

A Hybrid Genetic Algorithm-Based Secure Multipath Routing Protocol with Trust-Aware Clustering for Performance Optimization in MANETs

M.Parvathi¹, T.Shanmugavadivu², J.Jenshya³, Balasubramaniam C⁴, S.D.Vijayakumar^{5*}, Nanthini P⁶, S.B.Gopal⁷

¹Assistant Professor, Department of Artificial Intelligence and Data Science, Nandha Engineering College, Erode, Tamilnadu, India.

²Assistant Professor, Department of Computer Science, Nallamuthu Gounder Mahalingam College Pollachi, Tamilnadu, India.

³Assistant Professor, Department of Computer Science and Engineering, Nandha College of Technology, Erode, Tamilnadu, India.

⁴Assistant Professor, Department of Artificial Intelligence and Data Science, Nandha Engineering College, Erode, Tamilnadu, India.

⁵Assistant Professor, Department of Artificial Intelligence and Data Science, Nandha Engineering College, Erode, Tamilnadu, India.

⁶Assistant Professor, Computer Science and Engineering, Kangeyam Institute of Technology, Kangeyam, Tirupur, Tamilnadu, India.

⁷Associate professor, Computer Science and Design, Kongu Engineering College, Perundurai, Tamilnadu, India.

KEYWORDS:

Mobile Adhoc Network,
Routing,
Security,
Efficiency,
Optimization

ARTICLE HISTORY:

Received: 26.11.2025
Revised: 23.02.2026
Accepted: 14.03.2026

DOI:

<https://doi.org/10.31838/NJAP/08.02.16>

ABSTRACT

Due to significant improvements in wireless communication, Mobile Ad Hoc Networks (MANET) have been utilized in different fields, such as power conservation, and the Internet of Things (IoT), etc. The present routing protocols employed in MANETs are limited by the concomitant issues. The network's design challenges include limiting energy consumption and ensuring node security. This article presents the Hybrid Secured Routing Protocol (HSRP), which utilizes a Genetic Algorithm (GA) and an optimization approach to choose the most effective route in a multipath scenario. The research focused on selecting the most optimal route to reach the destination. The path with the most significant fitness score is considered optimal using density maxima and selected Cluster Heads (CHs) according to recent, indirect, and direct trusts. CHs select the best route using the cumulative characteristics of the ideal route, such as throughput, delay, and routing overhead. By obtaining a 17% improved packet delivery ratio, a 11% reduction in routing overhead with minimal attack detection time (68.6 sec) when compared to conventional procedures, the suggested HSRP model shows notable advantages over current approaches. These developments highlight the model's supremacy in energy conservation and dependable network performance.

Author's e-mail: mparvathicse@gmail.com, tvadivumca@gmail.com, jenshyaj@gmail.com, cbalu.cse@gmail.com, mail2vijay.sd@gmail.com, nanthumecse97@gmail.com, s.b.gopalece@gmail.com

Author's Orcid id: 0009-0005-6903-7615, 0009-0003-0180-0229, 0009-0006-2008-8945, 0009-0008-3477-6196, 0009-0002-1997-1707, 0009-0009-0160-9540, 0000-0002-3505-2412

How to cite this article: Parvathi M et al, A Hybrid Genetic Algorithm-Based Secure Multipath Routing Protocol with Trust-Aware Clustering for Performance Optimization in MANETs, National Journal of Antennas and Propagation, Vol. 8, No. 2, 2026 (pp. 188-204).

1. INTRODUCTION

CISCO predicts worldwide mobile devices will surpass 14 billion by 2025 [1]. The per capita ownership of

mobile devices will exceed 1.9. From 2018 to 2024, worldwide data traffic is projected to grow nearly sevenfold, reaching a monthly volume of 78.3 exabytes by 2025. Network devices would include integrated

Mobile-To-Mobile (M2M) modules (used for establishing device-to-device interactions without relying on ground stations), which act as the fundamental concept behind constructing MANET [2].

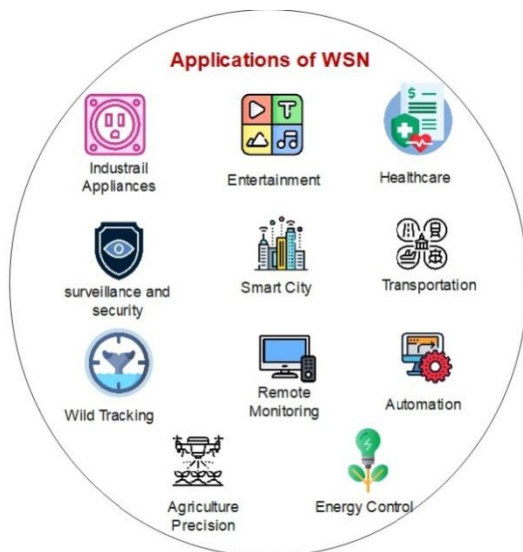


Fig. 1. Applications of MANET

MANETs are mobile devices that autonomously configure their settings to establish connections with other devices without depending on the base station. Despite their restricted capabilities, MANETs have proven to be a superior networking solution with flexible facilities. They have been utilized in various fields, such as surveillance and security, sophisticated grid setup, home automation, wild tracking, remote monitoring, smart city, energy control, agriculture precision, and many more, as shown in Figure 1.

Although MANET's characteristics provide attractive applications, they also bring significant disadvantages. One drawback of MANETs is the increased energy consumption caused by the frequent movement of nodes, mainly because no external energy source is available [3]. Ad hoc networks have considerable obstacles due to mobile nodes that rely on weak batteries, which need lengthy recharging or replacement periods. Further research is necessary to tackle this challenge by enhancing the effectiveness of protocol, system, and technological design. Hence, to improve the device's longevity and provide uninterrupted connection, the routing algorithm needs to include the power consumption of the end device.

However, if there are frequent changes in the topology, it might lead to an increased number of data collisions. This is because the links between nodes keep breaking. The topology changes while the node is in motion, heightening the likelihood of the connection experiencing a breakdown. When utilizing the typical shortest path, it is necessary to substitute the original connection with other ones or repeat the path discovery procedure. The routing method

considers the connection's stability while selecting a route to handle link failures caused by node movement [4]. These routing approaches determine the duration of the connection by calculating the received signal intensity of the node or the spatial mobility of the nodes. As the movement of nodes grows, the likelihood of collision in a network also increases, resulting in higher packet losses. This adversely affects the system's efficiency in multiple applications, such as location-based applications. When employing geolocation usage, if there is a delay in delivering messages due to congestion, the calculation of routes will be inaccurate. The nodes' motion in arbitrary directions at high-speed leads to a continual change in topological structure, resulting in increased energy consumption due to the calculation of new routes often.

It is necessary to protect the data's security and privacy by maintaining its integrity and confidentiality while preventing unauthorized communications [5]. The research becomes increasingly challenging due to the dynamic topology of MANET, the complicated infrastructure, fluctuating bandwidth requirements, insufficient safety measures, and the necessity for multi-hop communications. Wireless multipath routing often improves fault tolerance, replacing the initial single-path routing. Multipath routing reduces data failure by using many pathways [6]. Multipath routing is advantageous for reducing the impact of packets or attacks during the path-finding procedure. Choosing the optimal path from several available paths occurs in just one phase for multipath routing. Multipath routing decreases the frequency of path-finding activities by using a pool of pre-established routes. Minimizing overall latency and reducing energy consumption extends the lifespan of a network. Concurrent multipath transmission is a very efficient routing in MANETs due to advancements in wireless networks and mobile devices. This routing method is employed in apps such as streaming high-quality mobile films via several access mediums.

MANETs in particular have found numerous uses for their ability to transmit data in real-time. The present routing protocols employed specifically in WSNs are limited by the concomitant issues. The network's design challenges include limiting energy consumption during information transmission and ensuring node security. In the current routing protocols, a route originates from a source node that uses energy to send messages to its neighboring nodes in an attempt to find a path to the target node.

The rogue node obtains privilege over the underlying network traffic going to the intended destination after a sinkhole attack is successfully carried out. This traffic can then be manipulated in a number of ways by the attacker. As seen in Figure 2, one popular strategy is to just dump the packets, which essentially initiates a black hole assault. The intended recipients

lose all of their data as a result. But the rogue node's powers go beyond this, permitting a variety of further nefarious actions like data alteration, eavesdropping, and initiating more network attacks. For route discovery, reactive routing systems use a query-response method. A source node can broadcast a RREQ packet for route request across the network when it needs a path to a destination. This RREQ is forwarded by intermediate nodes, which monitors the length of the path by increasing the hop count. The destination node or a node with a new route to the destination sends back a route reply (RREP) packet in response to an RREQ. Based on parameters like path freshness and hop count which are denoted by a sequence number, the source chooses the best path. By deliberately creating an RREP message constructing an RREP message that fraudulently promotes a higher sequence number and a shorter path, a sinkhole attack takes advantage of this process. By tricking the source node into rerouting traffic over the attacker, this false information essentially creates a sinkhole that absorbs incoming packets.

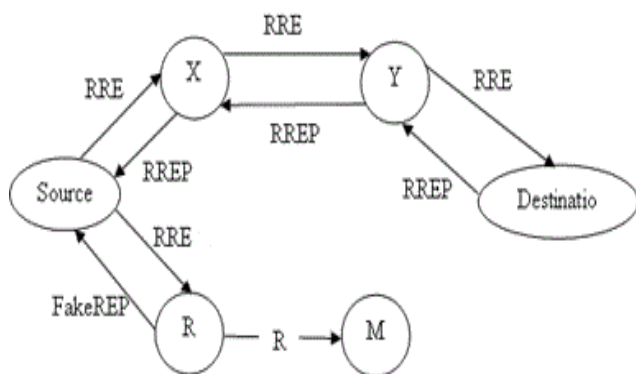


Fig. 2. Sinkhole attack in MANET

Enhancing energy efficiency and ensuring routing protocol security are problems for mobile ad hoc networks. In order to access secure data in a hostile environment, this research suggests a revolutionary security method called the Hybrid Secured Routing Protocol. The nodes in the suggested work are linked to a security policy in order to ensure safe data transfer throughout the network. Both nodes share a common enforcing policy under this policy, and they then communicate with one another. In order to choose the routing path based on the available energy threshold at the nodes in the network setup for packet forwarding, the transmission nodes must first demonstrate their authenticity. In addition to implementing the network's optimum shortest path, the routing protocol assesses the node's reliability by analyzing how well its trust policies are being enforced.

The main contributions of the proposed HSRP are given below:

- A trust-based Cluster Head selection is proposed to improve MANET security.
- A trust threshold level-based intrusion detection method is proposed to detect the normal and intruder nodes.
- A hybrid genetic algorithm proposes an optimized multipath routing in MANET.
- A fitness function is proposed to enhance the routing process with trust level in the Genetic Algorithm.

The following sections are organized in the following manner: Section 2 discusses the background and literature survey about different routing protocols in MANET. Section 3 discusses the proposed hybrid GA-based multipath routing algorithm and security enhancement. Section 4 discusses the simulation parameters, evaluation, and results. Section 5 concludes the research with findings and future studies.

2. LITERATURE SUMMARY

MANETs require aid for essential activities and resilience to provide a robust security design capable of effectively opposing malicious behavior aimed at compromising the performance of MANETs. During this process, communication paths are created between nodes, enabling the transmission of data from one device to another. Due to limited resources, MANETs employ single-path routing [7]. The network would experience a collapse if any nodes along the path were to die. The safety of the MANET is endangered if the path-finding method is compromised. In sensitive usage, reliability and accessibility are of foremost importance. Various pathways have been established to enhance the network's accessibility, durability, and reliability.

One of the biggest risks to wireless sensor reliant network is Denial of Service namely DoS attack, which wear down the device nodes and shorten their lifespan because energy can occasionally be low. The previous proposals for these networks' systems do not provide the best possible power and energy usage. To counter DoS attacks, thus the authors in [8] introduced Security Scheme. This method extends the lifespan of sensor nodes in a power-constrained network by preventing power draining attacks through the use of symmetric cryptography and SHA.

Shah et al. proposed a Topological Adaptive AOMDV Routing Protocol (TAARP) to minimize data traffic by leveraging Quality of Service (QoS) [9]. The main drawback is its poor performance in adaptive structures requiring path reliability and high node concentration. This approach marginally enhances efficiency, whereas other methods often exhibit superior performance. In order to improve the liveness of a sensor reliant network and reducing energy

consumption to perform various operations, the authors in [10] presented a unique fuzzy-based technique to arrange heterogeneous sensor nodes in various clusters and then choose the cluster head. The approach proposed a Multipath Routing Protocol (MPRP) that relies on the stability of links [11]. The MPRP method calculates the connection stability based on the flexibility concept and the size of the routing queues. This enhances the possibility of the connection being stable. The separation between nodes and the duration of route survival are evenly proportioned. The nodes in the network utilize a significant amount of energy due to constant changes in the route, which results in an enhanced node density involved in supporting network reliability.

The Congestion Management Approach (CMA) developed by Prema et al. is implemented in the AOMDV protocol [12]. The CMA system utilizes a rate-controlled data transfer method and buffer-controlled congestion management to improve the network's performance. The results showed enhanced transmission efficiency and decreased routing overhead. The capacity could be improved due to significant packet loss caused by collisions. The study presented in [13] discussed how different forms of attacks affect mobile nodes in two different types of networks like randomly distributed networks and consistently distributed immobile networks. consistently distributed immobile networks are more vulnerable to complex combination attacks, such as black hole attacks, even though they might provide greater defense against individual attacks. An artificial immune system method based on Optical Link State Routing (OLSR) [14] was presented. This protocol selects the optimum route by considering the following factors: hop counts, energy of intermediary devices, and length between origin and target devices. This method enhances system performance in terms of delay and performance. The primary issue of this protocol is the quantity of energy consumption needed for route estimation.

Shafi et al. [15] designed a Trust reliant AODV Routing Protocol namely to guard against attacks in MANETs. Tested in NS-2, the suggested protocol is contrasted with existing under-fire routing techniques. According to the simulation results, Trust reliant AODV Routing Protocol lowers latency, routing overhead, and packet loss while increasing throughput by 4% and dependability by 44%. Abu Bakar et al. [16] shown how to use smart software agents to identify Distributed DoS attacks. They tested their system's performance against the most advanced attack detection methods using the specially created dataset CICDDoS2019. They developed an agent-based approach for this system that combines sequential feature selection with machine learning. The system's learning phase rebuilt the Distributed DoS discovery software agent by choosing the best features from the dynamically

recognized Distributed DoS attack traffic. Their proposed technique offers speedier processing while achieving state-of-the-art detection accuracy.

Ali et al. introduced a routing method that utilizes Quality of Service (QoS) measures to improve communication efficiency between Uncrewed Aerial Vehicles (UAVs) and the ground [17]. The research developed a novel composite measure that integrates path accessibility, load capability, and delay to determine the most optimal route. This analysis presents an efficient broadcasting strategy to minimize the use of floods, with the primary objective of prolonging the lifespan of the links, achieving load balancing, reducing latency, and meeting the QoS criteria. Empirical findings have shown that the suggested procedure substantially enhances the system's efficiency compared to conventional methods.

Yadav et al. [18] utilized weighted based adaptive cache using clustering approach namely WACC to model network denial-of-service flooding assaults. The proposed WACC model uses the adaptive model to estimate the network's assault scenario. The proposed WACC model increases response rate, throughput, and false positive rate. The WACC model has a maximum packet delay of 35.41 ms, the regular TEV has a maximum delay of 38.15 ms, and the EMC has a maximum delay of 42.69 ms. Using the suggested WACC model, the expected throughput improvement is 88.35%. The study's findings demonstrate that the suggested WACC outperforms earlier strategies in preventing DDoS flood attacks. Monfared et al. introduced the Verified Anonymous, Secured Routing Protocol (VASRP) to fulfill specific criteria and protect against potential threats [19]. The path request messages are authenticated using a signature to safeguard against intruders while keeping the nodes' characters concealed. The experimental findings show that VASRP significantly enhances the efficiency of the current methods.

In order to obtain a dataset from the simulator, Mughaid et al. [20] employed a dropping attack to imitate non-orthogonal multiple access (NOMA). LR detected dropping attacks with 95.7% accuracy using machine learning algorithms and the recovered data. The study also suggests networks utilizing a range of deep learning and machine learning techniques. The suggested work is implemented and assessed using a comprehensive Wi-Fi network benchmark dataset. The KNN algorithm outperformed the neural network and DF in terms of accuracy rate, according to the testing. Attacks against authentication that verify the authenticity of nodes in the underlying network becomes crucial since energy is one of the limited resources for this type of network [21]. These types of attacks shorten the lifespan of nodes that are already a part of a WSN by draining their power. This article suggests a zonal node authentication method and ideal

data scheduling scheme that improves network lifetime and quality of service while delivering data.

Abdelhamid et al. [22] designed "anomaly discovery based on a support vector machine," a technique for identifying black hole attacks using support vector machine. This detection system's objective is to keep an eye on network activity and spot any unusual behavior from specific nodes. In contrast to normal nodes, nodes involved in performing black hole based attack exhibit unusual behavior. These traits are successfully detected by their lightweight detection technology. Dataset was collected using an OMNET ++ simulator and classified as either benign or malicious based on the identified malicious node. It has been demonstrated that the suggested method may accurately detect black hole attacks. The idea presented in [23] demonstrates an innovative hybrid deep learning technique that efficiently detects and mitigates flooding threats in MANETs by combining Convolutional Neural Networks, Long Short-Term Memory and Gated Recurrent Unit architectures. A special DECEHGS algorithm that combines two different techniques namely, Evolutionary Population Dynamics technique and Differential Evolution technique to maximize the model's efficiency, improving both convergence and performance. The authors claimed that a 12% increase in packet delivery ratio, and a 20% decrease in routing overhead over conventional approaches, the suggested model shows notable advancements over current approaches.

These measures fail to consider the impact of congested networks on energy consumption, namely the increased energy usage caused by unnecessary data retransmissions. The effect of nodes' mobility on losing information must be considered in any routing approach, along with energy and congestion management effectiveness. The research examines the limitations of the solutions to develop a novel and enhanced hybrid secured routing system for MANET.

3. Proposed secured and efficient multipath routing protocol

Routing is the basic procedure in MANETs that simplifies establishing transmission links between devices for transmitting and delivering messages. Data communication is the basis for several essential security areas, including secure data accumulation, localization, intrusion identification, and handling keys. Multiple routes are as susceptible to vulnerabilities as a single route. The application of numerous channels presents new safety alarms that should be considered. Safeguarding data from unwanted activity is as crucial in non-sensitive environments as maintaining network availability and reliability. It is essential to ensure the proper functioning of the routing tasks by effectively managing the multipath routing procedure. Figure 3

displays the block diagram of the suggested hybrid secured multipath routing system.

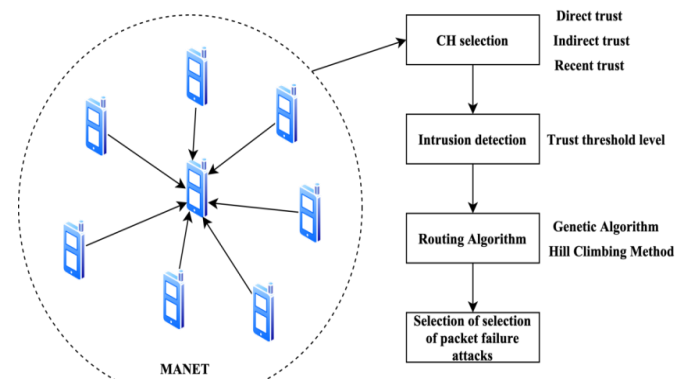


Fig. 3. Workflow of a multipath routing algorithm

This article presents a hybrid secured multipath routing system explicitly designed for MANETs. The technique relied on density maxima and selected CHs predictably, using recent, indirect, and direct trusts as criteria. The calculation depends on the trust boundary of the devices discovered. The CHs feature a network of linked devices, and a prediction protocol is used to create a selection of the optimal routes, which determines the optimal routes. The fitness function is calculated as the total remaining power in the nodes, the route's throughput, and the route's interdependence. The system can ensure the successful transfer of data packets from their origin to the target. It utilizes various routing methods, such as a hybridization method obtained through an integrated routing protocol called the Hybrid Genetic Approach (HGA). HGA combines the Genetic Approach (GA) and the Hill Climbing Approach (HCA). The objective function depends on the trail's capacity, throughput, and interaction. The suggested method integrates the benefits of the GA and the HCA procedures while reducing the time required for data mining and modification. Simulation findings about the selected packet-dropping threat will be evaluated.

3.1 Trust Controlling Method

1) Direct trusts

Direct Trusts (DT) are determined by the projected duration required to connect the origin device x and target device d . The measurement is calculated by subtracting the expected duration for the target device to confirm the public credentials created by the x^{th} origin device from the actual duration. The x^{th} node and d^{th} destination node's trust is indicated as DT. The direct trust is shown in Equation 1.

$$DT_x^n(d) = \frac{1}{3} \left\{ DT_x^n(d-1) - \left(\frac{d_a - d_e}{d_a} \right) + w \right\} \quad (1)$$

The variable d_a represents the expected duration, whereas d_e provides an anticipated timeframe for

estimating the time needed to validate the public credentials. The duration required for the target and the source device to exchange the credentials, including the period to receive and send out, is also recognized. Weight (w) is the variable that indicates the weightage of these nodes.

2) Indirect trusts

Indirect Trusts (IDT) represent a device containing the parameter. Without a trust factor, a device must utilize the IDT, which gets allotted DT via a specific process. The IDT is expressed in Equation 2.

$$IDT_x^n(d) = \frac{1}{r} \sum_{x=0}^{r-1} DT_x^n(d) \quad (2)$$

The variable r defines the vicinity around the node x.

3) Recent trust

When calculating trust, the research depends on DT and IDT, which assess fundamental credibility and determine the destination. The RT is expressed in Equation 3.

$$RT_x^n(d) = k * DT_x^n(d) + (1 - k) * IDT_x^n(d) \quad (3)$$

3.2 CH selection

The C-means method is an unsupervised learning approach that aims to optimize the objective function by repeatedly dividing a MANET. The C-means approach utilizes fuzzy equations to address the grouping problem. The cluster yield reflects nodes associated with a certain proportion of the overall membership of the grouping head.

Let the device count in the neural networks be denoted as R, where R is a set consisting of k elements: $r_1, r_2, \dots, r_k$. The entire device count is equivalent to n_x , with every device exhibiting overall p movements. A set of fuzzy clusters is created, and the group's head matrix $H = \{H_1, H_2, \dots, H_k\}$ is utilized. The objective of C-means is expressed in Equationn. (4).

$$J(X, Y) = \sum_{p=0}^C \sum_{q=0}^k (x_{pq})^m (n_{pq})^2 \quad (4)$$

The matrix $X = x_{pq}$ is a participation matrix with dimensions $n \times c$, where x_{pq} indicates the connection among Y_i and P_j . The expression $n_{pq} = P_j - Y_i$ denotes the Euclidean space among devices j and i. The variable m represents the fuzzified component used in the procedure.

The variable X represents the membership among Y_i and P_j , denoted as x_{pq} . X has a size of $n \times c$. The expression $n_{pq} = P_j - Y_i$ denotes the Euclidean length from the device to and ith node. Equation 5 shows the criteria to satisfy the c-means condition.

$$\sum_{x=0}^c x_{pq} = 1 \text{ for } j = 1, 2, \dots, k \quad (5.a)$$

$$0 < \sum_{x=0}^c x_{pq} < 1 \text{ for } i = 1, 2, \dots, c, j = 1, 2, \dots, k \quad (5.b)$$

$$0 < \sum_{x=0}^c x_{pq} < k \text{ for } i = 1, 2, \dots, c \quad (5.c)$$

The C-means technique achieved the minimum target function J(X,Y) via iterative improvement. The values of X and Y are obtained using Equations 6.a and 6.b.

$$x_{ij} = \frac{1}{\sum_{k=0}^{c-1} \frac{1}{m_{kq}^{m-2}}} \quad (6.a)$$

$$Y_i = \frac{\sum_{j=0}^{n-1} (x_{ij})^m p_j}{\sum_{j=0}^{n-1} (x_{ij})^m} \quad (6.b)$$

The C-means technique requires the allocation of group heads and group numbers, making it especially susceptible to the initial selection of group heads [24]. Given challenges such as many clustering rounds, slow convergence, local optimal solutions, and instability, it is straightforward to develop several alternative methods. The suggested technique is a unique approach based on density peaks for c-means clustering. To identify the clustering heads, the research will use the two variables, α_i and β_i , which represents the total number of nodes. The density proximity index μ_i to measure a given point's density, as shown in Equation 7.

$$\mu_i = \alpha_i * \beta_i \quad (7)$$

Iterate over the n total nodes and get the β_i values for each node. Utilize the arrangement of density proximity values to determine the z-coordinates. Transform the computed density range into a mean density range (μ_m), as shown in Equation 8.

$$\mu_m = \frac{1}{Z} \sum_{x=0}^1 \mu_x \quad (8)$$

Based on the density range values, μ_m demonstrates a diminishing trend. Locations of higher significance are more likely to become the central point of a group. The value of μ_i is greater than μ_m . Stating that C_x is now functioning as the clustering head implies that it refers to the present instant. Once chosen, the grouping head will be selected according to the highest trust value. In the first phase, the C-means method incorporates a CH, resulting in the acquisition of the clustering outcome. Once a node surpasses its fundamental trust standards, it might be labeled a group head. The principle of direct trusts, indirect trusts, and recent trusts, the Maximizing Function (MF), is formally stated in Equation 9.

$$MF = \frac{1}{3} (DV + IV + RV) \quad (9)$$

The direct trusts, indirect trusts, and recent trusts scores are represented as DV, IV, and RV, respectively.

3.3 Managing intruded devices

The network's infiltration is predicted once the appropriate CHs have been calculated. The last stage involves examining the positive aspects of these

devices, considering both end devices' perspectives. The perpetrator's identification has been ascertained, and access to the network has been revoked for the intruder node. The sink node utilizes a predetermined threshold (0.5J) to assess the existence of intruders. The threshold value is established depending on the system's needs, as the administrator decides.

A channel's communication capacity and link status are determined by evaluating the residual power of a specific device. When the power level is depleted, the probability of discovering an adjacent device diminishes, rendering the node disconnected from the network. Increasing the energy of a node might result in a boost in the communication power of that node. The primary objective of detecting attacks is to provide secure network connectivity while minimizing energy consumption and maximizing data delivery speed.

3.4 A hybrid routing method

The Hybrid optimization technique determines the most valuable leaps for constructing MANET routing. The proposed method aims to identify the paths with the highest likelihood of success. The need for real-time programming will indicate the answer to the optimization method, which is simply the pathways chosen for transportation in MANETs. The nodes' remaining energy defines the overall condition of the route, the route's throughput, and the path's availability. The fitness measure is a function that aims to maximize a specific value, as denoted by Equation 10.

$$F = \frac{1}{3}(E + Th + P) \quad (10)$$

The variables E, Th, and P represent energy, throughput, and path connection, respectively. These variables are determined by calculating the values of the nodes along the way.

3.5 Hybrid optimization

MANET is a dynamic system consisting of N interconnected nodes. The expense of the path between the devices is the metric of improvement. The total price is equivalent to the cumulative addition of the costs of every single hop. To do this, search for the path with the lowest overall expense (including both time and money) from the starting node to the target node.

3.5.1 Depiction of a chromosome

The GA method makes any path from the origin to and target devices feasible. Optimality is attained by selecting the option with the minimum length. When a randomized population of potential solutions forms the solution field, a solution is classified as acceptable

(possible) or unacceptable (impossible). Solutions that are unable to attain the aim are considered inadmissible. The solution to the optimization problem was discovered inside the chromosome. A routing route's Deoxyribonucleic Acid (DNA) consists of positive numbers that indicate the identities of devices. These identities are concatenated to produce a route for navigating to nodes. The journey begins at the origin node and progresses via the intermediary nodes until reaching the objective, which is the endpoint. This determines the upper limit of the length of a chromosome and establishes a universal optimum for chromosome size.

3.5.2 Evaluating the parameters of fitness

Fitness is computed using Equation 11.

$$f_x = \frac{1}{\sum_{j=0}^L C_g(j) + g_x(j+1)} \quad (11)$$

The parameter f_x represents the fitness score of the xth chromosome, whereas the parameter L denotes the size of the ith chromosome. The gene at the jth location on the ith chromosome is denoted as $C_g(j)$. There is a specified connection cost, denoted as C, among nodes. The connection expenses are considered uniform and have a value of 1. If the expense representing the shortest length is measured in terms of hops, then the cost will equal the number of hops.

3.5.3 Selection of Best Fit

The technique of picking the most suitable individuals from the population enhances the general caliber of the group. Chromosomes of higher quality have a greater chance of survival when the method is implemented. Ordinal-based choices rely only on ordered (ordinal) choices instead of proportional ones. Proportionate decision-making analyzes chromosomal traits about the traits of the whole community. This assortment has three different methods of random choice: roulette wheel decision-making, Stochastic Remainder Choice, and Stochastic Universal Choice. This article will use the concept of the roulette wheel, where values with a higher probability of being selected are allocated more significant results. Scores with the most accurate match are given more significant results, enhancing the likelihood of these values producing offspring.

3.5.4 Crossover

Crossover is a genetic procedure that combines genetic information from two parental genes to create a new gene. Midway crossover is a technique employed during the procedure of crossover on strings. Every parent's genes are divided into two halves. The offspring formed by crossing include additional qualities.

3.5.4 Mutation

During the modification of genes, the mutation function causes a change in the search to other regions within the solution space. If a mutation is performed, the subsequent iteration values will remain unchanged. Choosing the most efficient route using a hybrid optimizing strategy is advisable. The GA and the HCA are employed in tandem in the proposed hybrid optimization. HCA is the term used to describe the local search-related computational optimization process. An infeasible solution is suggested (an initial answer), which is then adjusted to assess whether the adjustment will provide a more favorable result. An innovative approach with a higher fitness level is implemented as the preferred option.

The previous solution is preserved. The iterative refining of a solution by neighborhood modifications will facilitate upward progress as long as possible. The critical factors for hill climbing progress are a defined objective, initial stages, scope, and systematic exploration. Expanding the range of parameter settings broadens the search space in the quest room for hill-climbing—fundamental concepts of search area: The search area must encompass an unquantified and non-negated set or collections. Whenever the self-assertive data rotates across a pivot, and an analysis is involved, the pivot influences the interpretations. Comparative change has asymmetry, but it consistently increases and does not decrease. Figure 4 displays the workflow diagram and Algorithm 1 shows the pseudocode for finding secure route between a source and destination node.

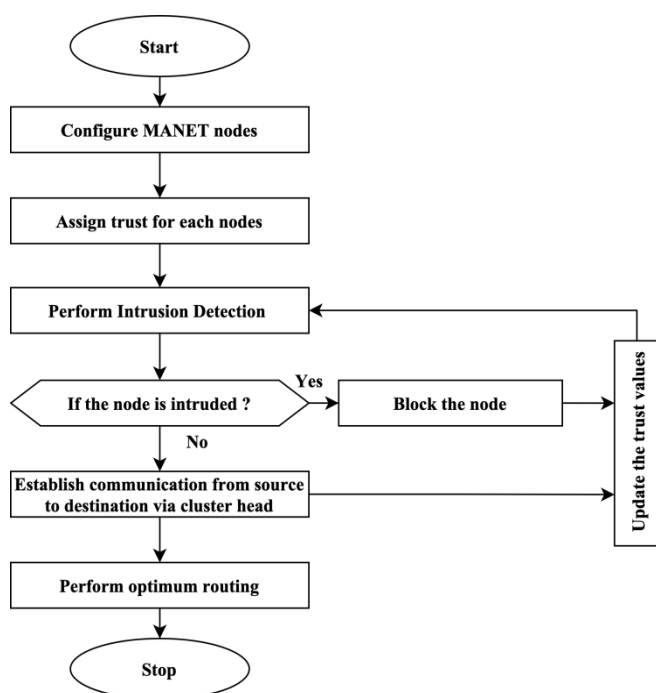


Fig. 4. Workflow of the optimum routing algorithm using GA and HCA

Algorithm 1. Secure Route Determination

```

Initialization: Initial Table
S: Source Node
n: neighbor
LR: Legitimate Route
for ( i = 1 to n)
{
    if (i == s)
        LR[i] = s
    else if (i == )
        LR[i] = s || n
    else
        LR[i] = empty
}
Broadcast LR[1 to n]
Update Path LR
for (i = 1 to n)
{
    if (S exists n LR)
        Discard
    else
        LR[i] = Trust(LR[i], (S || n))
}
Broadcast LR
}
    
```

3.6 Fitness value

The initial element of the fitness score is congestion protection, represented as F_c . To determine whether a route is experiencing a collision, it employs the Clear to Send (CTS)/Ready to Send (RTS) protocol [25]. Collision detection is achieved using the Carrier Sense Multiple Access (CSMA) with Collision Avoidance (CA), which incorporates the RTS and CTS mechanisms.

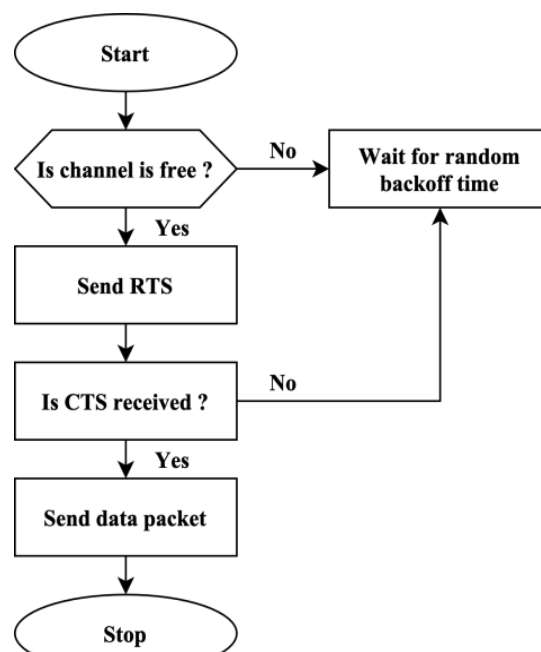


Fig. 5. Fitness update process with RTS and CTS

Figure 5 illustrates the use of the RTC/CTS method. Firstly, it verifies the channel's status to determine whether it is inactive. It will wait for a randomized backoff period if the link is inactive. After this period, it will re-evaluate the availability of the channel. After the channel becomes accessible, the sending node will transmit the RTS message to the receiving node. If the recipient device is unavailable, it will await a randomized period before checking once the specified time has passed. When the receiving node is accessible, it will transmit a CTS packet in response to the sending node. Upon receiving the packet, the sending node will begin the payload transfer. This guarantees that the link is accessible for interaction and prevents congestion.

A sending device transmits a greeting message to the devices along a particular path provided by AOMDV [26]. The proposal states that if no CTS signal is obtained, the value of F_c is set to 0, indicating a collision has been discovered. No collision has been observed if the CTS signal is received within the Round Trip Time (RTT). The fitness factor is expressed in Equation 12.

$$F_c = \begin{cases} \frac{1}{RTT} & \text{CTS is received} \\ 0 & \text{No CTS is received} \end{cases} \quad (12)$$

F_c represents the fitness factor that is determined by the occurrence of packet collisions. We provide a method that uses a genetic algorithm to optimize routes in order to circumvent unstable links with traffic issues. We present a novel fitness function in this context. Collision avoidance is the first part of our fitness function, represented by the letter F. We use the CTS/RTS protocol to determine whether a path has collisions or not. We start by determining if the channel is idle. It is required to wait for a random backoff period if it is not idle, and then we check again to see if the channel is still available. The RTS packet will be sent to the recipient node by the sender node as soon as the channel becomes open. The sender node will begin transmitting the data packet as soon as it gets this packet. This prevents collisions at all times and guarantees that the channel is open for conversation. In this instance, the nodes of a specified route that the suggested method returns receive a hello message from the sender node.

3.6.1 Queue length

This subsection determines the buffer size for every device in a specified path obtained from the AOMDV method. Eqn. (12) incorporates the variables Bandwidth (BW) (representing the capacity of the bottleneck connection), T (representing the lowest RTT), and Q (representing the buffer size).

$$Q = (RTT - T) * BW \quad (13)$$

Configure the threshold for the variable queue size to N, when A is fixed, ranging from 0 to 1, and Q_{max} at the maximum buffer size level. The queue size is indicated in Equation 14.

$$M = A * Q_{max} \quad (14)$$

Q and M are compared to analyze the congestion state. If the quantity Q exceeds the quantity M, packets were discarded along a specific route because of anticipated congestion at one of the terminals. Avoiding this path and excluding it from the optimal options is advisable. If Q is less than or equal to M, consider the parameters of the other elements of the fitness function; the assessed path is selected to be included in the pool of optimal paths.

The method involves a fitness function in which the congested fitness element, F_q will have a non-zero value or be reset to 0, depending on the constraint $Q < M$. The level is calculated, where B represents the queue length and shows if $Q < M$ is satisfied, meaning that the path receives packets for message transfer. Otherwise, the path is probably experiencing a collision at any or all of its devices, so assign a zero value to F_c , as shown in Equation 15.

$$F_q = \begin{cases} 1 - \frac{Q}{B} & Q < M \\ 0 & \text{else} \end{cases} \quad (15)$$

It determines the link stability using the notions of Link Breaking Possibility (LBP) and Pathway Stability Possibility (PSP).

3.6.2 LBP

Predicting the occurrence of MANET connection failure is a difficult task. It estimates the link's relative durability by assessing the signal levels from the past and present. Due to the fluctuation in signal intensity, it is permissible to use distance as a metric to measure the dependability of the connection. To construct an analytical approach, making specific hypotheses for simplicity is necessary. It is assumed that any nodes within a given area have identical movement variables and that the node's movement follows a Manhattan Grid Mobility Model. Every node within the region is evenly distributed in its original position. The Cross Density Function (CDF) of the length between two devices, distributed normally, is expressed in Equation 16.

$$CDF_l = P_{l < r} = r/R, 0 < r < R \quad (16)$$

Eqn. (15) denotes the CDF of the length (r) separating two devices beyond the communication range (R). To minimize the number of computing resources required, Equation 17 should be followed.

$$LBP_{(r,R)} = 1 - \exp\left(-\frac{r}{R}\right), 0 < r < R \quad (17)$$

3.6.3 PSP

Upon receiving a route repeat from the target node, the node retrieves the PSP value. It applies to compute the LBP value of the link connecting the two endpoints. The fitness value of the link security, F_s , is determined using Equations 18.a and 18.b.

$$PSP_x = \sum_{l=0}^L 1 - LBP_l \quad (18.a)$$

$$F_s = PSP_x \quad (18.b)$$

For route x , the Pathway Stability Possibility is computed for every channel l that is part of the collection of links L . Calculate the updated value of the PSP and make the necessary adjustments. It is utilized to determine the stable path among the many routes provided by the AOMDV algorithm, as given in Algorithm 2. It determines the shortest energy path for data transmission to the network's nodes with secured network data communication. Network lifetime and throughput and are increased by this algorithm's improved energy efficiency. By using energy-efficient management strategies, this algorithm optimizes the use of the energy available in the nodes

Algorithm 2: Fitness Calculation of Each Route

Input: For each route received

F_c = Collision element of fitness computation

F_q = Queue size element of fitness computation

F_s = Link stability element of fitness computation

n = all feasible routes

Output: List of fitness scores

For ($x = 0$; $x \leq n$; $x++$)

$$F_c = \begin{cases} 1 & \text{CTS is received} \\ 0 & \text{No CTS is received} \end{cases}$$

$$F_q = \begin{cases} 1 - \frac{Q}{B} & Q < N \\ 0 & \text{else} \end{cases}$$

$$F_{x-m} = \frac{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} F_{xij}}{n \times m}$$

If $F_c > F_{c-m}$

If $F_q > F_{q-m}$

If $F_s > F_{s-m}$

$$FF = F_c + F_q + F_s$$

End

End

End

End

Algorithm 2 calculates the fitness value by summing the mean collision, queue size, and Link Durability. The fitness metric is shown in Equation 19.

$$FF = F_c + F_q + F_s \quad (19)$$

F_c represents the fitness score for collision, F_q represents the fitness score for queue size, and F_s represents the fitness score for link reliability. It arranges the fitness scores decreasingly for every path from the origin to the target and chooses the most excellent FF value route.

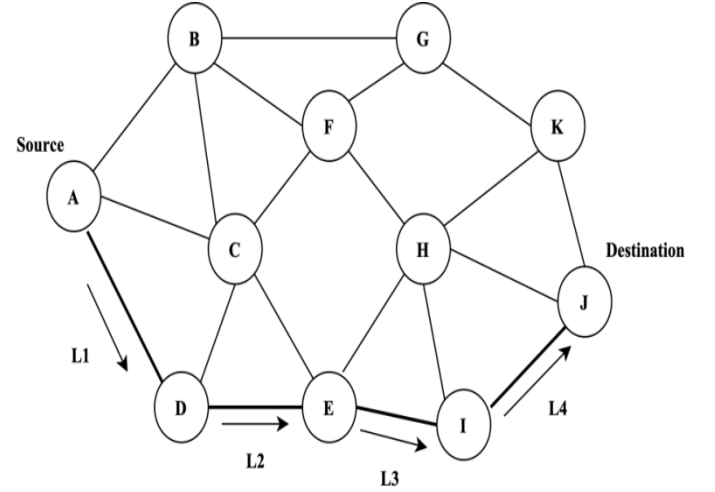


Fig. 6. Sample scenario for route selection using Equations 19 and 20

Figure 6 illustrates that several connections, such as L1, L2, L3, and L4, connect the origin A to the target J. It computes the values of F_c , F_q , and F_s for each connection and represents them as F_x . Equation 20 represents the forces, F_{c-m} , F_{q-m} and F_{s-m} . It establishes the mean level as the threshold and verifies whether every aspect has a fitness level that surpasses the mean level.

$$F_{x-m} = \frac{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} F_{xij}}{n \times m} \quad (20)$$

F_{xij} represents the force in each j channel out of m channels that make up an i route among n routes, wherein F_{xij} might be either F_c , F_q , or F_s .

4. Simulation analysis and Discussion

In order to implement and test the suggested model for performance improvement in WSNs, the NS3 simulation environment. The Windows Intel(R) Core™ i7-x64 processor with 16 GB of RAM was used to set up the simulation environment with 8 GB of storage was allotted for NS3 alone. It is proficient in evaluating and developing new routing algorithms. The tool was augmented with 100 devices in the simulated setting. The simulating duration is 100 milliseconds. To analyze the efficacy of the suggested routing method in different scenarios, including node densities and traffic loads, a range of variables and their corresponding values are used and indicated in Table 1.

Table 1. Simulation parameters

Parameters	Values
Tool used	NS-2
Node Count	100
TotalPower	100 W
Simulation Period	1000 S
Topology Area	500 m x 500 m
Crossover Possibility	0.4
Attack	Sinkhole attack
Mutation Possibility	0.2
Mobility Pattern	Manhattan Mobility Model
Packet Loss Ratio	2%
Mobility Velocity	10 m/s
MACModel	IEEE 802.11
Traffic Model	Constant Bit Rate

Table 1 shows that 100 nodes are considered, each initially allotted a comparable quantity of nodal power of 100W. The simulation region, in which nodes exhibit random movement, spans 500 meters by 500 meters and has a simulation duration of 1000 seconds. The MANET devices exhibit random movement in terms of both mobility and direction. The Media Access Control (MAC) layer method used is IEEE 802.11, and the traffic model is specified as Constant Bit Rate (CBR).

4.1 Performance Metrics

4.1.1 Packet Delivery Ratio (PDR)

PDR refers to the ratio of data packets successfully reaching the destination device compared to the total packets transmitted from the originating device. PDR offers insights into the efficacy of a protocol in transmitting packets over the networks. The calculation of PDR is shown in Equation 21.

$$PDR = \frac{\sum P_d}{\sum P_s} \times 100 \quad (21)$$

P_d represents the count of packets efficiently received at the destination, whereas P_s denotes the count of packets transmitted at the origin.

4.1.2 Throughput (Th)

Network throughput is a metric that quantifies the number of bits transmitted effectively over the network. It serves as a metric for evaluating efficiency and reliability. Packet loss decreased data communication throughput from the origin to the destination device. Throughput is indicated using Equation 22.

$$Th = \frac{\sum B_r}{T} \quad (22)$$

The variable B_r represents the cumulative number of bytes received, whereas T denotes the simulation duration.

4.1.3 End-To-End Delay (E-ED)

End-to-end delay refers to the period for a packet to be sent from its source to its recipient. E-ED is computed using Equation 23.

$$Delay = \frac{\sum t_x^r - t_x^s}{n} \quad (23)$$

t_x^r denotes the period at which the target node acquired the xth packet at the x moment. t_x^s denotes the instance when the originating device transmits the xth data at present, and n indicates the sum of data that have been accepted correctly.

4.1.4 Energy Consumption (EC)

EC refers to the aggregate amount of energy all devices utilize throughout the simulation. Equation 24 shows the energy consumption.

$$EC = \sum I_x - E_x \quad (24)$$

Let I_x be the starting energy of the xth node out of n nodes along a particular path, and E_x indicate the leftover energy after the simulation.

4.1.5 Routing Overhead (R)

Routing overhead refers to the amount of routing data that should be broadcast to receive via path identification and management. It impacts the network's resilience, which refers to the amount of power the nodes and bandwidth usage. The routing overhead is shown in Equation 25.

$$R = \frac{RO_p}{RO_p + DT_p} \times 100 \quad (25)$$

R represents the routing overheads, RO_p denotes the amount of routing data, and DT_p is the amount of data messages transmitted.

4.1.6 Collision Rate (CR)

CR refers to the frequency of data packet congestion or being dropped due to collisions. The expression for the R is shown in Equation 26.

$$CR = CC/O_{pkt} \quad (26)$$

CR represents the congestion level, CC represents the congestion measure, and O_{pkt} represents the number of outgoing messages.

4.2 Experimental Results

4.2.1 PDR

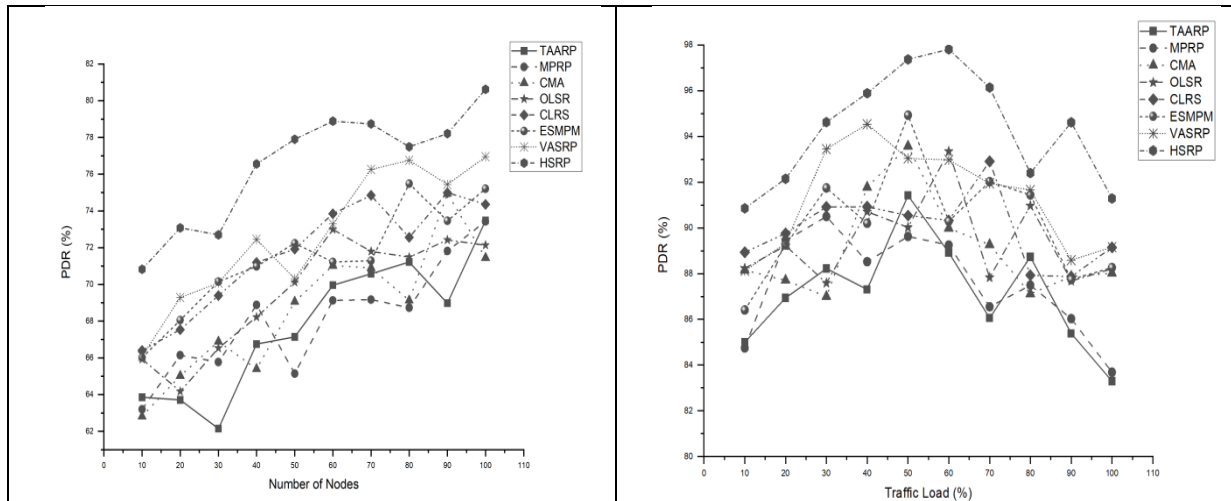


Fig. 7(a) Number of nodes vs. PDR analysis and Fig. 7(b). Traffic loads vs. PDR analysis

The PDR of various node densities and traffic loads is analyzed in Figures 7(a) and 6(b). According to the experiment, a higher node density leads to more message exchanges between the source and the destination, which are essential for route discovery and upkeep. Congestion at the connections' intermediary devices is a result of the increasing traffic. This leads to a higher number of dropped,

which negatively affects the network. But compared to other protocols, the recommended HSRP approach delivers a better PDR. Congested nodes result in low FF scores, which makes the routes connected to them unnoticed.

4.2.2. Throughput

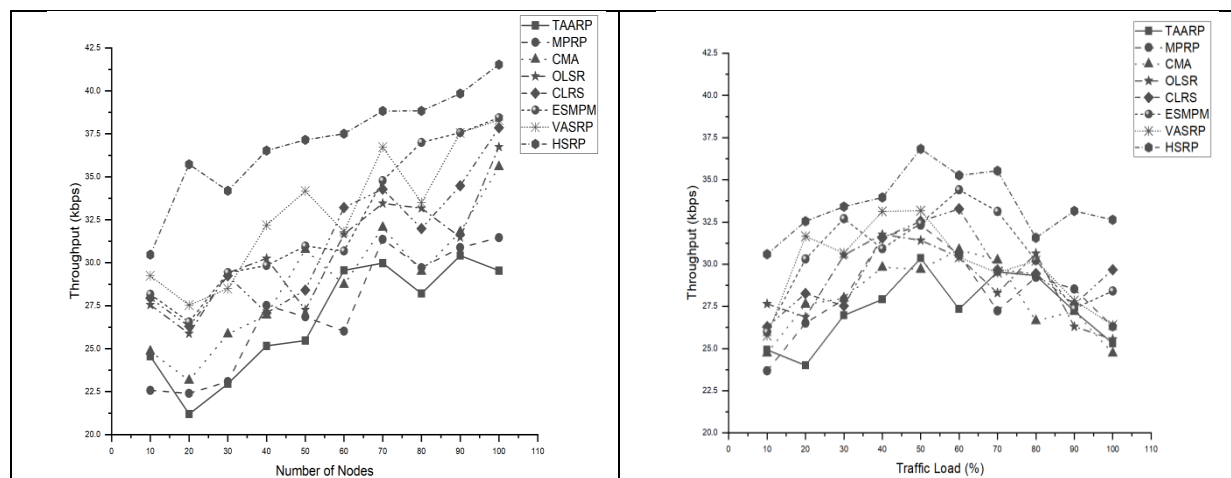


Fig. 8(a). Number of nodes vs. throughput analysis and Fig. 8(b). Traffic loads vs. throughput analysis

Throughput is assessed by considering the different node densities and different traffic loads. Figure 8(a) shows the effect of the network's device density on the throughput. As the node density increases, many opportunities to transport data packets are created. However, this could increase collisions at the intermediate nodes and cause more collisions. The throughput efficiency is negatively impacted. The proposed protocol reduces the probability of traffic issues such as congestion. These protocols prioritize picking the most stable and reliable path. Figure 8(b)

illustrates how different traffic loads influence the throughput in a specific network. Over time, the likelihood of congestion issues, such as data loss and collisions caused by the movement of random nodes, grows, resulting in a decrease in throughput. The protocols circumvent these unreliable paths, resulting in a superior throughput efficiency compared to existing protocols.

4.2.3. End-to-end delay

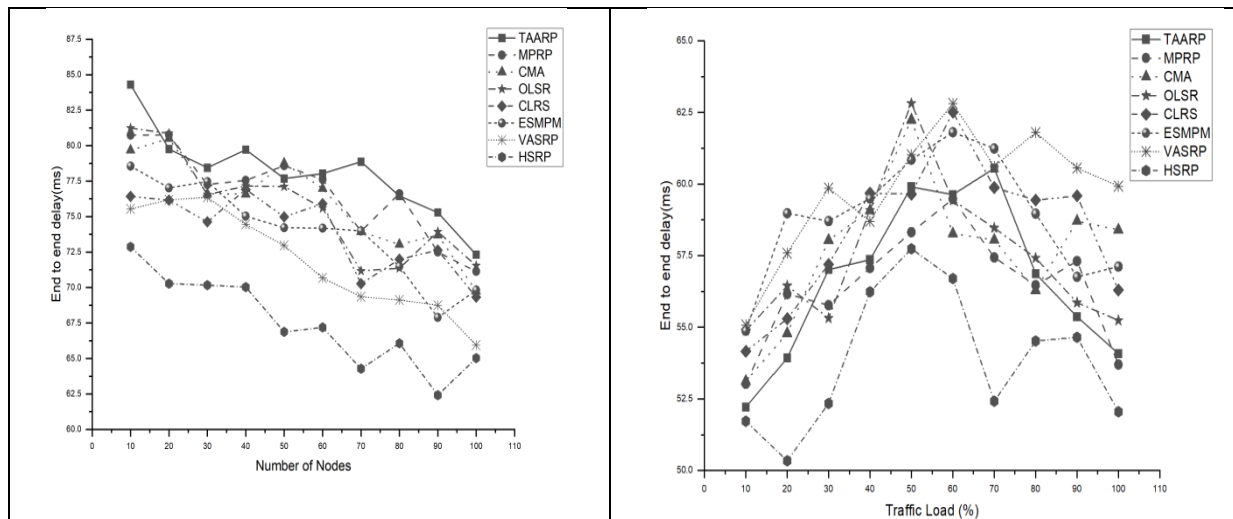


Fig. 9(a). Node density vs. end-to-end delay analysis and Fig. 9(b). Traffic loads vs. end-to-end delay analysis

As represented in Figure 9(a), a rise in the node density leads to more significant traffic difficulties, increasing data retransmissions. This would need a more substantial number of nodes and increased processing time to determine the most optimal paths. These elements will contribute to the total latency. The latency of the suggested method decreases as the message retransmissions decrease. The node becomes defective before or during data transmission. In the event of data transmission, a period will be taken to notify the source of the disconnection in the path, an alternative path will be investigated, and the process of transmitting the data again will be started. This will

increase the overall delay between the start and finish points. The procedures will actively circumvent such paths in the event of a defective node. Figure 9(b) indicates the end-to-end delay analysis of the different traffic loads. Due to the mobility of nodes, routes are prone to being lost, which leads to packet loss. Retransmitting data would contribute to the delay in transmitting data from the origin to the destination. The proposed method outperforms other rivals by effectively avoiding unstable pathways.

4.2.4. Energy consumption

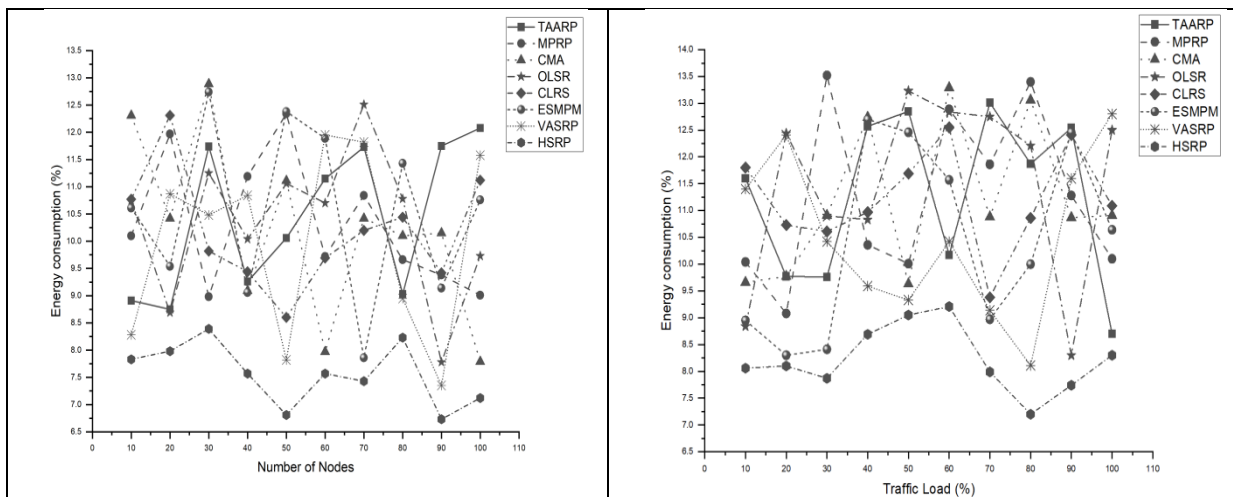


Fig. 10(a). Number of nodes vs. energy consumption analysis and Fig. 10(b). Traffic loads vs. energy consumption analysis

Figure 10(a) indicates the number of nodes vs. energy consumption analysis, and Figure 10(b) indicates the traffic loads vs. energy consumption analysis. The protocols effectively decrease the energy use of the nodes by reducing the need for packet

retransmissions. As the quantity of nodes or traffic increases, processing time is required, resulting in higher energy consumption.

4.2.5. Routing overhead

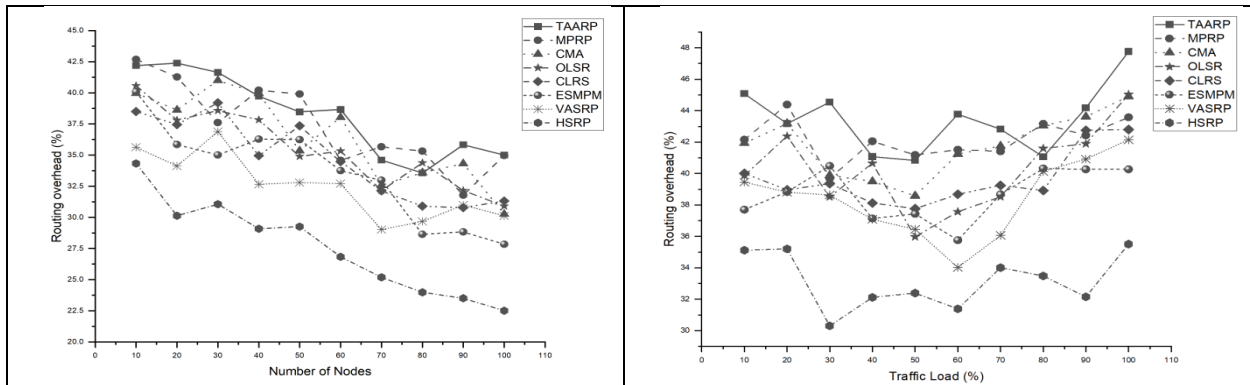


Fig. 11(a). Number of nodes vs. routing overhead analysis and Fig. 11(b). Traffic loads vs. routing overhead analysis

Figures 11(a) and 11(b) show the routing overhead using different node densities and traffic load protocols. As the number of nodes or simulation duration rises, the quantity of route request messages also rises, leading to a flood of signals in the network. This leads to a rise in network overhead. The overhead increases more often when the route identification

procedure is initiated due to node movement and route instabilities. The protocol improves the routes depending on the FF. The protocol has a negligible overhead compared to competing techniques.

4.2.5. Collision Rate

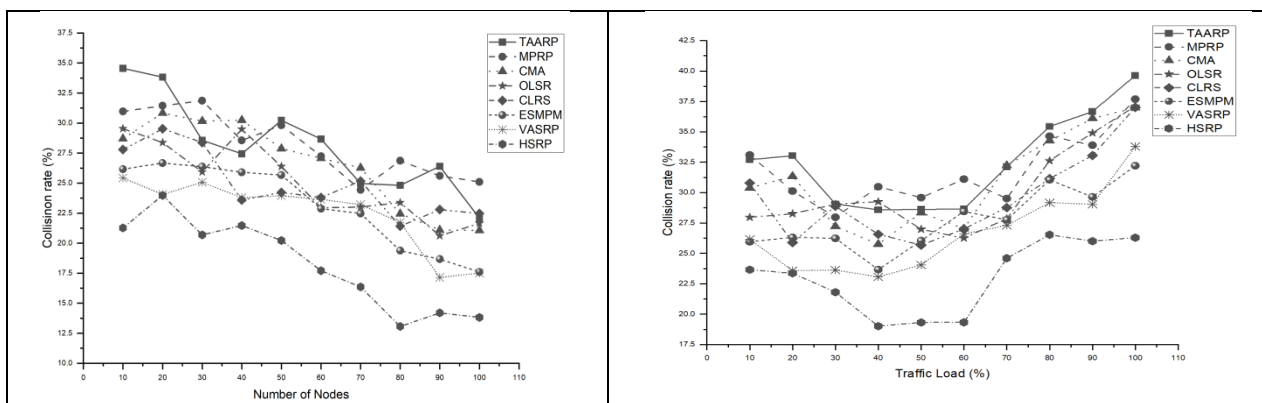


Fig. 12(a). Number of nodes vs. collision rate analysis and Fig. 12(b). Traffic loads vs. collision rate analysis

Figures 12(a) and 12(b) display the collision, representing the frequency of data packets that collide or get lost due to collisions for different node densities and traffic loads. As the node density rises, the data that must be transmitted also increases, increasing the likelihood of collisions. Using the RTT, the procedure determines the path with a lower collision probability. Node mobility or the presence of malfunctioning nodes leads to more frequent route disconnections. This leads to a rise in the number of route request frames broadcast, resulting in higher network flooding. There is a greater use of RTS/CTS exchanges. The protocols provide more dependable routes, decreasing the flood of route request signals and reducing the occurrence of RTS/CTS exchanges, hence decreasing the collision ratio.

important performance indicators, such as throughput, routing overhead, packet delivery ratio, and attack detection time.

4.3. Comparison with existing solutions

Additionally, the suggested method with current models using various performance metrics. The evaluation included a thorough examination of four

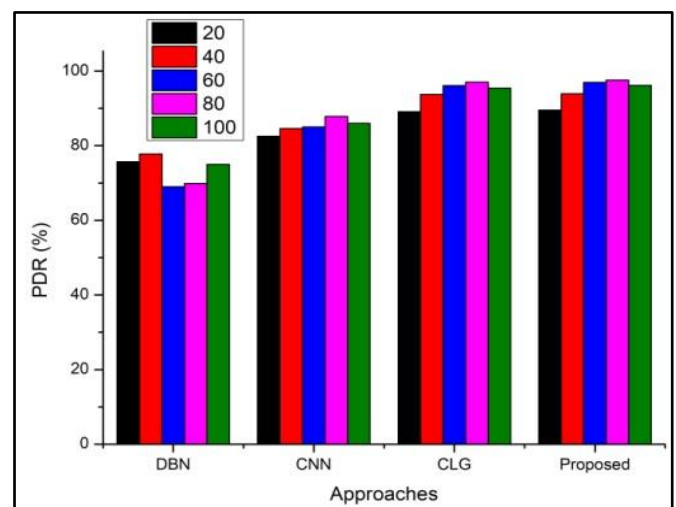


Fig. 13. Comparison using PDR

DBN incurred 69.02% of PDR, CNN incurred 85% of PDR, and CLG and the suggested model incurred 96.10% of PDR when there are 60 nodes. The combination of single models, such as CNN is what makes the presentation better. The display of all models is enhanced after the number of nodes increased. For example, the DBN is 74%, CNN is 86%, CLG incurred 95.43% whereas the suggested model is 96.15% when there are 100 nodes as shown in Figure 13.

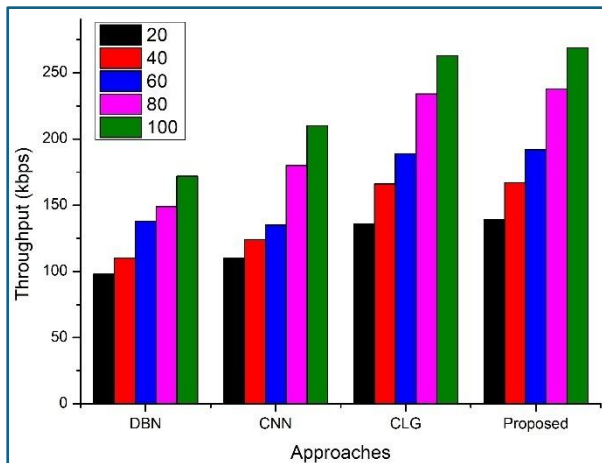


Fig. 14. Performance Comparison using Throughput

The CNN model incurred 110 kbps, the DBN incurred 98 kbps, the CLG model achieved 136 kbps whereas the proposed model obtained 139 kbps when there were 20 nodes. Better throughput performance demonstrates superior performance. In contrast to the current models, such as DBN and CNN, the CLG model achieved better throughput when the number of nodes increased from 40 to 100. The suggested model produced better throughput compared to the CLG model, for example, achieved 189 kbps for 60 nodes, 234 kbps for 80 nodes, and 263 kbps for 100 nodes. Figure 14 present these findings. As shown in Table 2, the proposed model performed better compared to the existing models in the routing overhead. For example, with 60 nodes, the suggested model obtained 0.49, CNN 0.70, and DBN 0.90 and CLG 0.53. The CNN incurred 1.0, the DBN incurred 1.23, the CLG incurred 0.83 whereas the suggested model 0.76 when there are 100 nodes.

Table 2. Performance validation using Routing Overhead

No. of nodes	DBN	CNN	CLG	Proposed
20	0.6	0.4	0.4	0.4
40	0.8	0.6	0.4	0.4
60	0.9	0.7	0.53	0.49
80	0.98	0.9	0.75	0.62
100	1.23	1.0	0.83	0.76

The suggested model's time analysis for attack detection is lower than that of the current methods as shown in Table 3. As an example, for 20 nodes, the suggested model obtained 20s, CNN 10s, and DBN 15s

and CLG 22s. Even when the number of nodes increased from 40 to 100 the suggested model takes minimal time for attack detection. This research makes it abundantly evident that the suggested model outperformed the others in terms of attack detection.

Table 3. Performance of the proposed method using Attack Detection Time

No. of nodes	DBN	CNN	CLG	Proposed
20	10	15	22	20
40	30	40	55	48
60	40	60	80	73
80	55	75	94	89
100	65	95	120	113

In contrast to sinkhole and delay assaults, the dropping attack has a noticeable effect. The dropping attack immediately discards packets when they are received, in contrast to the latter, which interfere with routing or delay transmissions. The PDR is significantly decreased as a result of this aggressive behavior. The average PDR in the randomly dispersed network falls to certain extent. Under a dropping assault, the throughput of the random network noticeably drops. Throughput decreases by about 20%, from 20,000,000 bits per second to 17,000,198 bits per second. When analyzing the effect of both dropping and combination attacks on end-to-end delay in the randomly dispersed network, it is critical to identify the attackers' initial starting movement pattern. Dropping packets eliminates them from the network completely, even though one may anticipate latency to rise with attacker interference. This removes their input into the computation of the total end-to-end delay. Since long-delay packets are the main target of the attackers' motion, removing them can lower the average end-to-end delay seen in the network. Analysis of sinkhole attack against PDR, throughput and end-to-end delay is given in Table 4.

Table 4. Performance of the proposed method against sinkhole attack

Attack Metrics /	PDR	Throughput	End-to-End Delay
Delay	0 to 0.52	0 to 20000000	0 to 0.017
Sinkhole	0 to 0.52	0 to 20000000	0 to 0.008
Dropping Packets	0 to 0.48	0 to 17000198	0 to 002

4.4. Limitation

Despite its great potential, the suggested strategy for improving Security and Transmission Efficiency in MANETs has few drawbacks. First off, the integration of various techniques requires a significant amount of memory and computing power, which may restrict its use in contexts with limited resources. Furthermore, the lively and uncertain character of MANET deployments in the real world might not be adequately captured by relying solely on simulation platforms like

NS2. This disparity may have an impact on the model's robustness and performance in real-world situations. Finally, there are still issues with the model's capacity to adjust to changing attack tactics. The suggested model requires frequent retraining and updates to preserve its efficacy as attackers constantly come up with new techniques, which could take a lot of time and resources.

5. CONCLUSION AND FUTURE SCOPE

Applications such as military applications, disaster relief efforts, medical emergencies, data monitoring, and certain commercial applications can all benefit from the suggested job implementation. The article makes a contribution and offers a solution to the problems with the current protocols that are related to security and routing energy. The routing, energy, and security issues of the protocols that improve network performance are the main objectives of this article. Wireless multipath routing is frequently employed to improve fault tolerance, replacing the initial single-path routing. The research illustrates how a hybrid method, based on GA and HCA, is used to solve multiphase problems. Before this implementation, the technique relied on density peaks and selected CHs using a projected approach, including recent, indirect, and direct trusts. The calculation depends on nodes with a trust threshold value, which is also included. The ideal route is determined by combining routes from these CHs, depending on the projected hybrid method and the aggregate parameters of the optimum route, including throughput, end-to-end delay, and routing overhead. This study uses the routes generated by the AOMDV approach and enhances their efficiency. It uses CSMA with the CTS/RTS method to identify and minimize collisions in the chosen routes. The protocol can forecast the reliability of connections and avoid busy paths. It provides a fitness measure and applies a GA to maximize the routes generated by the AOMDV technique in MANETs.

This proposed methodology was compared to the current approaches in scenarios where the selective dropping of intruders existed and in scenarios with and without the selective intruders to assess its effectiveness. The suggested method surpasses current rivals. In the future, deep learning methods can be included to identify intruders and enhance transmission efficiency.

REFERENCES

1. Koot, M., & Wijnhoven, F., 2021. Usage impact on data center electricity needs: A system dynamic forecasting model. *Applied Energy*, 291, 116798 <https://doi.org/10.1016/j.apenergy.2021.116798>
2. Quy, V. K., Nam, V. H., Linh, D. M., & Ngoc, L. A., 2022. Routing algorithms for MANET-IoT networks: a comprehensive survey. *Wireless Personal Communications*, 125(4), pp.3501-3525 <https://doi.org/10.1007/s11277-022-09722-x>
3. Gurung, S., & Chauhan, S., "A survey of black-hole attack mitigation techniques in MANET: merits, drawbacks, and suitability," *Wireless Networks*, vol. 26, 1981-2011, 2019, <https://doi.org/10.1007/s11276-019-01966-z>
4. Benatia, S. E., Smail, O., Meftah, B., Rebbah, M., & Cousin, B., "A reliable multipath routing protocol based on link quality and stability for MANETs in urban areas," *Simulation Modelling Practice and Theory*, 113, 102397, 2021, <https://doi.org/10.1016/j.simpat.2021.102397>
5. Pamarthi, S., & Narmadha, R., "Intelligent privacy preservation protocol in wireless MANET for IoT applications using hybrid crow search-harrishawks optimization," *Wireless Networks*, 28(6), 2713-2729 <https://doi.org/10.1007/s11276-022-02986-y>
6. Srilakshmi, U., Veeraiah, N., Alotaibi, Y., Alghamdi, S. A., Khalaf, O. I., & Subbayamma, B. V., "An improved hybrid secure multipath routing protocol for MANET," *IEEE Access*, vol. 9, 163043-163053, 2021, <https://doi.org/10.1109/ACCESS.2021.3133882>
7. Chen, Z., Zhou, W., Wu, S., & Cheng, L., "An adaptive on-demand multipath routing protocol with QoS support for high-speed MANET," *IEEE Access*, vol. 8, 44760-44773 <https://doi.org/10.1109/ACCESS.2020.2978582>
8. K. Muthumanickam, S. Elango, P.C. Senthil Mahesh and P. Vijayalakshmi, "EASS: Encryption and Authentication Based Security Scheme to Prevent Power Exhausting Attacks in Wireless Sensor Networks". *Ad Hoc & Sensor Wireless Networks*, Vol. 45, pp. 253-273, 2019
9. Shah, N., El-Ocla, H., & Shah, P., "Adaptive routing protocol in mobile ad-hoc networks using genetic algorithm," *IEEE Access*, vol. 10, 132949-132964, 2022, <https://doi.org/10.1109/ACCESS.2022.3230991>
10. K. Gowsic, K. Muthumanickam, A. Arthi and M. Saravanan, "An Enhanced Clustering Method for Optimal Energy Utilization and Improved Network Lifetime in IoT based WSN". *Ad Hoc & Sensor Wireless Networks*, Vol. 55, pp. 257-280, 2023
11. Singal, G., Laxmi, V., Gaur, M. S., Rao, D. V., Kushwaha, R., Garg, D., & Kumar, N., 2021. QoS-aware mesh-based multicast routing protocols in edge ad hoc networks: Concepts and challenges. *ACM Transactions on Internet Technology (TOIT)*, 22(1), pp.1-27 <https://doi.org/10.1145/3428150>
12. Prema, S., & Divya, M. P. (2023). Two-Tier Architecture for Congestion-Free Routing in Manet Using a Hybrid Optimization Algorithm. *Wireless Personal Communications*, 131(1), 507-526 <https://doi.org/10.1007/s11277-023-10442-z>
13. Baird, I.; Wadhaj, I.; Ghaleb, B.; Thomson, C. Impact Analysis of Security Attacks on Mobile Ad Hoc Networks (MANETs). *Electronics* 2024, 13, 3314.
14. Anish Pon Yamini, K., Suthendran, K., Arivoli, T., & Ravi, V. (2022). New approach for advanced energy efficiency in MANET (AEE-M) is improving optimized link state routing protocol version 2 (OLSRv2). *Wireless Personal Communications*, 125(3), pp.2369-2392 <https://doi.org/10.1007/s11277-022-09663-5>
15. Shafi, S., Mounika, S. & Velliangiri, S. Machine learning and trust based AODV routing protocol to mitigate flooding and blackhole attacks in MANET. *Procedia Comput. Sci.* 218, 2309-2318 (2023)

16. Abu Bakar, R., Huang, X., Javed, M. S., Hussain, S. & Majeed, M. F. An intelligent agent-based detection system for DDoS attacks using automatic feature extraction and selection. *Sensors* 23(6), 3333 (2023)
17. Ali, A. M., Ngadi, M. A., Sham, R., & Al-Barazanchi, I. I. Enhanced QoS routing protocol for an unmanned ground vehicle based on the ACO approach. *Sensors*, 23(3) (2022) 1431 <https://doi.org/10.3390/s23031431>
18. Yadav, K. et al. A secure multi-path communication through dynamic path identifiers to prevent denial-of-service flooding attacks. *Inter. J. Intell. Syst. Appl. Eng.*, vol. 11, no. 3s, pp. 22-28, (2023)
19. Monfared, S. K., & Shokrollahi, S., 2023. DARVAN: A fully decentralized anonymous and reliable routing for VANets. *Computer Networks*, 223, 109561 <https://doi.org/10.1016/j.comnet.2023.109561>
20. Mughaid, S. et al. Improved dropping attacks detecting system in 5 g networks using machine learning and deep learning approaches. *Multi Tools Appl.* 82(9), 13973-13995 (2023)
21. K. Baskar, P. Vijayalakshmi, K. Muthumanickam, A. Arthi, "A Novel Authentication and Access Scheduling Scheme to improve the Performance of WSN". *Neural Network World*, 33(4), pp. 205-225, 2023.
22. Abdelhamid, M. S., Elsayed, A. D., Jurcut & Azer, M. A. A Lightweight anomaly detection system for black hole attack. *Electronics* 12(6), 1294 (2023)
23. Pramodh Krishna D., E. Sandhya, Khaja Shareef Sk, Srihari Varma Mantena, Venkata Subbaiah Desanamukula, Ch Koteswararao, Srinivasa Rao Vemula & Maruthi Vemula, "Enhancing security and efficiency in Mobile Ad Hoc Networks using a hybrid deep learning model for flooding attack detection". *Scientific Reports*, 15:818, 2025.
24. Pantula, P. D., Miriyala, S. S., & Mitra, K., 2020. An evolutionary neuro-fuzzy C-means clustering technique. *Engineering Applications of Artificial Intelligence*, 89, 103435
25. Rath, M., & Pattanayak, B. K., 2021. Performance evaluation of optimized protocol in MANET. *International Journal of Information and Computer Security*, 14(3-4), pp.318-326 <https://doi.org/10.1504/ijics.2021.114708>
26. Sinwar, D., Sharma, N., Maakar, S. K., & Kumar, S., 2020. Analysis and comparison of ant colony optimization algorithm with DSDV, AODV, and AOMDV based on the shortest path in MANET. *Journal of Information and Optimization Sciences*, 41(2), pp.621-632 <https://doi.org/10.1080/02522667.2020.1733193>
27. <https://www.isi.edu/nsnam/ns/>