Intelligent Multimedia Processing & Communication Systems Journal

IMPCSJ

J IMPCS (2025) 21: 35-46
DOI 10.71856/IMPCS.2025.1210713

Research Paper

Detecting Destructive Nodes with the Aim of Reducing Black Hole Attack Using Response Time Based on Machine Learning Model in Mobile Case Networks

Fatimah Jasim Mohammed [1], Azam Andalib[2*], Hossein Azgomi[3], Seyed Ali Sharifi[4]

1. Department of electrical and computer engineering, Urmia University, Urmia, Iran
2. Department of Computer Engineering, Ra.C., Islamic Azad University, Rasht, Iran * *Corresponding Author*, Azam.Andalib@iau.ac.ir
3. Department of Computer Engineering, Ra.C., Islamic Azad University, Rasht, Iran
4. Department of computer engineering, Bon.C., Islamic Azad University, Bonab, Iran

Article Info

Article history:
Received: 23 Jun 2025
Accepted: 2 Aug 2025
DOR:

Keywords:
Black Hole Attack,
Deep Learning,
Destructive Node,
Fuzzy Inference,
Mobile Case Networks,
Routing.

ABSTRACT

Mobile case networks, self-configurable, self-organized networks of mobile nodes that can move freely and independently in any direction without any restrictions, and use wireless links to communicate without relying on any specific, pre-designed infrastructure. These networks are widely used in applications such as military and disaster relief. However, due to their dynamism, lack of infrastructure, and lack of certificate authorization, they are vulnerable to a variety of attacks and security threats. One solution to provide security in these networks is to deploy intrusion detection systems (IDS). Black hole attacks are among the most common attacks in mobile case networks, which are discussed in this article in order to detect and isolate the black hole attack, a four-phase approach is proposed, in the first phase, clustering is done using the k-nearest neighbor algorithm (KNN), in the second phase, using the beta distribution, the confidence of each node and its remaining energy is calculated. Then, in the third phase, the cluster node is selected using fuzzy inference and finally, in the fourth phase, the response time is calculated based on the deep learning model. The simulation results show that the proposed approach provides better results with less routing overhead calculations and has improved parameters such as packet loss rate, operational throughput, packet delivery ratio, total network latency, and normal routing load compared to other methods.

I. Introduction

Mobile case networks are a self-configurable network without the use of any specific infrastructure. And the elements in it have complete autonomy and freedom to move in any direction. Therefore, the communication between the elements is often changing. In these networks, each node is equipped with a transmitter and a receiver to communicate with the rest of the nodes through radio waves in two ways: peer-to-peer and all-broadcast. These nodes have no knowledge of its connections due to the dynamic structure of the network, so in order to send information to other nodes, it is necessary to do the process of discovering and maintaining the path and through the rest of the nodes [1]. The nodes that play the role of the pathfinder move the data to the destination. However, the mobility of the nodes has caused the network to constantly change and different paths are created between them, so the traditional routing protocols of wired networks are not applicable in these networks. The first goal of routing protocols in mobile ad-hoc networks is to create the optimal route between the source and the destination with minimal overhead and minimum bandwidth consumption so that packets are delivered on time. These networks are used in military applications, relief and emergency operations, transportation, environmental protection, and space communications. Among the classification algorithms in datamining, the K-Nearest Neighbor or KNN algorithm is theoretically less complex and aims to place the closest values in a cluster. The algorithm is a sample-based learning method and tags a sample of data based on the nearest neighbor K and the similarity score of each node is used as the weight of the cluster of the neighboring node [2].

These networks are insecure due to the use of radio-based shared wireless media and lack of central control, and are always exposed to threats from internal and external attackers and exploiters, creating security challenges. Data encryption, access control, identity and authenticity recognition and management and intrusion detection are one of the methods of protection against external attacks. But these methods do not have the ability to meet the security requirements against internal attacks. Also, most of the intrusion detection methods used in infrastructure-based networks are not used in mobile case-by-case networks. This lack leads to the risk of identity theft and man-in-the-middle attack (MITM) [3,4].

As mentioned earlier, mobile ad-hoc networks due to their nature and characteristics such as the lack of static infrastructure (lack of access to centralized and integrated structures such as routers and the need for decentralized, distributed and interoperable security solutions of all network nodes), the use of wireless links (the absence of common layers of defense such as firewalls in wireless links allows the attacker to target from any direction without the need for physical access), node autonomy in movement (mobile nodes are difficult to track due to mobility and movement), and multi-step discussion (in most routing protocols, nodes act as pathfinders and packets have a number of steps) have specific requirements and security issues. So, to overcome these problems and protect these networks, an additional layer of defense called intrusion detection is used, which focuses on detecting malicious activity by malicious nodes. And it can be divided into two categories: anomaly detection (comparing users' normal behaviors with the data collected) and detecting suspicious activity as Potential intrusion that is transmitted to the system administrator) and exploit detection (comparing the known pattern of attacks in the system with the collected data and identifying the matching pattern as a possible intrusion). Malicious nodes are nodes that somehow compromise the accuracy of the amount of data in the network [5]. This degradation can be a lack of convergence or convergence to the wrong amount of data on the network. Therefore, the main issue is to detect nodes that do not behave under the defined protocol. There are a large number of attacks in mobile ad-hoc networks that reduce network performance, which is described in Table 1 of the information on some of these attacks.

TABLE I Different Types of Attacks in Mobile Ad-hoc Networks

Attack Name	Type of attack	Description of the attack
Gray cavity	Active	Stealing the identity of the main node along with its path by the malicious node and deleting all data
Sinkhole	Active	Attracting all nodes to the malicious node and providing them with information about the wrong path
Voyeurism	Disabled	Obtaining and Intercepting Confidential Information
wormhole	Active	Logging all the information by the malicious node and sending it to another destination
Byzantine	Active	Participation of intermediate nodes in attacks and turning them into destructive nodes
torrential	Active	Spreading a large number of fake packets to all network nodes by malicious nodes
Black Hole	Active	Pretending to have the best path and deleting all data
Counterfeiting	Active	Get node information by inserting your attribute by malicious nodes

As mentioned above, mobile ad-hoc networks are also very vulnerable to insider attacks. One effective way to

counter attacks within the network is through a trust management system. In this paper, the criteria of communication behavior, energy behavior, and data behavior have been used in combination to calculate the reliability of nodes. Since the calculation of the trust value of nodes depends on the quality of the communication, we have developed a beta-based trust and reputation evaluation system (BTRES) that includes five characteristics: loss rate, sending frequency, receiving frequency, we used power consumption rates and node power measurement by monitoring the behavior of network nodes to validate and evaluate their trust, which led to a reduction in the risks of insider attacks and increased information security [6]. Malicious nodes in mobile ad-hoc networks can disrupt the routing mechanism by launching denial-of-service (DoS) attacks or by generating fake messages, in which case intrusion detection acts as a second wall of defense and is very important in high-security networks [7]. One of the attacks that responds to all packets requesting a route and pretends to have the best path to the destination node and then eliminates all incoming packets is a black hole attack, which is one of the most dangerous attacks active in mobile ad-hoc networks. It can be carried out by a single attacking node (single black hole attacks) or by multiple attacking nodes (cooperative black hole attacks). occur in the network and spoof the serial number and the number of steps of a routing message, and by finding the path, eavesdrop or delete all packets passing through it [8]. In this paper, using the time required to generate the path request packet, an approach is presented to detect and prevent black hole attack by malicious nodes, which can provide better results with minimal computations and reduced routing overhead. This approach is based on the first step node Next is in the reverse path to calculate the response time when receiving the path request packet from the initiator node. After calculating the response time, if this time is less than the threshold value, the initiator node is considered as a black hole node and the separation process begins.

II. Related work

In [9,10], the authors used two types of techniques, including IDS and digital signature with the concept of prevention, to detect black hole attacks. The results presented by them show that in parameters such as packet delivery rate (PDR), latency, and routing overhead, relative improvement has been achieved. which provides the ability to transmit data securely and reliably under black hole attacks. In this approach, messages are divided into different paths and the homomorphic encryption scheme 1 is used to secure the message transmission. The results of the simulations show better performance in network throughput and packet delivery rate. In [11], a two-step secure and trust-based routing approach including information retrieval mechanism (identifying and maintaining data transmission) and transmission mechanism (secure route prediction) in mobile case networks is proposed. But in this approach, the energy consumption of the nodes is high. In [12], the authors proposed an approach to mitigate the effects of a black hole through the Detection and Conservation Technique (ABIP), in which the number of sequential sequences will be processed according to the threshold value. The high receiver sequence number is generated by nodes that generate false information. Their results show that the proposed approach reduces the attack of the black hole and increases the performance of the network in terms of the delivery rate is closed. In [13,14] an effective and secure validation mechanism for authenticating nodes using digital signatures in mobile ad-hoc networks is proposed, which performs better in terms of quantity, compute overhead, latency, and packet delivery rate. In addition to the attacks, a trust-based approach to authenticating mobile ad-hoc networks is explored and through node trust estimation processing, healthy nodes are separated from destructive nodes. In this approach, old dummy packages of the origin node are used to send to the destination node. In [15], the authors proposed the Multi-Black Hole Attack Detection (D-MBH) approach to detect a single, cooperative black hole attack by adding three elements. The first element is the request for an additional path, which is made public without an address. The second element is the threshold value that has the mean Destination Sequence Number (ADSN). The received malicious path requests are shown in it, and the third element is represented by creating two lists (BH & CBH lists). The blackhole list is updated when nodes, route response packets, and fake route request packets include non-existent target addresses. The list of common black hole nodes, which is used when calling the proposed DCBH (Common Attack Detection Black Hole) algorithm, begins when a node receives a path response from a node that has already been identified in the list of problem holes. In this case, the source node checks whether the next-step node (NHN) of the node that sends the path response is on the BH list. If the response is positive, the path response is considered as a destructive node. This approach reduces routing overhead and computational overhead but it does not cause an improvement in storage overhead. In [16] a solution is proposed to detect and eliminate black hole attacks in untimely stages of path discovery through a slight change in the path response packet by adding a bit of credit. For the validity value, which keeps the original AODV mechanism unchanged, the additional bitfield is set only by a node that has a legitimate path or destination node. But if the path response packet is generated by a black hole node, the credit bit will be null because the black hole's attack is known about the mechanism. Each intermediate node that receives the path response packet, checks whether the credit bit is set to it before sending it to the next step. Otherwise, that path responses the packets without inserting them into the path

table. Detecting and preventing a black hole attack before data transfer begins leads to reduced processing and memory requirements [17]. In order to increase the security of the AODV routing protocol, a new IDSNAODV approach to the detection of malicious nodes has been proposed, which has been improved by introducing some rules that allow the detection of malicious nodes. In this approach, a node that produces a route request packet with the highest number of sequences and the lowest number of jumps may be destructive. A node that receives a significant number of packets but only sends one packet may be malicious. And a node that receives packets but doesn't send them to its neighbors is considered a malicious node. This approach has increased operational throughput and reduced the number of abandoned and delayed packages.

Trust management systems are among the most effective methods to prevent insider attacks and include the trust model, trust management plan, and protocol optimization. The authors in the Validity-Based Framework include five sections: Direct Validation Evaluation, Indirect Validation Evaluation, Credit Synthesis, Transformation and Trust Node Behavior, which provides a complete assessment of the overall process of trusting nodes. Then, based on the Beta distribution and Bayesian formula, the Beta Validation System for Mobile Case Networks were proposed. In [18] Also, according to the number of packets received by the nodes, direct trust and recommendation trust are selectively computed and an efficient distributed trust (EDTM) model for mobile case networks is proposed. To calculate direct trust, communication trust, energy trust, and data trust during computation, as well as to improve the accuracy of recommendation trust, trust reliability were considered. In [19] Gaussian reliability and validity are proposed for the fading of multiple-input multi-output networks (MIMOs) and in it, based on the multivariate Gaussian distribution and Bayesian theorem and considering the effect of channel fading, the direct and indirect validity information of the combination and the value of the trust were calculated and could In [20] based on the previous network trust management system and some new measurements, an improved trust building and dynamic management framework for mobile case networks is proposed. In [21], the authors proposed credit-based clustering and auxiliary anchor node auditing against Byzantine attacks in mobile ad-hoc networks. Byzantine attack defense strategies have high computational complexity and require specific information and assumptions. In the new approach of elastic trust management based on time window based on beta distribution, it is proposed to analyze the behavior of the nodes at risk for a specific period of time It uses differential judgment and trend analysis to detect the abnormal validity value of nodes. In this approach, the control factor and time window are used to confirm and remove malicious nodes that can defend attacks with different timings. Using an adaptive fuzzy neural inference system is proposed to generate a fuzzy system (ANFIS). The next move was to configure the inference system and then use the genetic algorithm (GA) to optimize the initial framework. This network performed better than other methods despite black hole attacks.

III. Proposed Approach

In this paper, in order to detect and isolate black hole attacks in mobile case networks, a four-phase approach is proposed as shown in figure 1.

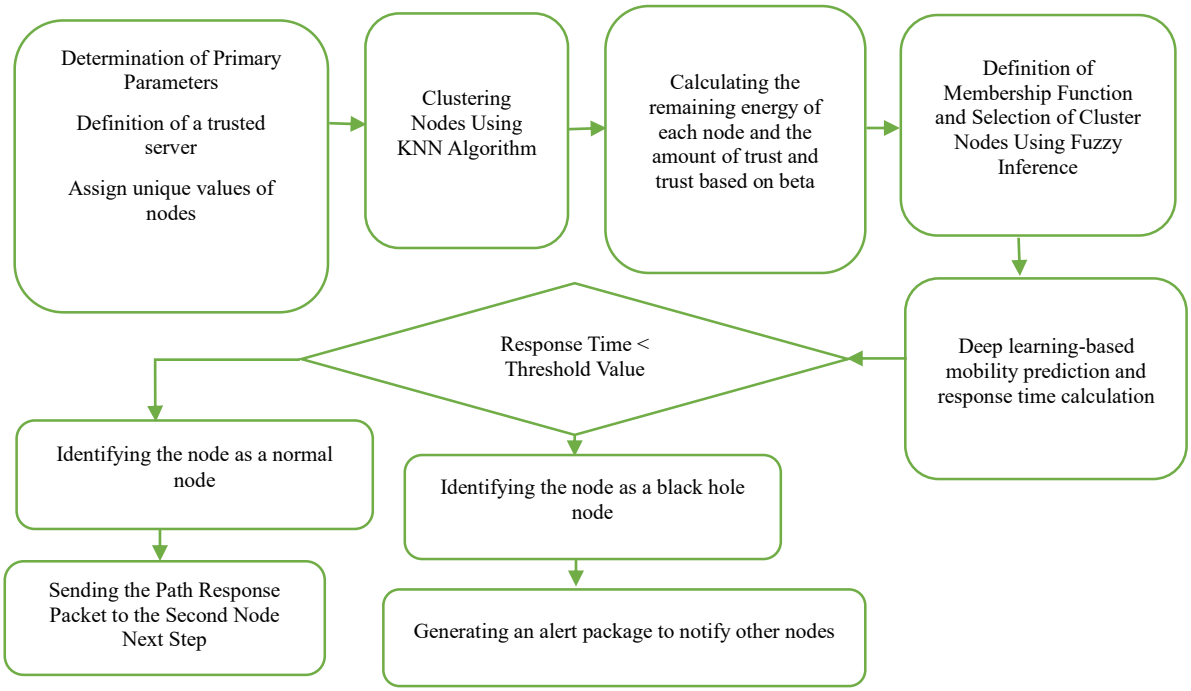

Fig. 1. Proposed Approach Flowchart

In the first phase, the K-algorithm of the nearest neighbor, which has less complexity, is used to place the closest values in a cluster. This algorithm is a sample-based learning method and labels a sample of data and the similarity score of each node is considered as the weight of the cluster. This weight is used to calculate the Euclidean distance of the nodes from each other according to the following equation and the clusters are formed.

$$d(x_i, x_j) = \sqrt{\sum_{i.j}(x_i - x_j)^2}$$

All the nodes in the network are stored in the multidimensional pattern space, and as soon as the new node enters the system, the KNN algorithm runs again and searches the template space for the existing nodes close to the new node and maps it to the appropriate cluster.

In the second phase, the remaining energy of each node and its level of trust in the surrounding nodes are calculated. In order to validate and evaluate trust, reduce the risks of internal attacks and increase information security, the trust and reputation assessment system based on the beta distribution includes the following features: loss rate, sending and receiving frequencies, energy consumption, etc. Node power is used by monitoring the behavior of network nodes. The beta distribution, defined by two parameters, α and β, is often used for random variables with a continuous value in the range [0, 1]. Considering that in mobile ad-hoc networks, nodes interact with each other and these interactions can have a positive or negative result, so each node can have normal or abnormal behaviors. α indicates the number of interactions with a positive outcome or normal behavior, and β indicates the number of interactions with a negative outcome or abnormal behavior. In order to correctly calculate the value of trust, three destructive nodes are considered: communication trust, energy trust, and data trust, which in relational trust, α and β indicate the number of cooperation and non-cooperation, respectively, in data trust, the number of normal data sequences and manipulated data sequences, respectively, and in Energy confidence is the number of times normal energy consumption and abnormal energy consumption, respectively. Therefore, to simulate the behavior of nodes according to the following relationship, the beta distribution can be used.

$$P(\sigma) = {Bin(\alpha+\beta,\alpha) * Beta(1,1)}/{\alpha+\beta+1} = Beta(\alpha+1,\beta+1)$$

As a result, to calculate the trust of each node, the following relationship is used, which is a number between 0 and 1.

$$Trst_{i,j} = E(R_{i,j}) = E(Beta(\alpha+1,\beta+1)) = {\alpha+1}/{\alpha+\beta+2}$$

The following steps are followed to calculate the total trust between nodes.

Calculating Communication Trust: If a malicious node attacks mobile ad-hoc networks, the number of non-cooperative connections increases. The need for trust, therefore, is a relational that is expressed by the following relationship.

$$CT = E(Beta(\alpha_c+1,\beta_c+1)) = {\alpha_c+1}/{\alpha_c+\beta_c+2}$$

where α_c the number of collaborative communications and the number of non-cooperative communications $\beta_c$that need to be counted over time.

Calculation of energy trust: The amount of energy consumption of nodes in the network is usually stable, but

the destructive nodes that carry out DoS or flooding carry out more energy than normal nodes. The amount of energy consumption per unit time is E_{cr}calculated from the following relationship.

$$E_{cr} = {|E_{t+\Delta t} - E_t|}/{\Delta t}$$

Where $E_{t+\Delta t}$ and E_t residual energy of each node is in time and respectively $t + \Delta t$ and t. The value obtained E_{cr} from the above relationship represents normal or abnormal energy consumption. With respect to the beta distribution, the energy confidence is calculated according to the following relationship.

$$ET = E(Beta(\alpha_e + 1, \beta_e + 1)) = {\alpha_e + 1}/{\alpha_e + \beta_e + 2}$$

where the α_e number of times you consume normal energy and the β_e number of times you consume abnormal energy at time is T.

Calculating Data Trust: In mobile case networks, the perceptual data by nodes in a given range are usually similar and follow a specific distribution, such as the Gaussian distribution. But if a malicious node is attacked, the sequence of perceptual data by it will be different compared to a normal node. Data trust is calculated from the following relation.

$$DT = E(Beta(\alpha_d + 1, \beta_d + 1)) = {\alpha_d + 1}/{\alpha_d + \beta_d + 2}$$

After calculating, communication trust (CT),energy trust (ET), and data trust (DT) are obtained directly according to the following relationship.

$$dir\_Trst = (w_1 * CT) + (w_2 * ET) + (w_3 * DT)$$

Where w_1, w_2 and w_3 in order the weight of communication trusts, energy and data $w_1 + w_2 + w_3 = 1$and.

The values of the weights depend on the values of communication, energy, and data trusts, in other words, if the values of the trusts are all greater or less than 0.5, the values of the weights will be equal to each other, so that the sum of all three weights is equal to 1. and if in the values of trusts, some values are less than 0.5 and some are greater than 0.5, the weights of trusts greater than 0.5 are considered to be 0 and the weight of the rest is allocated equally. If the value of any trust is less than 0.5, it means that there is an attack on it, and in calculating the overall trust, the values of the rest of the trusts are considered greater than 0.5, causing the attack to be not reflected in the network by the rest of the trusts with a value greater than 0.5.

Due to the dynamics of nodes and the topological structure of mobile case networks, the behavior of nodes may change in terms of communication, energy, and data [22, 23], so in order to accurately reflect the state of the network, it is necessary to update the trust values of the nodes dynamically. For this purpose, in this paper, a slippage time window that has several time slots has been used and in each time gap, an update has been made according to the relationship The following will take place.

$$int\_Trst(i+1)_{up} = \varphi_i int\_Trst(i) + \varphi_{i+1} int\_Trst(i+1)$$

where n is the number of time gaps, φ_i the value of the previous trust, andφ_{i+1} the value of the current trust.

According to the beta distribution, the validity of the nodes in terms of each other is calculated from the following relationship.

$$Rep_{i,j} = Beta(\alpha + 1, \beta + 1)$$

In order to determine the validity of each node, the results of the trust of other nodes in the desired node must be determined. In this way, each of the nodes within each cluster periodically sends its opinion to the cluster about the level of trust in each node, and the cluster node updates the value of the validity according to the following relationship.

$$Rep_x = \alpha_y T_{y\to x} + \alpha_k T_{k\to x} + \alpha_l T_{l\to x} + \ldots = \sum_{i=\{y,k,l,..\}}^{cnt} \alpha_i T_{i\to x}$$

where the Rep_x validity of the node, $T_{i\to x}$ the degree of trust of node i over node x, cnt is the total number of nodes that have commented on node x, the α_i weight factor of each comment and $\sum_{i=1}^{cnt} \alpha_i = 1$. The weight factor of each node is calculated according to the following relationship.

$$\alpha_i = Rep_i \Big/ \sum_{i=\{y,k,l,..\}}^{cnt} Rep_i$$

Cluster nodes use the validity values obtained from the above relationship to update and select new clusters. It also warns other nodes to be more careful in communicating with them by identifying the list of untrusted nodes and distributing them on the network.

In the third phase, with the help of fuzzy inference, which aims to draw an input to the output using fuzzy reasoning in the process, among the candidate nodes, the node with the most reliable neighbors at the desired energy level is selected as the cluster node. Fuzzy logic is able to make logical decisions in an environment of inaccuracy, uncertainty, and incomplete information. In fuzzy inference systems, after receiving the inputs and determining the degree of accuracy and weight, its output, which is a number between zero and one, determines the amount of membership in the fuzzy input set. Therefore, in this paper, due to the fact that energy is very important in mobile case networks, and also the boundary between normal and abnormal states is not well defined and security itself is ambiguous, therefore, in this phase, the residual energy and the level of trust of the nodes are considered as the inputs of the fuzzy system. The different outputs are aggregated in the fuzzy system and combined into a fuzzy set and the final decision is made. If the existing laws imply that a node is suspicious, then its suspicious level is calculated and an output called the suspicious level is created and the ID along with the suspicious amount is kept in it. The extent of dealing with

malicious nodes depends on the amount of suspiciousness it is, so if the amount of suspicion of the node is closer to the value of the threshold of destructiveness, the severity of the collision will be higher and if the amount of suspicion The farther the node is from the destructive threshold, the less severe the collision will be. The intensity of the collision means whether the node has been identified as a destructive node and should be eliminated or not.

In the fourth phase, deep learning-based mobility prediction (DL) and calculation of response time based on the first node of the next step in the reverse path are performed. Deep learning is a data learning approach with multi-layered supervised understanding and a subset of artificial neural networks. It is used in various problems of mobile case networks, such as anomaly and error detection, routing, estimation of data quality, and energy consumption. In this paper, deep learning methods are used with advantages such as the ability to accurately display complex spatio-temporal relationships in the movements of nodes and to make accurate predictions without human intervention. They have been trained to recognize complex patterns in the data. And they can predict the future movements of nodes based on their mobility history and communicate with minimal latency. Then, each node that is placed as the first next leap in the reverse path to the source node, when it receives the path response packet from the origin node, calculates the response time for this packet and compares it with the average time (threshold) required to generate and pass a packet.

Calculating the response time from the first node of the next step in the reverse path when receiving the path responses packet from the initiator node: In this way, it initially checks whether the destination is the packet or not. If it is not the destination, it checks in its routing table if there is a valid path to the destination. Otherwise, it creates a reverse path to the source node and the packet requests the route.to its neighbors. If it has the corresponding entry for the destination in its routing table, it must compare its destination sequence number with the destination sequence number in the route request packet. If the destination sequence number in the routing table is greater than or equal to the number in the route request packet, the node will generate a response request packet and integrate it through the origin node It does). With this, the response time of the black hole node will be less than the response time of ordinary nodes, which in this paper, this idea has been used to detect the black hole attack according to the response time. Considering that a path response is required to generate a packet, so in the proposed method, all nodes act as observers of their neighbors and in the next first leap when receiving the path response, the packet must calculate the response time for the node that generated this packet and compare it to the average value (threshold) If the response time is less than the threshold value, the node is treated as a black hole node and the separation process begins. The general idea in this phase is based on the fact that the black hole nodes immediately reconcile the packet when it receives the path request packet, without checking or updating it. Its routing table responds, so the time required to generate a path response packet for a black hole node will be less. Also, by adding the response table and the blacklist table requesting conformity verification to detect dummy packets, the network becomes cleaner and more reliable.

IV. Simulation of the proposed approach and evaluation of the results

In this section the proposed approach, using the NS 3.31 simulator in the scenarios without black hole attacks and under black hole attacks, the network parameters are evaluated and its results are evaluated with the results of trust-based techniques, three-layer artificial neural networks (ANNs) and SVM as a model. Supervised learning, fuzzy neural inference system (ANFIS), particle swarm optimization (PSO), bidirectional LSTM deep learning (Bi-LSTM), recurrent neural network (RNN) and recurrent neural network (ReNN) will be compared and finally the results of the comparisons will be analyzed and discussed. The simulated network parameters for the proposed approach and other comparison methods are shown in table 2.

TABLE II Simulation Parameters

Parameters	Value
Network Area	1000m*1000m
Number of Nodes	20,40,60,80,100
Pause time	5-40s
Mobility model	Random way point
Simulation time	600s
Packet size	512 bytes
Transmission range	250m
Maximum speed (m/s)	10

Performance Criteria

The performance evaluation parameters of the proposed method are as follows:

(1) Packet Loss Rate (PLR): The average number of packets lost and abandoned during the data migration process is called the packet loss rate and is calculated according to the following relationship:

$$PLR = \frac{N^{tx} - N^{rx}}{N^{tx}} * 100$$

where is the N^{tx} total number of packages sent and the total number of packages received. N^{rx}The lower the value

of this parameter, the faster the data transfer speed and the better the performance of the network.

(2) Operating Throughput (TH): The total number of successful packets received at one time by the destination calculated from the following relationship:

$$TH = \frac{N^{rx}}{T}$$

(3) Parcel Delivery Ratio (PDR): The total number of parcels received by the destination relative to the total number of parcels sent by the origin is called the parcel delivery ratio and is calculated from the following relation:

$$PDR = \frac{N^{rx}}{N^{tx}} * 100$$

(4) Total Network Latency (TND): The amount of time it takes for an information packet to be sent from the origin to the destination.

(5) Routing Overhead (NRL): The number of control packets associated with routing sent to the number of packets delivered at the destination which is calculated according to the following relationship:

$$NRL = \frac{N^{rsx}}{N^{dx}}$$

In whichN^{rsx} and N^{dx} the number of control packets related to routing has been sent and the number of packets delivered, respectively.

Evaluation of Simulated Network Performance with/without Black Hole Attack

To ensure the accuracy of the results, the average results obtained from the implementation of the proposed approach are presented 5 times. In the table 3, each of the network parameters is shown in the number of different nodes in the scenario without black hole attacks.

TABLE III Performance of simulated network without black hole attack with different number of nodes

Parameters	Number of Nodes				
	20	40	60	80	100
PLR	8.63	7.44	9.52	7.41	8.03
TH	174.91	154.08	189.11	161.47	153.29
PDR	91.42	92.61	90.53	92.64	92.02
TND	8.15	16.21	14.53	13.38	22.71
NRL	2.83	2.75	2.79	1.49	2.76

As can be seen, the lowest routing overhead value with 80 nodes, the highest throughput value with 60 nodes, the lowest latency value with 20 nodes, the highest packet delivery rate value with 80 nodes, and the lowest value for packet loss rate parameter with 80 nodes were recorded. The table 4 shows each of the network parameters in a different number of nodes in the scenario under black hole attack. As shown in the table, the lowest value of NRL with 80 nodes, the highest value of throughput with 60 nodes, the lowest value of delay with 20 nodes, the highest value of packet delivery rate with 80 nodes, and the lowest value for the packet loss rate parameter with 80 nodes are recorded.

TABLE IV Simulated network performance under black hole attack with different number of nodes

Parameters	Number of Nodes				
	20	40	60	80	100
PLR	9.53	8.72	10.19	8.26	9.54
TH	172.60	152.84	188.07	159.81	151.67
PDR	90.25	91.45	89.13	91.60	90.79
TND	9.12	18.37	15.82	14.58	23.95
NRL	4.28	4.16	4.18	2.47	4.08

In the table 5, each of the network parameters is shown by changing the number of connections in the scenario without black hole attacks.

TABLE V Performance of simulated network without black hole attack with different communicating nodes

Parameters	communicating nodes				
	10	20	30	40	50
PLR	956.37	9682.47	36281.35	75029.76	151695.72
TH	46281.26	52946.38	265489.84	452679.31	723679.27
PDR	98.91	71.05	52.28	41.45	37.28
TND	183.14	964.56	2326.85	2876.06	3168.26
NRL	1.41	4.16	4.74	5.64	6.19

According to the above table, when there are no black hole nodes in the network, the packet delivery rate in the number of communication nodes from 10 to 50 varies from 98.91 to 37.28, which indicates that with the increase in the number of communication nodes, the packet delivery ratio decreases. Also, the total latency of the network varies from 183.14 to 3168.26, which shows that with the increase in the number of communication nodes, the total latency The network is also increasing. According to the above table, the packet loss rate ranged from 956.37 to 151695.72, which indicates an increase in the number of packets lost. To discover the route between the origin and the destination, control packages must be produced. For this reason, according to the table, by increasing the number of communication nodes from 10 to 50, the routing overhead also increases. In the table 6, each of the network parameters is shown by changing the number of connections in the scenario under black hole attacks.

TABLE VI Performance of Simulated network under black hole attack with different communicating nodes

Parameters	communicating nodes				
	10	20	30	40	50
PLR	1025.48	12567.05	40638.17	83241.44	162359.39
TH	49678.83	56419.62	301583.46	524317.51	763814.92
PDR	98.82	70.14	51.91	41.13	36.81
TND	195.47	1076.91	2561.32	2691.54	3145.89
NRL	1.56	4.21	4.92	5.67	6.20

Usually, the packet delivery ratio of the network under black hole attack is drastically reduced compared to the scenario without a black hole attack because some packets are discarded by malicious nodes during the attack. But as it is clear in the above table, the packet delivery ratio in the proposed approach is not much different from the no-attack black hole mode and is the same in some values, which indicates that the approach The process of path discovery in the scenario under black hole attack is shorter because the malicious nodes respond immediately and pretend to have a valid path to the destination compared to the scenario without a black hole attack. The black hole node absorbs all packets between nodes and communicates in the network, so the results are expected to be very different for the parameter of the proportion of packets lost in the scenarios without the black hole attack and under the black hole attack, but as can be seen, the proportion of packets lost in both scenarios is almost the same, which indicates the proposed approach to avoid, shaking hands is a safe method. With the presence of black hole nodes, the routing overhead in the network also increases, but the comparison of the values of both scenarios shows that there is no significant difference in them and shows that the proposed approach has been successful in detecting black hole nodes and no additional control packages have been added to the network and have performed well in terms of routing overhead.

Comparison of the Performance of the Proposed Approach with Other Methods

In this section, the results obtained for each of the parameters considered in the previous section (packet loss rate, throughput, overall network latency, packet delivery rate, and routing overhead) for black hole attack detection are presented with the results of trust-based techniques (TBT), three-layer artificial neural networks (ANNs) and SVM as a learning model. Supervised, Fuzzy Neural Inference System (ANFIS) and Particle Swarm Optimization (PSO), Bidirectional LSTM Deep Learning (Bi-LSTM), Recurrent Neural Network (RNN), and Recurrent Neural Network (ReNN) are compared.

Packet Loss Rate: Increases the speed of data transfer and improves network performance. Therefore, one of the ways to increase the speed of data transfer is to reduce the packet loss rate. The figure 2 shows a comparison of packet loss rates in networks without black hole attack and networks under black hole attack using different approaches. As expected, as shown in the figure, the lowest value for the packet loss rate parameter compared to other approaches is related to the black hole-free network. However, by comparing other algorithms under black hole attack, the packet loss rate in the proposed approach shows lower values and is closer to normal conditions.

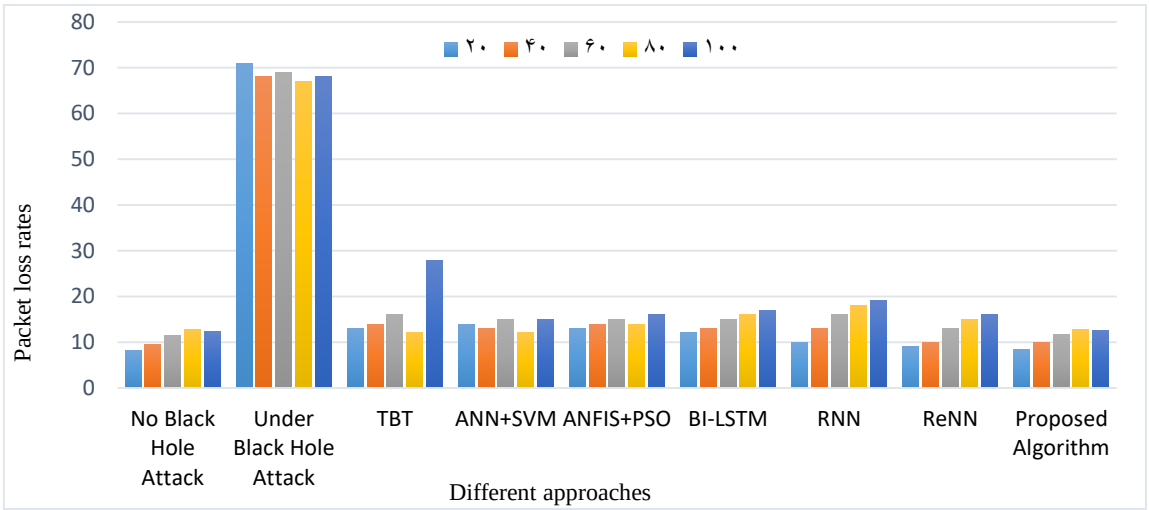

Fig 2. Comparison of packet loss rate in networks without black hole attack and under black hole attack using different approaches

Throughput: The results of the average throughput are shown in the figure 3. As can be seen, the average network throughput by the proposed approach and the scenario without black hole attack is almost equal and has a better performance compared to other methods.

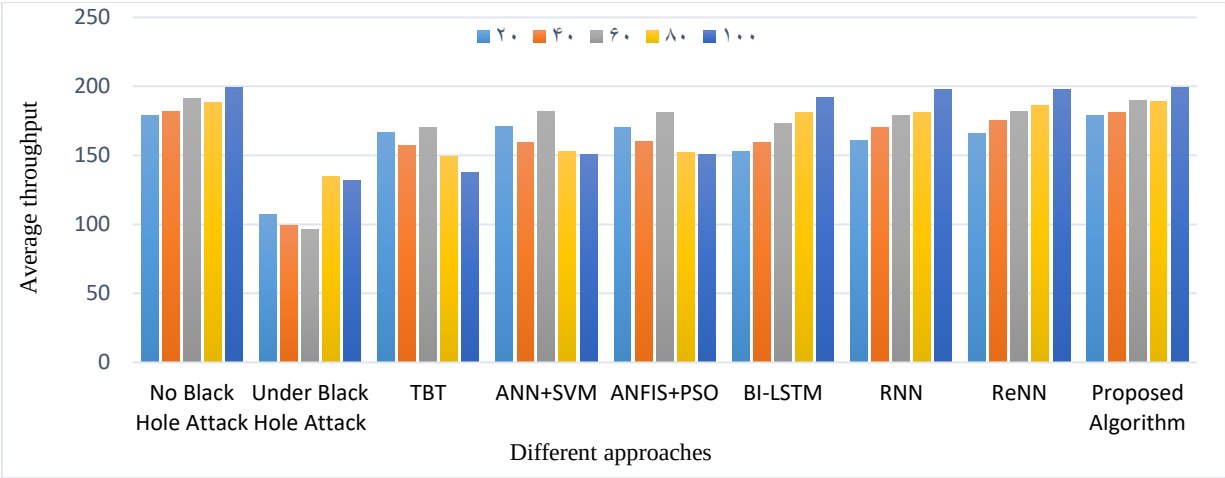

Fig. 3. Comparison of throughput in networks without black hole attack and under black hole attack using different approaches

Packet Delivery Rate: The packet delivery rate of the proposed approach and other methods in the scenario under black hole attack and without black hole attack for the number of nodes of 20, 40, 60, 80 and 100 is shown in the figure 4. According to the figure, the results of the implementation of the proposed approach are very close to the results of the scenario without black hole attack and its performance has been better compared to other algorithms.

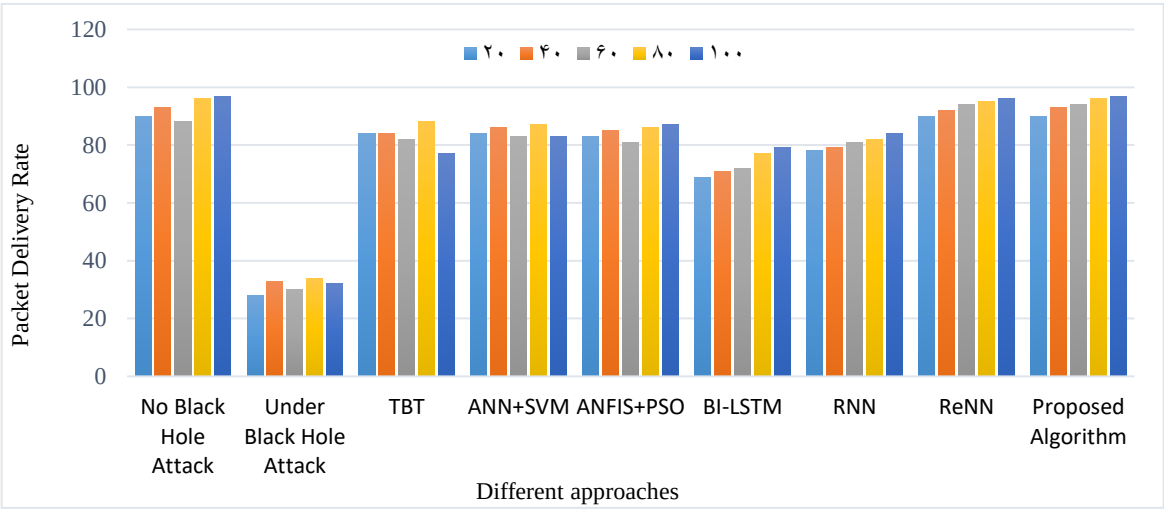

Fig 4. Comparison of packet delivery rate in networks without black hole attack and under black hole attack using different approaches

Total Network Latency: Reducing the total network latency leads to an increase in the speed of data transmission and improves its performance. The figure 5 shows the total network latency for different methods in the number of nodes 20, 40, 60, 80, and 100. According to the figure, in the non-attack black hole state, the latency of the entire network is at its minimum, and when the number of nodes is low, the total latency difference is very slight, and this difference increases as the number of nodes increases. However, the proposed approach works slightly better than other methods.

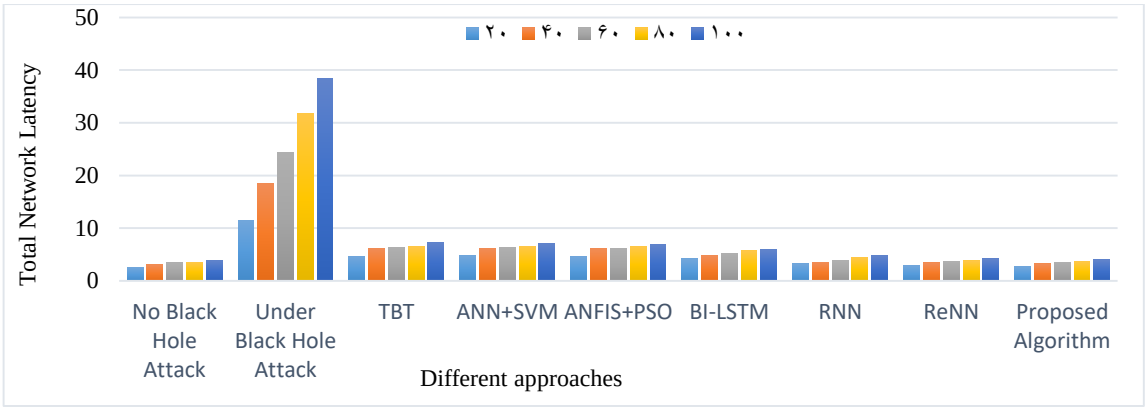

Fig 5. Comparison of total network delay in networks without black hole attack and under black hole attack using different approaches

Routing overhead: Reducing the changes and stability of the network topology make it necessary to perform less routing process because the routing tables in the nodes have fewer changes and are more stable. As a result, the time and resources of the network are spent on transmitting information packets instead of routing packets. The figure 6 shows the comparison of the routing overhead of the proposed approach and other methods.

As expected, if there are no attacks on the network, its routing overhead is less. However, in the event of a black hole attack, the proposed approach provides the best results for routing overhead compared to other methods and is closer to the conditions without a black hole attack.

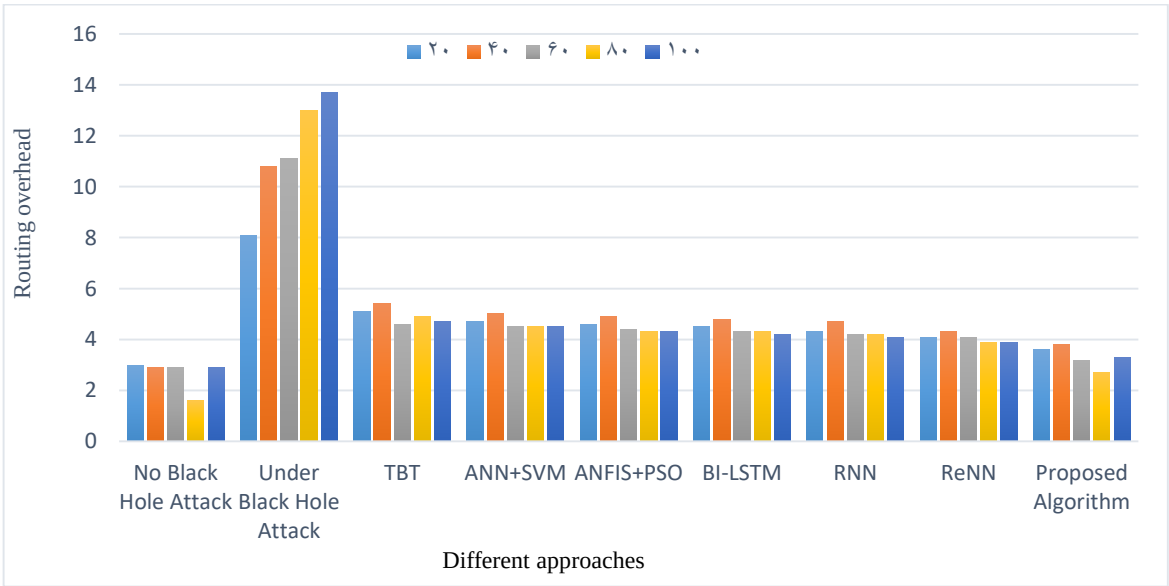

Fig 6. Comparison of routing overhead in networks without black hole attack and under black hole attack using different approaches.

V. Conclusions

Mobile ad-hoc networks are popular due to their unique features such as lack of infrastructure, ease of setup, and lack of centralized management. However, they suffer from different types of attacks, such as a black hole attack. The goal of a black hole attack is to disrupt the routing performance of the network by abandoning all packets sent between the origin and destination nodes is. Therefore, in these networks, security is a high priority. In this paper, in order to identify and isolate the black hole attack, a four-phase approach was proposed, in the first phase, clustering was done using the nearest neighbor K algorithm (KNN), in the second phase, using beta distribution, the trust of each node and its remaining energy was calculated, and then in the third phase, the cluster node was selected using fuzzy inference Finally, in the fourth phase, the response time was calculated based on the deep learning model. The simulation results show that the ANN+SVM-based approach has performed better than the trust-based K technique on average in most parameters, and the ANFIS + PSO-based approach has performed better compared to the ANN+SVM and trust-based approaches. However, the proposed approach, due to

the use of KNN algorithm for clustering and beta distribution and phase inference for node trust calculation, provides better results in all parameters with less routing overhead and provides parameters such as packet loss rate, throughput, packet delivery ratio, total network latency, and normal routing load compared to other methods and has been more successful in detecting black hole attacks on the network.

REFERENCES

[1] Sarbhukan, V.V., Ragha, L. Establishing secure routing path using trust to enhance security in MANET. Wireless Personal Communications, 110(6): 245-255, 2020, doi: 10.1007/s11277-019-06724-0.

[2] Vinayagam, J., Balaswamy, Ch., Soundararajan, K. Certain investigation on MANET security with routing and blackhole attacks detection. Procedia Computer Science, 165: 196-208, 2019, doi: 10.1016/j.procs.2020.01.091.

[3] Merlin, R.T., Ravi, R Novel trust_based energy aware routing mechanism for mitigation of black hole attacks in MANET. Wireless Personal Communications, 104: 1599-1636, 2019, doi: 10.1007/s11277-019-06120-8.

[4] Talukdar, M.I., Hassan, R., Hossen, M.S., Ahmad, K., Qamar, F., Ahmed, A.S. Performance improvements of AODV by black hole attack detection using IDS and digital signature. Wireless Communications and Mobile Computing, 2021, doi: 10.1155/2021/6693316.

[5] Elmahdi, E., Yoo, S.M., Sharshembiev, K., Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks. Journal of Information Security and Applications, 51: 102425, 2020, doi: 10.1016/j.jisa.2019.102425.

[6] Kowsigan, M., Rajeshkumar, J., Baranidharan, B., Prasath, N., Nalini, S., Venkatachalam, K. A novel intrusion detection system to alleviate the black hole attacks to improve the security and performance of the MANET. Wireless Personal Communications, pp. 1-21, 2021, doi: 10.1007/s11277-021-08530-z.

[7] C. Sauer, E. Lyczkowski, M. Schmidt, A. Nüchter, and T. Hoßfeld, "Testing AGV mobility control method for MANET coverage optimization using procedural simulation," Comput. Commun., vol. 194, no. June, pp. 189–201, 2022, doi: 10.1016/j.comcom.2022.07.033.

[8] N. S. Saba Farheen and A. Jain, "Improved routing in MANET with optimized multi path routing fine-tuned with hybrid modeling," J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 6, pp. 2443–2450, 2022, doi: 10.1016/j.jksuci.2020.01.001.

[9] Meddeb, Rahma, et al, "A deep learning-based intrusion detection approach for mobile Ad-hoc network," Soft Computing, vol. 27, no.14, pp. 9425-9439, 2023, doi: 10.1007/s00500-023-08324-4.

[10] M. Goswami, P. Sharma, and A. Bhargava, "Black hole attack detection in MANETs using trust_ based technique," International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 4, pp. 1446–1451, 2020, doi: 10.35940/ijitee.D1497.029420.

[11] Karthik, M Ganesh and Sivaji, U and Manohar, M and Jayaram, D and Gopalachari, M Venu and Vatambeti, Ramesh, "An intrusion detection model based on hybridization of S-ROA in deep learning model for MANET," Iranian Journal of Science and Technology, Transactions of Electrical Engineering, vol. 48, no. 2, pp. 719-730, 2024, doi: 10.1007/s40998-024-00700-6.

[12] G. Arulkumaran and R. K. Gnanamurthy, "Fuzzy trust approach for detecting black hole attack in mobile adhoc network," Mobile Networks and Applications, vol. 24, no. 2, pp. 386–393, 2019, doi: 10.1007/s11036-017-0912-z.

[13] A. U. Khan, G. Abbas, Z. H. Abbas, M. Waqas, and A. K. Hassan, "Spectrum utilization efficiency in the cognitive radio enabled 5G-based IoT," Journal of Network and Computer Applications, vol. 164, no. 102686, pp. 1–16, 2020, doi: 10.1016/j.jnca.2020.102686.

[14] Arappali, N., Rajendran, G.B. MANET security routing protocols based on a machine learning technique. Journal of Ambient Intelligence and Humanized Computing, 12(16): 6317-6331, 2021, doi: 10.1007/s12652-020-02211-8.

[15] Karthik, M. Ganesh, et al, "An intrusion detection model based on hybridization of S-ROA in deep learning model for MANET," Iranian Journal of Science and Technology, Transactions of Electrical Engineering., vol. 48, no. 2, p. 719-730, 2024, doi: 10.1007/s40998-024-00700-6.

[16] Sunitha, D and Latha, PH, "A secure routing and black hole attack detection system using coot Chimp Optimization Algorithm-based Deep Q Network in MANET," Computers \& Security., vol. 148, pp. 104166, 2025, doi: 10.1016/j.cose.2024.104166.

[17] N. C. Sattaru, M. R. Baker, D. Umrao, U. K. Pandey, M. Tiwari, and M. K. Chakravarthi, "Heart Attack Anxiety Disorder using Machine Learning and Artificial Neural Networks (ANN) Approaches," 2022 2nd Int. Conf. Adv. Comput. Innov. Technol. Eng. ICACITE 2022, pp. 680–683, 2022, doi: 10.1109/ICACITE53722.2022.9823697.

[18] Hussain, S Faizal Mukthar and Fathima, SMH Sithi Shameem, "Federated Learning-Assisted Coati Deep Learning-Based Model for Intrusion Detection in MANET," International Journal of Computational Intelligence Systems., vol. 17, no. 1, p. 285, 2024, doi: 10.1007/s44196-024-00590-w.

[19] S. R and A. H, “Adaptive fuzzy logic inspired path longevity factor-based forecasting model reliable routing in MANETs,” Sensors Int., vol. 3, no. August, p. 100201, 2022, doi: 10.1016/j.sintl.2022.100201.

[20] A. Bhatia, A. Kumar, A. Jain, A. Kumar, C. Verma, and Z. Illes, “Heliyon Networked control system with MANET communication and AODV routing,” Heliyon, vol. 8, no. August, p. e11678, 2022, doi: 10.1016/j.heliyon.2022.e11678.

[21] Rajkumar, M and Karthika, J and others, “multi-view consistent generative adversarial network for enhancing intrusion detection with prevention systems in mobile ad hoc networks against security attacks,” Computers \& Security., vol. 150, pp. 104242, 2025, doi: 10.1016/j.cose.2024.104242.

[22] Hajian, E., Asadi, N. Intrusion detection using deep learning in wireless body sensor networks. Journal of Intelligent Multimedia Processing and Communication Systems, 5(4): 1-13, 2023, doi: 10.71856/impcs.2024.1195000.

[23] Roknoddini, M., Norouzi, A. A hybrid deep neural network approach for intrusion prevention in computer networks. Journal of Intelligent Multimedia Processing and Communication Systems, 4(4): 57-65, 2022, doi: 10.71856/impcs.2024.903465.