Securing the MANET by Detecting the Flooding Attacks Using Hybrid CNN-Bi-LSTM-RF Model

B. Deena Divya Nayomi[1], L. Venkata Jayanth[2(✉)], A. Vinay[1,2], P. Subba Rao[1,2], and L. Shashi Vardhan[1,2]

[1] Department of CSE, G. Pullaiah College of Engineering and Technology, Kurnool, India
deena.divya20@gmail.com, subbaraopelluri23@gmail.com
[2] G. Pullaiah College of Engineering and Technology, Kurnool, India
jayanthpranay890@gmail.com

Abstract. Security in Mobile Ad Hoc Networks (MANETs) is complicated by attacks such request route flooding, which are simple to launch but hard to defend against. An attack can be launched by a rogue node by delivering a flood of route request (RREQ) packets or other worthless data packets to non-existent destinations. As the network's resources have been exhausted trying to handle this deluge of RREQ packets, it has been rendered incapable of performing its usual routing function. The majority of the available literature on identifying such a flooding assault use a threshold based on the rate of RREQ generation attributable to a certain node. These algorithms are effective to a point, but they have a high misdetection rate and hinder the efficiency of the network. Using a (CNN), a Bidirectional Long Short and the (RF) for classification, this study suggests a novel technique for detecting flooding threats. The method uses each node's route discovery history to recognise shared traits and routines among members of the same class, allowing it to determine whether or not a given node is malicious. The effectiveness of the projected method is measured by associating the results of NS2 simulations run under normal and RREQ attack scenarios with respect to attack detection rate, packet delivery rate, and routing load. Simulation findings demonstrate that the proposed model can identify over 99% of RREQ flooding assaults across all scenarios with route discovery, and outperforms state-of-the-art methods for RREQ flooding attacks in terms of packet delivery ratio and routing burden.

Keywords: Route request · Mobile Ad Hoc Networks · Flooding attack · Convolutional Neural Network · Random Forest

1 Introduction

A MANET is network that does not rely on a predetermined topology to facilitate communication activities. Temporary network formed by wireless nodes that rely on multi-hop communications since no underlying infrastructure is present [1]. Self-organization and decentralised control are hallmarks of MANETs, making it possible for individual

S. Kadry and R. Prasath (Eds.): MIKE 2023, LNAI 13924, pp. 148–160, 2023.
https://doi.org/10.1007/978-3-031-44084-7_15

nodes to work together to achieve the network's goals and ensure reliable communication. Issues with routing, security, access control, dependability, and power consumption are only some of MANET's difficulties [2]. To overcome these obstacles, a secure routing protocol is used in order to identify rogue nodes and isolate them from the communiqué network so that network performance may be improved. In MANETs, data announcement must be protected at all times. The majority of DoS attacks [3, 4] originate from security breaches caused by packet flooding on the network, which uses up more resources and leads to congestion. By using a trustworthy route, you may lessen the chances of interacting with malicious nodes. For MANETs to be a secure, low-infrastructure communication channel, trust management is essential [5]. The on-demand routing architecture employed by AODV relies heavily on routing protocols to determine which paths to take. Security parameters are included in the route reply packet and the discovery packet by changing them [6].

Without intermediary devices like routers or base stations, communication between MANET nodes is possible. Transmissions such as single-hop and multi-hop are used in MANETs to facilitate communication between mobile nodes via intermediary nodes that function as routers to transmit and relay messages [7, 8]. MANETs' instantaneous deployment and lack of need for a preexisting infrastructure make them a strong contender for use in a wide variety of contexts, including but not incomplete to: military and police communications; fire and rescue; inter-vehicle networks; emergency and disaster recovery; personal area networks; healthcare; and educational and medical settings. The cooperative and dispersed nature of a MANET's routing design makes it more susceptible to denial-of-service assaults [11]. DoS attacks are launched to stop their intended recipients from making use of the system's resources and, by extension, its services. Mobile nodes in MANETs are particularly vulnerable to intrusion, and once infiltrated, they may be used to achieve DoS assaults. (DoS) attacks occur when several nodes across a network all launch simultaneous DoS attacks. DDoS bouts are more hazardous and harder to counteract in real time [12].

There are two broad types of denial-of-service attack: vulnerabilities (in which a known flaw in the target process is exploited) and floods (in which a large number of service requests or fake traffic are generated). Hateful nodes will launch a large number of packets with route RREQ for IP addresses including destinations, draining the battery capabilities of intermediate nodes and increasing their energy consumption, in a flooding DoS attack [14]. In MANETs, the discovery of a route is often initiated packets containing the RREQ protocol; nevertheless, the flooding of such RREQ fake packets without any adherence for regulating rate in a network can have a profoundly degrading effect on system throughput [15].

The following are the most important results from this research.

Create an accurate attack-detection system using an ensemble CNN-BiLSTM-RF construction trained using ML and DL replicas.

Provide a module for data preprocessing that looks at the temporal features of the dataset.

To emphasise the importance of the proposed research, a comparison will be made between the suggested ensemble CNN-BiLSTM-RF construction and the more traditional learning and DL replicas.

The residue of the paper is organised as shadows: Sect. 2 summarises the relevant papers, and Sect. 3 provides a brief account of the suggested model. Sections 4 and 5 show the results of the validation analysis and draw a conclusion…

2 Related Works

Using security localization and an improved multilayer network, Gebremariam et al. [16] presented detection and localization against numerous assaults (MLPANN). The suggested approach detects and localises WSN DoS attacks using a combination of localization and machine learning techniques. Simulation in MATLAB is used to construct the suggested system, while the IBM SPSS toolbox and Python are used to handle the data. Using a multilayer perceptron artificial neural network, we can identify 10 different types of assaults, such as denial-of-service (DoS) attacks, by dividing the dataset into training and testing sets. Results from applying the proposed system to benchmark datasets show that it significantly outperforms the state-of-the-art with an average detection accuracy of 100%, 99.65%, for different types of DoS assaults, respectively. The proposed approach achieves better results than state-of-the-art alternatives in all measures of localization performance (accuracy, f-score, precision, and recall). Lastly, simulations are run to evaluate the security performance of the proposed strategy for identifying and pinpointing malicious nodes. This technique yields a low localization error approximation of the unknown node's position. The results of the simulations demonstrate the efficacy of the proposed system in detecting and securely localising malicious assaults in wireless sensor networks that are scalable and hierarchically distributed. With this method, we were able to reduce the worst-case localization error to 0.49 % and improve the average to 99.51 %.

A hybrid deep learning strategy, devised by Elubeyd and Yiltas-Kaplan et al. [17], integrates elements from three distinct deep learning algorithms. Both theoretical analysis and empirical testing showed that this method obtained very high accuracy (99.81% and 99.88%, respectively) on two separate datasets. Specifically for software-defined networks, this study represents a major advancement in the field of network security. DoS/DDoS attacks may be avoided and SDN security can be improved with the help of the suggested technique. Since SDNs play a key role in today's network architecture, safeguarding them from assaults is essential to preserving the reliability and accessibility of such resources. Overall, the work proves that a hybrid deep learning technique can effectively spot DoS/DDoS assaults in SDNs, and it points the way for further investigation into this topic.

Stacked auto-encoder based technique for MANET was presented by Meddeb et al. [18] to improve intrusion detection systems (Stacked AE-IDS) is a method for minimising correlation using neural networks in Machine Learning (ML). It employs numerous processing layers in an effort to model important aspects at a high level and to obtain a suitable representation feature from Data Correlation. When the input and output dimensions are the same, the Stacked AE-IDS approach attempts to recreate the input while minimising the correlation between the two. We suggest a two-stage process for implementing Deep Learning in IDS. Classification is performed using a Deep Neural

network (DNN) using the auto-output encoder's as training data (DNN-IDS). It leverages the most likely assaults to disrupt routing services in Mobile Network and zeroes down on DoS attacks within labelled datasets available for intrusion detection.

Tekleselassie et al. [19] provide a new way to project information about assaults on wireless networks onto a grid-like data structure, which can then be used to train the EfficientNet CNN model. Determine how the attribute values should be arranged in a matrix before it can be recorded as an image. The goal is to create an accurate and lightweight IDS module that can be implemented in IoT networks by merging the most significant subset of features with EfficientNet. Use the AWID dataset (which contains information on Wi-Fi assaults) to analyse the suggested model. Obtain a 99.91% F1 score of 0.11% for optimal performance. This indicates that the suggested model successfully leveraged the spatial information in tabular data to preserve detection correctness, and that its results were equivalent to those of previous statistical machine learning models. The false positive rate is kept at roughly 0.11 %. So, the suggested model was compared to three existing machine learning models, and it was shown to be competitive with their performance. Where it is assumed that the spatial info must be taken into account by mapping out the tabular data on a grid.

In this research, we suggest (CLPDM-SSA) using the sparrow search algorithm introduced by Venkatasubramanian et al. [20] and by [21, 22]. This proposal employs a cluster-based meta-heuristic detector to single out a malicious node in a real-world data gathering system hit by a packet drop (PD) assault. Results: Throughput,, and false positive rate are utilised to validate the deployment of NS-2. The results show significant improvements once SSA intelligence was integrated. The method analyses the central processing unit and memory to identify false positives of suspected malicious nodes.

A novel Intrusion Detection System (IDS) is presented to increase network performance by identifying DDoS assaults in wireless networks by Nalayini and Katiravan [23], and by [24,25]. In order to pick the features that contribute the most to improving classification accuracy, we present a novel approach Feature Optimization Method (SFSH-FOM). In this paper, We provide a new deep learning method, Fuzzy Temporal Features integrated Convolutional Neural Network, for accurate classification (FT-CNN). To further enhance performance, we also provide an unique cross-layer feature fusion technique in this study, which makes use of FT-CNN and LSTM. Using assessment criteria like detection IDS was put to the test on benchmark datasets including KDD'99, NSL-KDD, and DDoS; the findings demonstrate that the proposed IDS is more effective than competing methods.

2.1 Research Gaps

There have been a lot of studies showed in this area, but the threshold value has seldom been taken into account. The study also proposes a deep learning model to determine the threshold value.

While many studies have been conducted on filtering-based systems, trust, and game theory, there are still obstacles to overcome before an effective solution can be designed.

Thirdly, there is a lack of study on how to protect AODV-based mobile ad hoc networks from attacks like hello flooding. We are unaware of any method for protecting Mobile Adhoc Networks from hello flood attacks.

3 Proposed System

3.1 Problem Statement

The security of MANET is crucial for revealing and avoiding the many assaults that pose a risk to MANET. An example of a DoS attack that poses a danger to network operations is the Flooding attack, which sends out bogus packets in an effort to slow down or halt legitimate data transmissions between nodes. To discover the shortest way between network nodes, the original AODV is an on-demand routing protocol; however, it does not have any means of detecting or avoiding the Flooding attack.

3.2 Our Contribution

To that end, we investigated the nature of the Flooding assault and its impact on the network, and we improved the deep learning model's ability to withstand this type of attack. By empowering nodes in the network with the ability to decide whether the request is received from an attacker node or from a normal node, our proposed model helps to avoid false judgement on nodes by putting them in a suspicious list before judging them, thereby reducing the negative effects of fake request packets on the network. Lastly, we attempted to make the limit value..

In this research, we provide a new statistically-based method for preventing flooding attacks on Mobile Adhoc Networks. The suggested approach makes use of the distribution as a statistical justification for navigating to the node that is causing network disarray due to an excess of RREQs. Spreading in a Mobile Ad hoc Network is computed by determining the standard deviation of RREQs answered by nodes with different characteristics. The detection and prevention of Mobile Adhoc Networks operating under the AODV protocol are greatly aided by this method. The statistical cutoff value is the foundation of this technique. This cutoff is based on the dispersion of the RREQs generated by several nodes in the MANET relative to the mean. If there are 'n' nodes in the MANET, and that for each I in the range.

$$Mean\ of\ Route\ Requests(MRREQ) = \sum_{i=1}^{n} \frac{x_i}{n} \tag{1}$$

After the mean has been determined for all RREQs in the Mobile Adhoc Network, the next step is to determine their variance. The dispersion of all nodes' route requests from $x_1, x_2, x_3, x_4, \ldots, x_n$ is calculated as

$$Variance^2 = \frac{\sum_{i=1}^{n}(x_i - MRREQ)^2}{n-1} \tag{2}$$

$$Variance = \sqrt[2]{\frac{\sum_{i=1}^{n}(x_i - MRREQ)^2}{n-1}} \tag{3}$$

After different threshold values have been computed, flood attackers and malicious nodes in the MANET can be located with more ease. STV is what you'll get when you

plug in your mean and variance numbers.

$$STV = 2 * \sum_{i=1}^{n} \frac{x_i}{n} * \frac{\sum_{i=1}^{n} \frac{x_i}{n}}{\sqrt[2]{\frac{\sum_{i=1}^{n}(x_i - MRREQ)^2}{n-1}} + 1} \tag{4}$$

The STV is the cutoff point used to identify the MANET's bad actor. The suggested DL model for determining STV's worth is described in detail below. The total number of RREQs generated by the n unique nodes in the mobile ad hoc network is denoted by the variable x, where x ranges from 1 to xn. Now we can see if x i > STV holds true for every xi with I ranging from 1 to n. Node 'i' is sending fake RREQs in the mobile ad hoc network to decrease performance if the cost of x i > STV is genuine. After the rogue node has been identified, a packet will be sent out through the mobile ad hoc network to cut it off. This process of sending RREQs to many recipients is carried out by every node in a mobile ad hoc network. In a mobile ad hoc network, malevolent nodes are well isolated. For the forthcoming statistical and threshold-based approach, this algorithm is intended.

Step 1: Start
Step 2: Determine how many RREQs each network node sent and keep track of those numbers in variables. as $x1, x2, x3, x4, \ldots\ldots\ldots\ldots\ldots.., xn$ by increasing the source node pawn as xi + +
Step 3: Find out the mean of the network using Eq. (1).
Step 4: If you want to see how much variation there is in the RREQs sent by different network nodes, you may do it by using Eq. (2–3).
Step 5: Compute Statistical Threshold Value (STV) using Eq. (4).
Step 6: For slightly node x_i where $i = 1, 2, 3, \ldots\ldots\ldots\ldots, n$.
If $x_i > STV$ then change to step 7 else go to step 8.
Step 7: The RREQs from node I are being dropped since it has been identified as a malicious source attempting to flood the network..
Step 8: End.

This technique does a scan of the whole network in order to identify any potential attacker nodes. This approach of isolating malicious node is more effective than other arithmetical and threshold-based strategies flooding attacker harmful nodes in MANET because the value of variance is determined based on the deviation of RREQs made by each node in the network.

3.3 Proposed CNN-BiLSTM-RF Architecture

The suggested method consists of three main parts. In the input layer of deep learning networks, we feed them 111 pairs of Click fraud data. It consists of a single-dimensional (CNN) layer, which together permit sample-based discretization of parameters for feature recognition, speed up training, and avoid over-fitting. The Batch Normalization layer follows the Maxpooling layer to enable parameter normalisation across intermediate layers and save prolonged training durations. There are 64 filters in the 1-D CNN layer, and the activation function is Relu. The kernel size is 2. Maximum pooling length of 2

is used in the Maxpooling layer. The BiLSTM layer receives its input features from this map. The 128 memory blocks of a BiLSTM are used to acquire expertise in the time domain characteristics. After a Maxpooling layer with pooling length 2, and before a Batch Normalization layer, the BiLSTM layer is placed. Afterwards, the input will be Flattened in preparation for the subsequent Dense layers. Filters 128 and 64 are used to add two thick layers. The activation function Relu has been applied to both dense layers. Between the two thick layers, a 0.5-dropout layer is utilised. Even if Max Pooling is used in between each layer in the model, the Dropout Layer is still there to prevent Over Fitting. This is typically the case since combining CNN with BiLSTM increases the likelihood of over-fitting and hence leads to subpar results on the testing set. At last, the attributes are used as input into RF to distinguish between genuine and fake clicks.

In addition, a hybrid model is taught to function using f(X,y) Where X,y [S 1,…,S K]. In order to reduce training and validation error, the Adam optimizer is used to adjust the weights at the end of each training session based on the training and validation loss and accuracy. Accuracy throughout both training and validation is also recorded for each K-set. In order to train the RF model, the f method is used to the output of the trained hybrid CNN-BiLSTM model, which is then utilised to extract hidden features from input data (EF,ytrain). Following feature extraction and RF training, the hybrid DL model is used to extract features for unseen data through f(ENF; ytest) to yield ypred. Accuracy, Precision, Recall, F1 Score, and Area Under the Curve (AUC) are only few of the assessment criteria used to assess performance after prediction results are achieved..

4 Results and Discussion

4.1 Simulation Environment

This subsection provides an illustration of the planned DL-performance AODV's evaluation. The simulation is run for 50 randomly placed nodes in a 1000m x 1000m region using a random way point model. In order to pinpoint the source of the network breach, a simulation duration of 900 s is used, and each scenario is run 10 times. The additional variables and typical values used in simulations are shown in Table 1. The effectiveness of the proposed DL-AODV is demonstrated against an adversarial node density variation attack. Moreover, classic AODV and trust-based AODV systems are compared to the proposed DL-AODV.

The effectiveness of the new DL-AODV is measured by the next set of routing KPIs:.

- **Routing overhead:** Ratio of control/routing packets used to total packets is the metric…

$$Routingoverhead = \frac{Numberofroutingpackets}{Numberofdatapackets + Numberofcontrolpackets} \quad (5)$$

- The term "Packet Lost" refers to the sum total of all packets that were lost while running the simulation.

$$PacketLost = Numberofpacketssent - Numberofpacketsreceived \quad (6)$$

Table 1. Network Imitation parameters

Typical Value	Parameter
802.11p	MAC Protocol
10,20,30,40,50	Node densities
~ 250m	Communication Range(m)
CBR	Traffic Source
0–20 m/s	Max Speed
512 (bytes)	Packet size

- Throughput: The percentage of received data during the allotted simulation period is calculated. A more secure and efficient network is one with a high throughput value.

$$Throughput = \frac{\sum Successfully\ received\ data\ packets\ at\ destination}{Simulation\ time * 1024} \tag{7}$$

- Average round-trip waiting time: The latency of a network is measured in milliseconds, or the time it takes a data packet to get from one point to another (Fig. 1).

$$E2Edelay = \frac{\sum_{i=1}^{n}(ReceivingTime - TransmittedTime)}{TotalNumberofconnections} \tag{8}$$

- Reliability: The rate at which data packets are received is compared to the rate at which they are sent. This number is always between zero and one (Table 2).

$$R = \frac{sumofdatapocketsrecived}{sumofpocketstransmitted} \tag{9}$$

Table 2. Comparative Assessment of PDR

No. of nodes	Packet delivery ratio (%)			
	RF	CNN	Bi-LSTM	CNN-Bi-LSTM-RF
10	89.57	94.87	87.56	99.80
20	90.78	93.93	88.98	99.80
30	88.69	93.54	87.75	99.56
40	88.94	94	85.83	98.36
50	87.56	95.5	84.67	96.67

When the node is 30, the existing models achieved nearly 87% to 93%, where ensemble model achieved 99% of PDR. When the nodes are high, the PDR is low for every technique. For instance, RF achieved 87.56%, CNN achieved 95.5%, Bi-LSTM achieved 84.67% and proposed model achieved 96.67% of PDR (Table 3 and Fig. 2).

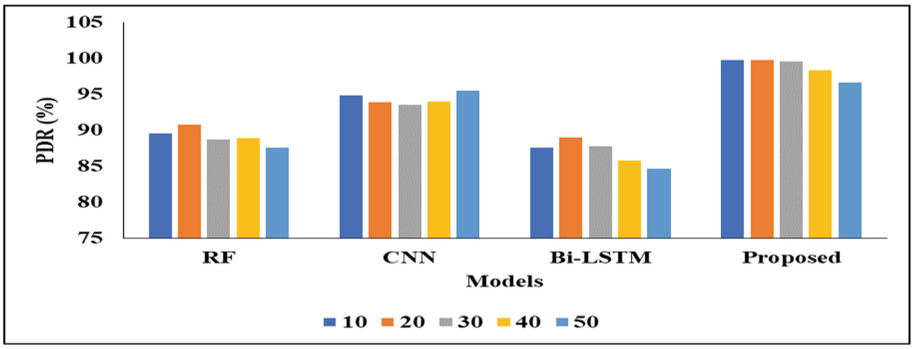

Fig. 1. PDR Analysis

Table 3. Comparative Assessment of throughput

No. of nodes	Throughput (bps)			
	RF	CNN	Bi-LSTM	CNN-Bi-LSTM-RF
10	67	250	95	700
20	38	148	70	520
30	45	125	74	425
40	40	178	69	345
50	35	185	73	240

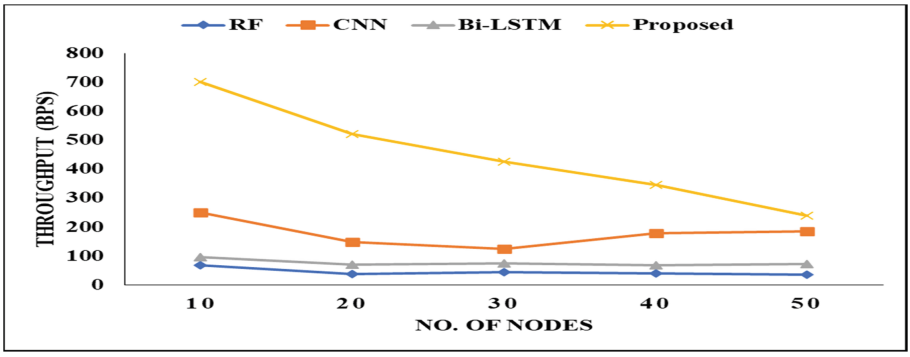

Fig. 2. Throughput Comparison

When comparing with all models, RF and Bi-LSTM achieved low performance on throughput analysis. For instance, when the node is 40, RF has 40bps, CNN has 178bps, Bi-LSTM achieved 69bps and proposed model achieved 345bps. The reason is that the RF works based on tree methodology, which needs to store all nodes in the memory. It consumes high computation for RF and provides poor performance (Table 4 and Fig. 3).

Table 4. Assessment of Energy consumption

No. of nodes	Energy Consumption (J)			
	RF	CNN	Bi-LSTM	CNN-Bi-LSTM-RF
10	10	10	11	6
20	16	17	15	9
30	19	21	18	12
40	25	27	23	16
50	33	34	26	19

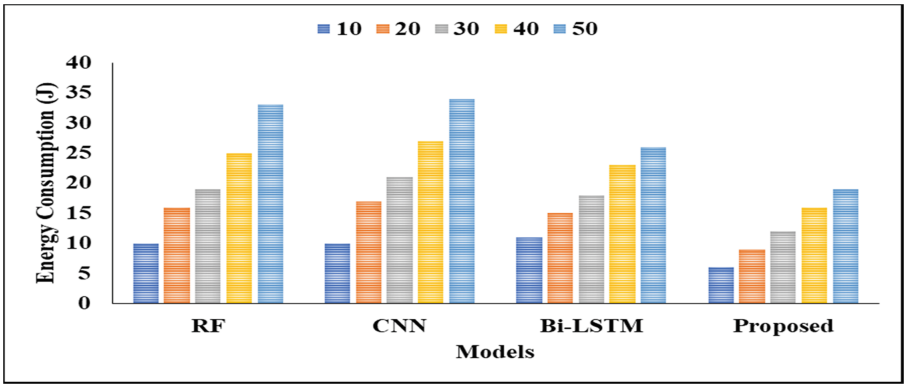

Fig. 3. Analysis of Energy Consumption

When the node is 10, CNN achieved 10J, RF achieved 10J, Bi-LSTM achieved 11J and proposed model achieved 6J. Less energy consumption means better performance of the model, therefore, the proposed model achieved 19J, CNN achieved 34J, RF achieved 33J and Bi-LSTM achieved 26J for the node 50 (Fig. 4).

Table 5. Evaluation of Network life time

No. of nodes	Network Lifetime (s)			
	RF	CNN	Bi-LSTM	CNN-Bi-LSTM-RF
10	60	119	98	150
20	75	140	115	300
30	86	186	140	420
40	94	230	167	530
50	120	265	198	580

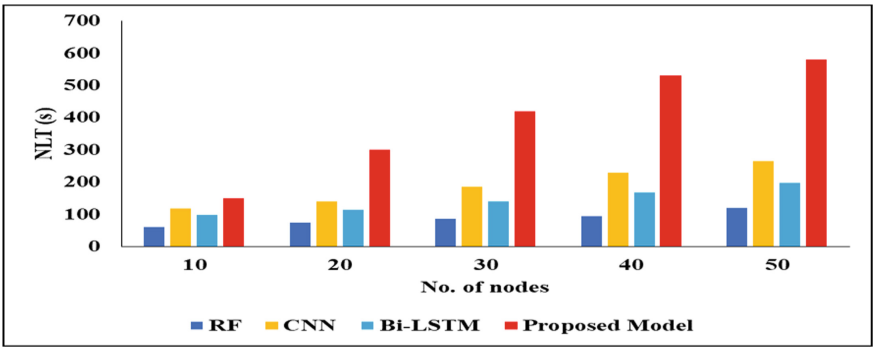

Fig. 4. NLT Comparison

More number of packets transferred to the destination without losing energy will have high network lifetime, which is analyzed in the Table 5. According to this theory, the proposed model has 300s, RF has 75s, CNN has 140s and Bi-LSTM has 115s for the node 20. When the node is 40, the RF has 94s, CNN has 230s, Bi-LSTM has 167s and proposed model has 530s. From this experimental analysis, it is clearly proves that proposed model achieved better performance than single classifiers.

5 Conclusion

In order to identify flooding attacks in MANETs, this study proposes a Secure AODV Routing Scheme (DL-AODV) that is powered by Deep Learning. For a variety of node densities, the effectiveness of DL-AODV was compared to that of standard AODV and trust-based AODV. Furthermore, the suggested DL-AODV significantly boosts the secure communication by enhancing the accuracy and throughput of intrusion detection with CNN and Bi-LSTM classifier. In addition, in comparison to previous DL based AODV protocols, the suggested method increases network burden. Just 50 nodes are included in this analysis of the planned DL-AODV, which has a top speed of 20m/s. As the node density and speeds in complete urban settings are very dynamic, DL-AODV is best suited for information transmission in semi urban environments.

References

1. Sbai, O., El boukhari, M.: September. Data flooding intrusion detection system for manets using deep learning approach. In: Proceedings of the 13th International Conference on Intelligent Systems: Theories and Applications, pp. 1–5 (2020)
2. Vatambeti, R., Sanshi, S., Krishna, D.P.: An efficient clustering approach for optimized path selection and route maintenance in mobile ad hoc networks. J Ambient Intell Human Comput **14**, 305–319 (2023). https://doi.org/10.1007/s12652-021-03298-3
3. Nandi, M., Anusha, K.: An optimized and hybrid energy aware routing model for effective detection of flooding attacks in a manet environment. Wireless Personal Communications, pp.1–19 (2021)

4. Archana, H.P., Khushi, C., Nandini, P., Sivaraman, E., Honnavalli, P.: Cloud-based Network Intrusion Detection System using Deep Learning. ArabWIC 2021: The 7th Annual International Conference on Arab Women in Computing in Conjunction with the 2nd Forum of Women in Research, Sharjah, UAE (2021). https://doi.org/10.1145/3485557.3485562
5. Banerjee, B., Neogy, S.: A brief overview of security attacks and protocols in MANET. In: 2021 IEEE 18th India Council International Conference (INDICON), pp. 1–6. IEEE (2021, December)
6. Kalime, S., Sagar, K.: A review: secure routing protocols for mobile adhoc networks (MANETs). Journal of Critical Reviews **7**, 8385–8393 (2021)
7. Kothai, G., et al.: A new hybrid deep learning algorithm for prediction of wide traffic congestion in smart cities. Wireless Communications and Mobile Computing, vol. 2021, Article ID 5583874, pp. 13 (2021). https://doi.org/10.1155/2021/5583874
8. Abdelhaq, M., et al.: The resistance of routing protocols against DDOS attack in MANET. Int. J. Electr. Comp. Eng. (2088–8708) **10**(5) (2020)
9. Fiade, A., Triadi, A.Y., Sulhi, A., Masruroh, S.U., Handayani, V., Suseno, H.B.: Performance analysis of black hole attack and flooding attack AODV routing protocol on VANET (vehicular ad-hoc network). In: 2020 8th International conference on cyber and IT service management (CITSM), pp. 1–5. IEEE (2020, October)
10. Divya, N.S., Bobba, V., Vatambeti, R.: An adaptive cluster based vehicular routing protocol for secure communication. Wireless Pers Commun **127**, 1717–1736 (2022). https://doi.org/10.1007/s11277-021-08717-4
11. Srinivas, T.A.S., Manivannan, S.S.: Prevention of hello flood attack in IoT using combination of deep learning with improved rider optimization algorithm. Comput. Commun. **163**, 162–175 (2020)
12. Mahajan, R., Zafar, S.: DDoS attacks impact on data transfer in IOT-MANET-based E-Healthcare for Tackling COVID-19. In: Data Analytics and Management: Proceedings of ICDAM, pp. 301–309. Springer Singapore (2021)
13. Nishanth, N., Mujeeb, A.: Modeling and detection of flooding-based denial-of-service attack in wireless ad hoc network using Bayesian inference. IEEE Syst. J. **15**(1), 17–26 (2020)
14. Kurian, S., Ramasamy, L.: Securing service discovery from denial of service attack in mobile ad hoc network (MANET). Int. J. Comp. Netw. Appli. **8**(5), 619–633 (2021)
15. Gebremariam, G.G., Panda, J., Indu, S.: Localization and Detection of multiple attacks in wireless sensor networks using artificial neural network. Wireless Communications and Mobile Computing (2023)
16. Elubeyd, H., Yiltas-Kaplan, D.: Hybrid deep learning approach for automatic Dos/DDoS attacks detection in software-defined networks. Appl. Sci. **13**(6), 3828 (2023)
17. Meddeb, R., Jemili, F., Triki, B., Korbaa, O.: A Deep Learning based Intrusion Detection Approach for MANET (2022)
18. Tekleselassie, H.: Two-dimensional projection based wireless intrusion classification using lightweight EfficientNet. J. Cyber Sec. Mobi. 601–620 (2022)
19. Kishen Ajay Kumar, V., et al.: Dynamic Wavelength Scheduling by Multiobjectives in OBS Networks. Journal of Mathematics vol. 2022, Article ID 3806018, 10 (2022). https://doi.org/10.1155/2022/3806018
20. Ramana, K., et al.: Leaf disease classification in smart agriculture using deep neural network architecture and IoT. J. Circ. Sys. Comp. **31**(15), 2240004 (2022). https://doi.org/10.1142/S0218126622400047
21. Dwaram, J.R., Madapuri, R.K.: Crop yield forecasting by long short-term memory network with Adam optimizer and Huber loss function in Andhra Pradesh, India

22. Ramana, K., et al.: A vision transformer approach for traffic congestion prediction in urban areas. IEEE Trans. Intell. Transp. Syst. **24**(4), 3922–3934 (2023). https://doi.org/10.1109/TITS.2022.3233801. April
23. Nalayini, C.M., Katiravan, J.: A New IDS for Detecting DDoS Attacks in Wireless Networks using Spotted Hyena Optimization and Fuzzy Temporal CNN. Journal of Internet Technology **24**(1), 23–34 (2023)