Journal of Information Systems Engineering and Management
2025, 10(22s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Kookaburra Node Aware Trustable and Enhanced Clustering and Routing in Mobile Ad Hoc Networks

[1]Divya Boya, [2] Dr. Syed Shabbeer Ahmad

[1] Research Scholar, Department of CSE, UCE, Osmania University, Hyderabad, India

[2] Professor, Department of CSE, MJCET , Hyderabad, India

E-mail: [1]divyaboya1291@gmail.com, [2] shabbeer.ahmad@mjcollege.ac.in

ARTICLE INFO

Received: 14 Dec 2024

Revised: 02 Feb 2025

Accepted: 18 Feb 2025

ABSTRACT

Researchers have created a wide range of Mobile Ad-hoc Networking (MANET) protocols to take advantage of the special communication opportunities that these devices present as a result of the growing availability and popularity of mobile wireless devices. Mobility awareness and energy efficiency are viewed as two key benefits in MANETs, where nodes periodically visit every path, limiting battery life and resulting in frequent topology modifications. This paper presents a Kookaburra Node Aware Trustable and Enhanced Clustering (KNATEC) for optimal routing in MANET. The clustering is proceeding with hierarchical clustering for generating node clusters. The cluster head selection is completed by using the Enhanced Kookaburra Optimization Algorithm (EKOA). The initial node detection is completed by developing the authentication technique that will authenticate the cluster heads. After that, a trust-based routing protocol (TRP) is obtained to identify and isolate both faulty and misbehaving nodes. This also assists in detecting common misbehavior attacks like Sybil and wormholes. After that, efficient routing is obtained by using EKOA. The proposed method is implemented in NS2, and performance is evaluated by performance measures of energy consumption, end-to-end delay, throughput, average delay, loss ratio, and packet delivery ratio. The proposed method is compared with the conventional routing process.

Keywords: MANET, kookaburra optimization algorithm, trust-based routing protocol, clustering approach, and security.

1. INTRODUCTION

An autonomous ad hoc wireless network with several nodes that move dynamically to alter the topology is called a mobile ad hoc network, or MANET. Wireless communication technologies like WiFi, ZigBee [1], and WiMAX support MANET, allowing it to communicate without centralized administration. To allow devices to be free both inside and outside of network coverage [2], MANET is typically utilized in locations where a permanent infrastructure cannot be built, such as disaster regions, battlefields, automobiles, military formations, ships, and airplanes meant to form temporary networks. Sophisticated computers, mobile phones, and sensors are examples of nodes in a MANET. Their battery life, computing power, storage capacity [3], dynamic topology, and limited bandwidth are some of their performance attributes. The mobility model used in the MANET simulation is separated into four groups: models with geographic limits, models with time dependence, models with spatial dependence, and random models [4,5]. While devices can route messages through intermediate nodes and communicate peer-to-peer directly using the wireless spectrum, there are

several routing and security issues that need to be resolved due to the nature of mobile devices and wireless shared communication before implementing a MANET [6].

Assaults typically take several forms. Particularly in wireless ad hoc networks, threats provide a very difficult challenge, making network security a very time-consuming procedure [7]. It is crucial to protect the information as securely as possible because these attacks are risky. Several frequent assaults include DoS attacks [8], flooding attacks, wormhole attacks, sinkhole attacks, black hole attacks, and so forth. The data packets are transmitted across nodes and the attacker drops the packets selectively in a black hole attack [9]. Therefore, a packet routed through a malicious intermediate node must experience a loss, either total or partial. The typical scenario for a flooding assault is that the router uses a non-adaptive routing algorithm to send the incoming packet to every outgoing link [10], except the node that the packet originated from. One kind of DoS (Deniel of Service) attack that is thought to occur is the gray-hole attack, which drips discriminating data packets during a conversation.

Because of this, security is crucial to modern technology, especially wireless technology. It's critical to focus on these assaults and take every precaution to secure the network. Using any energy routing metric, numerous researchers have created a variety of energy-efficient routing techniques for MANETs [11]. Because they overlooked changes in topology and node mobility, the majority of earlier research studies are less suitable for the distributed environment of MANETs. To optimize the routing path selection while taking node mobility and topological changes into account, the researchers had to adjust their tactics [12]. However, these methods used discontinuous multiple pathways for routing in an attempt to increase the network lifetime. This increased network overhead by requiring the use of distinct control messages to collect data from each path. Optimization methods were used in conjunction with pre-established parameters to select the best cost-effective path among several choices [13]. These techniques, however, attempted to extend the network's lifetime by using discontinuous multiple paths for routing. As a result, separate control messages were needed to gather information from each route, increasing network overhead. Therefore, optimization techniques were used in conjunction with preset parameters to select the optimal route among multiple possibilities without incurring additional expenditures [14]. Even if these methods work, stronger optimization algorithms can significantly improve performance. Furthermore, by selecting an efficient way and using just single-path routing, these approaches will cause the nodes along those specific paths to lose energy more quickly than other nodes [15].

This paper presents a KNATEC for optimal routing in MANET. The clustering is proceeding with hierarchical clustering for generating node clusters.

The cluster head selection is completed by using the EKOA. The initial node detection is completed by developing the authentication technique that will authenticate the cluster heads.

After that, a TRP is obtained to identify and isolate both faulty and misbehaving nodes. This also assists in detecting common misbehavior attacks like Sybil and wormholes. After that, efficient routing is obtained by using EKOA.

The remainder of the document has been prearranged as follows: The relevant work from the most recent MANET routing process study is provided in Section 2. In Section 3, the suggested architecture is displayed. In Section 4, the suggested method's outcomes are displayed. The paper's conclusion is provided in Section 5.

2. RELATED WORKS

For mobile nodes to be managed as efficiently as feasible, MANET routing protocol techniques were developed. The MANET routing system has developed and improved its performance through extensive research and development. When trying to increase the performance of MANETs, most research efforts are focused on figuring out how to make connections better. The most effective technique for increasing the quantity of interactions between nodes while maintaining a particular pace is to use metaheuristic algorithms.

Sandeep Jagonda Patil and colleagues (16) have presented a Blockchain-Based Trusted Distributed Routing Scheme for MANET using Latent Encoder Coupled Generative Adversarial Network Optimized with Binary Emperor Penguin Optimizer (LEGAN-BEPO-BCMANET). This scheme leverages blockchain technology to establish a fair proof-of-reputation system that ensures decentralized, reliable routing via transactions utilizing verified blockchain tokens. The method improves routing performance and security by merging the Latent Encoder Coupled Generative Adversarial Network (LEGAN) with the Binary Emperor Penguin optimizer (BEPO). A thorough protection analysis is performed with an emphasis on capabilities along with transaction distinguishability, self-change resistance, routing facts integrity, and anti-double-spending measures.

A novel approach for electricity prediction in a cluster-based routing gadget employing deep gaining knowledge of strategies was pronounced with the aid of V. Senthil Murugan et al. [17]. In order to assure the accuracy of energy prediction, the paper gives a singular energy prediction version referred to as Concatenation of Convolutional with Max-Avg Pooling layer in Deep Convolutional Neural Network (CCMAP-DCNN), which includes adding extra layers to the preexisting DCNN structure. Consequently, nodes are organized into clusters, and so one can pick out cluster leaders, cluster selection takes under consideration many characteristics like strength, agree with, latency, and distance. In order to enhance cluster head selection and green routing, the paper also indicates the usage of the hybrid Namib Beetle Upgraded Jellyfish Search Optimization (NBUJSO) set of rules, which mixes the NBO technique with the JSO algorithm.

Convolutional Gated Recurrent Unit Network (CGRUN), a unique deep getting to know architecture designed for powerful sequential information type within MANETs, became first supplied with the aid of Saravanan Selvaraj et al. [18]. To deal with lots of type tasks, CGRUN combines the advantages of convolutional neural networks (CNNs) and recurrent neural networks (RNNs). Furthermore, they put forth the Artificial Gorilla Troops Optimizer (AGTO), a singular optimization model designed to improve weight reduction tactics inside the context of the CGRUN framework.

B. Jaishankar et al. Presented the Hybrid Clustering Approach (SG-MFOA) using a Multi path Cross-Layer Design in the MANET network [19]. Here, data packet transmission via several routes is chosen with the assistance of hybrid routing. Additionally, based on the load balancing factor, residual energy, and expected transmission time (ETT), a cross-layer metric is obtained. Choosing a Cluster Head (CH) based on this transaction is essential for effective routing. Thus, the best choice for utilizing SG-MFOA is the cluster head. Therefore, the multipath route selection is carried out by the multi-objective functions that include bandwidth, congestion delay, transmission delay, and queuing delay at each connection Access Category from the available routes to a destination to guarantee the extension of network lifetime.

The shortest path between the nodes is found using the PBCS (Particle Bee Colony Swarm) algorithm, which Sherril Sophie Maria Vincent et al.,[20] have presented. This reduces the routing cost and improves the effectiveness and efficiency of the model. Moreover, the suggested model makes use of the Hybrid AdaBoost-Random Forest technique. By cutting down on training time, this model improves upon previous models in terms of dependability and efficiency. The Hybrid AdaBoost-Random Forest technique may be applied to large datasets and uses the random forest estimator to produce results with minimal loss and high accuracy.

3. PROPOSED KOOKABURRA NODE AWARE TRUSTABLE AND ENHANCED CLUSTERING

In this study, a KNATEC-based routing protocol is created to achieve dependable, trustworthy transmission across the MANET. Figure 1 displays the suggested model's architecture. In addition to lowering the number of rogue nodes on the network, the creation of energy-efficient trusted routes enhances packet delivery throughout the system. In the clustering strategy, the ideal cluster head is chosen using the suggested algorithm. From the source node to the destination node in the MANET, a secure data transmission route path is chosen. Even in cases when mobility is random, the model computes optimum power to maintain network connectivity.

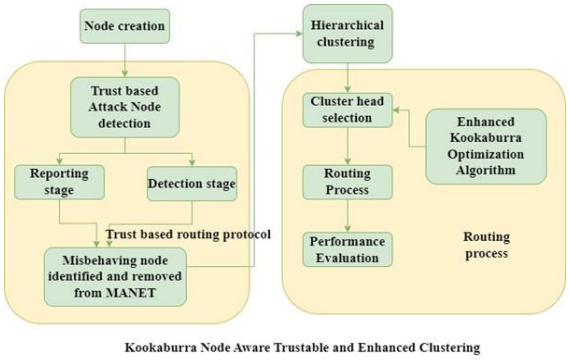


Figure 1: System Architecture

MANETs suffer from nodes' innate tendency toward selfishness. Performance is decreased overall. To strengthen a sound architecture, these sink nodes must be located and eliminated. Based on the AODV protocol, a suggested methodology for sink node detection is verified. Though there are a few inherent restrictions, the technique is the best. Cluster creation is achieved through hierarchical clustering, while cluster head selection is accomplished through EKOA. The method of verification that will verify the identity of the cluster heads is used to detect selfish nodes. Both malfunctioning and misbehaving nodes are found and isolated using a trust-based routing system. This helps detect misbehavior attacks in general, such as wormhole, selfish, and sybil attacks. The EKOA will be connected to trust-based routing and trust estimation.

3.1. Trust-Based Attack Node Detection

An attack is interpreted as a malevolent threat in the networking environment. This is where a second, malicious route emerges, changing the packet's course and perhaps causing data loss. In typical work, a distributed wormhole detection strategy is used to handle this problem. Data transmission via encryption [21] is finished to guarantee secure communication between the source and the sink. We ought to offer some recommendations to get this failure node detection.

- Before transmission, a valid node needs to update or register with the public server.
- Sender A will use a server method to determine B's identification if it wants to deliver information to recipient B.
- When sending information to B, A will encrypt it.
- Node B verifies whether the message is from a legitimate node based on the information it receives from A.
- B requires A's identifying details from the server.
- If verified, the subsequent transfer will be successful.

Data about nodes will be shared among the nodes in the network based on the previously mentioned stages. The predicted transmission count is taken into account as a crucial element in achieving popular wormhole detection. This is a node's probability of sending or receiving data packets. It produces novel or inventive packets during data forwarding that are absent from earlier transmissions. The reporting stage and the detecting stage are two of the phases that make up this process. A wormhole link will be detected by the first reporting stage of the network, and it will be confirmed by the second level before being quickly blocked.

3.1.1. Reporting stage

In this phase, the expected transmission count of nodes is considered.

- The sender will consider ETX while sending data to a recipient.
- The receiver will verify whether any additional packets are present based on the reception.
- The receiver's ETX rate will be compared to the sender's if it is computed.
- When the sender's ETX surpasses the recipient's ETX
- The sender node will be identified by the recipient as the wormhole.
- With the sender ID and signature parameters, create a report.
- After forming, the report is encrypted and sent to additional nodes.
- Close the if

3.1.2. Detection stage

At this point, an encrypted report containing information on wormholes is sent to the node. By verifying the ID data that can be retrieved from the server, it is determined whether or not the data was collected from a legitimate node. A node is deemed to be a wormhole and no communication with it will occur if its data is comparable to that of the majority of the underlying judge nodes.

3.2. Hierarchical Clustering Technique

Data is gathered as cluster trees as the hierarchical clustering process moves forward. It starts by treating each set of data as a distinct cluster [22]. It accomplishes the following repeatedly:

- Merge or combine the two largest equivalent clusters. Continue until all clusters are joined.
- Determine the two nearest clusters.

Creating a layered hierarchical succession of clusters is the main goal. A dendrogram that can visually represent the hierarchy is the best way to define this. The sequence of splitting or merging is eventually defined by what looks like an inverted tree. At least two and no more than four nearest clusters are specified for reduction and best results. More cluster connections will result in higher power consumption, which will impact overall performance.

In this step, a tree cluster is formed, and the hop **nodes and cluster head are computed. During the** setup process, the sink gathers information about the position and energy of all nodes. The distance [c]by the sink. The nodes are arranged in descending order of distance. Additionally, the nodes' average remaining energy is calculated. The design of a cluster head selection takes into account the distance between a sink and a node that still has energy. Assume that the residual energy mean is taken into account. The following formula is used to calculate the sensor nodes' remaining energy (mean):

$$e_{Average} = \frac{\sum_{n=1}^{N} e_{energy,in}}{n} \qquad (1)$$

Reducing the communication gap between nodes is the main goal. The sink node and the general node are regarded as forming a cluster based on their distance from one another. To create a cluster, two distance functions—for example, the distance between the Alpha and Sink nodes (DB) and the Alpha and Beta nodes (DS)—are computed. It is then contrasted with the B after that. If the B is less, the alpha is attached to the sink directly and, if the residual energy is more than the average mean energy, can appear as a cluster head. If not, beta connects alpha to sink. DT, or the distance between the beta and sink nodes, is smaller than DS, and measure DB is tiny. Here is how the routing process is put together:

$$MIN\{DB, DS\}, \quad for\ DT < DB \qquad (2)$$

Algorithm 1 presents the pseudocode of the intended sorting.

Algorithm 1: Pseudocode of the clustering technique

Input: Sensor node locations, energy, m and n

Output: Tree cluster which defines routing design

Initialize total energy, hop node state, temporary result, and minimum distance

For the parameter (I=1, I<=N, I++)

Compute total energy=Total energy+ Energy

End the for

consider average energy=Total energy

Sorted out saves the nodes related to the distance

For the parameter (Alpha=1: Alpha<=N; Alpha++)

Calculate D (sorted {Alpha}. node, sink node)

For the parameter (Beta=1, Beta<=Alpha-1; Beta++)

Calculate the distance D (sorted [Alpha], node, sorted [Beta]. node)

Calculate the parameter D (sorted [Beta]. node, sink node)

If the condition D (sorted [Alpha], node, sink node) < D (sorted [Alpha]. node, Sorted [Beta]. node and hop node states==false)) holds

Hop node states=false

Else validate (min D>D sorted [alpha]. node, sorted [beta]. node)

Upgrade hop nodes=nodes [beta]. node

Set hop node states=true

Upgrade min D=D (sorted [alpha]. node, sorted [beta]. node)

End the if

End the if

End the for

Validate the scenario if (hop node_states==true)

Sorted [alpha]. node connected to hop nodes.

Else

Sorted [alpha]. node connected to sink nodes.

End the if

set minimum D-sink node

set hop node states=false

End the for

The optimal outcome is a tree cluster with a routing process

In the clustering approach, the optimal cluster head is computed based on EKOA. The optimal cluster head is selected based on this algorithm.

3.3. Enhanced Kookaburra Optimization Algorithm

This proposed algorithm is utilized to select optimal cluster heads in the clustering approach. The proposed algorithm is a combination of oppositional function and KOA. It is generated based on the oppositional solutions with the kookaburra population. One of the land-dwelling species of birds in the group of terrestrial tree kingfishers is the kookaburra. The suggested KOA approach [23,24] is a population-related optimizer that may provide the necessary answers for optimization problems in an iterative procedure based on a random search inside the space of problems to be solved. Kookaburras that are situated in the problem-solving space make up this population, and each one of them computes parameters for the decision parameters associated with its location in the problem-solving space. Each kookaburra is therefore a potential vector-based solution to the problem. combined from the KOA population matrix, which is created using the population matrix. In the initial population, the random cluster head is created. It appears as follows:

$$Z = \begin{bmatrix} Z_1 \\ \dots \\ Z_I \\ \dots \\ Z_N \end{bmatrix}_{N\times M} = \begin{bmatrix} Z_{1,1} & \dots & Z_{1,D} & \dots & Z_{1,M} \\ \dots & \dots & \dots & \dots & \dots \\ Z_{I,1} & \dots & Z_{I,D} & \dots & Z_{I,M} \\ \dots & \dots & \dots & \dots & \dots \\ Z_{N,1} & \dots & Z_{N,D} & \dots & Z_{N,M} \end{bmatrix}_{N\times M} \quad (3)$$

$$Z_{I,D} = LB_D + R.(UB_D - LB_D) \quad (4)$$

Here, UB_D is an upper bound of the decision variable, LB_D is a lower bound of the decision variable, R is a random number in the interval [0,1], M is several decision parameters, N is several kookaburras, $Z_{I,D}$ is the dimension in search space, Z_I is the kookaburra and Z is the KOA population matrix.

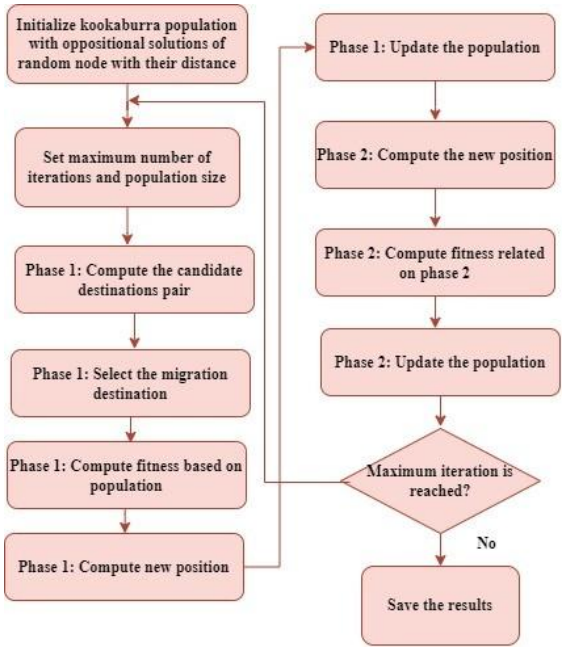


Figure 2: Flowchart of the proposed method

The objective function of the problem is computed taking into account the position of each kookaburra in the problem-solving space as a potential solution for the problem associated with each kookaburra [25]. A vector connected to the equation below is used to specify the two calculated parameters for the problem's objective function.

$$O = \begin{bmatrix} O_1 \\ \dots \\ O_I \\ \dots \\ O_N \end{bmatrix}_{N \times M} = \begin{bmatrix} O(Z_1) \\ \dots \\ O(Z_I) \\ \dots \\ O(Z_N) \end{bmatrix}_{N \times 1} \quad (5)$$

$$FF = MIN\{DB, DS\} \quad (6)$$

Here, O_I is the computed objective function related to the kookaburra and O is the vector of the computed objective function. To improve candidate solutions connected to the simulation of general kookaburra features in the wild, the suggested technique upgrades the position of kookaburras in the two stages, such as exploitation and exploration, in an iteratively related process. Following that, a plan is developed to upgrade the KOA population in the search area.

Phase 1: Hunting methodology (exploration)

The position of other kookaburras with the best goal function parameter is defined as the prey location in the KOA design for each kookaburra to imitate the hunting process of kookaburras. Therefore, an equation is used to calculate the available prey pair for each kookaburra based on the comparison of the objective function parameters.

$$cp_I = \{Z_K : f_K < f_I \text{ and } K \neq I\} \text{ here}, I = 1,2,\dots,N \text{ and } K \epsilon \{1,2,\dots,N\} \quad (7)$$

Where, f_K is the objective function parameter, Z_K is the kookaburra with the best objective function and cp_I is the pair of candidate prey. Every kookaburra is believed to randomly select a target and attack it in the KOA design. About the kookaburra's movement towards the prey during the hunting technique, the kookaburra's new location is calculated using the equation below. In this instance, if the objective function's parameter is increased at the new site, the associated kookaburra related to the equation below will move to its final location.

$$Z_{I,D}^{P1} = Z_{I,D} + R.\left(scp_{I,D} - i.Z_{I,D}\right), I = 1,2,..,N \text{ and } D = 1,2,..,M \quad (8)$$

$$Z_I = \begin{cases} Z_I^{P1} & O_I^{P1} < O_I \\ Z_I & Else \end{cases} \quad (9)$$

Here, M is the count of decision parameters, N is the number of a kookaburra, I is a random number from pair {1,2}, $scp_{I,D}$is the dimension of selected prey for kookaburra, R is a random number related to the normal distribution in the range of [0,1], O_I^{P1} is the objective function, $Z_{I,D}^{P1}$ is the dimension and Z_I^{P1} is the new suggested location of the kookaburra related to the initial stage of KOA.

Step 2: Giving the victim the means to end their life (exploitation)

The second distinguishing feature of kookaburra behavior is that, following an assault, the animal carries the victim with it and continues to strike the victim against the tree until it dies. These kookaburra traits in the KOA design are associated with their mobility close to the hunting site and at an arbitrary position. If each kookaburra's new position improves the parameter of the goal function connected to the equation below, it takes the place of the prior position.

$$Z_{I,D}^{P2} = Z_{I,D} + (1 - 2R).\frac{(UB_D - LB_D)}{T}, I = 1,2,..,N,$$
$$D = 1,2,..,M \text{ and } T = 1,2,..,t \quad (10)$$

$$Z_I = \begin{cases} Z_I^{P2} & O_I^{P2} < O_I \\ Z_I & Else \end{cases} \quad (11)$$

Where t is the maximum count of algorithm iterations, T is the iteration counter of the algorithm, O_i^{P2} is the objective function parameter, $Z_{I,D}^{P1}$ is the dimension, Z_i^{P2} is the new suggested location of the kookaburra related to step 2.

4. RESULTS AND DISCUSSIONS

The suggested KNATEC algorithm's performance is calculated through the use of in-depth simulations in the NS2 environment. The average of each simulation run is used to evaluate each implementation, and the results are compared with traditional methods for improving the security and routing procedures using the suggested algorithm and the comparable experimental variables listed in Table 1. The suggested methodology is validated by comparison with traditional methods like Particle Swarm Optimization (PSO), Grey Wolf Optimization (GWO), and Snake Swarm Algorithm (SSA). A variety of performance metrics, including energy consumption, drop, delivery ratio, delay, throughput, and network longevity, are used to evaluate the suggested approach. To improve the packet delivery ratio without needless re-clustering, the suggested method performs cluster formation and routing in each cluster. Figure 3 presents the misbehaving node, which has been found by trust-aware selection. Figure 4-6 shows the routing, startup, and clustering processes.

Table 1: *implementation variables*

S.No	Description	Parameters
1	Base station position	(50,50)
2	Data packet size	500 bytes
3	Number of cluster head	P*100
4	Probability of becoming cluster head	0.1
5	Initial energy	1J
6	Network size	100
7	Network terrain	100M²
8	Number of iterations	100
9	Lower bound	-100
10	Upper bound	100

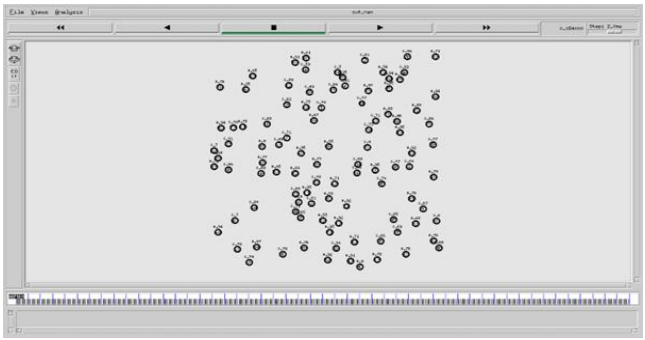


Figure 3: *Trust-aware selection*

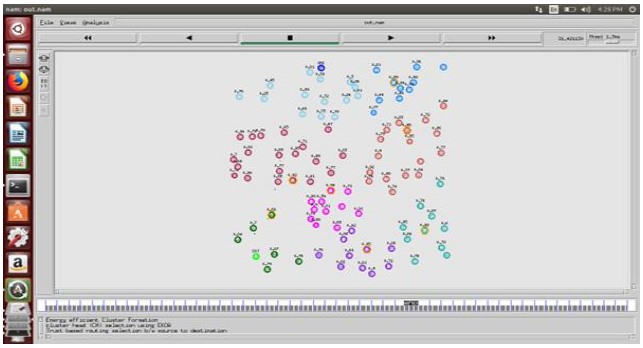


Figure 4: *Cluster Head Selection Using EKOA*

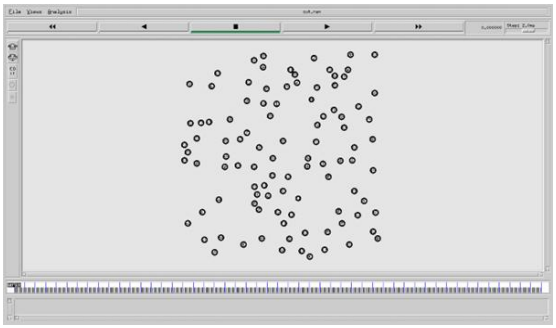
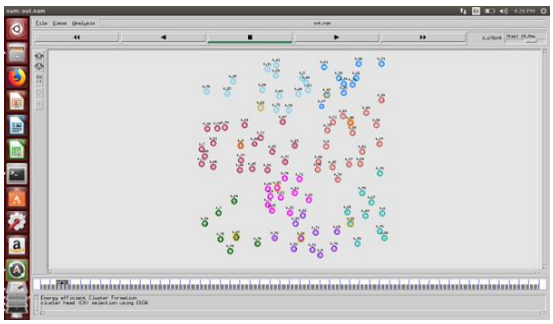


Figure 5: *Initialization*



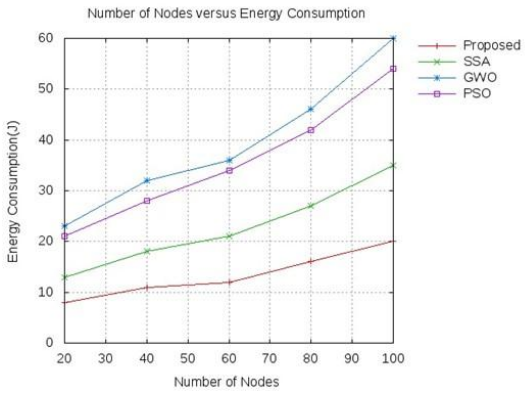


FIGURE 6: CLUSTER HEAD AND CLUSTERING

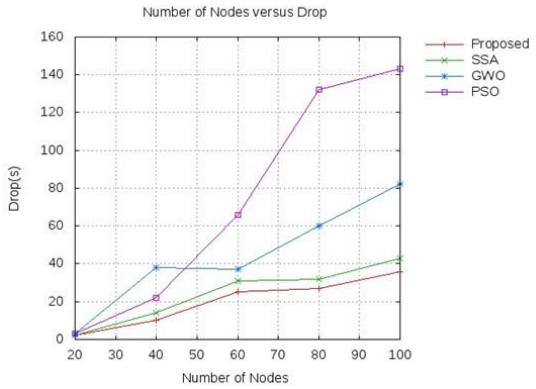


Figure 7: *Energy consumption*

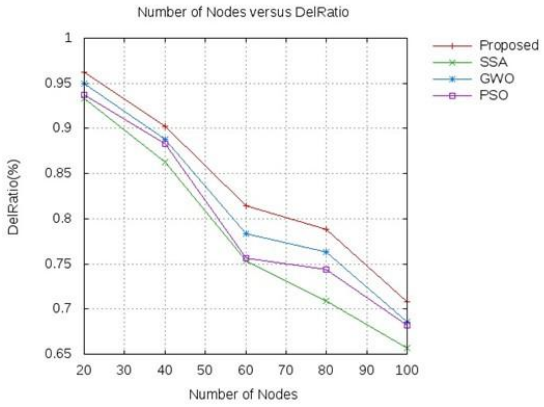


Figure 8: *Drop*

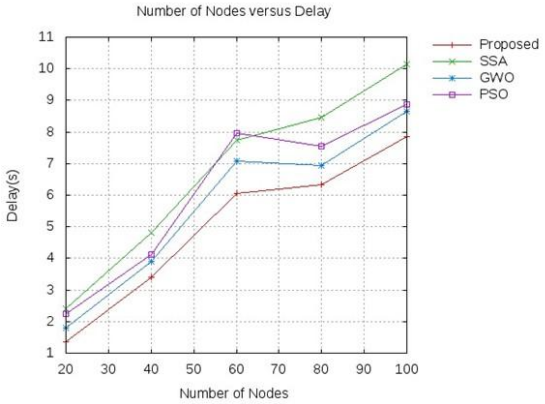


Figure 9: *Delivery ratio*

The energy consumption measure is used to examine the suggested methodology and it is presented in figure 7. The calculation and comparison of this measure is done with traditional methods including SSA, GWO, and PSO. Based on the quantity of nodes, this metric is calculated. The suggested approach consumed 11J of energy over 40 nodes. Furthermore, the energy consumption of the traditional methods is 18J, 28J, and 32J. The suggested approach produced 15 J energy usage over 80 nodes. Furthermore, the energy consumption of the traditional methods is 28J, 42J, and 44J. In keeping with this validation, the suggested method uses less energy than traditional approaches. The drop measure is used to examine the suggested methodology and it is presented in figure 8. The calculation and comparison of this measure is done with traditional methods including SSA, GWO,

and PSO. Based on the quantity of nodes, this metric is calculated. The suggested approach consumed 11s of drop over 40 nodes. Furthermore, the drop of the traditional methods is 18s, 21s, and 38s. The suggested approach produced 22s drop usage over 80 nodes. Furthermore, the drop of the traditional methods is 28s, 60s, and 122s. In keeping with this validation, the suggested method uses less drop than traditional approaches. The delivery ratio measure is used to examine the suggested methodology and it is presented in Figure 9. The calculation and comparison of this measure is done with traditional methods including SSA, GWO, and PSO. Based on the quantity of nodes, this metric is calculated. The suggested approach consumed 0.96 of the delivery ratio over 40 nodes. Furthermore, the delivery ratio of the traditional methods is 0.89s, 0.87s, and 0.86s. The suggested approach produced 0.72 delivery ratio usage over 80 nodes. Furthermore, the shipping ratio of the traditional methods is 0.Sixty five, zero.Sixty nine, and 0.Seventy one. In maintaining with this validation, the recommended method makes use of a better transport ratio than traditional methods.

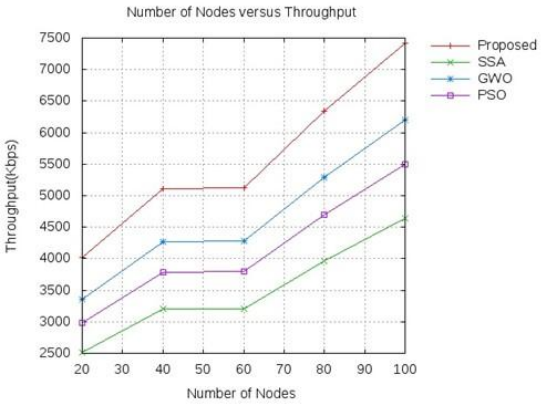


Figure 10: *Delay*

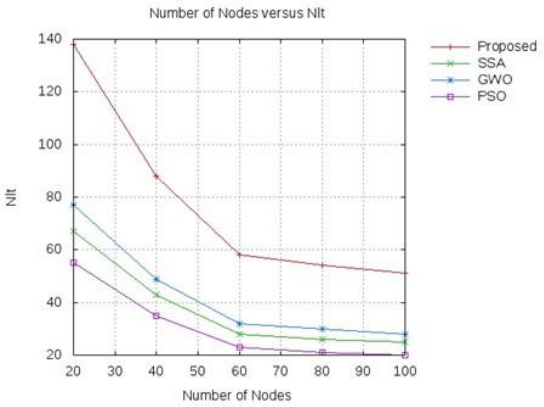


Figure 11: *Throughput*

Delay					Delivery ratio			
Nodes	**Proposed**	**SSA**	**GWO**	**PSO**	**Proposed**	**SSA**	**GWO**	**PSO**
20	1.35	2.42	1.81	2.25	0.96	0.93	0.94	0.93
40	3.39	4.82	3.89	4.11	0.90	0.86	0.88	0.88
60	6.06	7.73	7.07	7.9	0.81	0.75	0.78	0.75
80	6.31	8.46	6.93	7.55	0.78	0.70	0.76	0.74
100	7.85	10.13	8.65	8.86	0.70	0.65	0.68	0.68
Drop					**Energy**			
Nodes	**Proposed**	**SSA**	**GWO**	**PSO**	**Proposed**	**SSA**	**GWO**	**PSO**
20	2	2	3	3	8	13	23	21
40	10	14	38	22	11	18	32	28
60	25	31	37	66	12	21	36	34
80	27	32	60	132	16	27	46	42
100	36	43	82	143	20	35	60	54
Network lifetime					**Throughput**			
Nodes	**Proposed**	**SSA**	**GWO**	**PSO**	**Proposed**	**SSA**	**GWO**	**PSO**
20	138	67	77	55	4021	2515	3361	2980
40	88	43	49	35	5112	3200	4264	3790
60	58	28	32	23	5127	3210	4286	3795
80	54	26	30	21	6333	3965	5296	4694
100	51	25	28	20	7415	4647	6196	5494

Table 2: *Comparison analysis*

Figure 10 presents the delay measure, that's used to analyze the proposed methodology. This metric is calculated and in comparison using traditional techniques which include SSA, GWO, and PSO. This determine is calculated using the node depend as a basis. For 40 nodes, the recommended method required 3.2 seconds of latency. Furthermore, the conventional strategies had 3.8, 4.1, and four.Eight 2nd delays. The advised method resulted in 6.2s postpone use over 80 nodes. Furthermore, the traditional strategies had 7.Eight, 9.2, and 8.2 2d delays. This validation is like minded with the suggested strategy using less latency than the traditional strategies. The throughput measure, that is used to investigate the suggested technique, is proven in Figure 11. This degree is computed and contrasted with traditional strategies like SSA, GWO, and PSO. This figure is calculated using the node matter as a foundation. The cautioned answer used 5100 bps of throughput over 40 nodes. Furthermore, the traditional methods have a throughput of 3700, 3100, and 4500 kbps. Using 80 nodes, the counseled approach produced a throughput use of 6800 kbps. Furthermore, the traditional strategies have a throughput of 4600, 4000, and 5300 bps. The recommended technique uses a higher throughput than the conventional approaches, which is regular with this validation. The proposed methodology is examined using the network lifespan metric, which is shown in figure 12. This metric is calculated and compared using conventional techniques such as SSA, GWO, and PSO. This statistic is computed based on the number of nodes. Across 40 nodes, the recommended method used up 85 percent of the network lifetime. Moreover, the conventional approaches have a network lifespan of 55, 43, and 28. Over 80 nodes, the recommended method yielded 58 network lifetime consumption.

Moreover, the classic methods' network lifetimes are 35, 28, and 22. The proposed method utilizes less network lifetime than the conventional ways, which is consistent with this validation. Table 2 presents the comparative validation of the suggested methodology.

5. CONCLUSION

A KNATEC for optimal routing in a MANET is shown in this paper. To create node clusters, hierarchical clustering has been used in the clustering process. The EKOA has been utilized to complete the cluster head selection process. By creating the authentication method that would validate the cluster heads, the initial node detection has been finished. After that, a TRP was acquired to locate and isolate malfunctioning as well as misbehaving nodes. Additionally, this helps identify prevalent misbehavior attacks such as wormholes and Sybil. Following that, EKOA was used to achieve efficient routing. After the suggested approach was put into practice in NS2, its effectiveness was assessed using metrics for energy usage, throughput, average latency, loss ratio, packet delivery ratio, and end-to-end delay. The suggested approach and the traditional routing procedure have been contrasted. This review shows that the suggested approach produced effective results in terms of performance metrics. The suggested approach will be created for the analysis of various circumstances and situations that occur in real-time.

6. REFERENCES

[1]. Ravi, Srivel, Saravanan Matheswaran, Uma Perumal, Shanthi Sivakumar, and Srinivas Kumar Palvadi. "Adaptive trust-based secure and optimal route selection algorithm for MANET using hybrid fuzzy optimization." Peer-to-Peer Networking and Applications 16, no. 1 (2023): 22-34.
[2]. 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.
[3]. Chandra Sekar, Purushothaman, Pichaimuthu Rajasekar, Sundaram Suresh Kumar, Mittaplayam Arunchalam Manivasagam, and Chellappan Swarnamma Subash Kumar. "Firefly Optimized Resource Control and Routing Stability in MANET." Engineering Proceedings 59, no. 1 (2023): 18.
[4]. Saravanan, R., K. Suresh, and S. S. Arumugam. "A modified k-means-based cluster head selection and Philippine eagle optimization-based secure routing for MANET." The Journal of Supercomputing 79, no. 9 (2023): 10481-10504.
[5]. Jose, Mitha Rachel, and S. Maria Celestin Vigila. "F-CAPSO: Fuzzy chaos adaptive particle swarm optimization for energy-efficient and secure data transmission in MANET." Expert Systems with Applications 234 (2023): 120944.
[6]. Abbood, Zainab Ali, Doğu Çağdaş Atilla, and Çağatay Aydin. "Enhancement of the performance of MANET using machine learning approach based on SDNs." Optik 272 (2023): 170268.
[7]. Shafi, Shaik, and D. Venkata Ratnam. "Ant-colony optimization based energy aware cross layer routing protocol to improve route reliability in MANETs." Wireless Personal Communications 129, no. 3 (2023): 1865-1879.
[8]. Sankar, S. M., D. Dhinakaran, C. Cathrin Deboral, and M. Ramakrishnan. "Safe routing approach by identifying and subsequently eliminating the attacks in MANET." arXiv preprint arXiv:2304.10838 (2023).
[9]. Devi, E. Ahila, S. Radhika, and A. Chandrasekar. "An energy-efficient MANET relay node selection and routing using a fuzzy-based analytic hierarchy process." Telecommunication Systems 83, no. 2 (2023): 209-226.
[10]. Srilakshmi, Uppalapati, Saleh Ahmed Alghamdi, Veera Ankalu Vuyyuru, Neenavath Veeraiah, and Youseef Alotaibi. "A secure optimization routing algorithm for mobile ad hoc networks." IEEE Access 10 (2022): 14260-14269.
[11]. Jose, Mitha Rachel, and S. Maria Celestin Vigila. "F-CAPSO: Fuzzy chaos adaptive particle swarm optimization for energy-efficient and secure data transmission in MANET." Expert Systems with Applications 234 (2023): 120944.
[12]. Yadav, Amrendra Singh, Nitin Rakesh, Ankit Vidyarthi, Rabindra Kumar Barik, Ayushi Singhal, and Dharmender Singh Kushwaha. "Restoration and fuzzy logic-based formation of multipath routing protocol in MANET." International Journal of System Assurance Engineering and Management 14, no. Suppl 1 (2023): 117-132.
[13]. Gopalan, S. Harihara, V. Vignesh, D. Udaya Suriya Rajkumar, A. K. Velmurugan, D. Deepa, and R. Dhanapal. "Fuzzified swarm intelligence framework using FPSOR algorithm for high-speed MANET-Internet of Things (IoT)." Measurement: Sensors 31 (2024): 101000.
[14]. Jalade, Sangamesh C., and Nagaraj B. Patil. "Optimization technique for fault recovery and fast data transmission in MANET." Materials Today: Proceedings 81 (2023): 524-529.
[15]. 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.
[16]. 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.
[17]. Murugan, V. Senthil, and Bhuvan Unhelkar. "Optimizing Mobile Ad Hoc Network cluster based routing: Energy prediction via improved deep learning technique." International Journal of Communication Systems (2024): e5777.

[18]. Selvaraj, Saravanan, and Midhun Chakkaravarthy. "Enhancing security and efficiency in MANETs: a clustering-based approach with CGRUN and AGTO optimization for intrusion detection and path establishment." International Journal of Information Technology (2024): 1-11.
[19]. Jaishankar, B., Bharathi Gururaj, A. Muruganandham, and G. Nagarajan. "Hybrid Clustering Approach (SG-MFOA) using Multipath Cross-Layer Design in MANET Network." IETE Journal of Research (2024): 1-9.
[20]. Vincent, Sherril Sophie Maria, and N. Duraipandian. "Detection and prevention of sinkhole attacks in MANETS based routing protocol using hybrid AdaBoost-Random forest algorithm." Expert Systems with Applications 249 (2024): 123765.
[21]. Biradar, Manjula A., and Sujata Mallapure. "Multipath Load Balancing in MANET via Hybrid Intelligent Algorithm." Journal of Information & Knowledge Management (2024): 2450010.
[22]. Goswami, Subhrananda, Sukumar Mondal, Subhankar Johardar, and Chandan Bikash Das. "HS–WOA–MANET: a hybrid meta-heuristic approach-based multi-objective constraints for energy efficient routing protocol in mobile ad hoc networks." Journal of Reliable Intelligent Environments (2024): 1-26.
[23]. Anand, M., and S. Babu. "Predicting the Facial Expression Recognition Using Novel Enhanced Gated Recurrent Unit-based Kookaburra Optimization Algorithm." International Journal of Intelligent Engineering & Systems 17, no. 3 (2024).
[24]. Jamal, Raheela, Junzhe Zhang, Baohui Men, Noor Habib Khan, Mohamed Ebeed, Tanzeela Jamal, and Emad A. Mohamed. "Chaotic-Quasi-Oppositional-Phasor based Multi populations Gorilla Troop Optimizer for Optimal Power Flow Solution." Energy (2024): 131684.
[25]. Dehghani, Mohammad, Zeinab Montazeri, Gulnara Bektemyssova, Om Parkash Malik, Gaurav Dhiman, and Ayman EM Ahmed. "Kookaburra Optimization Algorithm: A New Bio-Inspired Metaheuristic Algorithm for Solving Optimization Problems." Biomimetics 8, no. 6 (2023): 470.