JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 39, 1233-1246 (2023)
DOI: 10.6688/JISE.202311_39(6).0001

Ensemble Deep Learning Classifier with Optimized Cluster Head Selection for NIDS in MANET

V. GOKULA KRISHNAN[1], P. A. ABDUL SALEEM[2], N. KIRUBAKARAN[3], VEERAMALAI SANKARADASS[4], ATA. KISHORE KUMAR[5], C. JEHAN[6], J. DEEPA[7] AND G. DHANALAKSHMI[8]

[1]*Department of CSE, Saveetha School of Engineering*
Saveetha Institute of Medical and Technical Sciences
Tamil Nadu, 602105 India
[2]*Department of CSE (DS), CVR College of Engineering*
Mangalpally, Hyderabad, Telangana, 501510 India
[3,4,6]*Department of CSE, Chennai Institute of Technology*
Tamil Nadu, 600069 India
[5]*Department of ECE, Sree Vidyanikethan Engineering College*
Mohan Babu University
Tirupati, 517102 India
[7]*Department of CSE, Easwari Engineering College*
Tamil Nadu, 600089 India
[8]*Department of IT, Panimalar Engineering College*
Tamil Nadu, 600123 India
E-mail: gokul_kris143@yahoo.com[1]; drsaleemprincipal@gmail.com[2]; Iamkiru70@gmail.com[3]; veera2000uk@gmail.com[4]; drkishore1609@gmail.com[5]; cjehan2001@gmail.com[6]; deepa.j@eec.srmrmp.edu.in[7]; dhanalakshmi4481@gmail.com[8]

A MANET security is more fragile and susceptible to the environment due to the lack of a centralized environment for monitoring the behavior of individual nodes during communication in this type of network. Both local and global invaders are able to access the networks they target. In MANETs, where nodes can move in any direction and topology is constantly changing, node mobility and node energy are two critical optimization challenges. As a result, remote monitoring of node performance and behavior is employed by Network Intrusion Detection Systems (NIDSs) as a solution to cope with the problem of intrusion into these networks. The proposed method is used to develop a Cuttlefish Algorithm with Ensemble Deep Learning Classifier (CFA-EDL) for multi-attack intrusion detection. A clustering algorithm for MANET cluster head election is developed in this research by focusing on the challenges of mobility and energy. To select the cluster head, the CFA uses the EDL Classifier, while the EDL Classifier identifies several attacks. Mul tiple attacks are identified using EDL Classifier. Extensive testing in MATLAB and comparisons with other existing methods are included in the planned research. Attack detection, memory ingesting and computing time for classifying an intruder are some of the metrics used to evaluate the suggested method's performance. The results of the simulation show that the suggested strategy significantly reduces IDS traffic and memory ingesting while maintaining an attack detection rate in the shortest amount of time possible.

Keywords: mobile ad hoc networks, security, attack detection, cuttle fish algorithm, deep learning classifier, network intrusion detection systems

1. INTRODUCTION

It is clear that MANETs are vulnerable to attack because of their open broadcast and mobile device tractability, making them prime targets for security measures. The use of

Received March 27, 2022; revised September 29, 2022; accepted October 1, 2022.
Communicated by Changqiao Xu.

MANET for Internet of Things (IoT) implementation is critical. As a result, it facilitates communication between the physical world and the computer systems of today. The MANET routing protocols [1] are used to route IoT nodes and devices connected to MANET nodes. Some mobile nodes have restricted computing power and energy sources [2, 3], as well. That's why it's difficult to have permanent security monitoring nodes in the network, and that's why MANET's nodes need to be controlled remotely, as resources are restricted [4, 5].

To support the belief that all mobile nodes in an extensive network are amenable to coordinating approach, MANETs use single jump joining layer protocol and multi bounce network layer protocol to communicate. Unfortunately, this assertion is not accurate when used in an unreceptive situation. Protocol specifications can be damaged by malicious attacks [6]. The prevalence of jamming attacks makes the network layer activities of MANET, such as packet routing and acknowledgement, vulnerable. In the event of a malicious node or attack, MANET must include robust support for data passing between legitimate nodes. Due to the open nature of communication in MANET, security is required to protect the network from malicious attackers. On-demand routing protocols, such as multipath AODV, can be exploited by attackers with little effort because of their vulnerability. An Intrusion Detection System (IDS) can be used to thwart attackers who are required by all mobile nodes, and hence the detection of routing issues under MANET [7].

Monitoring node or network traffic behavior is done by network intrusion detection systems (NIDS). NIDSs are designed to identify malicious nodes and anticipate future attacks on the network. Malicious nodes in the network are flagged as such, and an alert is created for further investigation. It is noteworthy that the success of IDS is dependent on the sort of approach utilized in this regard [9] for detecting NIDS attacks. In order to get the best results using NIDS, it's important to pick out representative characteristics from the larger dataset [10]. IDS performance can be improved by plummeting the number of features in the data set (such as node behavior and network traffic) without decreasing classification precision [11].

1.1 Motivation and Contribution

A cluster-based model with EDL has been proposed in this research to protect against multiple attacks. The intrusion node in MANET has been detected using two separate models. To begin, cluster leaders are chosen based on factors such as mobility and energy usage, and this encourages them to organize their systems into compact groups. EDL is used to assist the cluster head node in determining whether nodes are intruders. In a nutshell, the following is what this work has to offer the world.

- Using clustering and EDL, we've developed a new approach for enhancing NIDS attack detection rates. The IDS detection rate can be improved as much as feasible without sacrificing any of the IDS's effectiveness.
- A CFA-based optimization is employed for the selection of the cluster head and the construction of clusters in order to test our suggested strategy.
- As a last step, EDL Classifier is used to recognize multiple attacks.
- We demonstrate through simulation that our proposed way of optimizing IDS attack detection rates saves a significant amount of memory and calculation time.

2. RELATED WORKS

The previous several years have seen a considerable advancement in the field of communication technology. Despite the improvements, the networks are still vulnerable. Methods and techniques must be devised to minimize the occurrence of malevolent activity. NIDSs are a common mechanism in today's world. Network security and detection rate were improved by using a lightweight distributed technique described by Al-Jarrah and colleagues [12]. In Aloqaily *et al.* [13], distributed techniques for IDS in MANET were developed. Research on the application of machine learning to detect intrusions in MANETs was done by Cherkaoui and colleagues [14].

Ad hoc networks have come a long way in the previous few decades in terms of availability and use. Optimized routing detection and intrusion detection algorithms in Doss *et al.* [15] contributed to high detection rates and throughput. Data transmission was improved and security concerns were addressed in Gaurav and Singh [16] with an anonymity-based approach. In Gomathy *et al.* [17], a secure network architecture based on trust was presented to detect malicious nodes with little energy usage and greater detection accuracy. As quickly as possible, Kavitha *et al.* [18] discovered the jellyfish attack.

According to Rajendran *et al.* [19], a new integer optimization problem has been developed to lower the false alarm rate associated with Internet of Things (IoT) networks. Self-Organizing Tree (SOT) algorithms were examined in Sivanesh and Dhulipala [20] to reduce false alarm rates and energy usage. In Thanuja and Umamakeswari [21], an evaluation of intrusion detection systems for current automobiles based on MANET infrastructure was proposed. The packet-dropping situation was not a worry, despite the improvement in the false alert rate. Cooperative routing protocols were employed in Thanuja and Umamakeswari [22, 23] to dramatically enhance both the detection rate and the number of false positives. Identifying key nodes was made easier with Velliangiri and Pandey's (DCNI) approach [24].

3. PROPOSED SYSTEM

This paper outlines a brand-new approach to MANET intrusion detection. The MANET cluster head election ideal and the identification of NIDS are two independent parts of this intrusion detection technology. By assigning the intrusion detection duty to distinct cluster nodes, the previous part minimizes the general memory and computational time required for regulatory the IDS. Based on the mobility and energy consumption of mobile nodes, a cluster head node is selected. Intrusion detection services are delegated to a cluster head node for a predetermined amount of time. EDL-based identification of NIDS, which actually performs intrusion detection, is the second part of the proposed IDS architecture.

3.1 Cluster Head Selection using Cuttle Fish Algorithm (CFA)

For cuttlefish to change their skin color, the suggested method simulates the work of three cell layers. Cuttlefish employ a mechanism called the reflection process to reflect incoming light. This mechanism can take one of six forms. Cuttlefish mimic the patterns they see in their environment by adjusting their visibility to mirror the corresponding pattern clarity. Reflection and visibility are the foundations of the proposed CFA, which will

be used to develop new answers. NewP (newP) can be found by employing reflection and visibility to locate the new solution (1).

$$newp = reflection + visibility \tag{1}$$

To get the population started, CFA uses random solutions like other meta-heuristic algorithms. Then, the six scenarios are applied sequentially until the stop condition is achieved. The following is a breakdown of the CFA algorithm's main steps:

(1) To begin, use random solutions to populate the population. Then, determine and save the best answer and the average point value of the best solution.
(2) In Cases 1 and 2, the interaction operator among the chromophores and iridophores cells can be used to build a new solution based on the likeness and the visibility of the patterns (global search).
(3) Iridophores cells workers are used to compute novel solutions based on the best solution's reflected light and the visibility of matching patterns in Cases 3 and 4. (local search).
(4) Reflecting light from the area around the best solution and the visibility of the pattern can be used in Example 5.
(5) Leucophores cells can be used to generate a random solution by reflecting incoming light in Example 6 (global search).

3.1.1 Initialization

The P (number of cells) initial population of the N initial solutions random dots (points) are placed in the d-dimensional problem space using P = cells = points 1, 2, 3, ..., N in Eq. (2).

$$P[i].point[j] = random * (upperLimit - lowerLimit) + lowerLimit$$
$$i = 1, 2, \ldots, N; j = 1, 2, \ldots, d \tag{2}$$

A random number between upperLimit and lowerLimit in the problem domain is used as upperLimit (0,1).

3.1.2 Group 1, simulation of Cases 1 and 2

New solutions are found by utilizing chromatophors cells' stretching and contracting processes, as well as the reproduced light from iridophores cells and the discernibility of the pattern employed by cuttlefish to blend in with its surroundings. Eqs. (3) and (4) provide the detailed explanations of these procedures.

$$reflection_j = R * G_1[i].Points[j] \tag{3}$$

$$Visibility = V * (BestPoints[j] - G_1[i].Points[j] \tag{4}$$

Cells in G_1 represent chromatophore cells used to simulate the condition in Eqs. (3)

and (4) (1 and 2). Group G_1's ith cell is designated as i. The jth point of the ith cell is represented by $Points[j].Best$. The best solution points are represented by points. As a cell's muscles contract or relax, the saccule's stretch range can be determined using R, which is the reflection degree. The final pattern view's visibility level is signified by the letter V. The following formula is used to determine R's and V's values,

$$R = random() * (r_1 - r_2) + r_2, \tag{5}$$

$$V = random() * (v_1 - v_2) + v_2. \tag{6}$$

When using the random() function, you can generate anything from 0 to 1 at random (0, 1). In order to determine how much the chromatophors cells stretch, we use two constant values: r_1 and r_2. In order to determine the final view's degree of visibility, v_1 and v_2 are two constant numbers.

Then the *newP* can be found using Eq. (1) as follows,

$$newp[j] = reflection_j + visibility_j.$$

3.1.3 Group 2, imitation of Cases 3 and 4

The cells of the iridophores are light-reflecting, as was previously stated. Iridophores cells in Cases 3 and 4 reflect light from the environment, which is reflected in a certain hue. Organs can be hidden or protected using iridophores cells. We made the assumptions that the best solution represents the organs that aren't visible. For this reason, the method for finding the reflection remains unchanged, while the formula for finding the visibility is revised as follows,

$$reflection_j = R * Best.Points[j]. \tag{7}$$

Group R is set to 1, and Group V will be determined. This team conducts a local search using the interval around the best solution as a novel search region, based on the difference between the best solution and the solution.

3.1.4 Group 3, simulation of Case 5

The cells of leucophores function as mirrors. Thus, the majority wavelength of light emitted by the cells will be reflected back to the observer. They will reflect white light, brown light, and so on and so forth. Cells with unique color chromatophors are responsible for transmitting the light. Visibility is the source of the spacing utilized around the Best. Following are the changes to the two Eqs. (3) and (4) for finding the likeness and the visibility,

$$reflection_j = R * Best.Points[j], \tag{8}$$

$$visibility_j = V * (Best.Points[j] - AV_{Best}). \tag{9}$$

AV Best is the average of the finest points, as defined by AV Best. When the value of v is calculated, the value of R is set to 1, and Another local search, this time using the

change between best solution points and average points to create a tiny area around the best solution.

3.1.5 Group 4, simulation of Case 6

The leucophores cells will simply reflect the incoming light in this situation. The cuttlefish is able to blend in with its surroundings because to this operator. Any hue that is reflected from the environment can be represented by any random solution, as this is a simulation. Since the initialization uses Eq. (2) to find the new solutions specified in Section 3.1.1, this example works as expected here.

It remains the goal of this approach to select a cluster head with the smallest computational time for the starting network condition of I mobile nodes. In our work, we're able to accomplish this by combining three different strategies. Finally, the cluster head is elected with the least amount of memory and computing time possible using the dual significance factor.

While using the elected cluster head as an input, the goal is to achieve or build balanced clusters with a maximum objective function. A two-factor algorithm is used to achieve the goal. First, the cluster head node's energy consumption and stability divergence are used to calculate the cluster's fitness function, which maximizes the objective function and so forms balanced clusters.

3.2 Detection of NIDS using Ensemble Deep Learning (EDL) Classification

3.2.1 Recursive neural network (RNN)

As a neural network structure, standard RNNs are used to solve complex symbolic problems for compound symbolic constructions of arbitrary shapes (*e.g.*, logical terms or graphs). Fig. 1 explains the approach of RNN. When a sentence is given, RNN analyzes it in a binary semantic tree and calculates the vector symbol of each word. During the feed forward training period, the RNN calculates the parent vector in ascending order. The structure equation looks like this,

$$p_1 = f\left(W\begin{bmatrix} c_2 \\ c_3 \end{bmatrix} + b\right), p_2 = f\left(W\begin{bmatrix} c_1 \\ p_1 \end{bmatrix} + b\right). \tag{10}$$

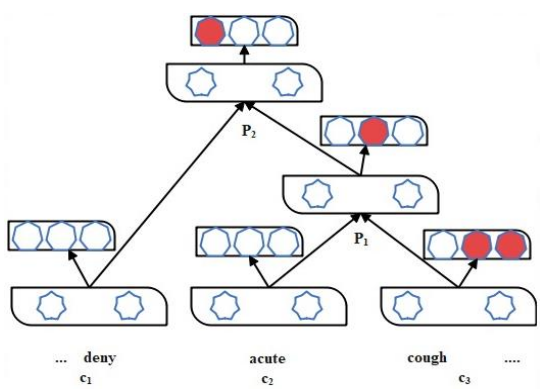

Fig. 1. RNN classification task models.

Where f is the activation function; $W \in \mathbb{R}^{d \times 2d}$ is the weight matrix, where d is the dimensionality of the vector; and b is the bias. Then, every parent vector p_i is assumed as a feature to a softmax classifier such as that distinct in Eq. (11) to calculate its probabilities:

$$y^p = softmax(W_s \cdot p). \tag{11}$$

Where $W_s \in \mathbb{R}^{3 \times d}$ is the classification matrix. In this recursive process, the vector and node classification results will gradually merge. Once the leaf node vector is specified, the RNN can eventually form an initial representation of the entire plant in the root vector.

3.2.2 Recurrent neural networks

It is clear that training the recurrent network ideal involves of two portions: forward and backward propagation. The direct propagation is in charge for scheming the output values and the back propagation is accountable for transmitting the accumulated residue to update the weight, which is not essentially diverse from traditional neural network training scheme. Fig. 2 provides the graphical illustration of recurrent network.

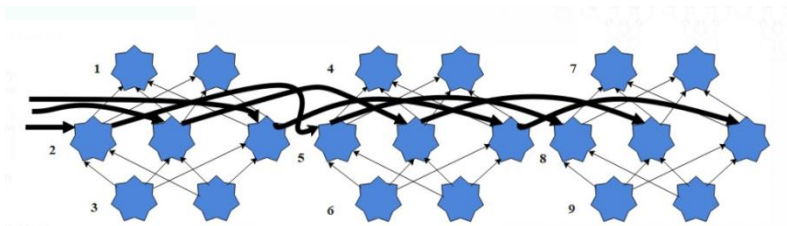

Fig. 2. The unfolded recurrent network; The following numbers defines the various parameters of RNN; (1) $\hat{y}_{t-1}$; (2) h_{t-1}; (3) x_{t-1}; (4) $\hat{y}_t$; (5) h_t; (6) x_t; (7) $\hat{y}_{t+1}$; (8) h_{t+1}; (9) x_{t+1}.

The regular recurrent network is formalized as follows: Given training trials $x_i (i = 1, 2, \ldots, m)$, a sequence of hidden states $h_i (i = 1, 2, \ldots, m)$, and a sequence of predictions $\hat{y}_i (i = 1, 2, \ldots, m)$. *Whx* is identified as input-to-hidden weight matrix, *Whh* is identified as the hidden weight matrix.

The recurrent network s for a single training pair (x_i, y_i) is defined as $f(\theta) = L(y_i : \hat{y}_i)$, where L is a space function which events the deviance of the predictions $\hat{y}_i$ from the actual labels y_i. Let η be the learning rate and k be the sum of current iterations. Given an arrangement of labels $y_i (i = 1, 2, \ldots, m)$.

3.2.3 Long short-term memory (LSTM)

RNN is the neural feedback network's extension. The gradient disappears or explodes, however, in the ordinary RNN. Long Shortened Memory Network (LSTM) was meant to alleviate the issues and has performed better than expected. Three gates and a single cell memory state make up the LSTM design. This is the LSTM seen in Fig. 3.

$$X = \begin{bmatrix} h_{t-1} \\ x_t \end{bmatrix} \tag{12}$$

$$f_t = \sigma(W_f \cdot X) + b_f \tag{13}$$

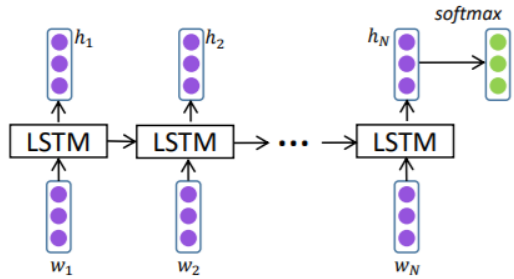

Fig. 3. The architecture of a standard LSTM.

$$i_t = \sigma(W_i \cdot X) + b_i \tag{14}$$

$$o_t = (W_o \cdot X) + b_o \tag{15}$$

$$c_t = f_t \odot c_{t\text{-}1} + i_t \odot \tanh(W_c \cdot X + b_c) \tag{16}$$

$$h_t = o_t \odot \tanh(c_t) \tag{17}$$

There are weighted matrices and biases of LSTM, in W_i, W_f, and W_o, $R(2d)$. Gates are built-in systems that can be used to switch the data flow. In a single sequence, these gates can determine which data should be saved or discarded. This enables it to convey relevant information to build job forecasts along the extended chain of sequences. The cell condition and its various gates are the core concepts of LSTM. Throughout the transmission of information, the cell state functions as a transportation channel. The condition of the cell during sequence processing may provide useful data. The impact of short-term memory can be diminished even if knowledge is acquired early in life. As the cell's condition changes, gates will add or remove information from the database. The gates can tell you what information you should or should not forget when training. In the following section, we'll explain how the proposed methodology was tested.

4. RESULTS AND DISCUSSIONS

There are weighted matrices and biases of LSTM, the short-term memory solution, in W_i, W_f, and W_o, $R(2d)$. They have built-in mechanisms that can control the flow of information, such as calendars. These results are reported in this part for the proposed multi-attack intrusion detection approach, CFA-EDL. Using MATLAB's simulated data, this experiment shows how well the proposed CFA-EDL approach works. Intrusion detection in MANET is studied using Security of Things (SOT), Transmission Line Security Monitor (TLM), and Data Center Network Infrastructure (DCNI) [20, 23, 24]. The ROC curve, attack detection rate, memory usage, and processing time are some of the performance parameters assessed. The network is constructed using a random waypoint mobility model. Consideration is given to the AODV routing protocol in MANETs. CFA was used to select a cluster head in a 50-node MANET for simulation purposes.

4.1 The Performance of Attack Detection Rate

The attack detection rate is the first statistic to be evaluated for intrusion detection

(ADR). The higher the detection rate, the more effective the approach is at detecting intrusions. The rate of assault detection is calculated as follows,

$$ADR = \sum_{i=1}^{n} \frac{mIDS}{m_i} * 100. \tag{18}$$

Attack detection rate (ADR) is calculated using the mobile nodes used in simulation and the mobile intruders that were successfully identified as intrusions, according to Eq. (18). It is expressed as a percentage (%), and the ADR is shown in Table 1.

Table 1. Attack detection ratio.

Mobile Nodes	Number of intruder nodes		Attack Detection Ratio (%)		
		SOT	TLM	DCNI	Proposed CFA-EDL
50	5	40	60	70	80
100	10	60	70	80	90
150	15	73	80	87	93
200	20	65	75	88	90
250	25	68	76	80	96
300	30	67	77	82	97
350	35	71	77	80	94
400	40	75	83	85	98
450	45	80	87	88	93
500	50	80	84	86	94

Table 1 represent that the Attack Detection Ratio of proposed model with TLM and DCNI scheme. In these comparisons proposed method reach best value in Attack Detection Ratio. The highest ratio of the proposed technique is 94% in Attack Detection Ratio.

4.2 The Memory Consumption Performance

For intrusion detection and prevention, the second measure to be considered is how much RAM is used to identify the intrusion in MANET. Since the detection rate should be improved, but also the amount of RAM used to identify the incursion, this metric is of critical importance. The memory use is expressed as follows,

$$MC = \sum_{i=1}^{n} m_i * MEM[AD]. \tag{19}$$

This Eq. (19) demonstrates how to determine how much RAM is being used during an intrusion detection process and how much memory is being consumed in the process. Kilobytes are the units of measurement (KB). Table 2 lists the amount of RAM used, as seen below.

Table 2 represent that the Memory consumption (KB)of proposed model with SOT, TLM and DCNI scheme. In these comparisons proposed method reach best value in Memory consumption (KB). The proposed CFA-EDL proposed technique reaches as 560 *t* 500 mobile node in Memory consumption (KB).

Table 2. Memory consumption (KB).

Mobile Nodes		Memory Consumption (KB)		
	SOT	TLM	DCNI	Proposed CFA-EDL
50	150	100	170	80
100	300	150	320	120
150	350	210	378	150
200	380	267	410	190
250	580	320	610	250
300	640	490	690	310
350	745	513	787	370
400	890	630	940	410
450	1101	790	1230	467
500	1345	960	1423	560

4.3 The Performance of Computational Time

Detecting the incursion takes time, which is measured and theoretically defined in the following way.

$$CT = \sum_{i=1}^{n} m_i * Time[AD] \tag{20}$$

The computing time *CT*, which is based on the number of mobile nodes *i*, and the amount of time it takes to identify an attack or intrusion *Time*[*AD*], is calculated from the aforementioned Eq. (20). The computation time is shown in Table 3 below.

Table 3 represent that the Computational time (ms) of proposed model with SOT, TLM and DCNI scheme. In these comparisons proposed method reach best value in Computational time (ms). The proposed CFA-EDL proposed technique reaches as 2.85ms in 500 mobile nodes in Computational time (ms).

Table 3. Computational time (ms).

Mobile Nodes		Computational Time (ms)		
	SOT	TLM	DCNI	Proposed CFA-EDL
50	1.6	1.8	0.75	0.75
100	1.85	2.10	0.83	0.83
150	2.15	2.40	0.93	0.95
200	2.40	2.70	1.05	1.05
250	2.85	3.10	1.15	1.15
300	3.16	3.30	1.45	1.45
350	3.35	3.55	1.95	1.95
400	3.55	3.80	2.15	2.15
450	3.97	4.10	2.35	2.35
500	4.27	4.45	2.85	2.85

4.4 The Performance of the ROC Curve

When it comes to detecting multi-attack intrusions, the receiver operating characteristic (ROC) curve is the most important instrument. False positive rates (FPR) and true positive rates (TPR) are plotted to create what's known as an ROC curve.

$$ROC\ curve = \frac{TPR}{FPR} \tag{21}$$

The true positive rate TPR, FPR are used to examine the Receiver Operating Characteristic (ROC) curve in Eq. (21). The ROC curve is shown in Table 4 below.

Table 4. ROC curve.

False positive rate		True Positive Rate		
	SOT	TLM	DCNI	Proposed CFA-EDL
0	0	0	0	0
0.01	0.78	0.81	0.70	0.87
0.02	0.82	0.85	0.74	0.88
0.03	0.83	0.87	0.78	0.91
0.04	0.84	0.88	0.82	0.93
0.05	0.87	0.89	0.86	0.95
0.06	0.89	0.90	0.88	0.96

Table 4 represents that the True Positive Rate of proposed model with SOT, TLM and DCNI scheme. In these comparisons proposed method reach best value in True Positive Rate. The proposed CFA-EDL proposed technique reaches as 0.97 in 0.92 false positive rate in True Positive Rate. By this comparisons ratio proposed technique reaches better True Positive Rate successfully.

5. CONCLUSION

MANET is a new field of study today because of its unique features. In addition to being more susceptible to malicious activity, the dynamic topology configuration of these systems makes them more error prone. We need to focus on the design of intrusion detection and MANET prevention mechanisms that have a high detection rate while using minimum memory and having minimal overhead. For MANET multi-attack intrusion detection, we presented a new NIDS approach termed CFA-EDL, which includes a cluster head node election model and identification of NIDS. The suggested method has a high detection rate while using less memory and computing time to run NIDS in MANETs. It does this through an improved CFA that selects the cluster head based on mobility and energy usage. Finally, the EDL classifier succeeds in improving the ROC curve. Memory consumption, calculation time, detection rate, and ROC curve were all assessed to see how well the system worked in terms of performance. In comparison to SOT, TLM, and DCNI, the CFA-EDL technique detects attacks 32% more frequently, uses 36% less memory, and saves 40% more computing time, according to the results and discussion. The NIDS datasets have a high rate of false alarms because of redundant and unnecessary features. This can be overcome by introducing an efficient technique for selecting the optimized features and model's hyper-parameters automatically as a future work.

REFERENCES

1. P. Sathyaraj and D. R. Devi, "Designing the routing protocol with secured IoT devices and QoS over Manet using trust-based performance evaluation method," *Journal of Ambient Intelligence and Humanized Computing*, Vol. 12, 2021, pp. 6987-6995.

2. S. Muruganandam, J. A. Renjit, and R. S. Kumar, "A survey: comparative study of security methods and trust manage solutions in MANET," in *Proceedings of the 5th International Conference on Science Technology Engineering and Mathematics*, 2019, pp. 125-131.
3. V. Singh, D. A. Singh, and M. M. Hassan, "Survey: black hole attack detection in MANET," in *Proceedings of the 2nd International Conference on Advanced Computing and Software Engineering*, 2019, pp. 522-525.
4. A. Gupta and A. Dubey, "A survey on various applications and blackhole attack in mobile ad hoc network," *Recent Trends in Parallel Computing*, Vol. 5, 2018, pp. 1-6.
5. R. Fotohi and S. Jamali, "A comprehensive study on defense against wormhole attack methods in mobile ad hoc networks," *International Journal of Computer Science & Network Solutions*, Vol. 2, 2014, pp. 37-56.
6. V. P. and R. P. Goyal, "MANET: Vulnerabilities challenges attacks application," *International Journal of Process Engineering & Management*, Vol. 11, 2011, pp. 32-37.
7. M. I. Talukdar, R. Hassan, M. S. Hossen, K. Ahmad, F. Qamar, and A. S. Ahmed, "Performance improvements of AODV by black hole attack detection using IDS and digital signature," *Wireless Communications and Mobile Computing*, 2021, pp. 1-13.
8. G. K. Ahuja and G. Kumar, "Evaluation metrics for intrusion detection systems – a study," *Evaluation*, Vol. 2, 2014, pp. 11-17.
9. P. Yang, Z. Li, P. Yang, and Y. Dong, "Information-centric mobile ad hoc networks and content routing: a survey," *Ad Hoc Networks*, Vol. 58, 2017, pp. 255-268.
10. A. Sultana and M. A. Jabbar, "Intelligent network intrusion detection system using data mining techniques," in *Proceedings of the 2nd International Conference on Applied and Theoretical Computing and Communication Technology*, 2017, pp. 329-333.
11. S. Sindhuja and R. Vadivel, "A study on intrusion detection system of mobile ad-hoc networks," *Soft Computing for Problem Solving*, 2020, pp. 307-316.
12. O. Y. Al-Jarrah, C. Maple, M. Dianati, D. Oxtoby, and A. Mouzakitis, "Intrusion detection systems for intra-vehicle networks: a review," *IEEE Access*, Vol. 7, 2019, pp. 21266-21289.
13. M. Aloqaily, S. Otoum, I. A. Ridhawi, and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," *Ad Hoc Networks*, Vol. 90, 2019, p. 101842.
14. B. Cherkaoui, A. Beni-hssane, and M. Erritali, "Variable control chart for detecting black hole attack in vehicular ad-hoc networks," *Journal of Ambient Intelligence and Humanized Computing*, Vol. 11, 2020, pp. 5129-5138.
15. S. Doss, A. Nayyar, G. Suseendran, S. Tanwar, A. Khanna, and P. H. Thong, *et al.*, "APD-JFAD: accurate prevention and detection of jelly fish attack in MANET," *IEEE Access*, Vol. 6, 2019, pp. 56954-56965.
16. A. Gaurav and A. K. Singh, "Light weight approach for secure backbone construction for manets," *Journal of King Saud University – Computer and Information Sciences*, Vol. 13, 2020, pp. 1292-1302.
17. V. Gomathy, N. Padhy, D. Samanta, M. Sivaram, V. Jain, and I. S. Amiri, "Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, Vol. 11, 2020, pp. 4995-5001.

18. T. Kavitha, K. Geetha, and R. Muthaiah, "India: Intruder node detection and isolation action in mobile ad hoc networks using feature optimization and classification approach," *Journal of Medical Systems*, Vol. 43, 2019, No. 179.
19. N. Rajendran, P. Jawahar, and R. Priyadarshini, "Cross centric intrusion detection system for secure routing over black hole attacks in MANETs," *Computer Communications*, Vol. 148, 2019, pp. 129-135.
20. S. Sivanesh and V. S. Dhulipala, "Accurate and cognitive intrusion detection system (acids): a novel black hole detection mechanism in mobile ad hoc networks," *Mobile Networks and Applications*, 2020, pp. 1-9.
21. R. Thanuja and A. Umamakeswari, "Unethical network attack detection and prevention using fuzzy based decision system in mobile ad-hoc networks," *Journal of Electrical Engineering and Technology*, Vol. 13, 2018, pp. 2086-2098.
22. R. Thanuja and A. Umamakeswari, "Black hole detection using evolutionary algorithm for IDs/IPs in MANETs," *Cluster Computing*, Vol. 22, 2018, pp. 3131-3143.
23. N. Veeraiah and B. Krishna, "An approach for optimal-secure multipath routing and intrusion detection in manet," *Evolutionary Intelligence*, 2020, pp. 1-15.
24. S. Velliangiri and H. M. Pandey, "Fuzzy-Taylor-elephant herd optimization inspired deep belief network for DDOS attack detection and comparison with state-of-the-arts algorithms," *Future Generation Computer Systems*, Vol. 110, 2020, pp. 80-90.

V. Gokula Krishnan is currently working as a Professor in the Department of Computer Science and Engineering in Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Tamil Nadu, India. He has more than sixtheen1years of teaching experience in various colleges in Chennai and Hyderabad. He has published several papers in reputed indexed journals and he also has presented various papers in national and international conferences.

P. A. Abdul Saleem is presently working as a Professor in Computer Science and Engineering (DS), CVR College of Engineering, Ibrahimpatnam, Ranga Reddy District, Telangana State, India. He has twenty-nine years of industrial, teaching and research experience. His research areas include wireless mobile adhoc networks, MANET security, machine learning and embedded systems *etc.*

N. Kirubakaran is currently working as a Professor in the Department of Computer Science and Engineering at Chennai Institute of Technology, Chennai. He has rich teaching, research and administrative experience for more than twenty-three years in Engineering Colleges, Autonomous Institutions and Universities. He has published more than fifteen papers in national and international conferences and in international journals.

Veeramalai Sankaradass is working as a Professor in the Department of Computer Science and Engineering at Chennai Institute of Technology affiliated to Anna University, Chennai, Tamil Nadu, India. He has published more than 40 research papers in reputed Internal National Journal and Conference. He served as reviewers for more than six international journals indexed in Scopus and SCI. He has more than twenty-five years of experience in teaching.

ATA. Kishore Kumar received his B.E. degree from Periyar University in 2004 and M.Tech degree from SRM University in 2006, respectively. He is presently working as an Associate Professor in the Department of Electronics and Communication Engineering, Sri Vidyanikethan Engineering College, Rangampet, Tirupathi, JNTUA. His areas of interests include low power VLSI design and reconfigurable architectures for image processing.

C. Jehan is currently working as an Associate Professor in the Department of Computer Science Engineering, Chennai Institute of Technology, Kundrathur, Chennai, Tamil Nadu, India. He has more than eighteen years of teaching experience in various colleges in Tamil Nadu. He has published several papers in reputed indexed journals and conferences. His research interests include WSN, mobile ad-hoc networks and computer networks, *etc.*

J. Deepa is currently working as an Assistant Professor in the Department of Computer Science and Engineering in Easwari Engineering College, Chennai. She has completed her Under-Graduation (B.E) in Madurai Kamarajar University, Post-Graduation (M.Tech) in National Institute of Technology, Trichy and Ph.D. in Anna University, Chennai. She has more than 13 years of experience in the teaching field and also published various papers in national and international conferences and journals.

G. Dhanalakshmi is currently working as an Associate Professor in the Department of Information Technology in Panimalar Engineering College, Chennai, Tamil Nadu, India. She has completed her Under-Graduation (B.E), Post-Graduation (M.E) in Anna University and she is perusing her Ph.D. in MGR University, Chennai, Tamil Nadu, India. She has more than 18 years of experience in the industry and teaching field, and she has published several papers in reputed conferences and journals.