Journal of Network Communications and Emerging Technologies (JNCET)
Volume 14, Issue 1, January (2026)

Performance Enhancement of Video Data Transmission in MANET

Hamela K
Department of Computer Science, Government First Grade College, Kolar, Karnataka, India.
hamela27@gmail.com

ABSTRACT

Network services can be supplied by a mobile ad-hoc network (MANET), which is very effective. Routing protocols have some design flaws that impact network performance because of the dynamic nature of the network. This work develops an optimization algorithm-based single candidate-based optimized link state routing (SCOLSR) protocol to enable optimum video streaming in MANETs. Initially, the internet database is used to gather the video data. Next, trust parameters are used to validate the nearby nodes. The best nodes are chosen depending on trust factors. The Modified Single Candidate Algorithm (MSCA), which chooses the effective feature connected to characteristics like connection stability and node stability, is then used to continue the routing process. Single Candidate Algorithm (SCA) and Self-Adaptive (SA) algorithms are combined in this MSCA. Finally, the interplanetary file system (IPFS) security of MANET data is improved by the use of blockchain technology. Subsequently, the delegated proof of stake (DPoS) consensus mechanism is used to validate the blockchain technology. The suggested approach is put into practice using MATLAB, and a comparative analysis is used to assess performance.

Index Terms – MANET, OLSR, SCOLSR, MSCA, Video Data, DPoS.

1. INTRODUCTION

In the current day, with the proliferation of wireless networks, one of the most significant research areas is MANETs. Every day, the mobile ad-hoc network (MANET) will become more and more popular. It has become the most vibrant and athletic area of communication for wireless networks [1]. MANET, or infrastructure network, is self-organized and decentralized. Thus, secure packet routing against network behavior is the fundamental goal [2]. Topology and location-based MANET routing protocols aim for this. Routing options included proactive, reactive/on-demand, and hybrid [3]. Most reactive packet transmission uses "Ad-hoc On-demand Distance Vector (AODV)" routing [4]. AODV directly distributes multimedia and emergency information in MANETs due to route identification and repair [5].

The table-driven “Optimized Link State Routing Algorithm (OLSR)” protocol uses three routing mechanisms: a path selection algorithm based on the shortest path first, a flooding control packet that uses “Multi-Point Relay (MPR)”, and a periodic HELLO message for neighbor sensing. A set of MPRs with reachable two-hop neighbors is selected by each network node using two-hop neighbors [6]. The nodes then only rebroadcast the messages they have received from the nodes that have been designated as MPRs. One advantage of this strategy is that broadcast control overhead is reduced [7]. As a result, each node contains a part of the graph of the entire network topology. The MPR nodes transmit Topology Control (TC) messages with the original node address and MPR selection group to notify the group. The sender node uses the shortest path first algorithm to choose a route. An optimization algorithm optimizes OSLR for efficient routing. This summarizes the paper's main contribution.

- This work develops an optimization algorithm-based SCOLSR protocol to enable optimum video streaming in MANETs. Initially, the internet database is used to gather the video data. Next, trust parameters are used to validate the nearby nodes. The best nodes are chosen depending on trust factors.

- The MSCA, which chooses the effective feature connected to characteristics like connection stability and node stability, is then used to continue the routing process.

- SCA and SA algorithms are combined in this MSCA. Finally, the IPFS security of MANET data is improved by the use of blockchain technology. Subsequently, the DPoS consensus mechanism is used to validate the blockchain technology.

The document's structure continues: Section 2 reviews prior studies. In Section 3, we briefly describe our research System Model. Section 4 justifies simulation and assessment tool choices. After explaining the work strategy and simulation configuration, Section 5 shows and analyzes the outcomes. Section 6 concludes and suggests more investigation.

2. RELATED WORK

Numerous efforts to enhance the quality of video transmission have been documented in the literature. In this area, not many works are reviewed. An extensive overview of prior research works is provided in this section to identify and address significant issues in this field of study.

Effective data transfer in a MANET requires a dependable and secure routing system, as shown by M.S. Gowtham et al. [8]. While current methods attempt to prevent rogue nodes, they have disadvantages such as a minimum packet delivery ratio, noticeable delivery delays, low throughput, high energy consumption, and the requirement for additional hardware. This study introduces a revised AODV routing system that incorporates “Artificial Rabbits Battle Royale Optimization (ARBRO)” and “Self-attention Multiscale Network (SMNet)”. The ARBRO algorithm chooses the optimum node properties to optimize the path. These node properties help SMNet find the BHA node.

P. Rahul et al. [9] developed CBS-OLSR, or "chaotic bat swarm optimization algorithm-based optimized link state routing," to improve MANET deep Q-learning networks. This protocol saves MANET energy with OLSR MPR. OLSR and CBS determine the optimum source-to-destination node route similarly. Improved deep Q-learning and OLSR algorithms that improve MPR set selection may reduce network topology energy consumption and automatically increase network lifespan. A blockchain-based trusted distributed routing system for MANET by employing a “Latent Encoder Coupled Generative Adversarial Network Optimized” with “Binary Emperor Penguin Optimizer (LEGAN-BEPO-BCMANET)” has been presented by Sandeep Jagonda Patil et al. [10]. By creating a fair proof-of-reputation system, this approach uses blockchain technology to ensure decentralized, dependable routing through transactions based on verified blockchain tokens. The scheme enhances security and routing efficiency by combining Binary Emperor Penguin Optimizer (BEPO) with “Latent Encoder Coupled Generative Adversarial Network (LEGAN)”. Full security analysis is carried out with special attention to features such as transaction distinguishability, routing information integrity, resilience to self-modification, and prevention of double-spending. The suggested methodology is incorporated into the NS3 program, and assessment parameters such as average energy consumption and blockchain token transaction throughput are noted.

Patil et al. [11] observed a connection failure to preserve the source-to-destination node route during multimedia file transmission. During multimedia file transmission, hostile nodes try to penetrate the network and disrupt routing. PKSE was created to tackle this problem and provide safe routing. The “GreyWolf Optimization (GWO)” method maximizes the secure “Ad-hoc Demand Multi-path Distance Vector (AOMDV)” technology and achieves global network convergence. Based on packet delivery volume, delay, and network quality, Op-PKSEA chose the next hop node.

“Sensory modality-based cuckoo search butterfly optimization (SM-CSBO)” uses “cuckoo search optimization (CSO)” and “butterfly optimization (BOA)” to find the best route between the source and destination. Deepa Jeyaraj et al. [12] devised a multipath routing protocol. Finding a way with improved connection quality and more stable links is the main goal for reliable data transport. An efficient MANET routing protocol considers multi-objective function, distance, normalized energy, packet delivery ratio, and control overhead.

3. PROPOSED ARCHITECTURE

To achieve security using routing protocols, the suggested model creates an ideal method. To provide the best possible video streaming on MANET, this suggested technique has been devised. The suggested study is divided into four phases: rationale, blockchain storage, trust value computation, and data gathering. First, open-source technology is used to gather the video input data. To verify the dependability of nearby nodes concerning the trust parameters, a trust parameter is then constructed. With MSCO's consideration, the routing is finally accomplished. In Figure 1, the suggested method's entire architecture is displayed.

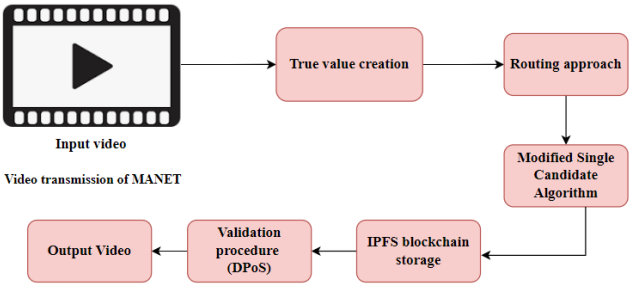

Figure 1 Architecture of the Proposed Method

The MSOC is utilized in this suggested model to identify the most effective approach based on factors like node stability degree and link stability degree. Using the "interplanetary file system (IPFS)" method, blockchain storage has been proposed to enhance MANET data security. The "delegated proof of stake (DPoS)" technique is used to demonstrate the blockchain technique's justification process. This technique secures MANETs and maximizes privacy. Based on the method's optimal performance, MSCO is ideal for MANET video transmission applications.

3.1. MANET Architecture

MANET is the most popular kind of wireless architecture due to its many behaviors and flexibility, including self-configuring and infrastructure-less capabilities. In any design, routing is choosing a path. A computing network is a collection of nodes and their links.

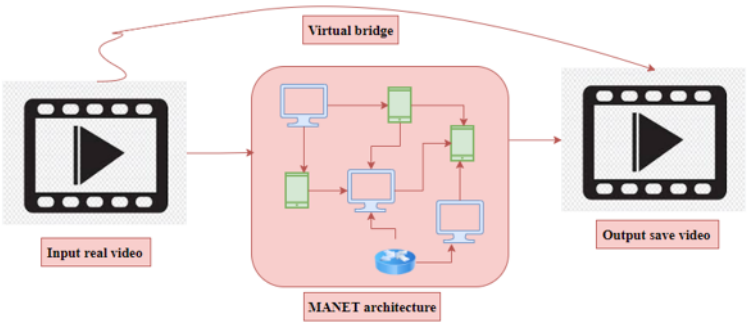

Figure 2 MANET Architecture

A connected network can have multiple channels of communication between two nodes. Routing is the process of deciding on the optimum course while following pre-pair directions. A peer-to-peer distributed database that functions similarly to a ledger is called a "blockchain." It is composed of a list of blocks, or continuously growing items, that are linked together and secured using public-key cryptography. In a distributed architecture, new data is added to a block and shown to each node via blockchain technology, rather than uploaded to a centralized database. The 256-bit safe hash cryptographic method recognizes every blockchain block and generates the hash parameter. By maintaining security, hackers and others cannot access sensitive data. Blockchain security is a big issue since it depends on blockchain networks. Transactions and the blockchain infrastructure are protected by blockchain security, a risk management technique. The suggested approach combines a number of elements to allow the nodes to send video. Figure 2 demonstrates how the suggested algorithm operates. The suggested architecture receives the input video first. Two" designs are used for the best possible video streaming on both sides. The video stream is correctly received on the output side of the proposed MANET system. Subsequently, the architecture's simulation designs collect features from the movies to test the architecture, and at last, the data is secured for storage.

3.2. Trust Parameter Evaluation

Using the communicated topology control and HELLO messages, the dependability of nearby mobiles is calculated while taking the MSOA into account. When the trust rate in a packet transmission meets the stated trust requirement, the mobile device is chosen. The neighbor gathering can be customized to incorporate the quantity of messages provided by each neighbor and the number of neighbors found to oversee the recently added designs. Every time these parameters are adjusted, the conveyed topology and HELLO message are reached. The likelihood of operating a “specific action expected by Y is denoted as $t_Y(N)$, is how the trust-related efficient routing also identified trustworthiness in a node N administered by a different node Y. Subsequently [13], Y can determine trustworthiness based on the information acquired from a particular operation by calculating the weighted average of the trust associated with each kind of action, including data transmission, route request, route error, and route reply. A message from N during this period, which states that ρ_C has been verified to be authentic, that ρ_a is the total number of transmission attempts, and ρ_s is the total number of successful transmissions”, which is composed as follows:

$$t_Y(N) = \frac{\rho_C + \varepsilon\rho_s}{\rho_t + \varepsilon\rho_a} \qquad (1)$$

Here, the weighting factor $0 < \varepsilon < 1$, is defined as the ratio of ideal transmissions, indicating a high likelihood of the transmission link operating efficiently. In this case, a different mathematical design from the trust level validation is taken into consideration, which is equivalent to the one used to compute link quality. Connection quality is also somewhat defined by the equation above when trustworthiness is taken into consideration. More comprehensive measurements are used to get a more accurate

trustworthiness grade. These measurements describe "link quality and include collision monitoring, signal separation techniques, power management techniques, and link adjustment. Here, consider that the measurement of $t_Y(N{:}J)$ for the jth trustworthiness, the upgrade stage is designated as $\hat{t}_Y\ (N, J+1)$, that is computed by assessing N's current characteristics while Y examines the authenticity and correctness of the messages that arrive. In the $(J+1)^{th}$ trustworthiness upgrade stage, create a count of trustworthiness, which is defined as $\hat{t}_Y\ (N, J)$. To generate a smooth computation, the moving average technique is formulated as follows,

$$\hat{t}_Y\ (N, J+1) = \alpha \hat{t}_Y(N{:}J) + (1-\alpha)\hat{t}_Y\ (N, J), \quad for\ N \epsilon N_1(Y) \qquad (2)$$

Here, $\hat{t}_Y(N{:}J)$ is defined as the trustworthiness of a node N as given by node Y by the trustworthiness upgrade cycle. The node maintains, calculates, and stores a weighted or trustworthiness score-shifting average model in response to fresh data.

Assume the path, $K \epsilon K_{s \to Y}$, in that $K_{s \to Y}$ is a gathering of pathways associated at a source node S and ends at a destination node Y, for instance $K_{s \to Y} = \{\ all\ paths\ from\ S\ to\ Y)$. After that, the trustworthiness of the path is denoted by $t_Y(K{:}J)$ and the path is specified by a node Y. The path of trustworthiness is formulated as follows,

$$t_Y(P{:}J) = \prod_{N \epsilon K} t_Y(N{:}J) \qquad (3)$$

Y can raise its" standing based on the results, which are connected to the reliability of its nearest nodes. To calculate routing decisions, a node uses the corrections as a measurement of its route.

3.3. Effective Protocol for Routing Link States

In general, nodes exchange network design data as part of the proactive routing architecture defined by the proposed routing protocol. Each network node chooses a pair of nearby nodes to act as multipoint relays. The additional protocols on the network are to be processed independently by this proposed routing protocol. Neither is the relationship between the protocol's layers used in any computation. For ad hoc network clusters like MANETs, it is utilized. Within the suggested protocol, control traffic meant for distribution over the entire architecture is transmitted by the multipoint relay [14]. Control messages become trustworthy and transmittable as a result of this multipoint relay's reduction in the number of transactions needed for an efficient design. Details on the connection status across the networks must then be provided as a particular task. In route processing, it is thought to be possible to create a path from two network nodes, linking at the additional end node and starting at the single source network. The suggested procedure is shown in Figure 3.

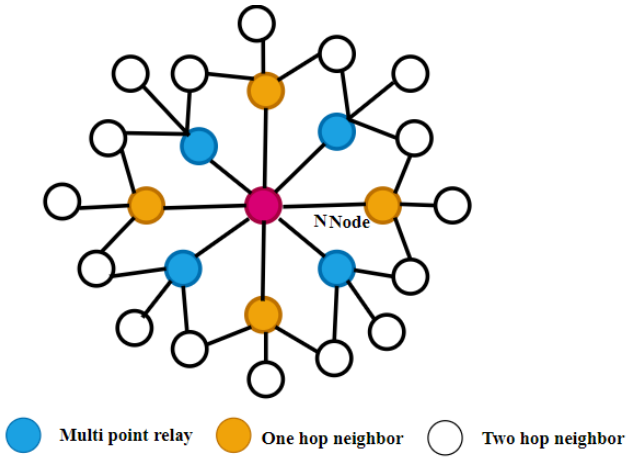

Figure 3 Routing Protocol

Design control and hello messages are the two message kinds used in the protocol. Each node in an architecture may need HELLO messages to learn the link state and nodes within two hops. Data is used to calculate the multi-point relay for each interaction node. Each node in an architecture sends messages to update packet routing data. Transmission control messages are regularly transmitted by several nodes to create a multi-point delay selection pair. Routinely improving the suggested routing reduces the effective periodic interval of response and the time required to issue transmission control messages.

For the suggested protocol to handle the routing operation, an integrated administration approach is not needed. Because there won't be a delay in computing a route there, it's used for some network operations where routes that are available through a routing list are present. Furthermore, the suggested protocol is enhanced by the multi-point routing technique most effectively in large networks. However, no capabilities for the quality of connection validation are provided by the proposed protocol rules. Once that's done, the frequent modifications to the routing table lead to an improvement in bandwidth usage. Subsequently, the suggested protocol is used to accomplish routing, occasionally it becomes more difficult to identify a multi-point relay.

3.4. Modified Single Candidate Algorithm

This is a new searching method that, in contrast to most traditional searching approaches that rely on a swarm of particles, uses only one candidate solution throughout the whole optimization algorithm to calculate optimal solutions. The suggested method divides the entire optimization process, which involves computations of T functions, into two phases, where each step consists of a separate upgrading of the location by the candidate solution. Two further meta-heuristic optimization strategies are used: one that is based on a single solution and the other that follows two phases [15].

Step 1: Initialization and self-adaptive technique

The self-adaptive population is one modification that can improve the SCA's efficacy. This balance between exploitation and exploration, as well as the long-range and random movement, may result in the best answers. To achieve the best balance between exploitation and exploration, this population dynamically modifies parameters and population size with issue behaviors and optimization techniques. By automatically adjusting to shifting issue dynamics, dynamically allocating computational resources, averting premature convergence, and preserving a diversified population, this adaptability improves efficiency. The following is the calculation of the starting population size before the method was established:

$$Size\ (X) = 10 \times Dim \qquad (4)$$

Here, Dim is a problem dimension. The process for computing the revised population size is presented as follows,

$$Size\ (X)_{NEW} = ROUND(Size(X) + \beta \times Size\ (X)) \qquad (5)$$

Here, β is a randomly generated integer between 0.5 to -0.5. The single-candidate and two-stage strategies are combined to create this resilient algorithm. The suggested method determines the best course of action by taking into account variables like the degree of node and network stability. The following is how these functions are expressed:

$$C_{IJ} = \lambda_1 lq_{IJ} + \lambda_2 X_{IJ} + \lambda_3 S_{IJ} \qquad (6)$$

Here, S_{IJ} is defined as the factor for identifying mobility, lq_{IJ} is defined as link quality, $\lambda_1, \lambda_2, \lambda_3$ is a weighting vector, X_{IJ} is a safety degree and C_{IJ} is a link stability from I and J.

$$v(Z) = \left(\sum_H \frac{Z_H^2}{N}\right) - \left(\sum_H \frac{Z_H}{N}\right)^2 \qquad (7)$$

Here, Z_H is defined as the message level acquired from each adjacent node, H is the total quantity of nodes, and $v(Z)$ is a variance.

Step 2: Fitness function

The suggested method determines the best course of action by taking into account variables like the degree of node and network stability. The following is how these functions are expressed:

$$\text{FF} = \text{MAX}(\text{link stability degree} + \text{Node stability degree}) \qquad (8)$$

Step 3: Exploration Stage

The two-stage technique requires offering diversity and a balance between exploration and exploitation. When α-function computations are carried out during the second stage of optimization, which includes $beta - function$ computations, the first stage of optimization comes to an end. In this case, $\alpha + \beta = T$. The candidate solution improves its position in this method's initial step in the way outlined below:

$$X_J = \begin{cases} GBEST_J + \left(w|GBEST_J|\right) & if\ R_1 < 0.5 \\ GBEST_J - \left(w|GBEST_J|\right) & otherwise \end{cases} \qquad (9)$$

Here, R_1 is a random variable. The computation of w is defined as follows,

$$w(T) = Exp^{-\left(\frac{BT}{t}\right)^B} \quad (10)$$

Here, t denotes maximum number of functions, T is the presented function an iteration or an evaluation and B is a constant. The deep search that is carried out in the second step of this algorithm begins with a thorough exploration of the area surrounding the ideal spot that was attained in the first stage [25,26]. The area to be searched is reduced in the following part of stage two, which makes it easier to concentrate on the one likely site. The candidate solution's second-stage location upgrade is depicted below.

$$X_J = \begin{cases} GBEST_J + \left(R_2 w\left(UB_J - LB_J\right)\right) & if\ R_2 < 0.5 \\ GBEST_J - \left(R_2 w\left(UB_J - LB_J\right)\right) & otherwise \end{cases} \quad (11)$$

Here, w is the essential factor in this algorithm that is responsible for balancing between exploration and exploitation, LB_J is a lower bound, UB_J is an upper bound, R_2 is a random parameter in the range of [0.1].

W in the formulation, decreases exponentially with an increase in the number of function computations is exponential. These qualities are important because, at the start of the search process, a relatively high parameter of W aids in the optimal exploration of the search space, and in the latter stages of the optimization process, a small value of W strengthens the exploitation capabilities. The primary drawback of the optimization method is becoming stuck in local optima, particularly in the later stages of the search. In different terms, a continuous improvement of candidate solution positions does not improve fitness. To address this problem, this approach upgrades the candidate solution's position in a different way in the second stage if, after M consecutive function calculations, no fitness enhancement is found.

Initialize the random population and define the parameters of M

Create the initial candidate solution

Apply self-adaptive mechanism

While T<maximum number of functions

if T<Alpha then

Upgrade the dimension position

Else

if P=0 then

C=C+1

End if

if C=M then

Reset the counter C=0

Upgrade the dimension

Else

Upgrade the dimension

End if

End if

Compute the fitness of the new candidate solution

If F(X) is better than the global best then

GBEST=X

F(GBEST)=F(X)

P=1

Else

P=0

End if

T=T+1

End while

Return GBEST"

Algorithm 1 Pseudocode of the Algorithm

Step 4: Exploitation Stage

The count of function evaluation M that cumulatively fails to achieve fitness improvement is represented by a count C. Whether the updated candidate can achieve successful fitness or not, it is calculated using a binary variable P. Exercise enhancement failure is defined by P = 0, and efficient exercise enhancement is defined by P = 1. A candidate solution is found in the second stage of this algorithm, where it is found using the above formulation. Additionally, if executing M consecutive function calculations does not improve the fitness parameter, the candidate solution finds a new location in the following manner:

$$X_J = \begin{cases} GBEST_J + \left(R_3\left(UB_J - LB_J\right)\right) & if\ R_3 < 0.5 \\ GBEST_J - \left(R_3\left(UB_J - LB_J\right)\right) & otherwise \end{cases} \quad (12)$$

Here, R_3 denotes random number. The process of updating positions enables the candidate solution to transition from exploitation to exploration, aiding in breaking free from the local optimum. Sometimes parameters will travel outside of their range or boundaries when their positions are upgraded. The upgraded positions are coupled in the following manner if their parameters surpass the lower and upper constraints to prevent parameters from going over the boundaries.

$$X_J = \begin{cases} GBEST_J & if\ R_J > UB_J \\ GBEST_J & if\ R_J < LB_J \end{cases} \quad (13)$$

According to the aforementioned equation, when the global best parameter of the upgrading position crosses a bound, the upgraded dimension of a candidate solution is assigned a corresponding parameter. This technique generates a single candidate solution at random and then iteratively improves it to get the optimal option. The following is an explanation of each phase of the suggested method. First, a candidate solution is randomly generated within the search space. This candidate is saved as the world's best after its fitness is determined. The first possible solution is presented as follows:

$$X_J = LB_J + R_4\left(UB_J - LB_J\right) \quad (14)$$

Here, R_4 denotes random number, UB_J is an upper bound and LB_J is a lower bound.

Step 5: Termination Condition

Upgrading the candidate solution's position is the first step in the iterative process that ends when T function computations are obtained. Stages one and two see an enhancement for the proposed solution X. The freshly created candidate solution's fitness function is assessed and contrasted with the world's best once it has been upgraded. Iterations continue if the fitness function outperforms global fitness. The best solution is saved. The process of iteration persists until the maximum number of function calculations (T) is achieved.

3.5. Interplanetary File System (IPFS)

The issue of information storage on MANET must be resolved by the suggested blockchain interaction. A distributed, peer-to-peer data storage network can be established with IPFS. IPFS allows large files to be preserved on a reliable path. It allows peer file sharing. Every file in the proposed system uses encrypted hashing and a parameter called the content identified, also known as the file address or hyperlink. Additional CID holders can access and receive the file. IFPS peers function as file servers, distributing and archiving massive amounts of data quickly [16].

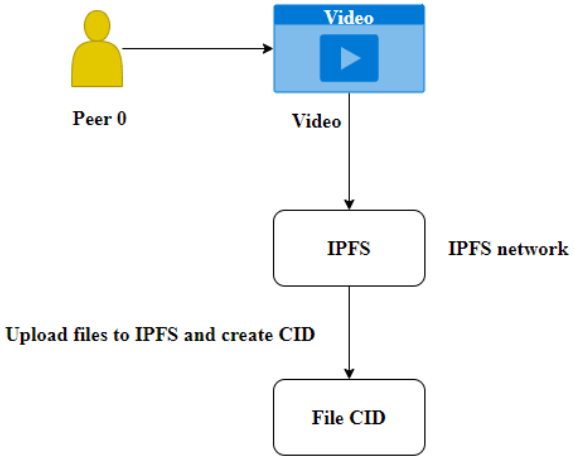

Figure 4 Interplanetary File System

Despite its ability to solve the blockchain's large redundant data storage problem, IPFS is classified as a responsive blockchain component. Peers may store layout files and documents in IPFS and add content IDs to blockchain activities to boost authenticity and reliability.

3.6. Delegated Proof of Stake

The suggested method uses network participants to vote and monitor block validation as part of DPoS[17]. Nodes that verify transactions are chosen by the proposed blockchain owners. Voting power is based on staked holdings. The nodes in charge of this situation are particularly affected by users with higher stakes. It defines the measure delegate for the designated odes. Under the suggested approach, each node inside the blockchain architecture can cast a vote about the assets and select the node that best fits its needs.

By design, the DPoS is more representative than other architectures since it takes into account an independent voting process. Rather than eliminating the confidence needed, the suggested approach enables users to authenticate and approve blocks throughout the entire network to carry out verification accurately and truthfully. Please validate that the reliable node is the origin of each verified block. The transaction is invalidated when DPoS has a certain number of unknown nodes. However, 3S processing is typically helpful. To encourage participation, each explanation may be different. It may reward selected users with a certain percentage of incentive money for forwarding a block. Many say the process will agree fast because there are no validators.

4. RESULTS AND DISCUSSIONS

This section details the suggested techniques' performance and comparison. MATLAB processes research using simulation results and system needs. The recommended approach is validated using online video [18]. Videos are gathered and considered while transmitting data via MANET. The suggested approach is compared with traditional techniques like “AODV-Grey Wolf Optimization (AODV-GWO)” and “AODV-Particle Swarm Optimization (AODV-PSO)” to validate its performance using performance measures like drop, energy consumption, throughput, delivery ratio, delay, bandwidth, and jitter. To validate the proposed methodology, the system model is designed and validated, and implementation parameters are listed in Table 1. Figures 5-8 show the MANET's trust node evaluation, routing process, initialization, and video data transfer.

Table 1 Implementation Parameters

S. No.	Description	Parameters
1	Base station position	(50, 50)
2	Data packet size	500 bytes
3	Number of cluster heads	P × 100

4	Probability of becoming cluster head	0.1
5	Initial energy	1 J
6	Network size	100
7	Network terrain	100 m²
8	Number of iterations	100
9	Lower bound	-100
10	Upper bound	100”

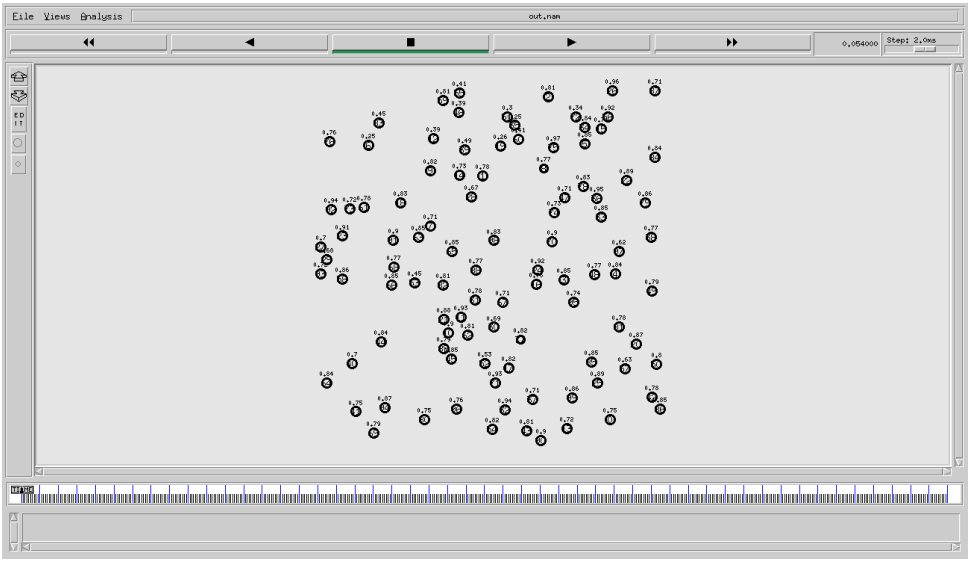

Figure 5 Trust-Node Evaluation

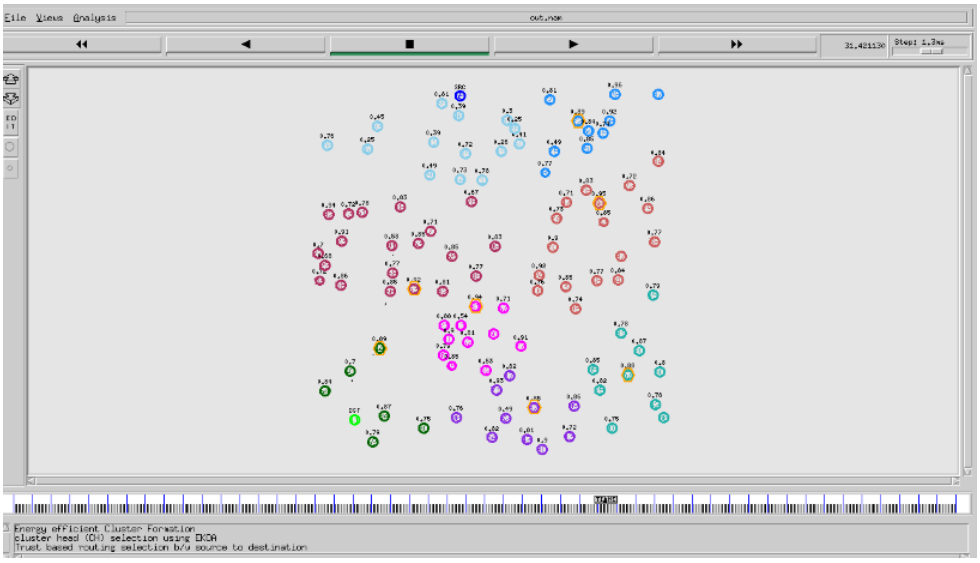

Figure 6 Routing Process

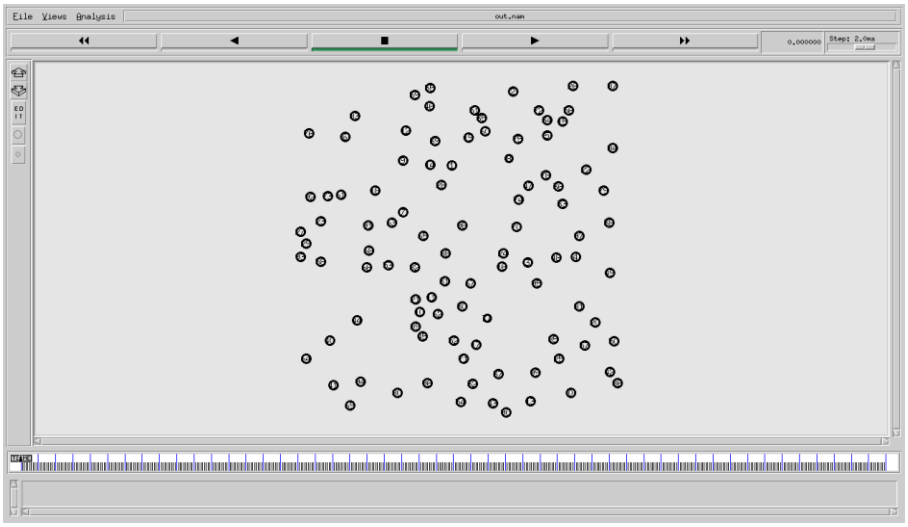

Figure 7 Initialization

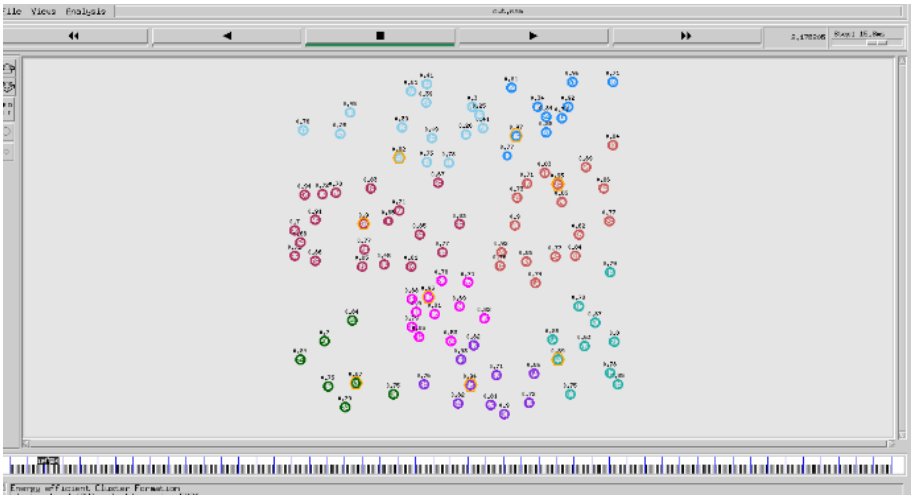

Figure 8 Video Data Transmission

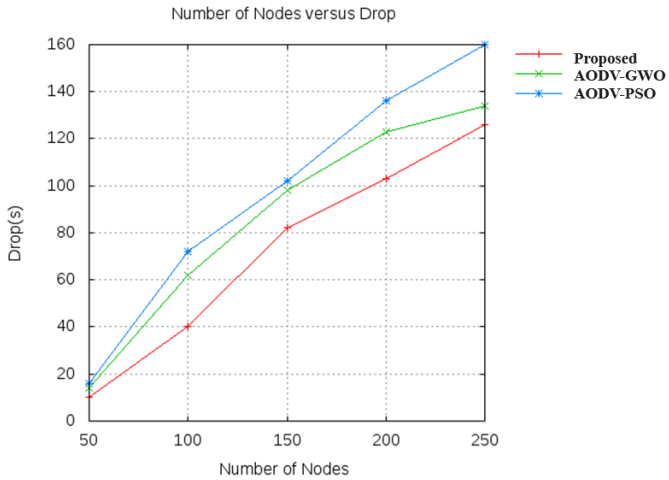

Figure 9 Drop

The drop measure, which is demonstrated in Figure 9, is taken into consideration and analyzed to validate the suggested method of MANET routing and security enhancement. Based on the decrease, this metric is calculated. Conventional methods like AODV-GWO and AODV-PSO are contrasted with the suggested approach. The suggested approach produced a 40-second reduction over the 100 nodes. Furthermore, the 62s and 72s drop the development of traditional procedures. With 200 nodes, the suggested approach obtained 121 s. In addition, the traditional methods obtain 125 and 160 s, respectively. This validation showed that during the video data transmission, the suggested strategy produced a low drop. The energy consumption measure, which is demonstrated in Figure 10, is taken into consideration and analyzed to validate the suggested method of MANET routing and security enhancement. Based on the decrease, this metric is calculated. Conventional methods like AODV-GWO and AODV-PSO are contrasted with the suggested approach. The suggested approach produced an 8.7J reduction over the 100 nodes. Furthermore, the 8.9J and 9.2s energy consumption are the development of traditional procedures. With 200 nodes, the suggested approach obtained 6.2J. In addition, the traditional methods obtain 6.4J and 7.5J, respectively. This validation showed that during the video data transmission, the suggested strategy produced a low energy consumption.

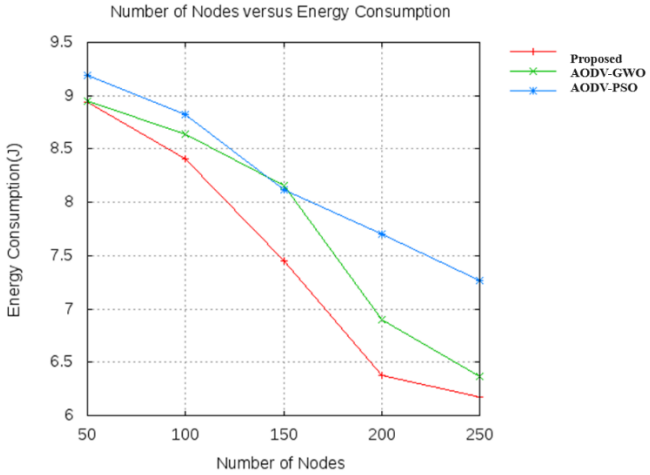

Figure 10 Energy Consumption

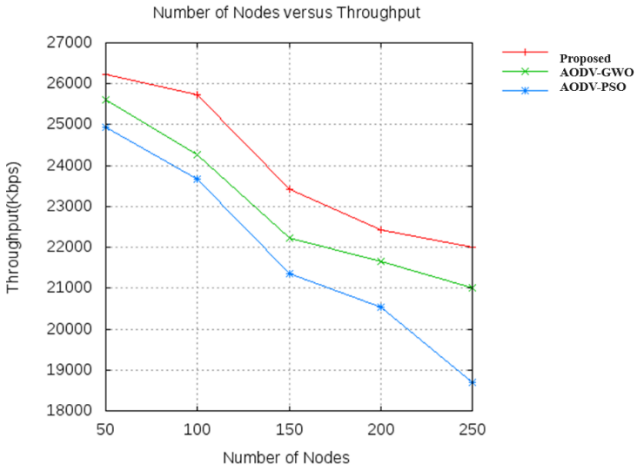

Figure 11 Throughput

The throughput measure, which is shown in Figure 11, is taken into consideration and analyzed to validate the suggested method of MANET routing and security enhancement. Based on the increase, this metric is calculated. Conventional methods like AODV-GWO and AODV-PSO are contrasted with the suggested approach. The suggested approach produced a 26005kbps throughput over the 100 nodes. Furthermore, the 25550kbps and 25000kbps energy consumption the development of traditional procedures. With 200 nodes, the suggested approach obtained 22350kbps. In addition, the traditional methods obtain 20004kbps and 18500kbps, respectively. This validation showed that during the video data transmission, the suggested strategy produced a high

throughput. The delivery ratio measure, which is shown in Figure 12, is taken into consideration and analyzed to validate the suggested method of MANET routing and security enhancement. Based on the increase, this metric is calculated. Conventional methods like AODV-GWO and AODV-PSO are contrasted with the suggested approach. Over the 100 nodes, the recommended method yielded a delivery ratio of 0.96. Additionally, the 0.92 and 0.90 delivery ratios represent the evolution of traditional approaches. With 200 nodes, the suggested approach obtained 0.66. In addition, the traditional methods obtain 0.58 and 0.52, respectively. This validation showed that during the video data transmission, the suggested strategy produced a high delivery ratio.

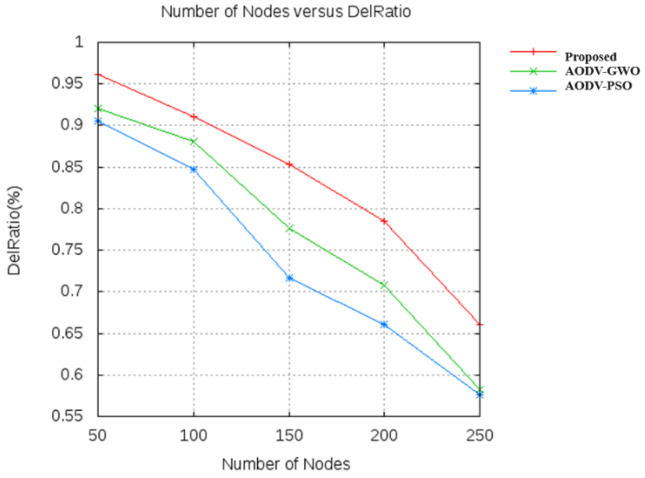

Figure 12 Delivery Ratio

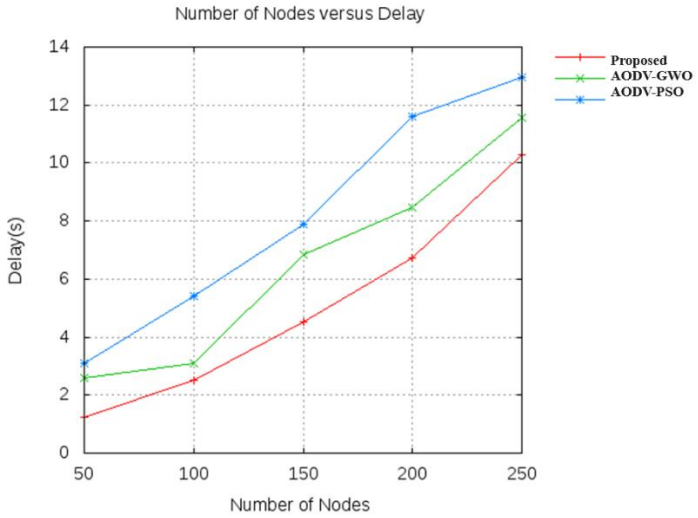

Figure 13 Delay

The delay measure, which is shown in Figure 13, is taken into consideration and analyzed to validate the suggested method of MANET routing and security enhancement. Based on the decrease, this metric is calculated. Conventional methods like AODV-GWO and AODV-PSO are contrasted with the suggested approach. The suggested approach produced a 1s delay over the 100 nodes. Furthermore, the 3s and 5s delay the development of traditional procedures. With 200 nodes, the suggested approach obtained 7s. In addition, the traditional methods obtain 8.1s and 11s, respectively. This validation showed that during the video data transmission, the suggested strategy produced a low delay. The bandwidth measure, which is shown in Figure 14, is taken into consideration and analyzed to validate the suggested method of MANET routing and security enhancement. Based on the increase, this metric is calculated. Conventional methods like AODV-GWO and AODV-PSO are contrasted with the suggested approach. The suggested approach produced a 2Mbps bandwidth over the 100 nodes. Furthermore, the 1.5mbps and 0.8mbps bandwidth the development of traditional procedures. With 200 nodes, the suggested approach obtained 3.6Mbps. In addition, the

traditional methods obtain 3.6Mbps and 3.1Mbps, respectively. This validation showed that during the video data transmission, the suggested strategy produced a high bandwidth. The jitter measure, which is shown in Figure 14, is taken into consideration and analyzed to validate the suggested method of MANET routing and security enhancement. Based on the decrease, this metric is calculated. Conventional methods like AODV-GWO and AODV-PSO are contrasted with the suggested approach. The suggested approach produced a 4s jitter over the 100 nodes. Furthermore, the 5s and 6s bandwidth the development of traditional procedures. With 200 nodes, the suggested approach obtained 15s. In addition, the traditional methods obtain 21s and 22s, respectively. This validation showed that during the video data transmission, the suggested strategy produced a high jitter.

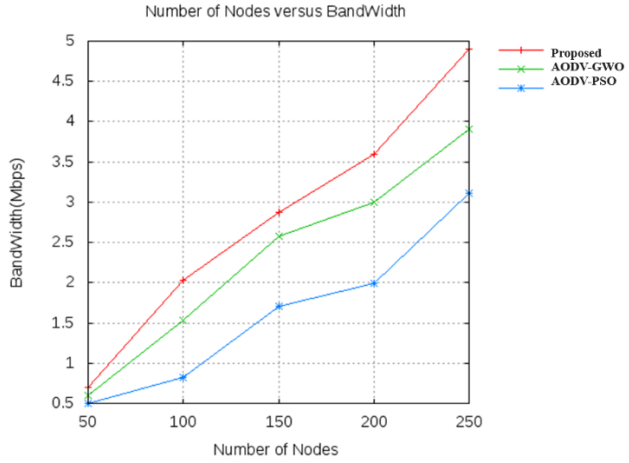

Figure 14 Bandwidth

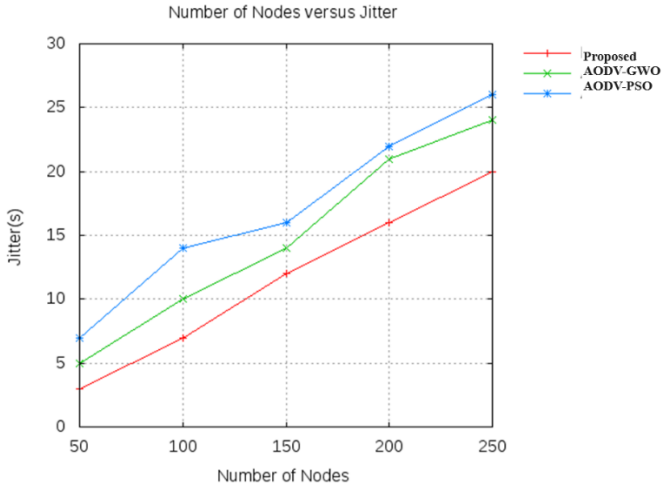

Figure 15 Jitter

5. CONCLUSION

To facilitate optimal video streaming in MANETs, this work has created an optimization algorithm-based SCOLSR protocol. The video data was initially collected via the internet database. The adjacent nodes are then verified using trust parameters. Based on trust-related criteria, the top nodes have been selected. Then, to carry out the routing procedure, the MSCA was utilized, which selects the effective feature linked to attributes like connection stability and node stability. In this MSCA, the SCA and SA algorithms have been integrated. Lastly, the application of blockchain technology has enhanced the IPFS security of MANET data. The blockchain technology has since been verified through the usage of the DPoS consensus mechanism. Throughput, energy consumption, delivery ratio, jitter, delay, drop, and jitter are performance metrics that have been used to assess this suggestion. The suggested methodology has produced the best outcomes, according to this evaluation. Moving forward, a new protocol will be taken into consideration for secure multimedia data transmission.

REFERENCES

[1] Patil, Sandeep Jagonda, Lalita Sunil Admuthe, Ashwini Sandeep Patil, and Saurabh R. Prasad. "Secure MANET routing with blockchain-enhanced latent encoder coupled GANs and BEPO optimization." Smart Science (2024): 1-14.
[2] Singh, C. Edwin, S. Sharon Priya, B. Muthu Kumar, K. Saravanan, A. Neelima, and B. Gireesha. "Trust aware fuzzy clustering based reliable routing in Manet." Measurement: Sensors 33 (2024): 101142.
[3] Janani, R. S., and R. Asokan. "Deployment of efficient MANET testbed using aggregation based archive population optimization." Biomedical Signal Processing and Control 96 (2024): 106556.
[4] Shanmugham, Kalaimani, Rajesh Rangan, Saravanan Dhatchnamurthy, and Sumit Pundir. "An efficient self-attention-based conditional variational auto-encoder generative adversarial networks based multipath cross-layer design routing paradigm for MANET." Expert Systems with Applications 238 (2024): 122097.
[5] Hande, Jayant Y., and Ritesh Sadiwala. "Data security-based routing in MANETs using key management mechanism." SN Computer Science 5, no. 1 (2024): 155.
[6] Nirmaladevi, K., and K. Prabha. "A selfish node trust aware with Optimized Clustering for reliable routing protocol in Manet." Measurement: Sensors 26 (2023): 100680.
[7] Reddy Yeruva, Ajay, Esraa Saleh Alomari, S. Rashmi, Anurag Shrivastava, M. Kathiravan, and Abhay Chaturvedi. "A secure machine learning-based optimal routing in Ad Hoc networks for classifying and predicting vulnerabilities." Cybernetics and Systems (2023): 1-12.
[8] Gowtham, M. S., M. Ramkumar, S. Syed Jamaesha, and M. Vigenesh. "Artificial self-attention rabbits battle royale multiscale network based robust and secure data transmission in mobile Ad Hoc networks." Computers & Security 142 (2024): 103889.
[9] Rahul, P., and B. Kaarthick. "Proficient link state routing in mobile ad hoc network-based deep Q-learning network optimized with chaotic bat swarm optimization algorithm." International Journal of Communication Systems 36, no. 1 (2023): e5324.
[10] Patil, Sandeep Jagonda, Lalita Sunil Admuthe, Ashwini Sandeep Patil, and Saurabh R. Prasad. "Secure MANET routing with blockchain-enhanced latent encoder coupled GANs and BEPO optimization." Smart Science (2024): 1-14.
[11] PATIL, ANITA R., and GAUTAM M. BORKAR. "Multimedia Data Transmission in MANETs Using the ACO-GWO Based AOMDV Protocol." Adhoc & Sensor Wireless Networks 57 (2023).
[12] Jeyaraj, Deepa, Justindhas Yesudhasan, and Ahamed Ali Samsu Aliar. "Developing multi-path routing protocol in MANET using hybrid SM-CSBO based on novel multi-objective function." International Journal of Communication Systems 36, no. 4 (2023): e5404.
[13] Shafi, Shaik, S. Mounika, and S. J. P. C. S. Velliangiri. "Machine learning and trust based AODV routing protocol to mitigate flooding and blackhole attacks in MANET." Procedia Computer Science 218 (2023): 2309-2318.
[14] Mahamune, Ankita A., and M. M. Chandane. "Trust-based co-operative routing for secure communication in mobile ad hoc networks." Digital Communications and Networks (2023).
[15] Shami, Tareq M., David Grace, Alister Burr, and Paul D. Mitchell. "Single candidate optimizer: a novel optimization algorithm." Evolutionary Intelligence 17, no. 2 (2024): 863-887.
[16] Li, Shunlei, Xia Fang, Jiawei Liao, Mojtaba Ghadamyari, Majid Khayatnezhad, and Noradin Ghadimi. "Evaluating the efficiency of CCHP systems in Xinjiang Uygur Autonomous Region: an optimal strategy based on improved mother optimization algorithm." Case Studies in Thermal Engineering 54 (2024): 104005.
[17] Dao, Thi-Kien, and Trinh-Dong Nguyen. "A Sensor Network Coverage Planning Based on Adjusted Single Candidate Optimizer." Intelligent Automation & Soft Computing 37, no. 3 (2023).
[18] https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds.

Author

Dr. Hamela K was born in Chennai, India. She received her MCA degree from Bharathidasan University, Tiruchirappalli, India in 2002, followed by an MPhil degree from Mother Teresa Women's University, Kodaikanal, India in 2004. She further earned an MBA degree from Alagappa University, Karaikudi, India in 2010. In 2020, she completed her Ph.D. in the area of "Mobile Ad Hoc Networks" at Mother Teresa Women's University, Kodaikanal. Currently, Dr. Hamela K is an Associate Professor and Head of the Computer Science department at Government First Grade College, Kolar, Karnataka, India.