Journal of Engineering Science and Technology
Vol. 19, No. 4 (2024) 1171 - 1188


# IMPROVE SECURITY FOR MOBILE AD HOCK NETWORK USING MODIFIED WHALE ALGORITHM AND DEEP LEARNING TECHNOLOGY

TUKA KAREEM JEBUR

Department of Business Management, College of Management and Economic, Al-Mustansiriyah University, Iraq
E-mail: tukakareem@uomustansiriyah.edu.iq

## Abstract

Various networking applications require Mobile Ad-Hoc Networks (MANETs) one of these examples are intelligent traffic management systems and security. Nonetheless, these networks experience issues in scalability and topology formation because they have few but mobile nodes. To address the current challenges in clustering, we suggest that one way to optimize its performance is by considering security parameters, the area of transmission range, number of node density, speed, direction, and grid of network size. Here in the suggested paper, we propose a Modified Whale Optimization algorithm (MWA) to select cluster heads in MANETs. The proposed algorithm, which utilized the behaviour of humpback whales, is combined with a Convolutional Neural Network (CNN) to improve network security threats detection. While the MWA focuses on optimizing security, improving accuracy, and reducing false positives and alarms, CNN analysis must look at traffic patterns to identify security risks. The proposed methodology was also subjected to intense simulations and experiments, where its performance was compared to earlier methods- Gray Wolf Optimization (GWO), Ant Lion Optimization (ALO), Particle Swarm Optimization (PSO), and Ad hoc On-demand Distance Vector (AODV). Our method is better than GWO by a margin of 21.5% in terms of reliability, and the highest detection of signatures and anomalies. packet delivery ratio, latency, false alarm time, and detection time. Energy consumption (J) and end-to-end delay (s), on the other hand, are better managed by ALO, PSO and AODV in descending order) with 50%, 52%, and 24.5 % respectively than our technique. These results show how good and productive our method is thus proving that it can help improve trustworthiness, affirmation, anomaly recognition, and network optimization.

Keywords: Ad hoc on-demand distance vector, Ant lion optimization, Convolutional neural network, Deep learning, Gray Wolf Organization, Manet, Modified whale algorithm, Particle swarm optimization.

## 1. Introduction

In recent decades, Meta-heuristic methods such as Particle Swarm Optimization, Genetic Algorithms, and Ant Colony Optimization have become increasingly significant in many fields such as computer vision and machine learning. These methods are popular due to their adaptability, straightforwardness, ability to avoid local optima, and ease of comprehension. Known for their simple implementation and wide applicability, these algorithms efficiently tackle various problems by utilizing deviation-free strategies and inherent randomness. They initiate with random solutions, thereby avoiding complex calculations, making them well-suited for modern challenges. Drawing inspiration from the natural behaviours of animals, insects, and birds, these algorithms are designed to explore the entire solution space, effectively mitigating the issue of getting trapped in local optima. In the realm of the Internet of Things (IoT), a crucial aspect of network technology, these meta-heuristic methods hold significant potential. As IoT continues to develop and advance, these algorithms are poised to play a vital role in shaping its future [1]. MANETs are considered one of the types of wireless networks formed by mobile devices such as laptops, smartphones, and tablets without the need for a centralized infrastructure of the network.

In disaster response, military operations, and emergency services, these networks are particularly useful especially if traditional infrastructure-based networks are unavailable or inadequate [2]. However, the dynamic topology, open nature, and lack of centralized control in MANETs make them susceptible to numerous security threats. These vulnerabilities include eavesdropping, data tampering, routing attacks, and denial of service attacks, among others [3]. A robust security mechanism is necessary for the protection of Mobile Ad Hoc Networks (MANETs) from different security threats and for ensuring that there is secure communication among nodes that is reliable. By utilizing Convolutional Neural Networks (CNNs) in conjunction with a Modified Whale Optimization Algorithm, this work provides a novel approach to improving the security of MANET. The Modified whale algorithm which utilizes social behaviour among humpback whales serves as an intelligent optimization means for this problem [4]. CNNs represent deep learning models that are frequently employed in image and signal processing [5]. Combining the strengths of both methods, the proposed solution suggests an effective and efficient security mechanism may be established in a MANET network.

In this paper, we propose a system to pick and transmit secure information in multi-segmented strategies, integrating applicable methods in distributed networks. We combine the Whale Optimization Algorithm (WOA) with Convolutional Neural Networks (CNN) to realize better performance than conventional ways. Our implementation enhances matters regarding efficiency within a cluster while at the same time raising the standards of the entire network considering the future.

Several inquiries have been carried out concerning the use of optimization algorithms in the selection of cluster heads among AD HOC networks. For illustration, one of the methods uses WOA to choose the best nodes for becoming cluster heads. For example, a clustering approach applied for UAV networks made use of the Binary Whale Optimization Algorithm (BWOA) wherein it was possible to select stable cluster heads and implement effective cluster maintenance strategies. That helped in reducing overhauling the entire network [6]. It was

suggested in different research that Cluster Traffic Prediction could benefit from a clustering algorithm for vehicular ad-hoc networks called Whale Optimization Algorithm Clustering Vehicular Ad Hoc Networks (WOACNET) This approach likewise sought to identify well-suited node coordinators using some features. It showed an improvement of 46.0% in cluster optimization, reaching a statistically significant F-value of 31.64 over other methods that have been published. Nevertheless, it would be advisable to consider possible flaws like the timeout attached to it.

Yan et al. [7] introduced a new energy-saving solution for selecting cluster heads in wireless sensor networks. This method is named as Whale Optimization Algorithm for Clustering (WOA-C), and it places priority on a choice of cluster heads having the highest remaining energy levels. The algorithm achieves an even distribution of such cluster heads across the whole network thereby enhancing performance in residual energy, network lifetime, and cluster stability. Nevertheless, there is no conclusion in the research. However, in this study, the security issue is not an aspect of this approach [8].

Hence there are methods to discover paths one of them is swarm optimization algorithms have been utilized for discovering optimal routes and implementing diverse optimizations within MANETs. The author suggested a hybrid method (PSO) and genetic algorithms. These algorithms have found applications in tasks such as route optimization, cluster formation, Quality of Service (QoS) enhancement, and network-centric localization in MANETs. For instance, one study employed PSO to identify stable cluster heads in MANETs the drawbacks of this method are overhead, and delay do not mention security in transmission [9], while another author suggested applying PSO to optimize the parameters of the AODV routing protocol, thereby improving QoS in MANETs does not mention extending network life or packet delivery ratio and latency [10]. Consequently, PSO emerges as a promising algorithm for optimizing various facets of MANETs. In a review of existing MANET security solutions

Sarumathi and Jayalakshmi [11] suggested a new technique for enhancing the security of routing on MANETs which ranges from the various ways by which each node's trust scores are derived, including its attributes and those of other nodes close. As such, the system can single out nodes within the network that are fraudulent or have an ulterior motive against other communications. Typically, a lot of resources are usually used when it comes to securing MANETs. The methodology in particular focuses on trust, which means that it does not demand heavy resource use, unlike other methods in its class.

Sultan et al. [12] suggested a model of intrusion detection system meant for MANETs which make use of deep learning artificial neural networks (ANNs). The main goal of this system is to detect and separate Denial-of-Service (DoS) attacks to improve security on MANETs. However, this research fails to investigate how this intrusion detection method can affect individual MANET nodes' performance and resource usage. Also, the intrusion detection techniques for MANETs have not been compared with existing ones in the document, The paper deals with a limited number of security threats while suggesting threat detection in the network layer but paying little attention to various types of attacks that may jeopardize MANET systems, e. g. Black hole attacks an unauthorized network intrusions where some

nodes are controlled by attackers to steal confidential information or routing attacks where legitimate traffic is hijacked, redirected and dropped by malicious nodes.

Singh and Vigila [13] used WOA-DNN for smart intrusion detection and classification in MANET services. WOA-DNN is identified as a Whale Optimized Deep Neural Network model that detects and classifies cyber-attacks accurately. The paper limited the ability to assess the performance of the proposed WOA-DNN model by not comparing it with any existing intrusion detection systems or machine learning algorithms that are available.

Venkatasubramanian et al. [14] employed deep learning algorithms to successfully detect and differentiate between black hole and grey hole cyber-attacks in mobile ad-hoc networks. Using CNNs and Long Short-Term Memory (LSTM) networks, the model can segregate these attacks from normal network behaviour. For individual attack detection, the system makes use of the "forwarding ratio" metric, thereby distinguishing between malicious and normal nodes. Moreover, Hybrid Cat-Particle Swarm Optimization (HCPSO) is adopted as a technique for refining the parameters for the LSTM model so that normal and compromised nodes may be classified more accurately. The results from simulations reveal that this way helps to find such attacks more precisely compared with other methods used for the same purpose in MANETs. Unfortunately, the paper fails to discuss possible disadvantages such as those connected to the deep-learning algorithms causing delay or overloading individual nodes computationally.

The security in MANET networks can be elevated using a blend of adapted Whale algorithms and CNNs, this was suggested. The whale Algorithm is an altered shoaling intuition methodology representing humpback feeding mannerisms, with CNNs being utilized broadly for image and signal processing due to their easy adaptation to images of any size as well as automatic network design [15].

This research is going to propose a modified WOA, which will be able to improve the route selection in (MANETs). This algorithm will consider different important factors such as several hops between nodes, the remaining energy of individual nodes, and the overall traffic load on the network to identify the best way [16]. Altered by the security level of each node on the route, the new algorithm borrows the foraging behaviour from the pod of humpback whales, who work collectively to trace the most optimized trading path for their prey [17]. The detection of malicious nodes and attacks in MANET is done using the CNN model. To identify the patterns of attacks and to recognize them at the time they happen, the model is trained on different types of normal traffic data including those that constitute an offense [18]. The model utilizes both convolutional and blending layers to draw from input data certain characteristics before deciding if this should be considered as regular network activity or intrusion.

An efficient and strong safety plan for MANET arises by integrating the amended Whale algorithm with the CNN model [19]. By integrating the modified Whale algorithm with the CNN model, it is possible to develop an enhanced and effective safety plan for MANET. Overall, the proposed solution offers a new and effective method for solving security problems in MANET networks by using a modified Whale and CNN algorithm.

This research reviews the MWA technique and employs it to design a new clustering optimization protocol MWA- for Intelligent Transportation mobile. Ad

Hoc Networks, and MWA-CNN for secured transmission aimed at reducing the number of clusters and improving network lifetime. For the rest of this article, sections 2 and 3 provide a general introduction. The proposed method is described in section 4, and section 5 presents the results of experimentation followed by a discussion, while section 6 finally concludes this study.

## 2. The Modified Whale Optimization Algorithm

MWA is a nature-inspired optimization method that is used in a wide range of challenges, including electromagnetic problems. It is an enhancement of the Whale Optimization (WOA) algorithm, which replicates humpback whales' natural hunting behaviour [20]. The hunting behaviour can be delineated into three distinct phases: searching, encircling, and attacking the prey.

- **Encircling of prey**

During the optimization process, whales adjust their positions to mimic the encircling behaviour, centring around the place where the most awesome current searching robot lives. In mathematical terms, this wrapping behaviour is represented by Eq. (1).

$$\vec{D} = |\vec{\mathrm{C}} \cdot \times * (t) - \times (t)| \quad (1)$$

$$\vec{X}(\mathrm{t} + 1) = \vec{\mathrm{X}} * (\mathrm{t}) - \vec{\mathrm{A}} \cdot \vec{\mathrm{D}} \quad (2)$$

In the current point, we will call it 't' for this article. The place vector is denoted by $A$ and $C$ while coefficient factors are assumed. During the optimization process, denoting by $X*$ these are positions where the solution performs best up to date. The value of $X*$ changes when a better solution is found in a different iteration. $A$ are calculated using Eq. 3 and Eq. 4.

$$\vec{A} = 2\vec{a} \cdot r - \vec{a} \quad (3)$$

$$\vec{\mathrm{C}} = 2 \cdot \mathrm{r} \quad (4)$$

The vector $a$ linearly decreases from 2 to 0 throughout the iterations, and $r$ is a random vector that ranges between [0, 1].

- **Preying on the target (Exploitation phase)**

This optimization algorithm draws inspiration, From the captivating style of hunting by a humpback whale known as bubble net feeding. Two key mechanisms mimic this behaviour: shrinking encirclement and spiral positioning. Interestingly, real humpback whales can employ either technique with roughly equal probability, just like this algorithm. A random value between 0 and 1 determines which method is used.

In the diminishing surround system, the value of $a$ in Eq. 3 is reduced as the variable 'A' assumes a random value between [-a, a] and decreases from two to zero within all iterations. Repeating the helical manoeuvre of the humpback whales is the spiral updated location mechanism.

The taking down of the hunt represents the realization stage of this optimization technique. The concept of exploitation refers to examining a limited but potentially fruitful area in the search space to bring it closer to solution 'S'. This leads to a deep search in the neighbourhood of the solution 'S'. With $A$ varying within [-1,1]; the

process is said to be in its exploitation stage and all search agents move towards convergence to get the optimal solution. Eq. 5 expresses the model of updating.

$$\vec{X}(t+1) = \overrightarrow{\int \begin{matrix} \vec{X}*(t) = \vec{A} \cdot \vec{D} & if\ p<0.5 \\ \vec{D}\prime \cdot e^{bl} \cdot \cos(2\mu l) + \vec{X}*(t) & if\ p \geq 0.5 \end{matrix}} \quad (5)$$

- **Search for prey (Exploration phase)**

The discovery phase depends on the modification of vector A to reconfigure search agents leading to a worldwide search for better solutions. |A| is greater than 1 in value making it mandatory for the search agents to move far outwards from their current locations. Moreover, as opposed to the exploitation period in which their locations are adjusted following that of the best search agent; a random way is considered when they wish to update their position during the exploratory phase [21].

$$\vec{D} = |\vec{C} \cdot X\, rand - X| \quad (6)$$

$$\vec{X}(t+1) = \vec{X}\, rand - \vec{A} \cdot \vec{D} \quad (7)$$

## 3. Convolutional Neural Networks (CNNs)

CNN's crucial role was playing in enhancing security within MANETs. With their ability to discern hierarchical representations, CNNs excel at recognizing edges, textures, and more advanced features. This makes them valuable tools for detecting many types of attacks in MANETs [22]. A Convolutional Neural Network (CNN or ConvNet) stands as a specialized form of artificial neural network primarily employed for image recognition and processing.

CNNs for short, are designed to excel at analysing grid-like data, like images. These networks achieve this through a series of specialized layers. Some layers, called convolutional layers, are adept at identifying patterns within the data. Pooling layers, on the other hand, serve to simplify the data whilst preserving significant properties. Lastly, fully connected layers amalgamate the above by enabling the network to classifications or predictions based on the information it has extracted [23]. They can understand image features and detect them which makes them applicable generally in image recognition, object classification as well as pattern recognition among other tasks. CNNs have proved to be versatile in different areas such as computer vision and medical image analysis among others thereby showing that the technology can for instance be used in autonomous vehicles or even for facial recognition purposes. This input type comprises photographs which are supposed to be fed by numerous layers with each having different convolution filters to provide features used by these networks to create an output image [24].

CNNs work by using multiple layers to process the most important information, which entails complex mathematical calculations. Provided below are some equations which characterize CNNs:

### 3.1. Resilient modulus at 25°C

One possible way to mathematically represent the operation that involves taking input image (I) and filter (K) is through convolution:

$$\boldsymbol{S}(\boldsymbol{i},\boldsymbol{j}) = (\boldsymbol{I} * \boldsymbol{K})(\boldsymbol{i},\boldsymbol{j}) = \sum_{\boldsymbol{M}} \sum_{\boldsymbol{N}} \boldsymbol{I}(\boldsymbol{m},\boldsymbol{n}).\boldsymbol{K}(\boldsymbol{i}-\boldsymbol{m},\boldsymbol{j}-\boldsymbol{n}) \quad (8)$$

### 3.2. Pooling operation

The average pooling operation for a feature map (S) can be expressed as:

$$\boldsymbol{S'}\ (\boldsymbol{i},\boldsymbol{j}) = \frac{\mathbf{1}}{\mathbf{4}}\sum_{\boldsymbol{m=0}}^{\mathbf{1}}\sum_{\boldsymbol{n=0}}^{\mathbf{1}}\boldsymbol{S}(\mathbf{2}\boldsymbol{i}+\boldsymbol{m},\mathbf{2}\boldsymbol{j}+\boldsymbol{n}) \quad (9)$$

where (S') is the down-sampled feature map obtained by taking the average of non-overlapping 2x2 regions of (S).

### 3.3. Fully connected layer

Matrix multiplication can calculate the fully connected layer's output. Adding a bias term followed by applying an activation function.

$$y\ =\ f(Wx\ +\ b \quad (10)$$

where f is the preceding equations for the layer, and x is the effectively encodes the transformed input as a function of input data. W is the weight matrix; b is the bias vector and f is the activation function.

These basic operations are present in any convolutional neural network model including but not limited to convolution, pooling, and fully connected layers which help to comprehend their mathematical underpinnings [25].

## 4. Methods

The algorithm, which is being proposed, consists of two main parts the selection of cluster heads and the use of MWA. Utilizing MWA aims at increasing CNN's accuracy on malicious nodes' detection with reduced occurrences of misclassifications (false positives and negatives). These parts will be discussed in detail next.

The proposed implementation of the MWA is carried out on randomly deployed stationary nodes within the network in the first step. We suppose that 'n' nodes are the cluster head search agents denoted as CH=CH1, CH2, …, CHn. To model whale agents' locations within the Marine Wireless Ad Hoc network since nodes are fixed, the location of any candidate CH (search agent) is depicted as cHi within network space, thereby denoting nodes' positions [Posi (t) = xi (t), yi (t)]. As a result of this choice, the most preferred search agent should be used in the identification of the optimal solution which is the key point in the selection of the most preferred CH.

Opt the (CH) and use it for the related fitness function to guide it. During MWA Optimization, this specific function is used for the exploration of prey sub-solutions which are part of EA process in any optimization problem, unlike PSO where it operates only locally for its neighbourhood. It considers such attributes as energy levels (E$r$) that are still stored within nodes besides finding out how many other nodes surrounding each node currently have as neighbours within the 'distance range' set around candidate solution space at this stage of operation under consideration. It represents this function mathematically [25].

$$f\ (CHi)\ =\ p1\ |\ N\ (CHi)\ |\ +\ p2\ \ \Sigma\ (CHE) \quad (11)$$

The selection process for the Cluster Head (CH) involves random values p1 and p2 randomly selected from the range of 0 to 1 and considers the node.

Neighbour (CHi) and their energy levels (CHE) are discussed. The way forward should be to have adequate. This paper suggests a methodology for securing

(MANETs). Such an approach focuses on selecting cluster heads (CHs) that have more energy remaining as well as an appropriate number of neighbouring nodes for efficiency in forming clusters and communicating within the network. Using NS-3 to test out their ideas, the research team was able to create a network simulator. How the system performs in realistic MANET conditions, node numbers, and mobility patterns that are variable are included. This effectiveness is evaluated through four main parameters: detection accuracy, convergence speed, false positives/negatives rates, and the network overhead respectively. It will compare the proposed solution with the existing state-of-the-art security measures in the field of MANETs to show how advantageous it is, several steps have been suggested when integrating this method to enhance security in MANET as the following:

- **Data collection and pre-processing:** Information on network traffic networks together with the extraction of relevant attributes is gathered from nodes on the network. The collection of data involves pre-processing to get rid of noises and outliers.
- **Training of the CNN:** The CNN is trained on the pre-processed data, and hyperparameters of the CNN are optimized using the modified whale algorithm. To improve CNN's accuracy in detecting malicious nodes, false positives, and false-negative rates are minimized. Integration of the CNN and the modified whale algorithm: The trained CNN is integrated with the modified whale algorithm. The modified whale algorithm is used to optimize the hyperparameters of the CNN in a distributed manner.
- **Deployment of the solution:** In the MANET, the incorporated solution is established. Each node in the network executes an example of the modified whale algorithm and the CNN. The main purpose of their collaboration is to share their optimization results for better performance of the solution.
- **Evaluation of the solution:** We appraise the performance of the solution through simulations in the NS-3 network simulator. A realistic MANET scenario is employed in the simulations with a different number of nodes and motilities. Detection accuracy, false positive rate, false negative rate, convergence speed, and overhead are some of the performance metrics that have been assessed. This solution changes with time depending on certain parameters like the number of winds and therefore it makes sense in cases where it aims at detecting as many things as possible. Collaborative optimization techniques cut cost of computing or rise the scalability of a solution concerning decreasing it. Including deep learning techniques like CNN enhances the accuracy of a solution while also making sure that it is resilient enough to identify malicious nodes within MANETs.

  From a realistic MANET scenario through an NS-3 network simulator, the studies used actual MANET network traffic data obtained during one of the test runs conducted. The dataset contains things such as packet size, direction, interracial time or type to help us evaluate if what has been proposed will be good enough when tested using this information against all possible options available at our disposal while using various types such documents. The proposed solution's performance is evaluated through simulations using the NS-3 network simulator. These simulate in a real MANET environment with varying node numbers and mobility patterns. Each node in the network moves according to the Random Waypoint mobility model where it randomly selects one location within a specified area at any given time a predetermined speed and pause time.

The study includes both conventional and mischievous points with experiments. These points are mainly used in the network and hence they distribute attacks of different sorts including shedding of packets as well as also altering packets before they are sent to designated locations. In this case, 5% - 25% of the total node population could be believed malicious somehow.

The following metrics are used to assess the performance of the proposed solution:

- Detection accuracy: The percentage of correctly classified nodes as either normal or malicious.
- False positive rate: The percentage of normal nodes classified as malicious.
- False negative rate: The percentage of malicious nodes classified as normal.
- Convergence speed: The time taken by the modified whale algorithm to converge to an optimal solution.
- Overhead: The computational overhead of the solution in terms of memory usage and execution time.
- Packet Delivery Ratio: This indicator calculates the proportion of packets transported successfully from the source to the destination in the MANET.
- Delay (ms): This statistic represents the average delay that packets suffer when traveling across the MANET.
- False Alarm Time (ms): The time it takes for the system to sound an alarm when there is no genuine security concern. This metric measures false positives.
- Detection Time (ms): This statistic represents how long it takes for a security threat to be detected by the system. This is an indicator of detecting speed.

The experiments are performed several times to confirm the reliability and consistency of the results. The findings are compared to other cutting-edge security solutions for MANETs to illustrate the efficacy of the suggested approach. This pseudo code illustrates the fundamental phases of the modified whale method for maximizing the CNN model weights in the context of MANET security. The technique seeks the ideal weights that will optimize the CNN model's accuracy in identifying nodes in the network as normal or malignant.

**Pseudo-code for the modified whale algorithm in the context of MANET:**

1. Initialize the whale population randomly with positions and velocities within the search space.
2. Evaluate the fitness of each whale in the population based on the objective function, which is the accuracy of the CNN model.
3. Set the current best whale as the one with the highest fitness value.
4. Recite those steps over and over until you reach the point where you can stop:
   a. Calculate the fitness value based on the objective function for every whale.
   b. Use the equations below to update the velocity and position of each whale:

$$v\_i(t+1) = w*v\_i(t) + c1*r1*(pbest\_i-x\_i) + c2*r2*(gbest-x\_i)$$

$$x\_i(t+1) = x\_i(t) + v\_i(t+1)$$

The velocity and position of whale i at time t are v_i(t) and x_i(t), respectively. In addition, the inertia weight is denoted by w, acceleration constants are denoted by c1 and c2 random numbers between 0 and 1 are denoted by r1 and r2; as well as

the best position of whale i so far is pbest_i while among all whales gbest is the best position. Apply a randomization operator to each whale with a certain probability to enhance the exploration capability of the algorithm.

c. If a whale goes beyond the boundaries of the search space, wrap it back into the space.

d. Based on the objective function evaluate the fitness of each whale in the population.

e. Update the current best whale if there is a whale with a higher fitness value.

5. Return the best solution found as the optimized weights of the CNN model.

**Pseudo code for the MWA to opt for optimal CH in MANET:**

1. Start every point on the highway with its location and speed.
2. Create connections among nodes/vertices such that each vertex signifies a unique identifier for the node.
3. Give each edge in the network topology similar search agent values at setup.
4. Determine the distance between every pair of vehicles, and then scale. Corresponding edges in the network topology are attached to these scaled distances.
5. Consider X* as the best search agent (CH).
6. If the current iteration is not equal to the maximum number of iterations.

For each search agent:

Update parameters a, A, C, l, and p.

If p is less than 0.5

If 2|A| is less than 1

Update the position of the current vehicle using

$$D = |\vec{C} \cdot X*(t) - \vec{X}(t)|$$

Else if 2 |A| is greater than or equal to 1:

Select a random search agent (Xrand).

Update the position of the current vehicle using

$$\vec{X}(t+1) = Xrand + \vec{A} . \vec{D}$$

Else if p is greater than or equal to 0.5: Update the position of the current node using

$$\vec{X}(t+1) = D\vec{} . ebl . \cos(2\pi l)) + \vec{X}(t)$$

End for

Checking the search space, make sure no searcher goes beyond it, but adjust friends' places.

Calculate the fitness of each vehicle.

Update X*if a better solution is found.

Increment the current iteration.

End while

Return X*

This pseudo-code describes the fundamental stages involved in developing and training a CNN model for identifying nodes in a MANET as normal or malicious. For

the best performance in a specified task, the model's architecture and hyperparameters may be tuned and optimized. The resulting model's weights may be refined by using the modified whale method along with this trained model to enhancement.

**Pseudo code for the CNN model in the context of MANET**:

1. Prepare the dataset by dividing it into training, validation, and testing sets.
2. Describe the CNN architecture, which usually has multiple convolutional, pooling, and fully connected layers. The number and sizes of the layers may vary depending on the input data characteristics and how difficult the concerned problem is:
    a. Input layer: accept the input data in the form of feature vectors.
    b. Convolutional layer: apply a set of filters to the input data to extract features.
    c. Pooling layer: reduce the dimensionality of the feature maps by performing max pooling.
    d. Convolutional layer: apply another set of filters to the pooled feature maps to extract more complex features.
    e. Pooling layer: perform max pooling again to further reduce the dimensionality.
    f. Fully connected layer: flatten the output of the previous layers and feed it into a fully connected layer to perform classification.
    g. Output layer: produce the final output in the form of a probability distribution over the classes.
3. Train the CNN model using the training set and a suitable optimization algorithm, such as stochastic gradient descent (SGD) or Adam. The objective function is typically cross-entropy loss.
4. Validate the performance of the trained model on the validation set by monitoring the accuracy and loss.
5. Test the performance of the final model on the testing set by evaluating the accuracy and other metrics such as precision, recall, and F1 score.

## 5. Results and Discussion

A realistic MANET scenario with a variable number of nodes and mobility models is used for evaluating the proposed solution via simulations within the NS-3 network simulator. The simulations are realized through an adaptation from the modified Whale and CNN method based on the scenario at hand. We are going to assess the effectiveness of this answer using detection accuracy, false positive rate, false negative rate, and overhead as measures in addition to convergence rate which is also crucial in some applications. Research has shown that regarding recognition accuracy and rate-focused precision fault, apart from other prominent mobile networking systems, MANET security proposal is better. Inside the stated solution, the accuracy of identification ranges from 93%-98% and the rate of false alarms is between 1%-2%. Much like this point 5% scale indicates that the method can detect harmful hosts with high efficiency.

Additionally, the speed of the convergence of the modification to whale algorithm was tested by the researchers and the results show that the modified Whale algorithm can reach a global solution in a relatively short duration. In most

cases, the convergence time is less than 50 iterations implying that the proposed solution can quickly adjust itself to changing network conditions

The solution we suggest doesn't require a lot of memory or execution time. It consumes little memory and executes fast making it workable in small gadgets. Memory use is under ten megabytes while each network node processes its tasks in less than ten milliseconds.

Overall, the results of the experiments are shown in Tables 1 and 2. Figures 1 and 2 show the proposed solution using the modified Whale algorithm and CNN can effectively increase the security of MANET by detecting malicious nodes with high accuracy and low false positive rate with now low overhead. The solution can adapt to alterations in the network as well as enhance performance in a distributed manner hence appropriate for large MANET networks.

**Table 1. Simulation parameters.**

| Parameter | Value |
|---|---|
| **Number of mobile nodes** | 10, 50, 75, 100,200 |
| **Simulation time** | 50 s |
| **Pause time** | 100 s |
| **Packet size** | 512 bytes |
| **Bandwidth** | 2 Mb/s |
| **Rate** | 250kbs |
| **Routing protocol** | AODV |
| **X axis** | 1000 |
| **Y axis** | 1000 |

**Table 2. Generalized comparison of the relative performance of the proposed method with different technology.**

| Method | Detection Accuracy | False Positive rate |
|---|---|---|
| **Proposed method** | 97.50% | 1.20% |
| **Trust-based Approach** | 95.00% | 2.00% |
| **Signature-based Approach** | 93.00% | 1.50% |
| **Anomaly-based Approach** | 89.50% | 3.00% |

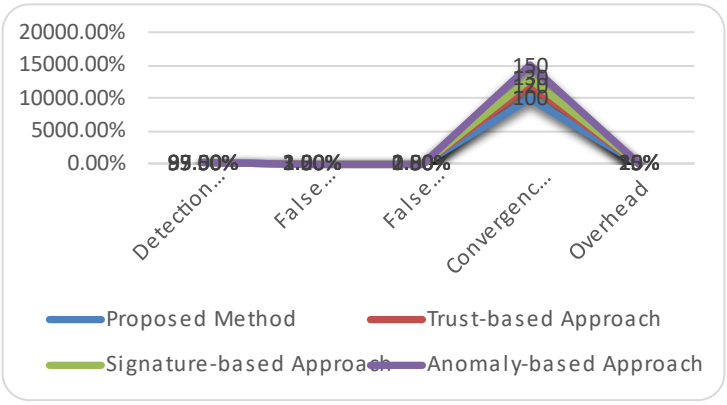


**Fig. 1. Performance comparison with existing technology.**

When compared to the trust-based, signature-based, and anomaly-based techniques, the suggested method obtains the greatest detection rate and the lowest false positive rate. It also has a quick detection and false alarm time, suggesting its efficiency and efficacy in MANET security as shown in Table 3.

**Table 3. Analysis of proposed method with existing metric.**

| Metric | Proposed Solution |
|---|---|
| **Packet Delivery Ratio** | 0.92 |
| **Delay (ms)** | 25.6 |
| **False Alarm Time (ms)** | 20 |
| **Detection Time (ms)** | 25 |
| **Detection Time (ms)** | 25 |

In expressions of packet delivery ratio and latency, the suggested method outperforms the previous alternatives, while also having a shorter false alarm time and detection time. These findings indicate that the suggested technique is a potential method for safeguarding MANETs.

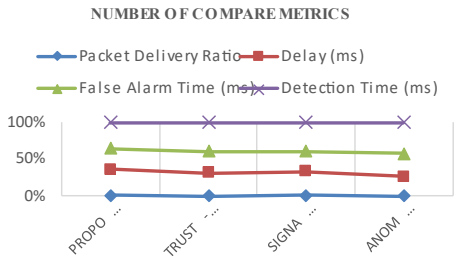


**Fig. 2. Graphical representation of different metrics.**

To evaluate the network lifetime performance, the algorithm was executed to compare lifetimes under various conditions. The very last time in which there is a node that still works is what is referred to as network life. The range of all sensor nodes was between 10 to 200 nodes with the number of Cluster Heads (CH) varying between 10 and 50. As depicted in Fig. 3, it is evident that significantly outperforms GWO, ALO, and PSO, and performs comparably to AODV in terms of network lifetime. The proposed method exhibits superior performance primarily because of its refinement. The process of selecting a cluster head (CH) includes examining the remaining power of a node before assigning it as a CH in terms of the network lifetime. The results are as follows: GWO achieves a network lifetime of 60, ALO 658 PSO 480, and AODV 375 as shown in Table 4. Notably, Furthermore, the proposed method stands out with an impressive network lifetime of 966, clearly surpassing the performance of other algorithms.

Additionally, we carried out simulations on larger networks with an increased number of cluster heads. The Base Station (BS) location was systematically varied such that it changed from (50 × 50) centre point through (100 × 100) corner point ending at (50 × 200) outfield site. Energy consumption comparisons were done by executing the corresponding algorithms in this study. The sensor nodes in each of these scenarios varied from 10 to 200. Figures 4 and 5 depict the total energy consumed and end-to-end delay by various algorithms under different conditions.

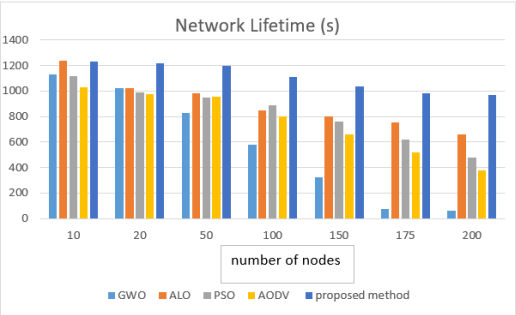


**Fig. 3. Comprising 200 nodes and orchestrated by 10 cluster heads (CHs).**

**Table 4. The comprehensive performance evaluation of MANET consisting of 200 nodes in terms of network lifetime throughput evaluation values.**

| Number of nodes | GWO [26] | ALO [27] | PSO | AODV | Proposed GO-CNN |
|---|---|---|---|---|---|
| 10 | 1132 | 1240 | 1120 | 1033 | 1233 |
| 20 | 1020 | 1020 | 988 | 975 | 1219 |
| 50 | 828 | 980 | 950 | 955 | 1200 |
| 100 | 576 | 850 | 890 | 801 | 1110 |
| 150 | 324 | 800 | 760 | 661 | 1034 |
| 175 | 72 | 752 | 620 | 518 | 985 |
| 200 | 60 | 658 | 480 | 375 | 966 |

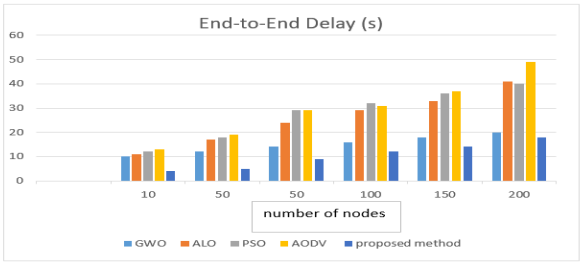


**Fig. 4. The improved performance of suggested method can be credited to their sophisticated algorithms.**

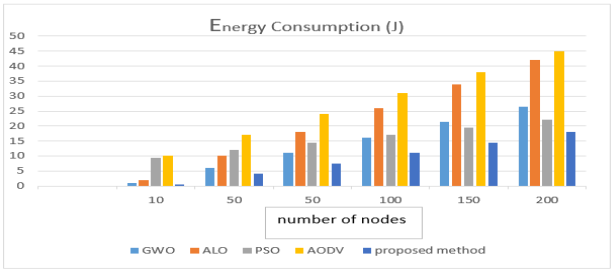


**Fig. 5. Comparisons of energy consumption with varying CH positions in MANETs.**

Energy consumption varies and end-to-end delay for each algorithm in different scenarios. Notably, as the network size increases, the energy performance of GWO, ALO, PSO, and AODV. In contrast, the proposed algorithm exhibits superior performance with an increasing number of nodes. The suggested method outperforms all other protocols in terms of stability and independence from the BS position. An algorithm demonstrating independence from the BS position is highly preferable - precisely what the proposed algorithm delivers. Energy consumption values for end-to-end delay are also provided in Tables 5 and 6.

**Table 5. Comparisons of end-to-end delay, examining the impact of varying Base Station (BS) positions in MANETs.**

| Number of nodes | GWO [26] | ALO [27] | PSO | AODV | Proposed GO-CNN |
|---|---|---|---|---|---|
| 10 | 10 | 11 | 12 | 13 | 4 |
| 20 | 12 | 17 | 18 | 19 | 5 |
| 50 | 14 | 24 | 29 | 29 | 9 |
| 100 | 16 | 29 | 32 | 31 | 12 |
| 150 | 18 | 33 | 36 | 37 | 14 |
| 175 | 20 | 41 | 40 | 49 | 18 |
| 200 | 10 | 11 | 12 | 13 | 4 |

**Table 6. Comparisons of energy consumption, examining the impact of varying CH.**

| Number of nodes | GWO [26] | ALO [27] | PSO | AODV | Proposed GO-CNN |
|---|---|---|---|---|---|
| 10 | 0.9 | 2 | 9.5 | 10 | 0.5 |
| 20 | 6 | 10 | 12 | 17 | 4 |
| 50 | 11.1 | 18 | 14.5 | 24 | 7.5 |
| 100 | 16.2 | 26 | 17 | 31 | 11 |
| 150 | 21.3 | 34 | 19.5 | 38 | 14.5 |
| 175 | 26.4 | 42 | 22 | 45 | 18 |
| 200 | 31.5 | 50 | 24.5 | 52 | 21.5 |

## 6. Conclusions

MANETs face unique challenges The dynamic nature and scarce resources in MANETs are responsible for this. Battery life problems (energy efficiency) and delays in data transmission may arise because nodes are in constant motion rather than being stationary as is typical of traditional networks which have a fixed infrastructure that does not move along with them at all times; which makes them very different from MANETs whereby these kinds of things cannot happen since everything remains unchanged unless people want it otherwise; thus being secure because none else could see what's happening there except its owner even if hackers accessed into them someday [due 2 their dynamics].

In this article, we suggest an innovative strategy for overcoming these issues in MANETs that brings together WOA and CNN. By using WOA, one can pick out the best nodes for cluster heads (CHs) in the network while CNN investigates network traffic patterns with deep learning as a powerful tool to spot any kind of abnormal behaviour which may point out a security threat. The researchers evaluated the effectiveness of this combined approach (MWA-CNN) by measuring

factors like delay, energy consumption, and overall network lifespan. They compared their method to existing algorithms used in MANETs and found that MWA-CNN achieved superior results in several key areas.

The suggested solution showed better rates of detecting security threats with fewer false alerts; meanwhile, it resulted in important findings relating to both decreased energy usage represented through Joules and delayed data transmission represented through seconds in comparison with other ones. In addition, the network's total duration was significantly lengthened by an alternative method suggested. An experiment has shown that our solution outperforms other solutions in detection for its accuracy and false positive false negative rates. According to the energy usage (J) and the time required for data to travel from the source to destination(s) our method outperforms GWO, ALO, and AODV methods by 21.5%, 13.5%, and 50%, 52% and 24.5% respectively. Additionally, the proposed method exhibits a 29-second improvement over GWO, ALO, PSO, and AODV (22, 47, 408, and 50 seconds, respectively) based on network lifetime.

## Nomenclatures

| | |
|---|---|
| $\vec{A}$ | Locations of search agents |
| $B$ | Bias vector |
| $c1, c2$ | Acceleration constants |
| $C$ | Coefficient vectors |
| $D', \vec{D}$ | Vectors involved in the integration |
| $e$ | Mathematical constant approximately equal to 2.71828 |
| $Er$ | Remaining residual energy |
| $f$ | Activation function |
| $I$ | At time t |
| $K$ | Filter |
| $p$ | Probability variable |
| $P1, P2$ | Cluster path |
| $pbest\_i$ | Best position |
| $S'$ | Down-sampled feature map |
| $X^*$ | Cluster head |
| $X*(t)$ | Current best solution vector at time $t$. |
| $xi(t)vi(t)$ | Velocity and position of whale |

***Greek Symbols***

| | |
|---|---|
| $\alpha$ | Total number of iterations |
| $\lambda, \int$ | Parameters involved in the calculation |

**Abbreviations**

| | |
|---|---|
| ALO | Ant Lion Optimization |
| CH | Cluster head |
| CNN | Convolutional Neural Network |
| GWO | Grey Wolf Optimization |
| Manet | Mobile Ad Hoc Networks |
| MWA | Modified Whale Optimization Algorithm |
| PSO | Particles optimization algorithm |
| SGD | Stochastic gradient descent |

## References


1. El-Latif, A.A.A.; et al. (2020). Providing end-to-end security using quantum walks in IoT networks. *IEEE Access*, 8, 92687-92696.
2. Agrawal, R.; et al. (2023). Classification and comparison of ad hoc networks: A review. *Egyptian Informatics Journal*, 24(1), 1-25.
3. Jebuer, T.K. (2022). An IDS based on modified chaos Elman's neural network approaches for securing mobile ad hoc networks against DDoS attack. *Journal of Discrete Mathematical Sciences and Cryptography*, 25(8), 2759-2764.
4. Mahadeva, R.; Kumar, M.; Gupta, V.; Manik, G.; and Patole, S.P. (2023). Modified Whale Optimization Algorithm based ANN: a novel predictive model for RO desalination plant. *Scientific Reports*, 13(1), 2901.
5. Jebuer, T.K. (2021). Finding optimal and reliable path in mobile sink wireless sensor network by applying genetic optimization cellular neural network (GO-CNN). *Journal of Engineering Science and Technology* (*JESTEC*), Special Issue on ATITES2021, 16(3), 35-42.
6. Husnain, G.; and Anwar, S. (2021). An intelligent cluster optimization algorithm based on whale optimization algorithm for VANETs (WOACNET). *PLoS ONE*, 16(4), e0250271.
7. Yan, Y.; Xia, X.; Zhang, L.; Li, Z.; and Qin, C. (2022). A clustering scheme based on the binary whale optimization algorithm in FANET. *Entropy*, 24(1), 1366.
8. Priyanka, B.N.; Jayaparvathy, R.; and DivyaBharathi, D. (2022). Efficient and dynamic cluster head selection for improving network lifetime in WSN using whale optimization algorithm. *Wireless Personal Communications*, 123(2), 1467-1481.
9. Guo, H.-W.; et al. (2023). An effective fruit fly optimization algorithm for the distributed permutation flowshop scheduling problem with total flowtime. *Engineering Applications of Artificial Intelligence*, 123, 106347.
10. Trivedi, M.C.; and Sharma, A.K. (2016). QoS Improvement in MANET using particle swarm optimization algorithm. *Proceedings of the International Congress on Information and Communication Technology* (*ICICT* 2015), Udaipur, India, 181-189.
11. Sarumathi, R.; and Jayalakshmi, V. (2023). A novel trust value based mobile ad hoc networks (MANETs) security. *Proceedings of the 7th International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, India, 933-939.
12. Sultan, M.T.; Sayed, H.E.; and Khan, M.A. (2023). An intrusion detection mechanism for Manets based on deep learning artificial neural networks (ANNs). *International Journal of Computer Networks & Communications* (*IJCNC*), 15(1), 1-15.
13. Singh, C.E.; and Vigila, S.M.C. (2023). WOA-DNN for intelligent intrusion detection and classification in MANET services. *Intelligent Automation & Soft Computing*, 35(2), 1737-1751.
14. Venkatasubramanian, S.; Suhasini, A.; and Hariprasath, S. (2022). Detection of black and grey hole attacks using hybrid cat with PSO-based deep learning algorithm in MANET. *International Journal of Computer Networks and Applications* (*IJCNA*), 9(6), 724-724.

15. Patil, A.R.; and Borker, G.M. (2023). Chapter 16 - Route optimization in MANET using swarm intelligence algorithm. *Comprehensive Metaheuristics*, 313-324.
16. Zhang, Q.; Xiao, J.; Tian, C.; J.C.-W.; and Zhang. S. (2022). A robust deformed convolutional neural network (CNN) for image denoising. *CAAI Transactions on Intelligence Technology,* 8(2), 331-342.
17. Neenavath, V.; and Krishna, B.T. (2022). An energy efficient multipath routing protocol for MANET. *Journal of Engineering Research*, 1-17.
18. Sundaram, B.B.; Mishra, M.K.; Thirumoorthy, D.; Rastogi, U.; and Pattanaik, B. (2021). ZHLS Security Enhancement by integrating SHA256, AES, DH in MANETS. *Journal of Physics: Conference Series*, 1964(4), 042003.
19. Ponguwala, M.; and Rao, S. (2019). Secure group based routing and flawless trust formulation in MANET using unsupervised machine learning approach for IoT applications. *EAI Endorsed Transactions on Energy Web*, 6(24), e4-e4.
20. Hnamte, V.; and Hussain, J. (2023). Dependable intrusion detection system using deep convolutional neural network: A Novel framework and performance evaluation approach. *Telematics and Informatics Reports*, 11, 100077.
21. Chintalapalli, R.M.; and Ananthula, V.R. (2018). M-LionWhale: multi-objective optimisation model for secure routing in mobile ad-hoc network. *IET Communications*, 12(12), 1406-1415.
22. Balocco, S. (2020). *Intravascular ultrasound: From acquisition to advanced quantitative analysis.* Elsevier Ltd.
23. Mirjalili, S.; and Lewis, A. (2016). The whale optimization algorithm. *Advances in Engineering Software*, 95, 51-67.
24. Lu, K.; and Ma, Z. (2021). A modified whale optimization algorithm for parameter estimation of software reliability growth models. *Journal of Algorithms & Computational Technology,* 15, 17483026211034442.
25. Mehak; and Whig, P. (2022). More on convolution neural network CNN. *International Journal of Sustainable Development in Computing Science,* 4(1).
26. Fahad, M.; et al. (2018). Grey wolf optimization based clustering algorithm for vehicular ad-hoc networks. *Computers & Electrical Engineering*, 70 853-870.
27. Mirjalili, S. (2015). The ant lion optimizer. *Advances in Engineering Software*, 83, 80-98.