JOURNAL OF INTERNATIONAL CRISIS AND RISK COMMUNICATION RESEARCH
ISSN: 2576-0017
2024, VOL 7, NO S12

Detection of Intrusive Attacks in Mobile Ad-hoc Networks based on ConvNext Model

Amruth Veerabhadraiah[1]*, Devaraj Verma Chitragar[2]

1. Department of Information science and Engineering, Maharaja Institute of Technology Mysore, India and Jain(Deemed to be University), Bengaluru, India
2. Department of CSE (AI), Jain(Deemed to be University), Bengaluru, India

* Corresponding author's Email: amruthv_ise@mitmysore.in

Abstract: A Mobile Ad Hoc Network (MANET) is composed of multiple mobile nodes that operate without a fixed infrastructure, and the random mobility of nodes leads to changes in the network topology. However, the dynamic nature of MANET and intrusive attacks are major problems in MANET leading to loss the critical information. To overcome these limitations, a Deep Learning (DL) model ConvNext is proposed which is an improved version of the residual network incorporating transformer elements to detect intrusive attacks in MANET. The proposed ConvNext's deep architecture allows it to handle large-scale MANETs with complex attack patterns and adapt to different network topologies and traffic conditions, making it suitable for the dynamic nature of MANETs. Initially, the data are obtained by simulation in NS-3 and acquired from the KDD'99 cup dataset for comparison results. Then, these data are converted into numerical values by label encoding. Finally, the intrusive attacks in the MANET are detected and classified based on the attacks accurately. The experimental results of the proposed method achieved an accuracy of 99.5% for simulated data and 0.991 for the KDD'99 cup dataset which is higher than existing approaches such as Hybrid Adaboost-Random Forest (HARF) and Fuzzy Extreme Learning Machine (FELM).

Keywords: ConvNext model, Deep Learning, Hybrid Adaboost-Random Forest, Label Encoding, Mobile Ad-hoc Network, Residual network.

1. Introduction

An ad hoc mobile system is a self-grouping arrangement of wireless-connected mobile devices that are not in the permanent infrastructure due to dynamic changes in the environment. In a Mobile Ad-hoc NETwork (MANET), each node acts as a router to transmit the packet from the source node to the destination node [1-3]. The MANET involves an active tradition for utilizing the self-configuring mobile strategies or nodes, which are interconnected in a straight path, with every other device without a static setup [4,5]. Therefore, MANET nodes accomplish both host and router tasks to improve packet transmission to the destination based on routing practice [6-8]. The MANET is an economically feasible media for communication that applies to many applications [9,10]. In this network, each node has a limited range that is used for transmitting or receiving packets [11-13]. In MANET, many protocols provide better security, however, it is challenging to handle security in wireless networks because of the heterogeneity of devices that are networked together [14]. The MANET are susceptible to numerous attacks such as wormholes, black holes, sink holes, gray holes, and Denial of Services (DOS) that lead to the risk of losing information, hence these risks are crucial to identify at an early stage for providing suitable measures [15]. To overcome these limitations a ConvNext modelis proposed for detection of intrusive attacks in MANET. The main contributions of this research are:

- The label encoding method is utilized to convert the categorical data into numerical values and make it suitable for input into DL models. This is crucial for attack types in MANETs, which are often categorical, such as wormhole, blackhole, and grayhole attacks.
- The proposed ConvNext model is an improved version residual network and incorporates elements from the Transformer, leading to improved accuracy in detecting and classifying network intrusions.
- The ConvNext model accurately identifies the various subtle intrusion patterns results in higher detection rates of intrusive attacks in MANETs and improves network security by reducing vulnerabilities.

This research paper is structured as follows: Section 2 discusses the literature review. Section 3 describes the proposed methodology. The results and discussion are illustrated in Section 4. The conclusion of this paper is given in Section 5.

2. Literature review

The advantages and limitations of existing ML detection approaches in detecting intrusive attacks like wormhole, black holes, and gray holes in MANET are discussed below:

Vincent and Duraipandian [16] designed a Hybrid Adaboost-Random Forest (HARF) model for the detection of sinkhole attacks in MANETS. The designed HARF model was utilized to detect and prevent various types of intrusive attacks as well as to make an efficient routing protocol of MANET. The advantage of the HARF model was the Adaboost approach focused on the classification of instances, whereas random forest handles the diverse attack scenarios

effectively. However, the integration of two models in the designed HARF increased the delay in detecting the intrusive attacks.

Abdan and Seno [17] explored ML-based classification models for the detection of wormhole attacks in MANET. The explored various ML models were utilized for wormhole detection with simulated data consisting of normal nodes, malicious nodes and eight selected features. An advantage of the explored model has increased the effectiveness of detection performance by handling high dimensional data. However, the explored ML models face challenges in detecting the wormhole attack accurately due to the evolving nature of the attack pattern.

Singh and Vigilia [18] developed a Fuzzy Extreme Learning Machine (FELM) for the detection of attacks in MANET. The developed FELM model was employed to detect intrusive attacks based on the features extracted by the principal component analysis technique. The rapid learning capability of the developed FELM model enhanced the detection of attacks by adapting the dynamic nature of the environment effectively. However, the extracted features with irrelevant information led to degrade the developed FELM model's performance which mainly depends on the information utilized for detection.

Sathiya and Yuvaraj [19] presented an optimization-based probabilistic ELM model for the detection of attacks. The presented model integrated a Gudermannian activation with a binary swarm optimization model for effective feature selection to improve attack detection in MANET. An advantage of the presented ELM model with probabilistic nature allows one to make more nuanced decisions to improve the detection of attacks. However, the presented ELM model was sensitive to the choice of parameters that led to suboptimal results and directly impacted on detection performance.

Shukla [20] represented an ML model to detect black hole and gray hole attacks in MANET based on mutation-based Artificial Neural Network (MB-ANN). The represented model utilized a cluster-based ant bee colony optimization algorithm to increase network performance in hostile environments and enhance detection. The main advantage of the represented mutation-based learning strategy permits the ANN model to evolve and adapt quickly, reducing the transmission delay across nodes. However, the represented MB-ANN model with a random nature of mutation led to inconsistent performance at certain conditions.

Dr. S.B. Ninu [21] explored an intrusion detection system model based on Deep neuro Fuzzy Network (DNFN) method. The explored DNFN model with Exploring Henry Gas Solubility Optimization (EHGSO) algorithm was utilized to improve detection performance in MANET. The main advantage of the explored DNFN model was that instantly locates the intrusion and malicious nodes in the MAENT environment effectively. However, the explored DNFN model failed to adopt evolving nature of attacks that affect the accurate detection performance.

The above-mentioned detection approaches have limitations in detecting intrusive attacks in MANET such as dynamic network environment, inappropriate information about intrusive attacks, and changes in attack patterns. To overcome these limitations, a ConvNext model is proposed to detect intrusive attacks in MANET which is an improved version of ResNet architecture with transformer elements. The deep layers of ConvNext enhanced feature extraction with information about subtle differences and adapted the dynamic network and pattern of attacks effectively.

3. Methodology

The proposed framework for intrusive detection in MANET includes four stages: dataset acquisition, preprocessing, feature selection and proposed detection model. The flowchart of the proposed ConvMext model is illustrated in Fig. 1. Initially, the data used for detection are obtained from simulated and benchmark datasets. Secondly, the data are preprocessed by normalization technique and then features that are relevant for detection of intrusive attacks are extracted. Finally, the proposed ConvNext model is proposed to detect intrusive attacks such as blackhole, wormholes, gray holes and other malicious attacks in MANET.

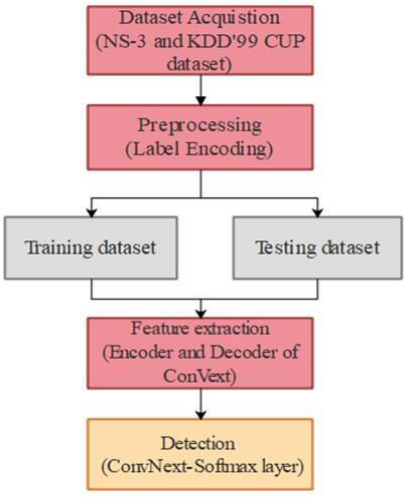

Figure. 1 The flowchart of the proposed ConvNext model

3.1 Dataset acquisition

In this research, simulated data and benchmark data are utilized to enhance the detection of intrusive attacks in MANET.

3.1.1. Simulation data

In this research, the data of blackhole and wormhole attacks are simulated by NS-3 simulation software. Some of the nodes from this data represent the attacks and data collection behaviour as a training set. Initially, the malicious and normal nodes are defined in the MANET environment. Then, the system collects *.pcap files at each node and transfers the data for the feature extraction and selection process by the proposed detection model. The selection of a set of features from the simulated data is a combination of basic and derived features. The simulation data was obtained from the system configuration of MATLAB 2022b in an ad hoc network environment with 48 regular nodes and two malicious nodes. Finally, simulated data and extracted features are stored in the database.

3.1.2. KDD'99 CUP dataset

The KDD'99 cup dataset is the most widely used dataset for the estimation of anomaly detection in wireless networks [22]. This dataset consists of relatively 4,900,000 single connection vectors each of which comprises 41 features. These features are used to categorize based on two classes normal and attack, with absolutely one definite type of attack and fall in one of the subsequent four classes. The DoS, Probe, Remote to Local (R2L) and User to Route (U2R) are the four different attack classes in the KDD'99 cup dataset.

3.1.3. NSL KDD dataset

The NSL-KDD [23] is the most widely used dataset for intrusion detection system. This dataset is publicly available dataset which is used to evaluate the proposed detection system in this research. The dataset includes normal network traffic data and four types of intrusions such as Denial of Services (DoS), U2R, R2L and Probe. These data are fed to the preprocessing phase for converting the categorical attack data into numerical form.

3.2 Preprocessing

The data obtained from the simulation network and KDD'99 cup dataset are then fed to the preprocessing phase to improve the data format. For preprocessing, the label encoding method (one-hot encoding and data normalization is utilized to transform string/categorical data into numerical data, and then all the numerical value is scaled into a uniform range individually. The hot encoding method is a kind of label encoding that is applied to convert the categorical data into numerical values and make it equal range and suitable format for input into DL models. This is crucial for attack types in MANETs, which are often categorical, such as wormhole, black hole, sink hole and gray hole attacks.

After encoding into numerical values, the normalization technique is used to adjust values to a common scale without changing differences in ranges of values. The min-max normalization technique is utilized to normalize the data into a range of [0,1]. The mathematical representation of the normalization technique is expressed in Eq. (1) and Eq. (2).

$$r' = \frac{r - r_{min}}{r_{max} - r_{min}} \qquad (1)$$

$$r_{max} = max\{r\} \qquad (2)$$

Where, r_{min} and r_{max} represents minimum and maximum eigenvalues; r and r' denotes original and normalized eigenvalue. These preprocess numerical data are fed to the proposed intrusive attack detection model.

3.3 Problem definition

The routing interruption attacks impact on selection of routes and data transmission process in MANET. Malicious nodes can pass in a wireless network easily and attract routing packets during route creation by false data. The attacker nodes are dynamic and primarily change the sequence number, and hop count, and transmit the acknowledgement packets. The MANET consists of a source and Destination node with several normal nodes which are used for transmission of data [22]. The intrusive attacks by malicious nodes in MANET are categorized into four types of Wormhole, Black hole, Gray hole, Sink hole attacks and other malicious attacks such as DoS, Probe, R2L and U2R. The attack behaviour of wormhole and black hole attacks in MANET is represented in Fig. 2 and Fig. 3. The malicious node receives data packets from neighbour nodes and sends false acknowledgement packets, which also create a tunnel where data packets through which data packets enter and exit.

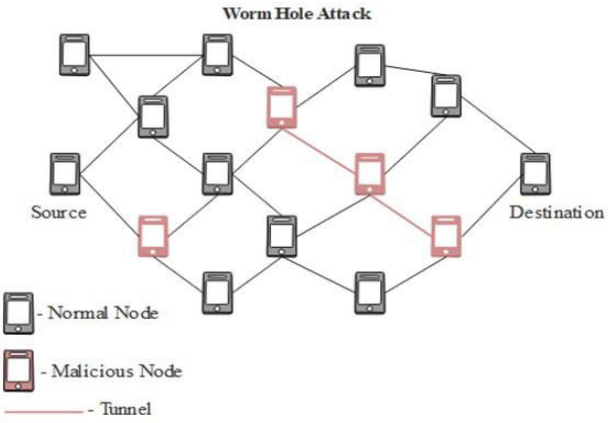

Figure. 2 Wormhole Attack

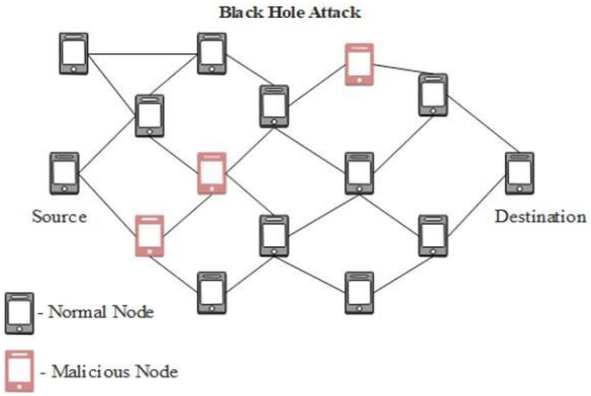

Figure. 3 Black Hole Attack

3.4 Proposed ConvNext

The acquired data is fed to the proposed intrusive attack detection model to identify the malicious behaviour in MANET. ConvNext is a type of convolutional neural network which is an improvised version of a Residual Network (ResNet) which incorporates the elements of transformers to enhance the intrusive attack detection process. The architecture of the proposed ConvNext model is represented in Fig. 4. Based on the design limits and spaces that the proposed network reached depends only on convolutional network modules. The proposed ConvNext model is classified into two main blocks encoder and decoder for accurate detection of intrusive attacks in MANET. The deep architecture with several convolutional layers in ConvNext leads to precise detection of subtle anomalies which was one of the drawbacks of existing intrusion detection systems. As a result, there is a substantial reduction in false positives and false negatives, that improve overall network security.

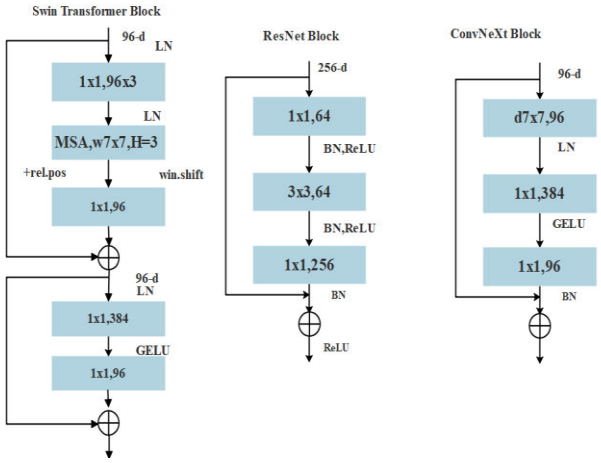

Figure. 4 Architecture of ConvNext Model

3.4.1. Encoder

The main steps in detection using ConvNext encoder block are described in the following way:

1. The initial step involves adjusting the distribution of computations across different stages of the model. This is accomplished by altering the number of blocks assigned to every phase in a multi-stage design. The feature map dynamically alters the resolution according to stage, depending on the hierarchical structure of the network.
2. Instead of the traditional ResNet stem, a 4×4 non-overlapping convolution layer known as the patchify stem is employed. This approach draws inspiration from patchify layer used in hierarchical transformers, which creates more compact feature representations. By processing the input as patches, ConvNeXt extracts more meaningful and localized features from network data. This enhances the ability to detect distributed attacks, such as blackhole, wormhole attacks, etc., which are difficult to detect by traditional fully-connected methods. This patchify Stem helps to focus on specific regions of network data, by detecting subtle attack patterns effectively.
3. A depth-wise convolution is adopted for feature extraction which is a form of grouped convolution layers. This operation mirrors the channel-wise attention mechanism in self-attention models by applying convolutions independently for each channel, mixing information along the spatial dimension. Paired with a subsequent 1×1 convolution, this setup enables separate handling of spatial and channel dimensions, which is a key architectural principle of transformers.
4. An inverted bottleneck is implemented, following a design pattern commonly found in hierarchical transformers. The Multi-head Self-Attention (MSA) precedes the MLP layers in the transformers by a large kernel (e.g., 7×7) which is positioned before the 1×1 dense convolution. This ordering enhances the model's capacity for capturing spatial dependencies before channel mixing.The mathematical representation of output obtained by the MSA layer in encoder which concatenates all heads is represented in eq. (3) and (4):

$$head_i = Attention\left(QW_i^Q, KW_i^K, KW_i^K\right) \quad (3)$$

$$MultiHead(Q,K,V) = Concat\ (head_1, \dots, head_h)W^oW^o \in \mathbb{R}^{hd_v \times d_{model}} \quad (4)$$

Where, Q, K and V represents query, key and vector; $head_i$ denotes output of head for i head in attention; h indicates number of heads.

5. The Rectified Linear Unit (ReLU) activation function in the ConvNext is replaced with the Gaussian Error Linear Unit (GELU), which is widely used in transformer models due to its smoother and more consistent gradient flow. Additionally, the number of activations per block in the network is reduced to one. The batch Normalization layer (BN) is replaced with Layer Normalization (LN), which reflects the practices of transformer-based models. The number of normalization layers per block in the ConvNext is also reduced to one, which simplifies the architecture.

3.4.2. Decoder

The decoder incorporates two kinds of skip connections to effectively collect data from the encoder:

1. The skip connections provide direct access for the decoder to obtain outputs of residual blocks at each phase of the encoder. This allows for a seamless flow of detailed information across stages, preserving crucial features during the decoding process.
2. These connections link the decoder to the outputs of down-sampling layers, with the patchify stem. This facilitates the flow of lower-level spatial information into the decoder, complementing the residual skip connections and helping maintain symmetry between the encoder and decoder.

Both types of skip connections ensure the integration of encoder feature maps into the decoder, balancing low to high-dimensional transitions during the reconstruction process. In parallel to ConvNext-Base encoder design, the decoder also employs divide upsampling layers at starting of every decoder phase. These layers are critical to incorporate information coming from the skip connections into the decoder's reconstruction process. At each stage, the decoder uses a combination of upsampling layers and de-convolution blocks. Each decoder phase has a certain number of de-convolution blocks corresponding to the number of encoder stages. Each block receives two inputs: The first input comes from a skip connection that transfers encoder representations. The second input comes either from the output of the prior de-convolution block or directly from a distinct upsampling layer, depending on the block's position in the stage.

The inputs are integrated by element-wise summation, which results in mixing spatial data from both the encoder and decoder. After combining the inputs, a 1×1 de-convolution layer with stride 1 is employed in the network. The number of kernels in this layer equals to number of channels in added inputs. The dimensions remain consistent because of element-wise summation which is followed by the de-convolution step, then the output is normalized by a layer normalization. Lastly, the activation function is used to produce the final output of the de-convolution block.

At the end of the decoder, a 4×4 de-convolution layer with stride 4 is added. This layer uses 3 kernels, and its output is passed through a sigmoid activation function employed element-wise to generate the final output. An input to this layer comes from a feature vector produced by the ConvNext encoder. At last, a Softmax function is applied elementwise in ConvNext, which yields the overall detection output obtained from the network in MANET. At last, the Softmax layer in

ConvNeXt outputs a probability distribution over the classes to detect various types of intrusion attacks in a MANET effectively.The ensemble output from vision transformer and Convext is represented in eq. (5):

$$S_f = \alpha S_v + (1-\alpha)S_c \quad (5)$$

Where, S_v and S_c represent the classification scores from transformaer and ConvNext respectively. This incorporation of transformer in the ConvNext model improved the learning of attack patterns effectively that enhanced the detection of intrusive attacks in MANET precisely.

4. Results and discussion

The performance proposed ConvNext method-based detection of intrusive attacks in MANET is evaluated by different performance metrics. In this research, the proposed ConvNext model is simulated using MATLAB R2020b with a system configuration of i7 processor, 16 GB RAM and Windows 10 OS. Performance measures used for evaluation are Accuracy, Precision, Recall/ Sensitivity and Specificity. The mathematical expression of performance metrics are represented in Eqs. (6) to (9).

$$Accuracy = \frac{TP+TN}{TN+TP+FN+FP} \times 100 \quad (6)$$

$$Precision = \frac{TP}{TP+FP} \quad (7)$$

$$Sensitivity = \frac{TP}{TP+FN} \quad (8)$$

$$Specificity = \frac{TN}{TN+FN} \quad (9)$$

Where, TN is True Negative, FN is False Negative, TP is True Positive, and FP is False Positive respectively.

4.1 Quantitative and qualitative analysis

The quantitative and qualitative analysis of proposed ConvNext method utilizing simulated dataset (NS3) is represented in Table 5. Performance metrics such as accuracy, precision, recall/sensitivity and specificity are used for performance evaluation of proposed method is represented in this section.

The performance analysis of the proposed ConvNext method-based detection of intrusive attacks in MANET is illustrated in Table 1. The proposed ConvNext algorithm is evaluated and compared with existing optimization algorithms like Support Vector Machine (SVM), Random Forest (RF), ANN, and CNN. The ConvNext attains an accuracy of 98.8%. 98.8%, 98.5%, 98.3% for the wormhole, black holes, sink hole, and gray hole respectively.

Table 1. Performance analysis of the proposed method for Accuracy (%)

Methods	**Attacks**			
	Worm hole	**Black hole**	**Gray hole**	**Sink hole**
SVM	97.1	94.2	93.8	92.4
RF	94.6	95.7	97.2	97.8
ANN	96.4	98.2	91.8	92.3
CNN	97.9	97.6	96.4	95.2
Proposed ConvNext method	98.8	98.8	98.5	98.3

The ConvNext deep layers extract hierarchical features that help to detect subtle patterns associated with various types of attacks effectively. This helps the model to differentiate between normal and intrusive behaviour to achieve higher accuracy than existing approaches.

The quantitative results of the proposed ConvNext method in terms of precision for the detection of various intrusive attacks in MANET are illustrated in Table 2. The proposed ConvNext algorithm is evaluated and compared with existing optimization algorithms such as SVM, RF, ANN, and CNN. The ConvNext attains precision of 99.4%, 98.3%, and 98.2%, for wormholes, black holes, sink holes, and gray holes respectively. The layer normalization and enhanced residual connections ensure a stable gradient flow that reduces the false positives and results in precise intrusive attacks.

Table 2. Performance analysis of the proposed method for Precision (%)

Methods	**Attacks**			
	Worm hole	**Black hole**	**Gray hole**	**Sink hole**
SVM	94.2	92.9	95.7	91.3
RF	96.4	93.1	94.9	95.6
ANN	97.7	96.5	96.9	96.7
CNN	97.6	98.3	97.7	97.4
Proposed ConvNext method	98.4	98.3	98.2	97.9

The quantitative results of Sensitivity achieved in the detection of various attacks in MANET are illustrated in Table 3. The proposed ConvNext algorithm is evaluated and compared with existing optimization algorithms such as SVM, RF, ANN, and CNN. The ConvNext attains sensitivity of 97.9%, 97.3%, 93.4%, and 92.7% for wormhole, black hole, sink hole, and gray hole respectively. The larger receptive fields in ConvNext help in the detection of the smallest anomalies in the traffic which leads to attaining high sensitivity compared to existing detection methods.

Table 3. Performance analysis of the proposed method for Recall/ Sensitivity (%)

Methods	**Attacks**			
	Worm hole	**Black hole**	**Gray hole**	**Sink hole**
SVM	93.2	91.9	82.7	86.3
RF	92.4	83.1	75.9	84.6
ANN	96.8	82.5	84.9	79.7
CNN	95.6	92.3	95.7	91.4
Proposed ConvNext method	97.9	97.3	93.4	92.7

The quantitative results of Specificity achieved in the detection of various attacks in MANET are illustrated in Table 4. The proposed ConvNextalgorithm is evaluated and compared with existing optimization algorithms such as SVM, RF, ANN, and CNN.

Table 4. Performance analysis of the proposed method for Specificity (%)

Methods	**Attacks**			
	Worm hole	**Black hole**	**Gray hole**	**Sink hole**
SVM	91.2	91.9	90.7	89.3
RF	93.4	82.1	89.9	74.6
ANN	92.8	78.5	82.9	76.7
CNN	95.6	81.3	79.7	72.4
Proposed ConvNext method	97.7	97.2	96.8	95.7

The ConvNext attains specificity of 97.7%, 97.2%, 96.8%, 95.7% for the wormhole, black hole, sink hole, and gray hole respectively. The proposed ConvNext model focuses more on relevant features which represents more information about the intrusive attack behaviour that led to increased specificity of the proposed model than the existing detection method.

4.2 Comparative Analysis

The comparative analysis of the proposed method with existing detection techniques utilizing KDD'99 Cup dataset are illustrated in this section. The existing intrusive attack detection methodslikeFELM [18] and PELM [19]which utilizing KDD cup datasetare used for comparative analysis for the proposed method.The comparative analysis of the proposed method with existing detection methods utilizing the KDD'99 Cup dataset such as FELM [18] and PELM [19] in MANET is illustrated in Table 5. The performance metrics used for comparative analysis are accuracy, precision, recall/sensitivity and specificity.

The comparative analysis of the proposed method with existing detection methods utilizing the NSL-KDD dataset such DNFN [21] in MANET is illustrated in Table 5. The performance metrics used for comparative analysis are accuracy, precision, recall/sensitivity and specificity.

Table 5. Comparative analysis of the proposed method

Methods	**Dataset**	**Accuracy**	**Precision**	**Recall/ Sensitivity**
FELM [18]	KDD'99 Cup dataset	0.990	0.920	0.941
PELM [19]		0.900	0.920	0.960
Proposed ConvNext method		0.991	0.972	0.974
DNFN [22]	NSL-KDD dataset	N/A	0.921	0.908
Proposed ConvNext method		0.993	0.986	0.974

The proposed ConvNext model attains accuracy of 0.991 and 0.993 for KDD'99 Cup dataset and NSL-KDD dataset which is higher than the existing detection models.

The features extracted by the encoder and decoder of the proposed ConvNext model indicate the malicious activities and abnormal activities in the network effectively lead to the accurate detection of attacks in MANET.The proposed ConvNext adapts the evolving nature of MANET environment and learns the complex patterns of attacks efficiently that enhance the detection performance.

4.3 Discussion

The proposed ConvNext model achieved better results by detecting intrusive attacks in MANET. The existing approaches have several limitations such as HARF [16] the integration of two models in designed HARF that increased delay in detecting the intrusive attacks. ML models [17] face a struggle to detect accurately the wormhole attack when it

is in a new pattern or sophisticated manner. FELM [18] depends on the quality of features utilized for detection, the extracted features with irrelevant information led to degrade the model's performance. Probabilistic ELM [19] is sensitive to the choice of parameters that lead to suboptimal results and directly impact on detection performance. MB-ANN [20] model with a random nature of mutation that led to inconsistent performance at certain conditions. To overcome these limitations, a ConvNext is proposed for detecting intrusive attacks in MANETs effectively. The hierarchical representation layers of ConvNext allow for capturing both low-level features such as packet size, and routing information and high-level features such as network traffic patterns, and delay variations. These features indicate the malicious activities and abnormal activities in the network effectively lead to the accurate detection of attacks in MANET.

5. Conclusion

The ConvNext DL model is proposed which is an improved version of the residual network to detect intrusive attacks in MANET. ConvNext's deep architecture handles large-scale MANETs with complex attack patterns and adapts to different network topologies and traffic conditions, making it suitable for the dynamic nature of MANETs. The proposed Convnext model incorporated with transformer-based encoder with MSA mechanism extracts the features with significant information about traffic data that helps to improve accurate intrusion detection performance in MANET. The simulated data are pre-processed by a One-hot encoding technique to convert categorical data into a numerical form that allows ConvNext to efficiently differentiate between normal traffic and multiple intrusion types, and reduce the chances of misclassifying attacks. The advanced architecture of the proposed ConvNext's model adapts to dynamic environments and detects intrusive attacks effectively even when the network structure changes frequently. The experimental results of the proposed method achieved an accuracy of 99.5% for simulated data and 0.991 for the KDD'99 cup dataset and 0.993 for NSK-KDD dataset. which is higher than existing approaches such as HARF and FELM. In future, advanced DL methods with optimization algorithms will be implemented to enhance the detection of intrusive attacks in MANET.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

The paper conceptualization, methodology, software, validation, formal analysis, investigation, resources, data curation, writing—original draft preparation, writing—review and editing, visualization, have been done by 1st author. The supervision and project administration, have been done by 2nd author.

References

[1] R. Vatambeti, S.V. Mantena, K.V.D. Kiran, S. Chennupalli, and M.V. Gopalachari, "Black hole attack detection using Dolphin Echo-location-based machine learning model in MANET environment", *Computers and Electrical Engineering*, Vol. 114, p. 109094, 2024.

[2] R. Reka, R. Karthick, R.S. Ram, and G. Singh, "Multi head self-attention gated graph convolutional network based multi-attack intrusion detection in MANET", *Computers & Security*, Vol. 136, p.103526, 2024.

[3] P. Rani, Kavita, S. Verma, D.B. Rawat, and S. Dash, "Mitigation of black hole attacks using firefly and artificial neural network", *Neural Computing and Applications*, Vol. 34, No. 18, pp.15101-15111, 2022.

[4] V. Mankotia, R.K. Sunkaria, and S. Gurung, "AFA: Anti-flooding attack scheme against flooding attack in MANET", *Wireless Personal Communications*, Vol. 130, No. 2, pp.1161-1190, 2023.

[5] N. Veeraiah, and B.T. Krishna, "An approach for optimal-secure multi-path routing and intrusion detection in MANET", *Evolutionary Intelligence*, Vol. 15, No. 2, pp. 1313-1327, 2022.

[6] S. Dilipkumar, and M. Durairaj, "Epilson Swarm Optimized Cluster Gradient and deep belief classifier for multi-attack intrusion detection in MANET", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 14, No. 3, pp.1445-1460, 2023.

[7] N. Sivanesan, A. Rajesh, S. Anitha, and K.S. Archana, "Detecting distributed denial of service (DDoS) in MANET using Ad Hoc on-demand distance vector (AODV) with extra tree classifier (ETC)", *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, Vol. 48, No. 2, pp.645-659, 2024.

[8] V. Mankotia, R.K. Sunkaria, and S. Gurung, "DT-AODV: A dynamic threshold protocol against black-hole attack in MANET", *Sādhanā*, Vol. 48, No. 4, p.190, 2023.

[9] S. Kaushik, K. Tripathi, R. Gupta, and P. Mahajan, "Enhancing reliability in mobile ad hoc networks (MANETs) through the K-AOMDV routing protocol to mitigate black hole attacks", *SN Computer Science*, Vol. 5, No. 2, p.263, 2024.

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

[11] A.M. Eltahlawy, H.K. Aslan, M.S. Elsayed, A.D. Jurcut, and M.A. Azer, "Detection of sequence number attacks using enhanced AODV protocol in MANETs", *Computers and Electrical Engineering*, Vol. 118, p.109395, 2024.

[12] S. Singh, and H.S. Saini, "Intelligent ad-hoc-on demand multipath distance vector for wormhole attack in clustered WSN", *Wireless Personal Communications*, Vol. 122, No. 2, pp.1305-1327, 2022.

[13] D. Hemanand, N.S. Ram, and D.S. Jayalakshmi, "FSSAM: A Five Stage Security Analysis Model for Detecting and Preventing Wormhole Attack in Mobile Ad-Hoc Networks Using Adaptive Atom Search Algorithm", *Wireless Personal Communications*, Vol. 128, No. 1, pp.487-506, 2023.

[14] I. Baird, I. Wadhaj, B.Ghaleb, and C. Thomson, "Impact Analysis of Security Attacks on Mobile Ad Hoc Networks (MANETs)", *Electronics*, Vol. 13, No. 16, p.3314, 2024.

[15] A. Abdelhamid, M.S.Elsayed, A.D.Jurcut, and M.A. Azer, "A lightweight anomaly detection system for black hole attack", *Electronics*, Vol. 12, No. 6, p.1294, 2023.

[16] S.S.M. Vincent, and N. Duraipandian, "Detection and prevention of sinkhole attacks in MANETS based routing protocol using hybrid AdaBoost-Random forest algorithm", *Expert Systems with Applications*, Vol. 249, Part C, p.123765, 2024.

[17] M. Abdan, and S.A.H. Seno, "Machine learning methods for intrusive detection of wormhole attack in mobile ad hoc network (MANET)", *Wireless Communications and Mobile Computing*, Vol. 2022, No. 1, p.2375702, 2022.

[18] C.E. Singh, and S.M.C. Vigila, "Fuzzy based intrusion detection system in MANET", *Measurement: Sensors*, Vol. 26, p.100578, 2023.

[19] R. Sathiya, and N. Yuvaraj, "Swarm Optimized Differential Evolution and Probabilistic Extreme Learning based Intrusion Detection in MANET", *Computers & Security*, Vol. 144, p.103970, 2024.

[20] M. Shukla, B.K. Joshi, and U. Singh, "A Novel Machine Learning Algorithm for MANET Attack: Black Hole and Gray Hole", *Wireless Personal Communications*, Vol. 138, No. 1, pp. 41-66, 2024.

[21] Ninu, S.B., 2023. An intrusion detection system using exponential Henry gas solubility optimization based deep neuro fuzzy network in MANET. *Engineering Applications of Artificial Intelligence*, *123*, p.105969.

[22] Kdd'99 CUP Dataset: https://www.kaggle.com/datasets/galaxyh/kdd-cup-1999-data (Accessed on August 2024).

[23] NSL-KDD dataset: https://www.kaggle.com/datasets/hassan06/nslkdd (Accessed on October 2024)

[24] M. Prasad, S. Tripathi, and K. Dahal, "An enhanced detection system against routing attacks in mobile ad-hoc network", *Wireless Networks*, Vol. 28, No. 4, pp.1411-1428, 2022.