A NOVEL FIREFLY-BASED NODAL GRADIENT ARTIFICIAL NEURAL NETWORK TO MITIGATE BLACK HOLE AND GREY HOLE ATTACKS

S. MAHESWARI[1], R. VIJAYABHASKER[2], KANDASAMY K[3]
[1, 2, 3]Department of Electronics and Communication Engineering,
[1, 2, 3] Anna university Regional Campus Coimbatore, Tamilnadu, India.
E-mail: maheswariselvaraj5@gmail.com;vb@aurcc.ac.in;kkandasamy.03@rediffmail.com

Abstract.

Wireless connectivity and the newest advancements in mobile devices are employed to develop "a Mobile Ad Hoc Network (MANET)", which would be a grouping of mobile nodes connected without needing a permanent structure. Those networks are vulnerable to various attacks, comprising the black-hole attack (BHA), gray-hole attack (GHA), and so many others. Numerous scientists have focused on the identification and prevention of specific assaults, either GHA or BHA. Yet MANET's security over a dual-threat is weak. Hence, this paper introduces a novel firefly-based nodal gradient artificial neural network approach that is used to protect the attacks in MANETs. Finding the second cluster head inside the primary clusters eliminates the need for re-clustering, a Cuckoo search-based optimization approach is utilized. Dynamic threshold-based AODV routing protocol must be adaptive in the network structure and preserve routing data for packets to be routed to respective endpoints. The results portion of this paper explains how the system's performance can be enhanced by carefully selecting the optimum nodes for transmitting data packets throughout the network. The findings indicate that the provided method outperforms the prior work in terms of attack performance and that findings are depicted in graphical form by using the Origin tool.

Keywords: *Mobile Ad Hoc Network (MANET), black-hole attack (BHA), gray-hole attack (GHA), Cuckoo search-based optimization, Dynamic threshold-based AODV routing protocol, firefly-based nodal gradient artificial neural network*
DOI Number:10.14704/nq.2022.20.8.NQ44478 **NeuroQuantology 2022; 20(8): 4489-4500**

1. Introduction

Nodes in wireless networks could move around freely and cheaply without the support of cables or wide-ranging infrastructural facilities, which is why they are so well-known in network access. A network device and wireless device are the two major parts of a mobile medium, to become more precise. Since wireless networks use an open medium, their topology changes frequently, there is no centralized point for monitoring or management, and there is no clear line of defense, nodes in wireless networks are prone to attacks than nodes in wired networks (traditional). MANET, on the other hand, is a network with no underlying infrastructure, allowing users to roam freely**(Tu et al. 2021)**. Since the network topology is dynamic and frequently changes, the nodes can move freely around it. Because of their challenging utilizations in civilian and

military, environmental monitoring, and industrial innovation, MANETs have emerged as potential experts. Due to their minimum cost and ease of use, the nodes can be deployed anywhere. Aside from this, they don't have a lot of ability to combat a variety of malicious attacks. However, because of the unique characteristics of MANETS, several security attacks have been discovered. It is possible to launch a "black-hole and grey-hole attack." In figure 1, architecture of MANET is provided**(Srilakshmi et al.2021)**.

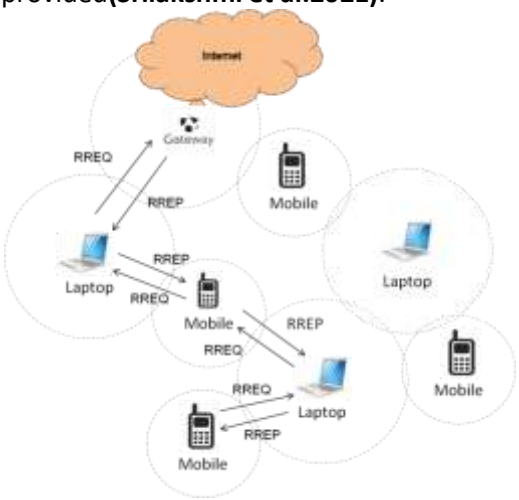


Figure 1: Architecture of MANET

It is often used in a wide range of settings, including crisis response, mobile computers, corporate meetings, and the military, among others. This kind of network has several unique properties such as node mobility and restricted capabilities including limited memory storage, low power consumption, and limited network due to the open wireless channel. Predictive, reactive, and hybrid routing protocols are all now used in such networks. A mobile node in a bar counter network has knowledge about the route for those other nodes as well as exchanges routing messages with each other to have a current and accurate path, while in a reactive (on-demand) network source nodes do not have enough way for receiver node and must create the route on supply whenever they want to interact with their target. There is a dual routing protocol that combines both proactive and reactive routing techniques across one.

All packets traveling via a rogue node known as a "Blackhole" are dropped in this attack**(Jari et al. 2021).** There's one network device that utilizes the routing protocol to establish that its route to an end node is the most efficient. This attack does not forward the packets but rather drops them. As a result, the Packet Drop attack is another name for the Black Hole attack. Group attacks are used in the event of Collaborative Black Hole attacks. Every time information is transmitted from one node to another, an RREQ packet has been sent. The RREQ is likewise accepted by the hazardous nodes. The initial response from the Black Hole node is an RREP. “Internal and external black-hole attacks are divided into two categories based on the existence of attacker nodes”. Additionally, the assaults may be classified in many ways depending on how creative the attacker nodes are, such as “single black-hole attack and collaborative black-hole attack”. Figure 2 shows the framework of black and grey hole attacks.

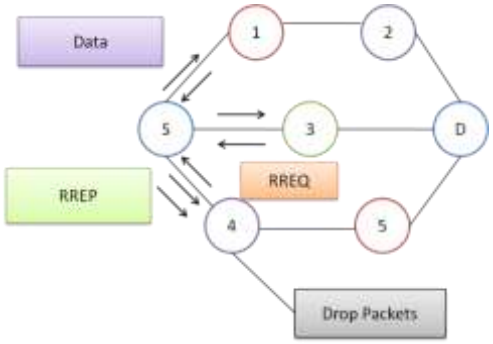


Figure 2: Framework of black and grey hole attack

The grey-hole attack is a selected dropping attack that may be defined as a specific instance of a black-hole attack that an attacker node, like a black hole assault, mainly consists of the network's path and does not discard all packets of data sent via it. Initially, an attacker node may appear to be a valid network to believe, however, later on, it may choose to delete packets with a high likelihood from selected nodes or in a specified pattern. As a legitimate node in the processes of routing protocol and data exchange, the grey hole assault participates in the grey hole attack. Detecting the discovery of attacker nodes in this form of assault is challenging because these nodes discard

transmissions routed via them for some time before acting properly as genuine nodes again for the rest of life**(Kumar et al. 2021).**

Due to their compact size, limited memory, as well as poor processor power capacities, MANET nodes offer limited computing capability. Each node serves as a server and a router at the same time. "To interact with one another, routing protocols such as Ad-hoc On-Demand Distance Vector, Source Routing, and are employed, that assist in the discovery of the most efficient path between the transmitter and the receiver". Traditional MANET routing protocols presume that almost all nodes are trustworthy and collaborative, but in practice, nodes' activity might vary and they may or may not communicate with one another. Like a function of this presumption, MANET's routing protocols include several flaws that an attacker might use to disrupt the information exchange**(Kalime and Sagar 2021).** This paper presents the framework for mitigating black and grey hole attacks. Hence, this paper proposed the firefly-based nodal gradient artificial neural network to mitigate such attacks.

The remainingportion of the article is structured as shown: section II offers the related works and problem statement. Section III discusses the suggested methodology. Section IV provides the result analysis and section V concludes the entire paper.

2. RELATED WORKS

In their investigation of WSN and MANET convergence in the Internet of Things, Quy et al. (2021) took into account a crucial issue, namely how a converged network gives quality of service (QoS) assurances to rich multimedia utilizations. They investigated the WSN-MANET QoS-guaranteed routing technologies. An effective trust establishment-based routing evidence strategy (ETERE) that worked in the generation and modification of mental representation of specified data was suggested by Yamini et al. (2022). In contrast to existing approaches, Tahboush and Agoyi (2021) proposed hybrid wormhole attack detection (HWAD) method that is capable of detecting both in-band wormholes through the performance of round-trip time (RTT) depending on its hop count and packet delivery ratio (PDR), as well as out-of-band wormholes through the performance of transmission range between succeeding nodes. By avoiding completing wormhole identifications for every available node in the network, HWAD decreased the latency and energy. There is no specialized hardware or middleware required for HWAD. Trust and trust calculations are discussed by Kumar and Shekhar (2021). In order to lessen the consequences of assaults, a trust-based fuzzy bat (TBF) optimization framework is suggested and put into practice in this study. The K-nearest neighbor (KNN) method for clustering and fuzzy inference for choosing the cluster head is novel techniques that should be used in MANETs to identify black hole attacks (Farahani (2021)). The confidence of each node will be determined using the beta distribution and Josang mental reasoning. Fuzzy inference will choose the cluster head based on reputation and remaining energy. The trust server then verifies the target node. If permitted, it alerts the cluster head; if not, it recognizes the node as a malicious node participating in a black hole assault on the cluster. The general-purpose "ad hoc on-demand distance vector (AODV) protocol" was subjected to denial-of-service assaults like black hole assaults (Talukdar et al. 2021). It employs three methods: "standard AODV, black hole AODV (BH-AODV), and detected black hole AODV (D-BH-AODV)", and shows that black holes significantly reduce network behavior. Using two methods, an "intrusion detection system (IDS)" and an "encryption technique (digital signature)" with the idea of prevention, they have been able to identify black hole assaults inside networks. Additionally, by modifying the count of nodes, packet size, and simulation timeframes, the regular protocols are examined for several QoS factors, such as PDR, latency, and overhead. Singh and Khari (2021) identified a

black hole attack and enabled secure data transfer. A hybrid protocol that combines the ideas of AODV for route discovery, EECBR for packet forwarding under black hole attack, and greedy routing for reducing network overhead during path selection is suggested for this purpose. The detection of the attacker node is performed during the route building. Ram et al. (2021) suggested a strategy that employs the dynamic threshold to recognize the attacker nodes and prevent the complete path containing the attacker nodes. Comparing and analyzing the most recent research on the development of grey and black holes is done by (Hamdi et al. (2022)). The black hole and the worm hole assaults were the two main attacks that Shukla et al. (2021) attempted to concentrate on. They have used two different kinds of protocols, including scalable-dynamic elliptic curve cryptography and AODV. According to Khan et al. (2021), the usage of the validity bit in the current approach has a flaw. This essay also offers a comparison of several academics. Black hole attacks are detected and prevented by the source node utilizing a binary partition clustering-based algorithm. The Blackhole attack is discussed in Gaber and Azer's (2022) analysis of MANETs utilizing a variety of settings for single and multiple connections. Kuadey et al. (2021) discuss research constraints on the suggested works, necessary follow-up study, and remedies put forward to prevent black hole threats. Reddy and Dhananjaya (2022) promote the use of threshold assessment and cryptographic verification in the OSPFV protocol integration with built-in security.

3. Problem Statement

For network authentication, they should be limited by the maximum transmission response time and minimal end-to-end delay. The timing considerations were employed to identify the problematic node by employing the quick response rounds travel time. It is necessary to provide an efficient route detection mechanism for received packets across the shortest route. To discover the shortest path between source and destination nodes, the efficient protocol is needed. To maintain proper identification of severe assaults like black holes and grey hole attacks, advanced techniques are needed.

4. PROPOSED METHODOLOGY

The suggested solution to prevent “black hole and grey hole attacks” in MANETs is described in this paper, which uses a firefly-based nodal gradient artificial neural network. In this paper, the study uses cuckoo search-based optimization to choose cluster heads. After that, the network arrangement and source node were employed. Then, to mitigate, it uses AODV with dynamic thresholds and a firefly-based nodal gradient artificial neural network. Finally, the receiver node is received by the mobile system. Figure 3 shows the complete flow of thisresearch.

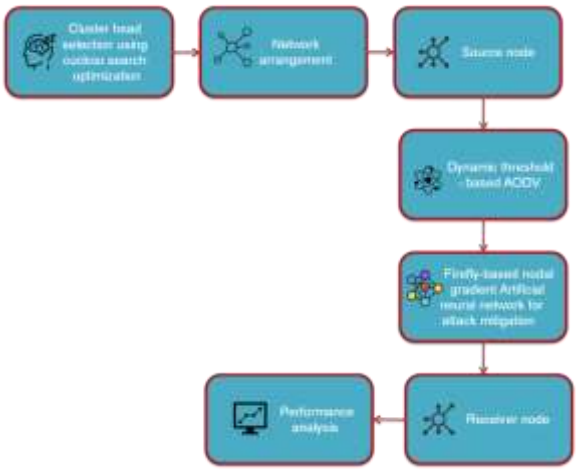


Figure 3: Complete flow of this research

A. Cluster Head Selection Using Cuckoo Search Optimization

The Cuckoo search method is used to provide a foundation for safe transportation including an efficient cluster head (CH) selection. The initial CH selection is mostly dependent upon that trust organization’s prior record of power as well as trust level for the nodes. Following that, cluster construction is done by the cluster head, which accepts control signals from the broadcaster's mobile nodes. With its expertise in detail and reliability of the optimal solutions for the optimized backup cluster

head selection, the path selection system includes the Cuckoo search-based optimization technique. Algorithm 1 presents the pseudo-code for the cuckoo optimization.

Algorithm 1: Cuckoo search optimization algorithm

start
Object function f(x), x = (x1,.....,xd)^T
Create initial population of n host nests xi(i =1,2,....,n)
While (t < MaxGeneration) or (stop criterion)
Obtain a cuckoo by levy flights in a random manner
estimate its fitness F_i
Select a nest randomly among n (say j)
if $F_i > F_j$
Substitute j by the new solution;
stop
A portion (Pa) of the worst nests is removed, and new ones are constructed.
maintain the finest solutions or create excellent solution nests;
Determine the current best by ranking the solutions
Stop while
Outcomes from the processing stage and visualization
Stop

The pseudo code using cuckoo search constructed in a biased style involving unpredictable step sizes is shown in Algorithm 1. The biased randomized step size of the cuckoo search may be calculated using equation (4.1)-(4.3).

$stepsize = slgval^{*}(nest(slg(m)) - nest(slg(m))$ (1)

$New\_nest = nest + stepsize^{*}Q$ (2)

where

m: Number of host nests

slg : Random value

$Q = rand(size(nest)) > gh$(3)

The cuckoo search-based cluster head optimization is shown in Figure 4, as well as the specific processing methods for producing the optimized cluster head are always as below.

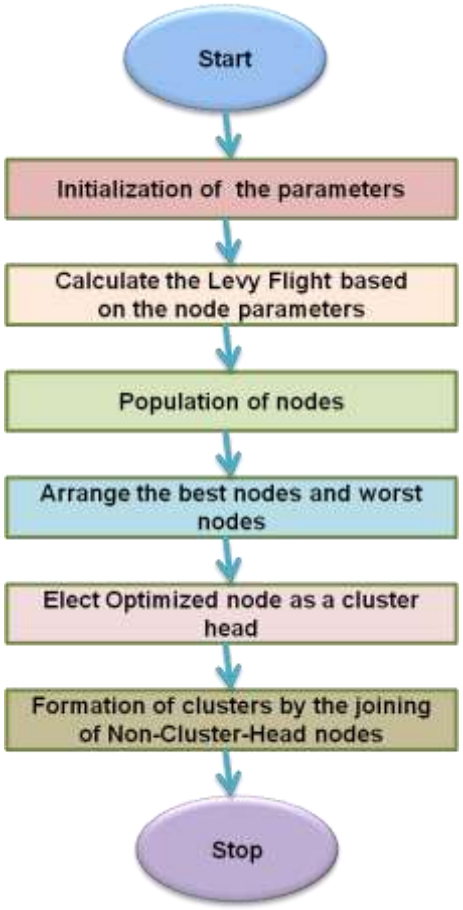


Figure 4: Flowchart of cuckoo search optimization

Step 1: Initialization

To begin the search, consider the usage of mobile nodes and node characteristics to still be cuckoo nests with eggs within nesting, with many eggs for each nest representing a range of solutions. Assume a mobile ad hoc network with several nodes then the initial confidence level and power level of the node, where T, as well as E, is still the trust level and the power level of the access points, respectively.

Step 2: Levy Flight Calculation

When the Levy flight provides a moving average, the randomized maximum number of generations is chosen out of a Levy distribution.

$Levy \sim v = r^{-\lambda}; (1 < \lambda \leq 3)$(4)

The Levy has an unlimited variation as well as average, which effectively constitutes a randomness method with such a simple linear dynamic threshold distribution as well as a big-tailed around the best solution found

so far, generating many innovative solutions which accelerate up a local searching.

The Levy flight is computed using pair independent variables, *R andF* that have a regular Distribution function as a result of the nonlinear transformation.

$$u = R \,/\, |F|^{\frac{1}{\beta}} \quad (5)$$

The combination of factors inside the nonlinear activation function given adequate normalization is shown in the following expression.

$$X_i = \frac{1}{i^{\frac{1}{\beta}}} \sum_{q=1}^{i} u_q \quad (6)$$

Eq. (6) conforms just to the Levy probability density function of bigger *i*, where β is the number of stages.

Step 3: Node Population

Several nodes are formed at irregular intervals at the start of the growth process by breaking the cluster criteria *R* and *F*. The production of new community responses $y(r+1)$ for the next production is shown in the equation below.

$$y_j^{(r+1)} = x_i^r + \beta \oplus Levy(\lambda) \quad (7)$$

Where β> 0 denotes a larger step length and $\oplus$signifies entry-by-entry multiplying.

Initialize minimum price values with all nodes in a network and then use the objective functions *j* (λ) for a node to get the initial cluster value. Every time a search is performed, the occupancy quantity of nodes is updated.

Step 4: Selecting the Best and Worst Nodes

The greatest node is communicated to the next generations with an excellent quality the cluster characteristics which are calculated to use the probability variable Pa because the worst networks get sent to the next generations with only a poor quality of network characteristics which are calculated to use the probability function Pa. The very worst nodes, on either extreme, are identified and excluded from future computations.

Step 5: Optimized Node as a cluster head

A large mass for a given cluster would be chosen from among the optimized nodes with highly suggested node characteristics from the ordered queues, implying that the cluster head node's trust, as well as power levels, will be adequate to handle accident connectivity.

B. Network Arrangement

MANET would be a network technology made up of a large number of mobile nodes that are joined at random throughout a network. Zones leaders play an important role in this suggested paradigm since can perform network connectivity alongside the communications node. Every zone leader has a zone member assigned to them, as well as promotes continuous improvement serve as routes. Data transmission operations are carried out by the zone leader using communications nodes to move packets ahead. Zone members are similar to kid nodes with zone leaders. A promote continuous improvement and zone members may move around freely only within the movement zone. The zone leaders with communications nodes are paired together. Under highly mobile, this coupling evolves and has been typically built using multiple pathways. To enable the whole network's capabilities, all nodes participating in networks will be created on the mobile agent environment.

C. Source Node

The Source node (SN) network model is made up of two major techniques that enable ad hoc networks to locate and maintain source nodes. Because all routing choices are constantly updated within the mobile nodes, source routing does not need an intermediate node to update routing information to route packets. Route discovery and route maintenance are two methods found in SN. Source nodes flood the designated route demand packets during route discovery. The technique in which node (S) transmits packets to the destination (D) while also having access to the source S is known as route discovery. The protocol offers three distinct processes for path selection. The packet forwarding S detects whether the communication network has changed, and the route to the destination D could be utilized because of two nodes mentioned in the route will be out of reach of each other. When route

maintenance reports that the source node is broken, S sends out using a route error packet. Sender S may try asking route service for a security code using any other route towards D.

D. Dynamic Threshold-Based AODV

AODV is a network protocol. Routing is detected anytime an appropriate to route data throughout this protocol. When finding the route, a source node initiates the route to the destination. Routing protocol, as well as route maintenance, is the two aspects of the mobile nodes. An RREQ application is sent to locate the route during the routing process. The RREQ information is transmitted across the system until something identifies the indirect route only with the terminal's latest current routing information. The RREQ application also provides an identifier to guarantee that path is not looped and also that the response contains just the most recent data. When RREQ queries are sent from one node to the next, the data are maintained for each node's record. Once the demand is returned to the source, the node raises the record to the appropriate level. When one of the intermediate nodes moves, the surrounding node detects that a connection failure has happened and transmits the packet losses signal to its upwards neighboring node until something reaches the origin.

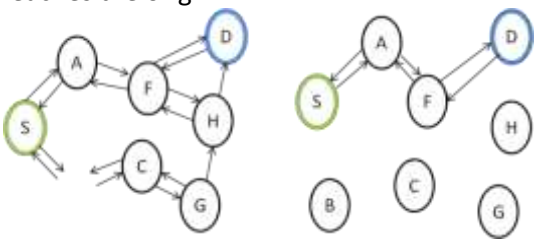


Figure 5: AODV routing model

As indicated in Figure 5, the network's source is 'S,' and the network's destination is 'D.' These clear arrows represent PREQ transmission, whereas the grey ones represent reverse route inputs. A dynamic threshold-based AODV model has been developed, in which the level of made the performance, i.e., the trustable and non-trustable value, is determined dynamically by employing several secure and timely packets to a destination identifier. It computes the variance from several interactions between integrated packets to a destination identifier for threshold calculation. The degree of trust ability (DT) is computed as

$$DT = \sqrt{\sum_{k=1}^{i} E_i^2 / l} \qquad (8)$$

E is the destination sequence number that has been the i^{th} response packet; when i is the sequence of ensuring the data. All suspicious nodes are determined by their large wireless range as well as routing latency. The trusting assessing node evaluates the overall trustworthiness of the neighbor node (NN) in the designated communication line. The modified and ultimate threshold of NN then is data in structured on directly and indirectly different levels. The ultimate trust calculation might be done either passively or actively

A. Firefly–based Nodal Gradient Artificial Neural Network for Attack Mitigation

The firefly algorithm, created and developed by Yang one of the most effective environment systems, models the lighting and movements of fireflies. The appeal of each firefly is defined by its brilliance; hence they attempt to advance toward bright light in their social activity. The brilliance of each firefly is determined by its fitness rating.

Algorithm 2: Pseudo-code for firefly algorithm

Start
Define objective function f(x)
Create an initial population of fireflies
Calculate light intensity I
State the absorption coefficient Y
While (t < Max_Generation)
For i = 1 to n (all n fireflies)
For j = 1 to n (all n fireflies)
If (I_J> I_i), shift firefly i towards firefly j
End if
Analyze fresh ideas and update light output
End for j
End for i
Choose the current top fireflies by ranking them
End while
Stop

Yang suggests using Eq. (9) to determine the average of the two fireflies' y_l and y_x during these algorithms.

$$z_l^{k+1} = z_l^k + \beta_0 e^{-\gamma v_{lx}^2}\left(y_l^k - y_x^k\right) + \propto \in_x^k \quad (9)$$

Because of this$\gamma = 0$, we can use these equations to get the $\beta =$ attractiveness of an object when its v_{lx} =distance from another object y_l and y_x is equal to its distance from itself. We can also use these equations to derive the $\gamma =$ light absorbance value. The Firefly Algorithm's efficiency functioning relies on such variables.

To develop a Classifier network consisting of two hidden units, the Firefly Algorithm is used. The inputs component of the ANN was used to determine the best path. There are two important factors to consider while using this method: how many fireflies are present in a given FA and how they are selected as an optimization process. Strength training, as well as bias matrices length, is required for n firefly in the FA community to be determined. By counting the number of connection weights,

$$p = (j+1) \times g + (g+1) \times g + \cdots + q \times (g+1) \quad (10)$$

For example, in this example, p is the total number of weights; j=13 is the count of input synapses; q=5 is the count of output neurons, and g=10,7 is the number of hidden layers. A Firefly algorithm creates random numbers in the search area after determining the matrix's size. The effectiveness of the method is unaffected by the arrangement of the starting date. A position in the entire search space becomes more enticing to all fireflies after a certain number of repeats. As a consequence, we've located the Earth's lowest level.

$$E\frac{1}{n}\sum_{l=1}^{k}(x - \hat{x})^2 \quad (11)$$

There are n observations in the validation set, wherein x seems to be the actual value as well as $\hat{x}$ is the target value. A Firefly method was a major motivator for developing the Artificial Neural Network for its excellent locally optimal avoiding with quick convergence speed in the algorithm.

E. Receiver Node

When the receiver gets the RREP packet, it decides the path to take to get to the destination. During connection, it makes a key exchange demand to its instructor node without transmitting any information to its destination. It's time for the sender to put together the message it intends to deliver after getting the shared session key. This is the format of the message that is sent from S to R. When the intermediate node gets this data packet, it transfers the packet toward the destination. When the data packet comes to its final destination, the process repeats. When this data packet is received inside the time stamp period, the initial post is re-created. The destination node sends an acknowledgment if the message is legitimate. The destination node asks the central server for the connection secret before transmitting the approval.

5. RESULT AND DISCUSSION

This paper proposed the firefly-based nodal gradient artificial neural network to mitigate black and greyhole attacks. "A Mobile Ad Hoc Network (MANET) is a network of linked wireless sensor nodes that interact via limited capacity wireless access". Each connection node may function as a transmission, recipient of the message, or controller. When a node is a transmitter, it can send messages to every network with one point. As a transmitter, it may accept information from other networks. One of the most susceptible types of assault is the black and grey hole attack, which is closely tied to routing protocol in MANETs such as AODV and DSR. A packet may be relayed to the endpoint or next routers in the path once the nodes act as a gateway. Every node may delay information pending transmission is appropriate.

A. Accuracy rate

Figure 5 shows the comparison of the accuracy rate. The accuracy rate for information is the proportion of right observations. It indicates that once we have a 95 percent accuracy rate for Classification methods, we should expect 85 accurate

forecasts from every 100. The proposed method of firefly-based nodal gradients artificial neural network has a greater accuracy rate when contrasted to the conventional methods like decision tree, support vector machine, k-nearest neighbor, and naïve Bayes.

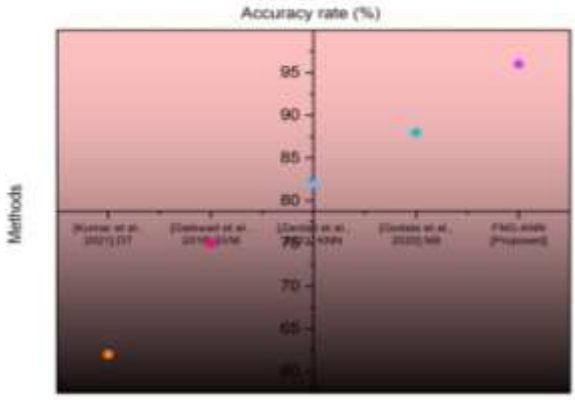


Figure 5: Comparison of accuracy rate

B. Packet delivery ratio

Figure 6 reveals the comparative analysis of the PDR. PDR is estimated as a percentage of total packets received obtained there at the endpoint divided by total packets transmitted by the continuous data rate source. The efficiency of networking improves as the packet delivery ratio values rise. The proposed work has the greatest PDR than that of the traditional methods throughout this examination.

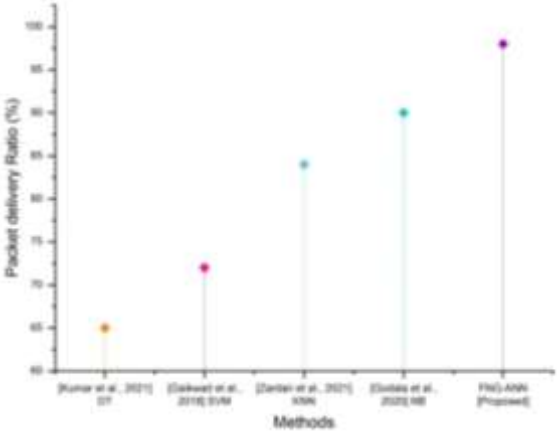


Figure 6: Comparison of packet delivery ratio

C. Packet loss

Figure 7 depict the packet loss. Packet loss may be calculated as a percentage of the number of packet losses throughout delivery owing to delay and every other cause based on the number of packets transmitted. With lower packet loss levels, a network's performance improves. The proposed work has a minimal packet loss than that of the existing approaches throughout this examination.

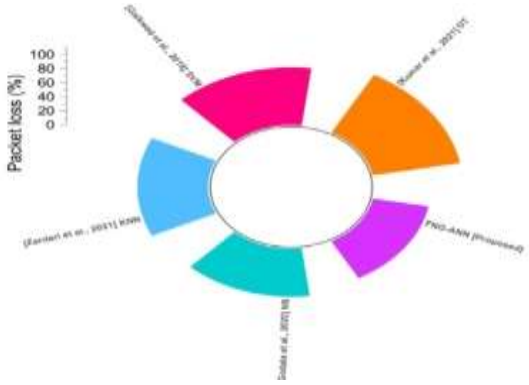


Figure 7: Comparison of the packet loss

D. Network throughput

Figure 8 depict the network throughput. Network throughput is a ratio of the total of thoroughly assess transferred from source to the destination in a certain period, expressed in bits per second. With higher data transmission levels, a network's performance is improved. The proposed work has the greatest network throughput than that of the existing approaches throughout this examination.

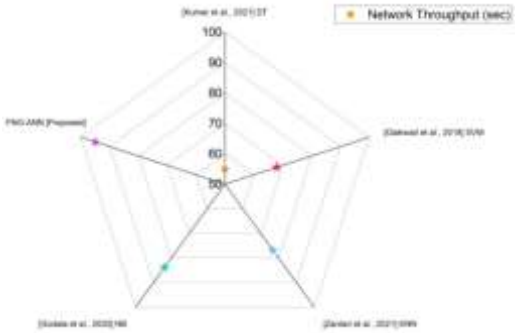


Figure 8: Comparison of the network throughput

E. Packet generated

Figure 9 depicts the total amount of packets generated for all nodes during the experiment. Networks impacted by the grey-hole attack produced more packets than the networks impacted by the black-hole attack,

as seen in Figure 9. Throughout simulations of each situation with varied numbers of nodes, different numbers of packets are created. It can be observed that the number of packets created is dependent on the count of network nodes. When the count of nodes is low, the count of produced packets is similarly low. When the count of nodes is set to the maximum, the count of created packets is likewise set to the maximum. It is observed that a network subjected to a grey Hole assault produces more packets than one subjected to a Black Hole attack. As a consequence of the Black Hole assault dropping all types of packets, it will create fewer packets. Gray hole attacks, on the other hand, only drop a certain sort of packet. As a result, black hole attacks have a greater effect on the network than grey hole attacks.

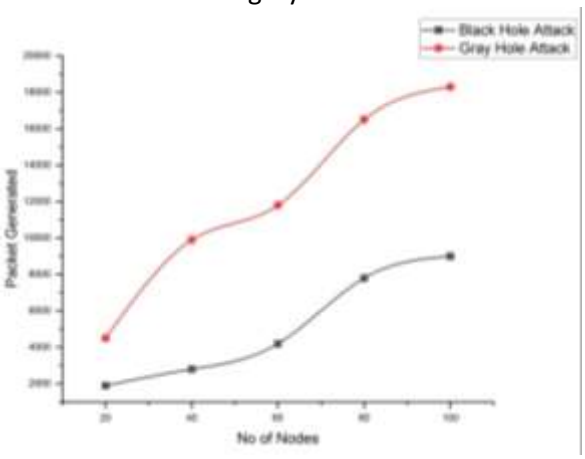


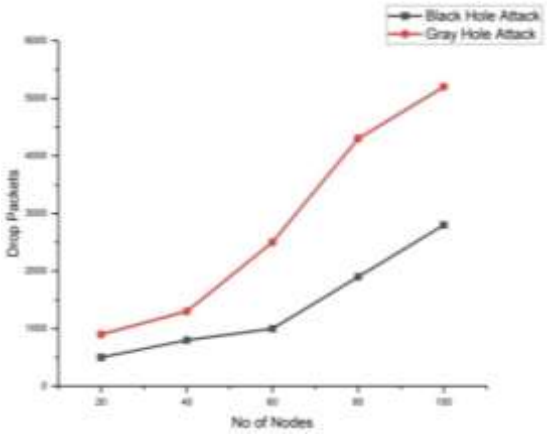
Figure 9: Packet generated

F. Drop packet

Figure 10 depicts the total count of drop packets obtained by all nodes during the experiment. It illustrates that the system impacted by the grey-hole attack has a larger number of drop packets than the networks damaged by the black-hole attack. Throughout computations of each condition with varied nodes, variables relating to packets are created. As a result of the Black Hole attack dropping all types of packets; it blocks network traffic as well as different types of packets such as management and acknowledgment packets. As a result, the maximum count of generated packets by a system impacted by a Blackhole assault is lower than the total quantity of generated packets by a system impacted by a grey-hole attack. As a result, the maximum count of drop packets by a system impacted by a black-hole attack is fewer than that of the overall number of drop packets by either network impacted by a grey-hole assault.

6. CONCLUSION

MANETs are identity and infrastructure-free networks made up of mobile nodes which can connect with one other across a variety of different mediums. Every mobile node in MANET may freely travel in any direction and regularly changes its connections with other devices. Ad hoc networks need a high level of security. We proposed the firefly-based nodal gradient artificial neural network to mitigate black hole and grey hole attacks. Since MANET has no centralized infrastructure, its dynamic routing algorithm makes it susceptible to



attacks like the "black hole" and "grey hole" In

Figure 10: Drop packet

a black hole attack, the attacker user claims to have the quickest route to the target, the highest sequence number, and falsely responds to the route request (RREQ), and then removes all received packets completely. Because it drops packets with a strong chance and acts like nodes over a period of time, the grey hole attack is more difficult to detect than other types of attacks.

References

1. Tu, J., Tian, D. and Wang, Y., 2021. An active-routing authentication scheme in MANET. IEEE Access, 9, pp.34276-34286.

*e*ISSN1303-5150

2. Srilakshmi, U., Veeraiah, N., Alotaibi, Y., Alghamdi, S.A., Khalaf, O.I. and Subbayamma, B.V., 2021. An improved hybrid secure multipath routing protocol for MANET. IEEE Access, 9, pp.163043-163053.
3. Jari, H., Alzahrani, A. and Thomas, N., 2021, November. A Novel Indirect Trust Mechanism for Addressing Black hole Attacks in MANET. In Proceedings of the 11th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications (pp. 27-34).
4. Kumar, T.A., Devi, A., Padmapriya, N., Jayalakshmi, S. and Divya, P., 2021. A Survey on Advance Black/Grey hole Detection and Prevention Techniques in DSR & AODV Protocols. International Journal on Wireless, Networking & Mobile Communication Innovations [ISSN: 2581-5113 (online)], 5(1).
5. Kalime, S. and Sagar, K., 2021. A review: secure routing protocols for mobile adhoc networks (MANETs). Journal of Critical Reviews, 7, pp.8385-8393.
6. Quy, V.K., Nam, V.H., Linh, D.M., Ban, N.T. and Han, N.D., 2021. A survey of QoS-aware routing protocols for the MANET-WSN convergence scenarios in IoT networks. Wireless Personal Communications, 120(1), pp.49-62.
7. Yamini, K.A.P., Stephy, J., Suthendran, K. and Ravi, V., 2022. Improving routing disruption attack detection in MANETs using efficient trust establishment. Transactions on Emerging Telecommunications Technologies, 33(5), p.e4446.
8. Tahboush, M. and Agoyi, M., 2021. A hybrid wormhole attack detection in mobile ad-hoc network (MANET). IEEE Access, 9, pp.11872-11883.
9. Kumar, R. and Shekhar, S., 2021. Trust-based fuzzy bat optimization algorithm for attack detection in manet. In Smart innovations in communication and computational sciences (pp. 3-12). Springer, Singapore.
10. Farahani, G., 2021. Black hole attack detection using K-nearest neighbor algorithm and reputation calculation in mobile ad hoc networks. Security and Communication Networks, 2021.
11. Talukdar, M.I., Hassan, R., Hossen, M.S., Ahmad, K., Qamar, F. and Ahmed, A.S., 2021. Performance improvements of AODV by black hole attack detection using IDS and digital signature. Wireless Communications and Mobile Computing, 2021.
12. Singh, P. and Khari, M., 2021. Empirical analysis of energy-efficient hybrid protocol under black hole attack in manets. In Research in intelligent and computing in engineering (pp. 725-734). Springer, Singapore.
13. Ram, A., Kulshrestha, J. and Gupta, V., 2021. Secure Routing-Based AODV to Prevent Network from Black Hole Attack in MANET. In Proceedings of 6th International Conference on Recent Trends in Computing (pp. 633-642). Springer, Singapore.
14. Hamdi, M.M., Flaih, A.F., Jameel, M.L., Mustafa, A.S., Abdulelah, A.J., Jubair, M.A. and Ahmed, A.J., 2022, June. A study review on Gray and Black Hole in Mobile Ad Hoc Networks (MANETs). In 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-6). IEEE.
15. Shukla, M., Joshi, B.K. and Singh, U., 2021. Mitigate Wormhole Attack and Blackhole Attack Using Elliptic Curve Cryptography in MANET. Wireless Personal Communications, 121(1), pp.503-526.
16. Khan, A.U., Puree, R., Mohanta, B.K. and Chedup, S., 2021, April. Detection and Prevention of Blackhole Attack in AODV of MANET. In 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS) (pp. 1-7). IEEE.
17. Gaber, M.M. and Azer, M.A., 2022, May. Blackhole Attack effect on MANETs' Performance. In 2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC) (pp. 397-401). IEEE.

18. Kuadey, N.A., Bensah, L., Twumasi, B.A., Ankora, C., Maale, G.T. and Kuadey, A.M., Black Hole Attack in Mobile Ad Hoc Networks: Challenges and Directions. International Journal of Computer Applications, 975, p.8887.
19. Reddy, B. and Dhananjaya, B., 2022. The AODV routing protocol with built-in security to counter blackhole attack in MANET. Materials Today: Proceedings, 50, pp.1152-1158.
20. Kocher, G. and Kumar, G., 2021. Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges. Soft Computing, 25(15), pp.9731-9763.
21. Zardari, Z.A., He, J., Pathan, M.S., Qureshi, S., Hussain, M.I., Razaque, F., He, P. and Zhu, N., 2021. Detection and prevention of Jellyfish attacks using kNN algorithm and trusted routing scheme in MANET. International Journal of Network Security, 23(1), pp.77-87.
22. Gaikwad, S.S., 2018. Detection and prevention of flooding attack in MANET using support vector machine (SVM). International Journal for Research Trends and Innovation, pp.81-85.
23. Godala, S. and Vaddella, R.P.V., 2020. A study on intrusion detection system in wireless sensor networks. International Journal of Communication Networks and Information Security, 12(1), pp.127-141.