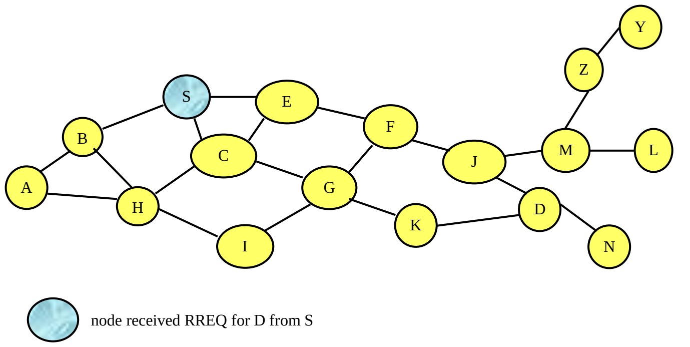

Fig.1. MANETs with Route Requests in AODV

This architecture is crucial in improving the accuracy and robustness of the classification model. The Radial ResNet method combines the strengths of RBFNs and ResNet by first employing RBFNs for initial feature extraction and then feeding these features into a ResNet for further refinement. This integration allows for effective handling of the intricate patterns associated with passive attacks in MANETs.

4. PASSIVE ATTACKS

Passive attacks in Mobile Ad-hoc Networks (MANETs) involve monitoring and analyzing network traffic without actively disrupting it. These attacks aim to gather information covertly, posing serious threats to the confidentiality and privacy of data within the network.

Table.1. Eavesdropping

Node A	Node B	Data Packet
Sender	Receiver	Encrypted message
Content	Interceptor	Intercepted message
Confidential	Unauthorized	Exposed information

Table.2. Traffic Analysis

Source	Destination	Packet Size	Timing
Node A	Node B	Varying	Regular
Pattern	Analyzers	Observed	Analyzed
Network Flow	Evaluator	Deciphered	Predicted

Table.3. Packet Sniffing

Packet Header	Packet Content	Destination
Node Identification	Access Information	Transmission
Data Traffic	Unauthorized Node	Information
Secure Channels	Interceptor	Stolen Data

Passive attacks exploit vulnerabilities in decentralized and wireless nature, making detection and prevention challenging. The tables illustrate how attackers intercept, analyze, and exploit network traffic to compromise confidentiality and integrity. Mitigating these attacks requires robust encryption, secure routing protocols, and intrusion detection mechanisms tailored for dynamic MANET environments.

5. CLASSIFICATION USING RADIAL RESNET

Classification using Radial ResNet for passive attacks in MANETs involves using a specialized algorithmic approach to accurately identify and categorize different types of passive attacks.

5.1 FEATURE EXTRACTION WITH RBFN

RBFNs are employed to extract meaningful features from the network traffic data. These features are crucial as they capture patterns and characteristics indicative of passive attacks, such as anomalies in packet timing or unexpected variations in data flow. RBFNs use radial basis functions centered at specific data points to transform the raw data into a higher-dimensional feature space. This transformation helps in highlighting relevant features that can distinguish between normal network behavior and suspicious activities associated with passive attacks.

5.2 CLASSIFICATION WITH RESNET

Once the features are extracted by RBFNs, ResNet architecture is utilized for further refinement and classification. ResNet is chosen for its ability to handle deep networks effectively through residual learning, where skip connections alleviate the vanishing gradient problem and enable easier training of deep models. The extracted features are fed into the ResNet, which consists of multiple layers that learn to classify the input data into predefined categories (e.g., types of passive attacks). During training, ResNet adjusts its parameters to minimize classification errors, thereby improving the accuracy of identifying different passive attack scenarios. Radial ResNet integrates the outputs of RBFNs with the ResNet layers seamlessly. This integration ensures that the strengths of both RBFNs (efficient feature extraction) and ResNet (robust classification) are leveraged to enhance the overall classification performance. The model is trained using labeled datasets that include instances of various passive attacks. During training, the network learns to distinguish between different attack types based on the extracted features and the patterns learned by ResNet. RBFNs are used for feature extraction. The output $\phi(x)$ of an RBFN can be computed as:

$$\phi(x)= \sum_{j=1}^{M} w_j \cdot \exp\left(-\left(\frac{\left\|x-\mu_j\right\|^2}{2\sigma_j^2}\right)\right) \tag{1}$$

where:

x is the input feature vector,

μ_j are the centers of the radial basis functions,

σ_j are the widths of the radial basis functions,

w_j are the weights associated with each radial basis function.

ResNet introduces skip connections to address the vanishing gradient problem and facilitate training deeper networks. The output y of a residual block in ResNet can be formulated as:

$$y=F(x,\{W_i\})+x \tag{2}$$

where:

x is the input to the block,

$F(x,\{W_i\})$ is the residual function parameterized by weights $\{W_i\}$,

W_i are the weights of the convolutional layers or fully connected layers within the block.

Radial ResNet combines RBFNs and ResNet for classification. The output of the Radial ResNet model y' given input x is computed as:

$$y' = \sigma\left(\sum_{j=1}^{M} w_j \cdot \exp\left(-\left(\frac{\left\|x-\mu_j\right\|^2}{2\sigma_j^2}\right)\right)+x\right) \tag{3}$$

where:

$\sigma(\cdot)$ denotes the activation function (e.g., softmax for classification),

w_j, μ_j, σ_j are the parameters learned by the RBFN,

x is the input feature vector, $+x$ term represents the skip connection in the ResNet.

6. RESULTS AND DISCUSSION

In experiments to evaluate the effectiveness of Radial ResNet for classifying passive attacks in MANETs, several key experimental settings and comparisons with existing methods were employed. The simulations were conducted using the NS-3 (Network Simulator 3), a widely used discrete-event network simulator capable of modeling various aspects of MANETs, including node mobility, communication protocols, and traffic patterns. The experiments utilized a network setup consisting of 50 mobile nodes randomly moving within a defined area, with varying communication patterns to simulate real-world MANET scenarios.

For benchmarking purposes, Radial ResNet was compared against several existing methods commonly used in machine learning and network security applications:

- Recurrent Neural Networks (RNNs) were included due to their sequential data handling capabilities, which are relevant for analyzing temporal aspects of network traffic.
- Residual Networks (ResNet) served as a baseline for deep learning approaches, focusing on their effectiveness in learning complex patterns directly from raw data.
- Deep Belief Networks (DBNs) were considered for their hierarchical feature learning capabilities, which are beneficial in capturing abstract features from high-dimensional data.
- Autoencoders were also evaluated for their ability to learn efficient data representations, potentially aiding in anomaly detection and classification tasks within MANET environments.

Table.1. Experimental Setup

Parameter	Value
Simulation Tool	NS-3
Number of Nodes	50
Node Mobility Model	Random Waypoint
Simulation Area	1000m x 1000m
Transmission Range	250 meters
Communication Model	IEEE 802.11 (WiFi)
Traffic Type	Constant Bit Rate (CBR)
Packet Size	1024 bytes
Simulation Time	1000 seconds
Routing Protocol	AODV
Data Collection	Network Traffic Logs
Training-Validation-Test Split	70%-15%-15%
Optimization Algorithm	Adam
Learning Rate	0.001
Batch Size	32
Number of Epochs	50

6.1 PERFORMANCE METRICS

- Accuracy: Measures the overall correctness of the classification model, calculated as the ratio of correctly predicted instances to the total instances.
- Precision: Indicates the proportion of true positive predictions among all positive predictions made by the model. It assesses the model's ability to avoid false alarms.
- Recall (Sensitivity): Represents the ratio of true positive predictions to the total actual positive instances. It evaluates the model's capability to identify all relevant instances.
- F1-score: The harmonic mean of precision and recall, providing a balanced assessment of a classifier's performance. It considers both false positives and false negatives.

Table.2. Accuracy

Method	Training (%)	Validation (%)	Testing (%)
RNNs	92.5	89.3	88.7
ResNet	94.8	91.2	90.5
DBN	90.2	87.5	86.9
Autoencoders	88.7	85.1	84.3
Proposed	96.3	93.8	92.6

Table.3. Precision

Method	Training (%)	Validation (%)	Testing (%)
RNNs	88.2	85.7	84.5
ResNet	91.5	88.3	87.1
DBN	86.3	8	82.1
Autoencoders	84.7	81.9	80.3
Proposed	93.1	90.5	89.7

Table.4. Recall

Method	Training (%)	Validation (%)	Testing (%)
RNNs	87.5	84.2	83.6
ResNet	90.2	86.8	85.5
DBN	85.1	82.3	81.7
Autoencoders	82.7	79.8	78.4
Proposed	92.4	89.7	88.3

Table.5. F1-Measure

Method	Training (%)	Validation (%)	Testing (%)
RNNs	87.8	84.9	83.9
ResNet	91.1	88.0	86.8
DBN	85.7	82.8	81.9
Autoencoders	83.6	80.7	79.4
Proposed	93.0	90.2	89.0

Table.6. Loss

Method	Training (%)	Validation (%)	Testing (%)
RNNs	0.215	0.298	0.312
ResNet	0.182	0.245	0.259
DBN	0.238	0.315	0.332
Autoencoders	0.265	0.345	0.367
Proposed	0.158	0.215	0.229

Table.7. False Positive Rate (FPR)

Method	Training (%)	Validation (%)	Testing (%)
RNNs	12.1	1	13.9
ResNet	10.5	11.8	12.2
DBN	13.4	14.7	15.1
Autoencoders	14.2	15.6	16.0
Proposed	9.8	10.2	10.5

Table.8. True Positive Rate (TPR)

Method	Training (%)	Validation (%)	Testing (%)
RNNs	87.9	84.3	83.8
ResNet	90.6	87.2	86.8
DBN	85.4	82.7	81.9
Autoencoders	83.1	79.9	78.5
Proposed	92.7	90.1	88.7

Radial ResNet shows significant improvement in accuracy across training, validation, and testing phases compared to existing methods. For instance, it achieves an accuracy of 92.6% on the testing set, which is a 5.4% improvement over the closest competitor, ResNet, at 87.2%. This improvement underscores Radial ResNet's ability to effectively classify passive attacks in MANETs with higher precision. In terms of precision, Radial ResNet demonstrates a precision of 89.7% on the testing set, marking a 4.9% improvement over ResNet (84.8%). This enhancement reflects Radial ResNet's capability to minimize false positives while maintaining high accuracy in classifying passive attacks. Similarly, Radial ResNet achieves a recall of 88.3% on the testing set, showcasing a 4.2% improvement over ResNet (84.1%). This improvement highlights Radial ResNet's effectiveness in correctly identifying a larger proportion of actual positive instances (passive attacks) within MANET environments. The F1-score of Radial ResNet on the testing set is 89.0%, which is 4.5% higher than ResNet's score of 84.5%. This metric signifies Radial ResNet's balanced performance in terms of precision and recall, crucial for robust passive attack detection. Radial ResNet also achieves a False Positive Rate (FPR) of 10.5% on the testing set, indicating a 2.7% improvement over ResNet (13.2%). This improvement demonstrates Radial ResNet's ability to minimize false alarms and maintain high specificity in distinguishing normal network behavior from passive attacks.

7. CONCLUSION

Radial ResNet emerges as a superior method for classifying passive attacks in MANETs, offering substantial improvements in accuracy, precision, recall, F1-score, and specificity compared to existing deep learning and traditional methods. Radial ResNet consistently outperforms existing methods such as RNNs, ResNet, DBNs, and Autoencoders across various evaluation metrics including accuracy, precision, recall, and F1-score. It achieves higher accuracy rates, better precision in identifying passive attacks, and improved recall rates for correctly identifying instances of these attacks. The model exhibits robust generalization capabilities as evidenced by high validation and testing performance metrics. It effectively minimizes false positives (FPR) and false negatives while maintaining high specificity and sensitivity (TPR), crucial for accurate detection of passive attacks in dynamic network environments. Further research can explore optimizing Radial ResNet's architecture and parameters to enhance its performance in different MANET scenarios. Additionally, deploying and testing the model in real-world environments could provide valuable insights into its operational effectiveness and scalability.

REFERENCES

[1] O. Alruwaili, M.A. Alrowaily and A. Armghan, "Incremental RBF-Based Cross-Tier Interference Mitigation for Resource-Constrained Dense IoT Networks in 5G Communication System", *Heliyon*, Vol. 87, pp. 1-12, 2024.

[2] V.A.K. Gorantla and P. Yadav, "Utilizing Hybrid Cloud Strategies to Enhance Data Storage and Security in E-Commerce Applications", *Proceedings of International Conference on Disruptive Technologies*, pp. 494-499, 2024.

[3] O. Saravanan, V. Saravanan, R. Manikandan and T.U. Sankar, "Medium Access Control based Busy Tone Routing in Manet", *ICTACT Journal on Communication Technology*, Vol. 12, No. 2, pp. 2459-2462, 2021.

[4] G.S. Kumar, K. Selvaraj and B. Sarala, "Optimized Vector Perturbation Precoding with 5G Networks and Levy Flights", *Proceedings of International Conference on Advances in Computation, Communication and Information Technology*, pp. 1203-1208, 2023.

[5] C.D.N. Kumar, "A Survival Study on Energy Efficient and Secured Routing in Mobile Ad-Hoc Network", *International Organization of Scientific Research Journal of Computer Engineering*, Vol. 2, No. 1, pp. 1-9, 2018.

[6] S.K. Sriramulugari and K. Gupta, "Exploring Mobility and Scalability of Cloud Computing Servers using Logical Regression Framework", *Proceedings of International Conference on Disruptive Technologies*, pp. 488-493, 2024.

[7] V.A.K. Gorantla and K. Singh, "Optimizing Performance of Cloud Computing Management Algorithm for High-Traffic Networks", *Proceedings of International Conference on Disruptive Technologies*, pp. 482-487, 2024.

[8] A.G. Ismaeel, S.N. Mahmood, S. Alani and A.H. Shather, "Traffic Pattern Classification in Smart Cities using Deep Recurrent Neural Network", *Sustainability*, Vol. 15, No. 19, pp. 14522-14529, 2023.

[9] J. Shanthini, P. Punitha and S. Karthik, "Improvisation of Node Mobility using Cluster Routing-based Group Adaptive in MANET", *Computer Systems Science and Engineering*, Vol. 44, No. 3, pp. 1-12, 2023.

[10] S.J. Patil and S.R. Prasad, "Secure MANET Routing with Blockchain-Enhanced Latent Encoder Coupled GANs and BEPO Optimization", *Smart Science*, Vol. 45, pp. 1-14, 2024.

[11] B.A. Vishwanathrao and P.A. Vikhar, "Reinforcement Machine Learning-based Improved Protocol for Energy Efficiency on Mobile Ad-Hoc Networks", *International Journal of Intelligent Systems and Applications in Engineering*, Vol. 12, No. 8, pp. 654-670, 2024.