International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/217705 Volume 9, Issue 6, November – December (2022)

RESEARCH ARTICLE

Detection of Black and Grey Hole Attacks Using Hybrid Cat with PSO-Based Deep Learning Algorithm in MANET

S. Venkatasubramanian
Department of Computer Science and Engineering, Faculty of Engineering and Technology, Annamalai University, Chidambaram, Tamil Nadu, India.
veeyes@saranathan.ac.in

A. Suhasini
Department of Computer Science and Engineering, Annamalai University, Chidambaram, Tamil Nadu, India
suha_babu@yahoo.com

S. Hariprasath
Electronics and Communication Department, Saranathan College of Engineering, Trichy, Tamil Nadu, India.
hariprasath-ece@saranathan.ac.in

Received: 24 September 2022 / Revised: 13 November 2022 / Accepted: 15 November 2022 / Published: 30 December 2022

Abstract – The newest example of wireless networks, known as mobile ad hoc networks (MANETs), offers some qualities, including a topology that can change dynamically, a baseless network, a range of transmission, a routing procedure, and reliability. In a black hole attack on a computer network, packets are deleted as opposed to being forwarded through a router. This often happens when a router has been corrupted by several circumstances. A routing attack called a "black hole" has the power to bring down an entire network. One of the most common types of assaults on MANETs is the Grey Hole Attack, in which a hostile node allows routing but prevents data transmission. MANET security is a top priority because they are far more susceptible to assaults than wired infrastructure. This study focused on detecting black and grey-hole attacks in MANET by using deep learning techniques. The forwarding ratio metric is used in the individual attack detection phase to distinguish between the defective and normal nodes. The encounter records are manipulated by malicious nodes in the collusion attack detection phase for escaping the detection process. The attacks are detected by using different deep learning techniques like Convolutional Neural Network (CNN) and a Long Short-Term Memory (LSTM) network. The parameter tuning operation is carried out by using the Hybrid Cat-Particle Swarm Optimization (HCPSO). The simulation results shown in our proposed system detect with better accuracy.

Index Terms – Black Hole Attack, Convolutional Neural Network, Mobile Ad-Hoc Networks, Long Short-Term Memory, Hybrid Cat-Particle Swarm Optimization, Grey Hole Attacks.

1. INTRODUCTION

The nodes in MANET are mobile and can link with one another without being physically connected to a backbone network [1]. MANETs are better suited for a broad variety of uses, including but not limited to Military needs, Disaster Recovery, Entertainment, and Education [2] due to its self-regulating structure and mobility freeing of nodes. In this configuration, each node is independent and does not rely on a central network to relay information. On the other hand, adaptable nodes work together to relay information across devices that can't establish direct communications within the same local area. Mobile ad hoc networks' routing techniques can adapt to any kind of topology change [3]. For data to go from its source to its destination, a path must be created between the nodes involved in the transmission of the data (the "intermediate nodes"). Path creation requires the identification of the best possible starting point, which necessitates the use of a reliable and safe method [4, 5].

Due to the lack of a central substructure that controls communication between nodes, Mobile Ad hoc Networks are vulnerable to various forms of attack and danger. Each node must rely on itself to transfer information to the correct node. Last but not least, a malevolent node may alter the intercommunication link between nodes or relinquish the information that was sent [6]. When seen from a different angle, mobile ad hoc networks have several limitations, including short battery life, small memory, and hostile nature.

There are two distinct categories of attack against MANETs. There are two chief categories of attacks: active and inert [7]. In an active attack, the attacker makes deliberate changes to the data or creates completely false data. In a passive attack, the attacker is simply interested in eavesdropping and will merely monitor the transmission to ensure that no alterations are made to the data [8]. A black hole attack is a severe form of cyberattack that uses manipulation of the network's transport protocol to steal previously sent information. The basic goal of most well-known routing protocols, such as AODV and DSR, is to locate the optimal path to the terminus node. Route discovery requests in these protocols are sent using a ROUTE REQ packet, while responses are sent using a ROUTE REP packet [9]. The initiator node initiates this type of black hole attack by sending a route request packet to the neighbor node. If, upon receiving the route-reply packet, the source node only responds to the node—the wicked node—and ignores the other intermediate nodes, a black hole attack will result. The attacked nodes will stop forwarding data [10]. To avoid this disturbance, we must develop a protected algorithm that finds the safest and fastest route between two given nodes.

Assigning a resource in a network with a distinct name and a password is the most standard and straightforward method of security [11]. Attacks like a black hole and grey hole denial of service, distributed denial of service assault (DDoS) [12], cross-site scripting, network sniffing, etc., pose a threat to MANET. There are two types of assaults that can be particularly damaging to cloud networks: black holes (false reports) and grey holes (packet drops). Black-Hole attacks [13] occur when a rogue node with enough buffer storage deliberately drops or re-routes the message packet, causing the network to use more energy than necessary. The Black-Hole Node (BHN) was accepted without checking if it led to the intended destination. Figure 1 depicts the forwarding of dropped packets. Gray-Hole attacks involve the intentional dropping of data packets at a predetermined rate, such as one every t seconds or every n packet end route to a specific target on the network.

As shown in Figure 2, when node A transmits a message to node F, the Gray-Hole Node (GHN) drops the route reply, and node D forwards the packets back to A [14, 15]. Misconduct including message dropping, reduces throughput and wastes time and energy of intermediate nodes that have transported and forwarded the dropped messages. A mechanism is robust against trust-related assaults and can handle selfish behavior.

1.1. Research Contribution

In this work, a deep learning-based methodology for identifying strange behavior in measurements caused by the black and grey hole attacks is done. This study detailed a detection strategy that makes use of a combination of CNN and LSTM.

This study uses a deep learning model to identify network attacks. To improve the LSTM model's classification accuracy, HCPSO is applied to its parameter tuning process. Section 2 presents the results of the paper's research into previous works in the field. In Sections 3 and 4, we lay out the problem and briefly explain the assaults that could be made against it. Sections 5 and 6 detail the reasoning behind the proposed model and its validation across a wide range of inputs. Section 7 provides the study's final findings.

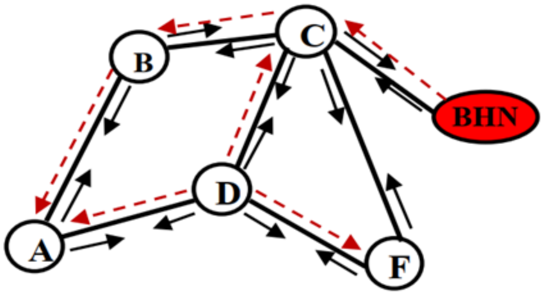

Figure 1 Attack as Black-Hole

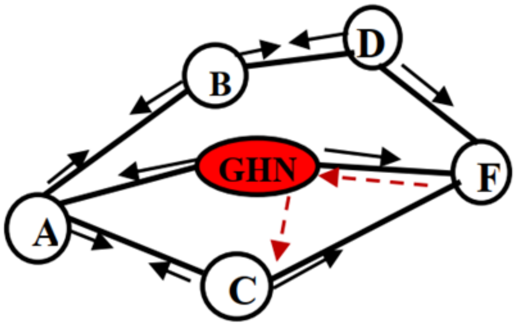

Figure 2 Attack as Gray-Hole Attack

2. RELATED WORK

To prevent black hole and gray hole attacks, Prasanna, D.J.D. [16] proposed a lightweight security method in addition to the concept of Connected Dominating Sets (CDS) for establishing a virtual backbone of Cloud MANET nodes. Public key infrastructure is built up to simulate blockchain-based security, and the algorithm employs the Q learning technique to learn before establishing the CDS in the Cloud MANET. The implementation of a "smart contract" guarantees that all transactions are recorded and that any hacked nodes in the CDS are quickly identified and removed. This suffers from the huge storage and delay in cloud interactions

Hassan, Z., and others [17] present an ACV-specific intelligent black hole attack detection system (IDBA). Hop Count, Destination Sequence Number (DSN), Packet Delivery Ratio (PDR), and End-to-End Delay were taken into account throughout the construction of the scheme (E2E). IDBA was measured against the AODV with Black Hole (BAODV), Intrusion Detection System (IdsAODV), and EAODV models. Extensive replication results demonstrate that IDBA excels above state-of-the-art methods in terms of PDR, E2E, routing overhead, packet loss rate, and throughput. The accuracy of the results is medium.

Rani, P., [18] looked at black hole attacks, in which compromised nodes expose themselves as the node with the shortest path to the destination node by using routing protocols. The suggested method specifically improves the AODV routing protocol against black hole attacks by combining the Firefly Algorithm and an Artificial Neural Network (ANN-FF). Numerical data from several experiments are used to assess performance, with variables like computing overhead, packet delivery rate, throughput, and delay all taken into account. From the numerical findings, it is clear that the proposed method is superior to the conventional methods. The accuracy and the precision are not taken.

According to Sathyaraj, P. [19], an Improved Crossover Chicken Swarm Optimization (ICCSO) method and the notion of Enhanced operation were proposed, and the best fitness values were found to counteract the black hole assault in MANET. Step 1 of the ICCSO process entails parameter initialization, during which attacked nodes and non-attack nodes are independently generated using parameters like PDR and RSSI. Also, if a node is attacked, it is removed from the network, and data is sent through a different, unaffected node. The AODV protocol is used to handle routing. CNN model is not used here.

To prevent grey hole and black hole assaults, Janakiraman, S. [20] devised a technique called Improved Rider Optimization Algorithm-based Link Aware Fault Detection (IROA-LAFD). Using techniques including neighbor and route discovery, attack detection, link analysis, secure packet transmission, and link fault detection with the IROA Algorithm, this system aims to efficiently reduce the occurrence of dropped packets. Specifically, IROA is used to investigate the trust nodes' interconnections with one another. The suggested IROA-LAFD method was found to improve PDR by 13.42%, throughput by 12.84%, and link failure detection rate by 15.48% in simulated trials compared to the benchmarked techniques. The focus is only on establishing a trusted link path.

Using the idea of an ANN-based ABC optimization technique, Rani, P. [21] investigated and offered protection against dual attacks for black and grey-hole attacks. The results portion of this paper explains how the system's performance has been improved through the selection of appropriate and optimal nodes for data packet transmission. MATLAB is used with the communication and neural network toolboxes to construct and simulate networks. Results reveal that the presented methodology outperforms the prior art in both black hole and grey hole attack scenarios. Our work improvises on this by using CNN.

In this work, Ramachandran, D. [22] improved AODV by employing a less resource-intensive technique based on timing and baiting for detecting and distinguishing between single and cooperation black hole attacks. There is no centralized control in MANETs, and instead, each mobile device establishes its wireless connection to others in the network. Threats to secure communication include black holes, insider assaults, grey holes, parallel universes, defective nodes, and packet drops. The results of the simulations show that the suggested method greatly exceeds the conventional methods in terms of round-trip delay, throughput, packet delivery ratio, and average energy. Our proposed strategy for protecting MANET from black holes employs a multipath approach. The proposed method's resilience against assault is evaluated in a virtual environment.

Srinivasan, V. [23] focuses particularly on the vulnerability of the network to a black hole attack, a type of suction assault. Studies into using intelligent agents with Long-Short Term Memory (LSTM) in a technique called Honeypot Agent-based detection scheme (HPAS) to discover such attacks. Honeypots are mobile, virtual software administrators that generate Route Request (RREQ) packets to lure and ensnare black hole attackers; this is why the suggested approach is called High Probability Attack Simulation with Long Short-Term Memory (HPAS-LSTM). The proposed detection method is shown to exist using extensive model results obtained from the ns-2 simulator. The simulation results show that the proposed method has better throughput (TH), packet loss rate (PLR), packet delivery ratio (PDR), and total network delay than the existing black hole identification methods (TND).

3. PROBLEM DEFINITION

In this study, we investigate the following assumptions to model black-hole and grey-hole assaults in MANETs. Many studies in these fields rely on these assumptions [24, 25]. They can give us an overarching picture of the network and attack types, aid in modeling the system's many moving parts, and evaluate potential countermeasures.

- Assumption 1: The network consists of a single node acting as the starting point and another acting as the final destination. When a message is a broadcast, it is the source node's job to do the sending, while the target node's job is to do the receiving.
- Assumption 2. The N intermediary nodes in the network may send a forged route reply message to the requesting node.
- Assumption 3. The timestamps created due to the messages in route requests, as well as route replies, follow

an exponential distribution for both black-hole and grey-hole attacks.

- Assumption 4. While m assaults are visible from a single intermediate node, an IDS in the network can identify them all. There may be more attacks than the setting m allows for, but the IDS won't pick them up unless they're all coming from the same node.
- Assumption 5. After an intermediary node has attacked a route request message in a black-hole attack, it will very definitely also attack the other messages. In case of middle node attacks the earlier message, then to the terminus node, a safe route request message cannot be delivered.
- Assumption 6. The black-hole attack is characterized by a single node attacking all route request packets.
- Assumption 7. After the initial grey-hole attack, route request messages can still be sent to their final destination without risk. To rephrase, each grey-hole attack operates in isolation from the others.
- Assumption 8. Each grey-hole attack might be carried out by a different assailant. The node that has attacked in earlier stages is more likely to attack subsequent route request messages.

Section 5 and Section 6 detail the suggested deep learning models while taking into account the aforementioned assumptions.

4. BACKGROUND OF BLACK AND GREY HOLE ATTACKS

Every node keeps track of an EDRI (extended data re-routing information) table.

FROM: This accessibility display of the specified junction, in this case, node 1, has offered analysis services that were initiated at the specified junction id. A value of 0 indicates that the information is false in that no specifics have been provided. A single alternative route via which investigation presents were prompted.

THRU: This value, like in the past, will be 1 if the details offer issued through junction 1 was instructed by the junction identification. Understand that a lack of a charge in the form and via information does not necessarily mean that the junction is harmful or that you should not use it; rather, it signals that you should treat the information with caution because it is not a true junction. In all honesty, no such debate has ever taken place.

CTR: CTR keeps tabs on how severe the junction's conditions were.

BH: If the junction id can be dangerous in its current relationships, this availability is 1, otherwise it is 0. To find a different solution, the BHID package is implemented. In this context, for instance, junction 10 is treated like a black hole.

TIMER: This area of study provides the time beyond which the junction may no longer be considered risky for route planning. Utilizing the CTR subject fee, the value is quantified. This present instance, for instance, involves determining the cost of this position from CTR in a very short amount of time using an extremely efficient goal.

Also crucial is the requirement of continuity in the EDRI principles; if X instructs via junction Y, then junction X must have a 1 in thru Y must have a 1 within the shape available for X. As a result, the black-hollow node can be identified by its apparent consistency in shape and by information strength.

When it comes to managing paths just between hubs that need to communicate, the Ad Hoc On-Demand Vector Routing (AODV) strategy is a subtle direction-finding method for ad hoc and mobile frameworks. Distraction tactics are met with a wide array of counterattacks. One such attack, known as a "dull hole strike" [26] and a type of "Refusal of Service" (RoS) [27, 28], occurs when a malicious hub takes advantage of the inadequacies of the road locating bundles of the steering practice to present itself as the quickest route to the hub whose bundles it needs to recognize.

This strike aims to alter the method of navigation so that all traffic is routed through an enemy-controlled node. Path Discovery involves the source hub sending RREQ packets to the boosted hubs to pinpoint a direct route to the destination. Unhealthy nodes react instantly to the seed hub because they have no connection to the directing work area. The resource node announces that the street-discovery technique is complete, disregards RREP data from other nodes, and instead directs data packets through the harmful node. The unreliable core does this by providing the reaction group with a generous buffer zone for its arrangement.

5. PROPOSED METHODOLOGY

The flow diagram of the proposed methodology is given in figure 3.

The system is not only able to detect individual attacks but also collaboration attacks. The proposed system has four primary components: (i) the creation of Encounter Records (ER), (ii) the determination of specific assailants, (iii) the avoidance of detecting inappropriate behavior, and (iv) the determination of cooperative assaults. An ER is created and saved in memory at the commencement of the detection procedure on both the sending and receiving nodes. There will be fields in each ER for the sender, receiver, time, sequence number, and message content. ER is employed to modify the detection of specific adversaries. To identify the bad actor node, we will mostly use Encounter Records as input. The arrangement of the resulting ER is verified as well. The order of the sequence and the timestamps should be in continuous rising order, and this should be done in addition to some tempering. The ER can be used to calculate the outcomes of researching a community's archives. Researching the locals with the help of ERs is one way to gauge a neighborhood's health. Once any of these three criteria are not met, the packets are immediately denied on the premise that an ER forgery attempt was performed.

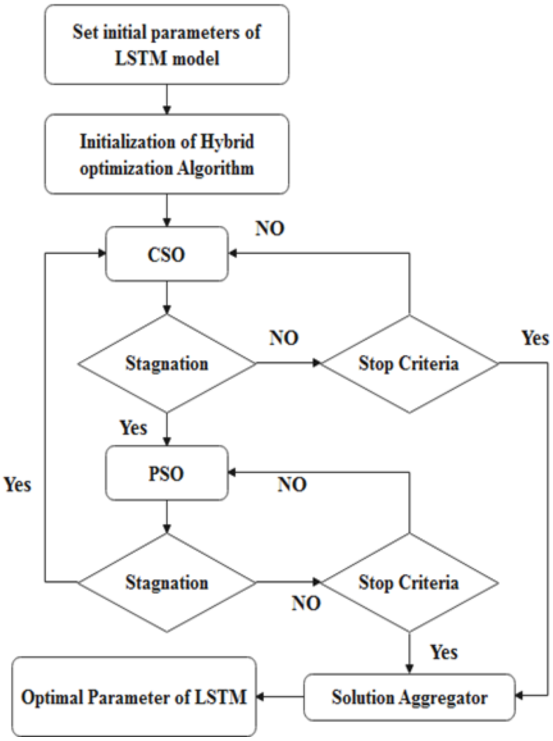
Set initial parameters of LSTM model
Initialization of Hybrid optimization Algorithm
CSO
NO
Stagnation
NO
Stop Criteria
Yes
Yes
PSO
Yes
NO
Stagnation
Stop Criteria
NO
Yes
Optimal Parameter of LSTM
Solution Aggregator

Figure 3 Working Flow of Proposed Hybrid Optimization

If the message packets are not found to be tampered with, the dropping misbehaviors detection phase is carried out automatically after the ER update. Attackers generate larger sections of communications while omitting others to hide their genuine purpose. We evaluate the relevance of the observation of inappropriate behavior abatement using the Relayed Ratio (RR) and the Self-forwarded Ratio (SR). The Relayed Ratio is intended by dividing the total number of messages sent and conventional by the total sum of messages received, as opposed to the total number of messages transmitted. Suppose node n is the endpoint; its RR is found using Eq.(1).

$$RR = \frac{RFM_n}{RMR_n} \quad (1)$$

Where RFM n is the total sum of relayed messages from node n. The sum of the times node n received a message as a relay but did not forward it to another node is denoted by the variable RFM n.

Several messages created and sent by a similar user separated by the total sum of messages sent = Self-Forwarding Ratio as shown in Eq.(2).

$$SR = \frac{GSM_n}{SM} \quad (2)$$

GSM n represents the sum of all messages produced and directed by node n. The total sum of messages (SM) that have been broadcast. The malicious node has a higher SR. The defended node has comparatively high RR and low SR (Well behaved node). When RR is low and SR is high, reputations suffer. In a MANET setting, both Black-Hole and Gray-Hole attackers are cooperating to conceal their activities. "Detection of Collusion Attackers" was created to ascertain if an attacker is collaborating with another malicious user to bypass security measures. Here, the system will check the ER of a frequently-used node to relay messages. If the ratio of messages transmitted to total messages is high, the node may be participating in a coordinated effort to manipulate the results. To preserve their credibility, the attackers and their cohorts utilize the emergency room as a cover. The goal is to manipulate the RR and SR in such a way that a completely made-up ER is produced. To make up for the lost information, the attacker adjusts the ER of the malicious node within the allowed margin of error. In the event of a large number of colluders, the attacker selects a peer node that will have the fewest encounters in the ER's past as the source for the forged record. The malicious node has finished its mission after the desired colluders' signatures have been inserted. This method investigates the potential measurements (RR & SR) with valid records to spot these situations because the conspiring attackers cannot hide the oddity of both measures at a similar time.

Deliberate a and n to be colliding nodes, with n having a history of ER collisions with a. A definition of the FXS measure is given in Eq.(3).

$$FXS_a^n = \frac{M_a^n}{F_a^n} \quad (3)$$

Both M_a^n and F_a^n denote the total sum of exchanges between a and n in this formula (frequency). The FXS metric is useful for identifying fake encounters, and a high abnormality ratio is required to distinguish false ER from genuine ER with the aid of thresholds. The FXS metric analysis clears the ER of the colluder suspicious list and discards any false records. Finally, the filter window compares the RR and SR to the target value. If they go too high, the trusted node is deleted and the overall trust score is calculated.

5.1. Detection of Attacks using Convolutional Neural Network

Convolutional neural networks (CNNs or ConvNets) are the most fundamental type of neural network used in artificial intelligence, consisting of multiple nodes stacked in layers with data only flowing from input to output. Convolutional Layers, Pooling Layers, and Fully-Connected Layers are the three primary types of layers used to construct a CNN construction in this work. Layer by layer, CNN converts the input tensor into a final output, which can be a class score. Specifically, activation functions, biases, and weight values in the input volume are used by each layer to effect a change. Gradient descent optimization will be used to train the CNN's parameters so that they minimize the loss between the CNN's computed outputs and the labels in the training dataset.

5.2. Long Short-Time Memory

Today, LSTM neural networks are the most often used RNNs in practice. When compared to a single-gate, plain RNN, LSTM shows significant performance gains when it comes to remembering both recent and distant events. What follows is a description of how LSTM cells process information as given in Eq.(4) to Eq.(8).

$$Kf_t = \sigma_g(W_f x_t + KU_f kh_{t-1} + bi_f) \qquad (4)$$

$$il_t = \sigma_g(W_i x_t + KU_i kh_{t-1} + bi_i) \qquad (5)$$

$$ol_t = \sigma_g(W_o x_t + KU_o kh_{t-1} + bi_o) \qquad (6)$$

$$cl_t = Kf_t{}^\circ cl_{t-1} + il_t{}^\circ \sigma_c(W_c x_t + KU_c ah_{t-1} + bi_c) \qquad (7)$$

$$ah_t = o_t{}^\circ \sigma_h(cl_t) \qquad (8)$$

Where sigmoid function (_g()) and tangent function (_c()) stand in for the element-wise product and stand for the sigmoid function. The hidden unit vector (h) and the cellular state vector (c) are denoted below. The HCPSO algorithm is used to fine-tune the LSTM's parameters.

5.3. The PSO Algorithm

In 1995, Russell Eberhart and James Kennedy were the first to introduce the metaheuristic Particle Swarm Optimization (PSO) method. A natural swarm, such as birds or fish, inspires the PSO algorithm. Most optimization problems, AI computation, and design/scheduling are just a few of the many uses for the PSO method [21]. Every one of the N particles in the PSO algorithm stands in for a potential answer. Each particle's initial position and speed in search space are generated at random using the PSO algorithm. Particles adjust their speed and location with each iteration, using their current best position P I and the global best position P g. Using the Invalid source supplied, we first update the particle's velocity with Eq. (9), then its position with Equation (10). (10).

$$Vel_i(t+1) = \omega Vel_i(t) + ac_1 rv_2 \left(P_g(t) - X_i(t)\right) + ac_2 rv_2 (P_i(t) - X_i(t)) \qquad (9)$$

$\omega$is the inertia weight used to achieve a balance between the global and local searches, where ac_1 and ac_2 are acceleration coefficients in the range [0,2], $r_1$is consistently distributed random variable in the range [0,1], and t and t+1 are the current and next iterations as in Eq.(10) and Eq.(11).

$$X_i(t+1) = X_i(t) + Vel_i(t+1) \qquad (10)$$

The inactivity weight ω is linearly reduced

$$\omega = \omega_{max} - t * \frac{\omega_{max} - \omega_{min}}{Numiter} \qquad (11)$$

where ω_{max}, ω_{min}, correspondingly, are weight, and $NumIter$ is a sum of iterations.

5.4. The CSO Algorithm

The ability to hunt is essential for survival, but a house cat also shows a great interest in shifting objects out of the way. Cats may spend a lot of time napping, but while awake, they are extremely perceptive. They maintain vigilant surveillance to detect the presence of food or threat. Seeking mode and tracing mode are the two sub-strategies that make up the CSO algorithm, both of which are based on these two behaviors. To determine whether the cats will be in seeking mode or tracing mode, the method employs a mixture ratio (MR).

While the cats are sound asleep, the situation is modeled using the searching mode. The searching memory pool (SMP), the seeking ranger of selected dimensions (SRD), the counts of dimensions to change (CDC), and the self-position considering (SPC) is the four elements defined in the seeking mode.

Each cat's SMP is the size of its searching memory. The individual cat will randomly select a new memory location using a Roulette Wheel. Variations in the values of the selected dimension that fall within the range can be managed with the help of range-based SRD. The number of adjustable dimensions is calculated with CDC. The SPC variable is a boolean one. SPC (1) is true if and only if the cat is the fittest individual, and untrue otherwise (0). If SPC is one (1), the cat will generate j copies of a new candidate position, where j = SMP. If SPC is zero (0), the cat will generate j = SMP one copy, where j = SMP is the current position.

Cats typically employ the tracing mode to track down their prey or targets in theoretical situations. Every tracking cat adjusted its position in response to the change in speed. The CSO algorithm adjusts kitty speeds according to optimal placement. Here we detail the eight steps of the CSO algorithm's procedure.

Step 1: Create the starting coordinates and speeds for N cats in the search space.

Step 2: Determine which location is most advantageous in terms of fitness, and then store that value as xbest.

Step 3: Separate the felines into seeking and tracing teams.

In case the cat is in a searching mode.

Step 4: is to generate a new set of possible positions using Eq. (12), and step 5 is to randomly select one of those positions to replace the existing one.

$$x'_{j,d} = x_{j,d} \pm SRD * r * x_{j,d} \quad (12)$$

Where r is a random sum and $x_{j,d}$, $x'_{j,d}$ are values of dimension $d$correspondingly.

Step 5: Update the cat's velocity with Eq. (13) if it is tracing, and its location with Eq. (13) and (14)

$$v_{k,d}(t+1) = v_{k,d}(t) + c_1 r_1 (x_{best,d}(t) - x_{k,d}(t)) \quad (13)$$

$$x_{k,d}(t+1) = x_{k,d}(t) + v_{k,d}(t+1) \quad (14)$$

$$d = 1,2, \dots, D$$

Where c 1 is the acceleration coefficient, r 1 is a random sum, t is time, v (k,d) (t), v (k,d) (t + 1) are the velocities at time t, and x (k,d) (t + 1) are the coordinates at time t.

Step 6: Six, combine the cats in tracking and looking modes into one.

Step 7: Recalculate the optimum starting point based on the current fitness value.

Step 8: Examine the criteria for closing the project. The method terminates if the condition is met; else, the control passes back to Step 3.

5.5. The HCPSO Algorithm

The ability to hunt is essential for survival, but a house cat also shows a great interest in shifting objects out of the way. Cats may spend a lot of time napping, but while awake, they are extremely perceptive. They maintain vigilant surveillance to detect the presence of food or threat. Seeking mode and tracing mode are the two sub-strategies that make up the CSO algorithm, both of which are based on these two behaviors. To determine whether the cats will be in seeking mode or tracing mode, the method employs a mixture ratio (MR).

While the cats are sound asleep, the situation is modeled using the searching mode. The searching memory pool (SMP), the seeking ranger of selected dimensions (SRD), the counts of dimensions to change (CDC), and the self-position considering (SPC) is the four elements defined in the seeking mode.

Each cat's SMP is the size of its searching memory. Each cat will randomly select a new memory location using a Roulette Wheel. Variations in the values of the selected dimension that fall within the range can be managed with the help of range-based SRD. The number of adjustable dimensions is calculated with CDC. The SPC variable is a boolean one. SPC (1) is true if and only if the cat is the fittest individual, and untrue otherwise (0). If SPC is one (1), the cat will generate j copies of a new candidate position, where j = SMP. If SPC is zero (0), the cat will generate j = SMP one copy, where j = SMP is the current position.

Cats typically employ the tracing mode to track down their prey or targets in theoretical situations. Every tracking cat adjusted its position in response to the change in speed. The CSO algorithm adjusts kitty speeds according to optimal placement. The CSO's Methodology In our research, we propose a novel hybrid method called the Hybrid Cat-Particle Swarm Optimization (HCPSO) algorithm. We join two well-respected metaheuristic algorithms, the CSO and the PSO. The HCPSO algorithm incorporates the whole CSO scheme procedure with a few tweaks. Like the PSO algorithm, it records both the global and local optimal positions. The PSO movement formula is then used while in tracing mode. In addition, the best position is used to adjust the value of the specified dimension in seeking mode, and the best candidate for the vacant post is selected accordingly. The goal of this hybridization is to provide a more convergent method without significantly increasing the runtime. This article details the entire HCSPO algorithm. Create the starting points (X) and velocities (V) for N searchers in the interval [0,1] shown in Eq.(15) and Eq.(16).

$$X = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1D} \\ x_{21} & x_{22} & \cdots & x_{2D} \\ \vdots & \vdots & \ddots & \vdots \\ x_{N1} & x_{N2} & \cdots & x_{ND} \end{bmatrix}, x_{kd} \in [0,1] \quad (15)$$

$$V = \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1D} \\ v_{21} & v_{22} & \cdots & v_{2D} \\ \vdots & \vdots & \ddots & \vdots \\ v_{N1} & v_{N2} & \cdots & v_{ND} \end{bmatrix} \quad (16)$$

Where D is the total number of product categories. First, use Eq. (17) to transform the location (X) into the MBKP-MC solution term (Y) with the help of Eq.(18).

$$Y = \begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1D} \\ y_{21} & y_{22} & \cdots & y_{2D} \\ \vdots & \vdots & \ddots & \vdots \\ y_{N1} & y_{N2} & \cdots & y_{ND} \end{bmatrix} \quad (17)$$

$$y_{kd} = round(x_{kd} * (b_d - a_d)) \quad (18)$$

1. Verify all of the limitations. Make that every solution lies in the infeasible region defined by the MBKP-MC constraints.

2. Find out how each option stacks up in terms of fitness (total profit). Make a note of C k for the best position of each person and C g for the best global answer.

3. Separate the people into two groups, seekers and trackers. To the extent that people are actively looking for

something. Make duplicates using each node's optimal position C k Eq. (19) and adjust the preferred size using the node with the best global solution Cg as in Eq. (20).

4. $x'_{j,d} = C_{k,d}, \;\; d = 1,2,\ldots D$ (19)

$$x'_{j,d} = C_{g,d} \pm SRD * r * C_{g,d} \qquad (20)$$

5. If people are actively looking for something, then the fifth condition applies. Adjust the speed and location per the PSO's motion, as described by Eq. (21) – Eq. (22)

$$V_i(t+1) = \omega V_i(t) + c_1 r_1 \left(C_g(t) - X_i(t)\right) + c_1 r_1 (C_i(t) - X_i(t)) \qquad (21)$$

$$X_i(t+1) = X_i(t) + V_i(t+1) \qquad (22)$$

Combine the cats in both the seeking and tracing modes into one, and check that their coordinates are all inside the range [0,1]. The solution needs to be translated using Eq.(23) if it is larger than the search space (23).

$$x_k = \begin{cases} \frac{x_k - \min(x_k)}{\max(x_k) - \min(x_k)}, & if \min(x_k) < 0 \\ \frac{x_k}{\max(x_k)}, & if \max(x_k) > 1 \end{cases} \qquad (23)$$

6. Transform the updated location X into the MBKP-MC term Y. Examine the fitness value once all constraints have been checked.

7. Please update both C_k, your best personal position, and C g, your greatest overall position. Inquire about the criteria for ending the project.

8. If the condition is met, the algorithm terminates with a solution of Cg. On the other hand, if the threshold is not met, return to the sixth stage.

6. RESULTS AND DISCUSSIONS

Table 1 presents the simulation parameters of the projected model.

Table 1 Simulation Restrictions Description

Parameter Description	Parameter Value
Total no of nodes	500
Size of Data packet	1000 bytes
Type of Traffic	CBR
Environment area	1800X 1800m^2
Parameters Observed	and End-to-end Delay, etc.
Transmission Range	250m
Time Delay	0.0347 ms

6.1. Attack Detection Evaluation

The Evaluation Metrics

The most common metrics for gauging a model's efficacy are accuracy, precision, recall, and F-score; these are calculated using the following Eq.(24) to Eq.(27).

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \qquad (24)$$

$$Precision = \frac{TP}{TP+FP} \qquad (25)$$

$$Recall = \frac{TP}{TP+FN} \qquad (26)$$

$$F - Score = \frac{2 \times Precision \times Recall}{Precision + Recall} \qquad (27)$$

Where the properly predicted values, True Positive (TP) and True Negative (TN), are contrasted with the misclassified occurrences, False Positive (FP) and False Negative (FN). The verified results of the suggested model are shown in Table 2. The measures are analyzed graphically in Figure 4–7.

Table 2 Comparative Analysis of Test Results

Algorithm	Accuracy	Precision	Recall	F-score
IDBA	80.10	87.21	80.15	80.43
ICCSO	85.71	84.32	85.93	83.45
ANN-FF	92.10	92.43	92.15	91.68
ANN-ABC	92.46	93.48	92.44	91.81
IROA-LAFD	89.52	90.21	89.54	89.03
HPAS-LSTM	94.53	96.61	92.52	92.24
CNN	94.16	96.17	92.32	92.10
LSTM-HCPSO	97.62	98.32	95.62	94.53

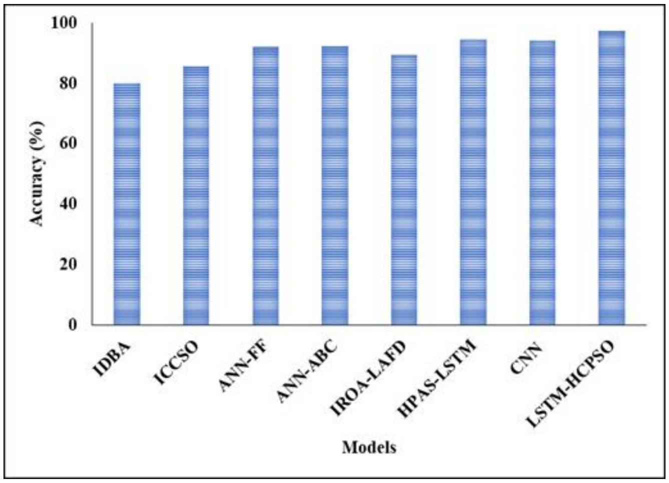

Figure 4 Accuracy

Figure 4 represents the accuracy comparisons of different techniques such as IDBA, ICCSO, ANN-FF, ANN-ABC, IROA-LAFD, HPAS-LSTM, CNN, and LSTM-HCPSO. In this comparison analysis, the proposed model attained better results than other compared techniques.

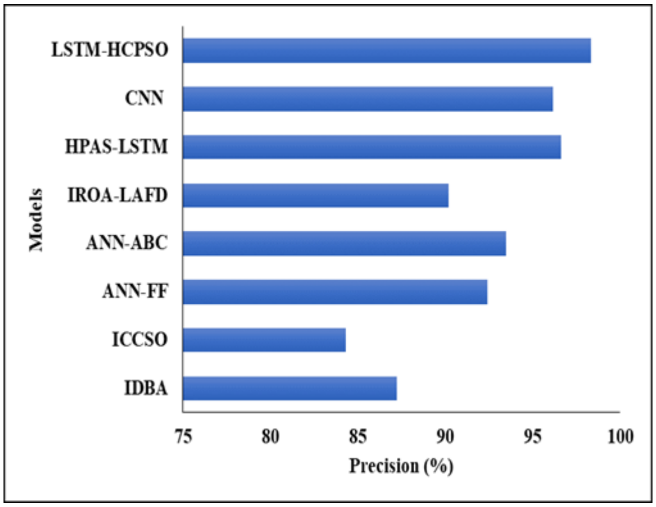

Figure 5 Precision Assessment

Figure 5 represents the Precision comparisons of different techniques such as IDBA, ICCSO, ANN-FF, ANN-ABC, IROA-LAFD, HPAS-LSTM, CNN, and LSTM-HCPSO. In this comparison analysis, the proposed model attained better results than other compared techniques.

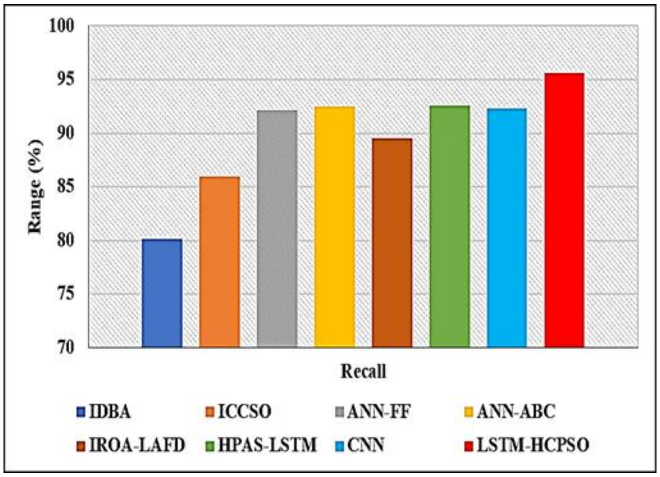

Figure 6 Recall Assessment

Figure 6 represents the recall comparisons of different techniques such as IDBA, ICCSO, ANN-FF, ANN-ABC, IROA-LAFD, HPAS-LSTM, CNN, and LSTM-HCPSO. In this comparison analysis, the proposed model attained better results than other compared techniques.

Figure 7 represents the F-score comparisons of different techniques such as IDBA, ICCSO, ANN-FF, ANN-ABC, IROA-LAFD, HPAS-LSTM, CNN, and LSTM-HCPSO. In this comparison analysis, the proposed model attained better results than other compared techniques.

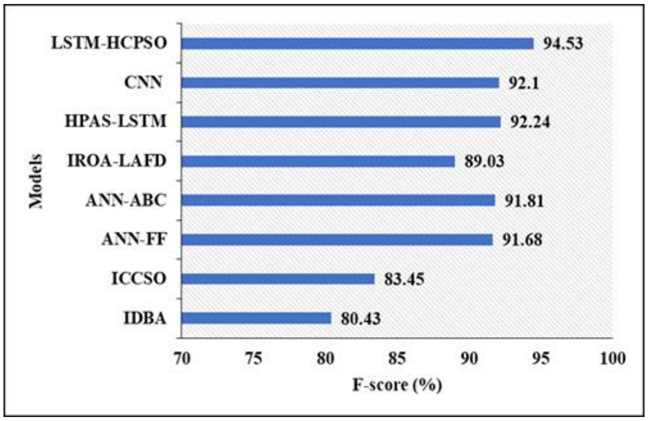

Figure 7 F-Score Assessment

6.2. Network Analysis

6.2.1. PDR Calculation

To estimate PDR, the incoming packet rate and transferred packet rate must be known. Using Eq.(28) shown below, PDR is calculated.

$$PDR = \frac{No.of\ \_attained\_datapackets}{No.of\ \_transmitted\_datapackets} \quad (28)$$

Table 3 shows the PDR values of the projected model and available models. In terms of pictorial representation, it is shown in figure 8.

Table 3 Comparative Analysis of PDR

No. of nodes	Packet Delivery Ratio (%)			
	ICCSO	IROA-LAFD	HPAS	HCPSO
100	89.57	94.87	87.56	99.80
200	90.78	93.93	88.98	99.80
300	88.69	93.54	87.75	99.56
400	88.94	94	85.83	98.36
500	87.56	95.5	84.67	96.67

Figure 8 represents the PDR Comparison of the Network of the proposed model, in this analysis, the proposed model takes the better packet delivery ratio.

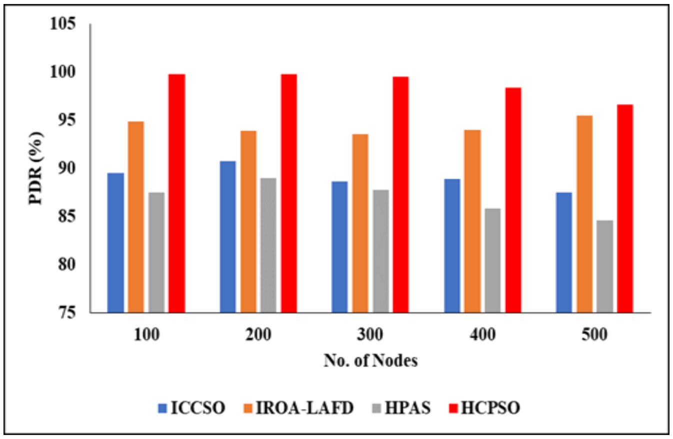

Figure 8 PDR Assessment

6.2.2. Throughput

The packet movement rate between the nodes is measured by estimating the throughput ratio shown in Eq. (29).

$$Throughput\ (bps) = \frac{Received\_packet\ (bytes) * 8}{1024 * (Endtime - startingtime)} \times 100 \quad (29)$$

The validity of the comparison of the proposed model with already developed techniques in terms of throughput ratio is shown in Table 4 and Figure 9.

Table 4 Comparative Evaluation of Throughput

No. of nodes	Throughput Ratio (bps)			
	ICCSO	IROA-LAFD	HPAS	HCPSO
100	67	250	95	700
200	38	148	70	520
300	45	125	74	425
400	40	178	69	345
500	35	185	73	240

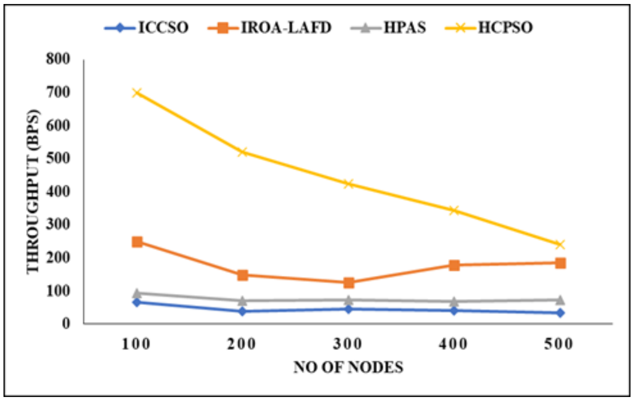

Figure 9 Throughput Comparison

Figure 9 represents the Throughput Comparison of the Network of the proposed model, in this analysis, the proposed model takes the better throughput ratio.

6.2.3. Energy Consumption

The amount of energy utilized by the model developed in this work is less than already developed techniques due to the maintenance of the route. The analysis is shown in Table 5 and Figure 10. According to the simulation time, the nodes' energy utilization is considered.

Table 5 Evaluation of Energy Consumption

No. of nodes	Energy Consumption (J)			
	ICCSO	IROA-LAFD	HPAS	HCPSO
150	10	10	11	6
200	16	17	15	9
250	19	21	18	12
300	25	27	23	16
400	33	34	26	19
500	39	43	30	21

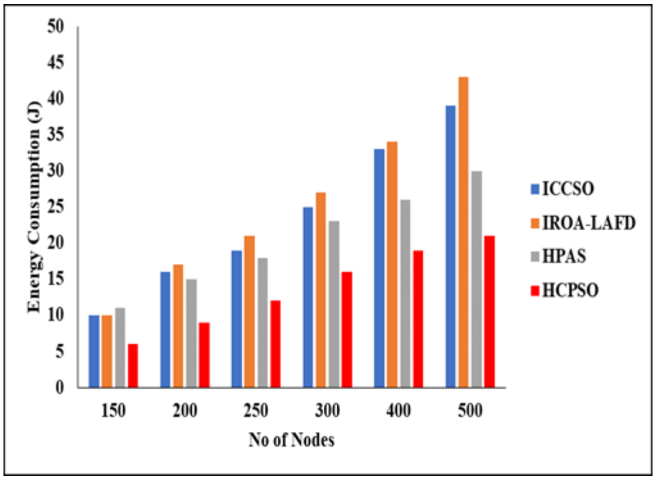

Figure 10 Energy Consumption

Figure 10 represents the Energy Consumption of the Network of the proposed model, in this analysis, the proposed model takes the better energy consumption ratio.

6.2.4. Network Lifetime

An essential parameter for efficient communication in MANET is network lifespan. For a network, lifespan and energy consumed by its nodes are directly proportional. The network's life expectancy is improved by the proposed method. Table 6 and Figure 11 show a comparison of the proposed technique with existing practices in terms of network lifetime.

Table 6 Evaluation of Network Lifetime

No. of nodes	Network Lifetime (s)			
	ICCSO	IROA-LAFD	HPAS	HCPSO
100	60	119	98	150
200	75	140	115	300
300	86	186	140	420
400	94	230	167	530
500	120	265	198	580

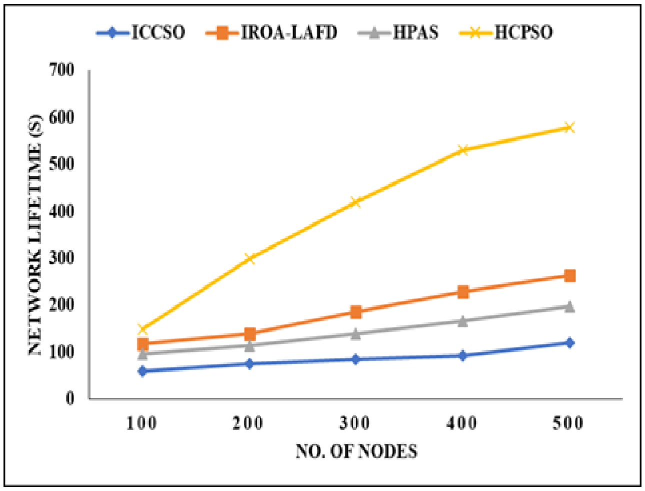

Figure 11 Lifetime of the Network

Figure 11 represents the Lifetime of the Network of the proposed model, in this analysis, the proposed model takes the better lifetime of the network ratio.

7. CONCLUSION

An intelligent threat to the MANET ecosystem, black hole and grey hole attacks are. In this paper, we suggest a deep learning-based methodology for identifying strange behavior in measurements caused by these two types of attacks. This study detailed a detection strategy that makes use of a combination of CNN and LSTM. The model is trained on non-attack data and can therefore detect attacks that have not yet been observed. As it is, they are responsible for defending a MANET from attacks that include dropping packets. When the number of colluding nodes and the frequency of packet dropping are both varied, the suggested detection approach can efficiently foil precise attackers, and the scheme attains colluding malicious nodes. The algorithm achieves a greater accuracy of 80% when comparing the actual values of network metrics like latency, PDR, energy consumption, etc. with their predicted threshold ranges.

REFERENCES

[1] Moudni, H., Er-rouidi, M., Mouncif, H. and El Hadadi, B., 2019. Black hole attack detection using fuzzy based intrusion detection systems in MANET. Procedia Computer Science, 151, pp.1176-1181.

[2] Gurung, S. and Chauhan, S., 2020. A survey of black-hole attack mitigation techniques in MANET: merits, drawbacks, and suitability. Wireless Networks, 26(3), pp.1981-2011.

[3] Eswaran, S., Rani, V., D., D., Ramakrishnan, J., & Selvakumar, S. (2021). An enhanced network intrusion detection system for malicious crawler detection and security event correlations in ubiquitous banking infrastructure. International Journal of Pervasive Computing and Communications, 18(1), 59–78. https://doi.org/10.1108/ijpcc-04-2021-0102.

[4] Manoranjini, J., Chandrasekar, A. and Jothi, S., 2019. Improved QoS and avoidance of black hole attacks in MANET using trust detection framework. Automatika: časopiszaautomatiku, mjerenje, elektroniku, računarstvoikomunikacije, 60(3), pp.274-284.

[5] Yasin, A. and Abu Zant, M., 2018. Detecting and isolating black-hole attacks in MANET using timer based baited technique. Wireless Communications and Mobile Computing, 2018.

[6] Sadhana, S., Sivaraman, E., & Daniel, D. (2021). Enhanced Energy-Efficient Routing for Wireless Sensor Network Using Extended Power-Efficient Gathering in Sensor Information Systems (E-PEGASIS) Protocol. Smart Systems: Innovations in Computing, 159–171. https://doi.org/10.1007/978-981-16-2877-1_16.

[7] Gurung, S. and Chauhan, S., 2018. A dynamic threshold based approach for mitigating black-hole attack in MANET. Wireless Networks, 24(8), pp.2957-2971.

[8] Thanuja, R. and Umamakeswari, A., 2019. Black hole detection using evolutionary algorithm for IDS/IPS in MANETs. Cluster computing, 22(2), pp.3131-3143.

[9] Rajendran, N., Jawahar, P.K. and Priyadarshini, R., 2019. Cross centric intrusion detection system for secure routing over black hole attacks in MANETs. Computer Communications, 148, pp.129-135.

[10] Daniel D., Preethi N., Jakka, A., & Eswaran, S. (2021). Collaborative Intrusion Detection System in Cognitive Smart City Network (CSC-Net). International Journal of Knowledge and Systems Science, 12(1), pp.60–73, https://doi.org/10.4018/ijkss.2021010105.

[11] Panda, N. and Pattanayak, B.K., 2018. Energy aware detection and prevention of black hole attack in MANET. International Journal of Engineering and Technology (UAE), 7(2.6), pp.135-140.

[12] Abood, M.S., Mahdi, H.F., Hamdi, M.M., Ibrahim, O.J., Mohammed, R.Q. and Ahmed, S.F., 2020, December. Black/Gray Holes Detection Tools in MANET: comparison and analysis. In 2020 IEEE 7th International Conference on Engineering Technologies and Applied Sciences (ICETAS) (pp. 1-8). IEEE.

[13] E. Sivaraman, "Dynamic cluster broadcasting for Mobile Ad Hoc Networks," 2010 International Conference on Communication and Computational Intelligence (INCOCCI), 2010, pp. 123-127.

[14] Arul Selvan, M. and Selvakumar, S., 2019. Malicious node identification using quantitative intrusion detection techniques in MANET. Cluster computing, 22(3), pp.7069-7077.

[15] Bhuvaneswari, R. and Ramachandran, R., 2019. Denial of service attack solution in OLSR based manet by varying number of fictitious nodes. Cluster Computing, 22(5), pp.12689-12699.

[16] Prasanna, D.J.D., Aravindhar, D.J. and Sivasankar, P., 2021. Block Chain based Grey Hole Detection Q Learning based CDS Environment in Cloud-MANET. Webology, 18(SI01), pp.88-106.

[17] Hassan, Z., Mehmood, A., Maple, C., Khan, M.A. and Aldegheishem, A., 2020. Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles. IEEE Access, 8, pp.199618-199628.

[18] Rani, P., Verma, S., Rawat, D.B. and Dash, S., 2022. Mitigation of black hole attacks using firefly and artificial neural network. Neural Computing and Applications, pp.1-11.

[19] Sathyaraj, P. and Kannan, K., 2021. Host based Detection and Prevention of Black Hole attacks by AODV-ICCSO Algorithm for security in MANETs.

[20] Janakiraman, S., Deva Priya, M., Aishwaryalakshmi, G., Suganya, T., Sam Peter, S., Karthick, S. and Christy Jeba Malar, A., 2022. Improved Rider Optimization Algorithm-Based Link Aware Fault Detection (IROA-LAFD) Scheme for Securing Mobile Ad Hoc Networks (MANETs). In 3rd EAI International Conference on Big Data Innovation for Sustainable Cognitive Computing (pp. 155-169). Springer, Cham.

[21] Rani, P., Verma, S. and Nguyen, G.N., 2020. Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network. IEEE Access, 8, pp.121755-121764.

[22] Ramachandran, D., Rajeev Ratna, V., PT, V.R. and Garip, I., 2022. A Low-Latency and High-Throughput Multipath Technique to Overcome Black Hole Attack in Mobile Ad Hoc Network (MTBD). Security and Communication Networks, 2022.

[23] Srinivasan, V., 2021. Detection of Black Hole Attack Using Honeypot Agent-Based Scheme with Deep Learning Technique on MANET. Ingénierie des Systèmesd'Information, 26(6).

[24] Liu, J., Jiang, X., Nishiyama, H. and Kato, N. (2013a) 'On the delivery probability of two-hop relay MANETs with erasure coding', IEEE Transactions on Communications, Vol. 61, No. 4, pp.1314–1326.

[25] Huang, H. and Zhou, Q. (2012) 'Petri-net-based modeling and resolving of black hole attack in WMN', The IEEE 36th Annual Computer Software and Applications Conference Workshops,Izmir, Turkey, pp.409–414.

[26] Charles E. Perkins, and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector (AODV) routing," Internet Draft, November 2002.

[27] A. Shevtekar, K. Anantharam, and N. Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers," IEEE Commun. Lett., vol. 9, no. 4, Apr. 2005, pp. 363–65.

[28] Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, "Black hole Attack in Mobile Ad Hoc Networks" Proceedings of the 42nd annual Southeast regional conference ACMSE 42, APRIL 2004, pp. 96-97.

Authors

S. Venkatasubramanian received a B.E. degree in Electronics and Communication from Bharathidasan University and M.E. degree in Computer science from Regional Engineering College, Trichy. He has 24 years of teaching experience. He is currently pursuing doctoral research in mobile Ad hoc networks. His areas of interest include mobile networks, Network Security, and Software Engineering. He has published several papers in international journals and international conferences, filed four patents, and authored 5 textbooks. At present, he is working as Associate Professor in the Department of Computer Science and Business Systems at Saranathan College of Engineering, Trichy, India. He has also received the Dr.Sarvepalli Radhakrishnan Lifetime achievement National award, Academic Excellence Award 2022, and Global teachers Award.

Dr. A. Suhasini is a Professor of Computer Science and Engineering at Annamalai University, Chidambaram. She has published several research papers in international and national journals and conferences of repute. She has been guiding several research scholars. Her area of interest includes Computer Networks, Image Processing, Machine learning techniques, Pattern classification Techniques, and Network security. She has more than 28 years of academic experience, and she is an active member of the Computer Society of India and ISTE.

S. Hariprasath is Working as Assistant Professor in Department of Electronics and Communication Engineering in Saranathan College of Engineering, Trichy. He obtained B.E Degree from Kongu Engineering College and M.E (communication systems) degree from Saranathan College of Engineering. He completed Advanced Post Graduate Diploma in VLSI (A.PG.D.VLSI) from Semiconductor Complex Limited (SCL). He has 19 years of teaching experience and 14 years of research experience. He is pursuing Ph.D degree in Anna University, Chennai. He has published 8 research papers in reputed international journals, 22 research papers in international conferences and 10 research papers in national conferences. He has published 3 patents. He has authored 3 books . His research interest includes Biometrics, Pattern Recognition, Image processing, FPGA Programming, HDL Programming and Machine Learning.

How to cite this article:

S. Venkatasubramanian, A. Suhasini, S. Hariprasath, "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), PP: 724-735, 2022, DOI: 10.22247/ijcna/2022/217705.