**CHAOTIC MAP PUFFERFISH OPTIMIZATION ALGORITHM (CMPOA) AND TRUST DEEP Q NETWORK (TDQN) ROUTING PROTOCOL FOR INTERNET-OF-THINGS-ENABLED SMART AGRICULTURE IN WIRELESS SENSOR NETWORK**

D.Udaya Suriya Rajkumar1, R.Sathiyaraj2, Mohan D4, Gowri

1\* Professor, Department of Computer Science and Engineering , Global Institute of Engineering and Technology, Ranipet, Tamil Nadu, India. Email: u\_suriya@yahoo.com

2Assistant Professor, Department of CSE, GITAM School of Technology,

GITAM University, Bangalore, Karnataka, India. Email: rsr026@gmail.com

4Assistant Professor, Department of Computer Science and Engineering,

Global Institute of Engineering and Technology, Melvisharam, Tamil Nadu, India. Email: dm.mohan14@gmail.com

4Assistant Professor, Department of Computer Science and Engineering,

Global Institute of Engineering and Technology, Melvisharam, Tamil Nadu, India. Email: gowrisiva1784@gmail.com

\*All correspondence shall be communicated to Udaya Suriya Rajkumar D

(u\_suriya@yahoo.com)

**ABSTRACT:** Internet of Things (IoT) has advanced its pervasiveness across the globe for the development of smart networks. It is aimed to deploy network edge that enables smart services and computation for the IoT devices. The IoT was made possible by the Wireless Sensor Network fundamental design. However, conserve energy in IoT enabled smart agriculture in WSN is solved by clustering Routing approach. The issue of node early death was faced by many current clustering protocols, due to the repeated selection of Cluster Head (CH). This CH selection contributes for forwarding and Data Aggregation, and it will lead to high Energy Consumption. It is never easy to accomplish the demands of quality of Service and reliability in sensor networking contexts. In this paper, Clustering Trust Energy Efficient Routing Protocol (CTEERP) was introduced to lengthen the Network Lifetime and improving the connections. The natural behaviour of pufferfish was simulated by the Chaotic Map Pufferfish Optimization Algorithm (CMPOA). CMPOA is used to select an efficient set of CH and route to destination. It picks the best CH and the shortest routes to the Base Station. Exploration and Exploitation are the 2 phases in CMPOA. In this case, the simulation of a predator attacking a pufferfish serves as the basis for exploration, the basis of exploitation is the simulations of the predator escaping from a spiny pufferfish. The Deep Q Network is derived considering trustworthiness, Quality of Service, and energy factors. It maps visual input sequence to the action value functions. To train a network in estimating the Q function value that maps state-action pairs to their expected returns by employing Deep Q Network model. The suggested model surpasses the current methods by the performance metrics was demonstrated in the experimental simulations.

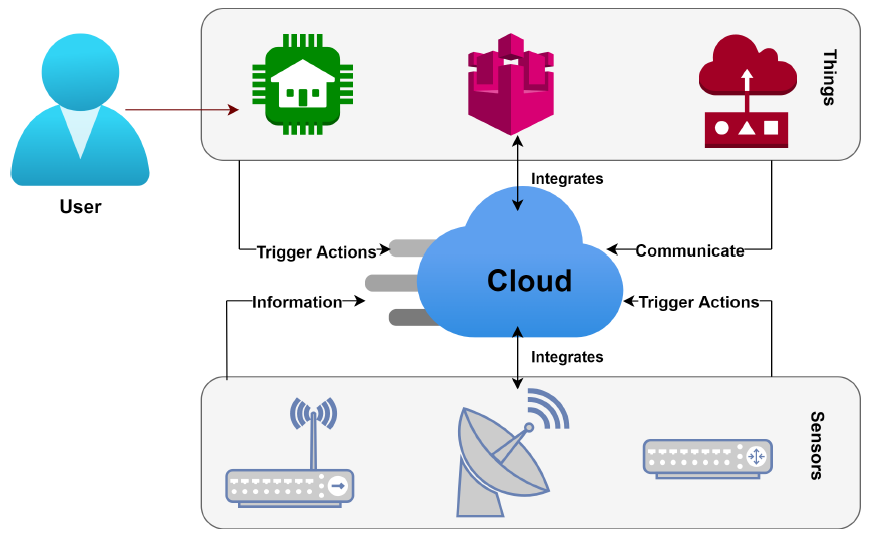
**KEYWORDS:** Internet of Things (IoT), Energy Efficient, Clustering Trust Energy Efficient Routing Protocol (CTEERP), Chaotic Map Pufferfish Optimization Algorithm (CMPOA) and Deep Q Network (DQN).

1. **INTRODUCTION**

In the Indian economy, agriculture is an important factor that will feed the whole population. It connects all the country’s related organizations. In Indian agriculture, farmers follow traditional procedures that affect crop growth and yield of a crop. The financial failures they face are commonly due to the wrong selection of crops. Technology is not implemented in agriculture industries because of the economic condition of most Indian farmers. With the rapid advancement of technology, agriculture has seen significant transformations through the adoption of the Internet of Things (IoT) and Wireless Sensor Network (WSN). An extensive amount of low-energy Sensor Node (SN) makes up a WSN. In order to gather a variety of environmental factors and send data to the Base Station (BS) for monitoring and application detection, WSN are randomly dispersed around a specific region [1]. Researchers have recently become interested in them because of their widespread applications in human health, military, surveillance, and forest fire detection, among other fields [2]. Recharging or changing the SN batteries is exceedingly challenging because WSN are typically employed in risky situations. Additionally, there are difficulties in applying WSN because of the network's extremely complex manual operation [3].

Energy-Efficient (EE) routing strategy is recommended for effectively minimizing Energy Consumption (EC), as Data Transmission (DT) accounts for the majority of the EC of Sensor Node (SN). Clustering has a vital role in any hierarchy procedure and can lengthen the Network Lifetime (NL). It is impacted by the amount of clusters, the Cluster Head Selection (CHS), and the clustering algorithm. Clustering methods are used to cluster SN. Numerous typical Cluster Member (CM) nodes and one CH are existing in every cluster. A BS receives the data that CM transmits to their own CH, which is responsible for receiving, combining, and forwarding it. A node is considered to be dead while its energy is consumed. The NL is the round in which every node has died. To effectively sent information from node to node or to the BS, routing becomes crucial for since the detected data must be sent to the BS for additional required action [5]. Thus, in order to extend the network life for clustered WSN, it is essential to balance the EC among SN [4].

In order to increase network performance and reduce EC, a variety of Routing Protocols (RP) have been established for conventional networks. Because of the complex and dynamic structure of the IoT in an unstable wireless environment, traditional methods are not optimal for IoT devices [5]. Due to the IoT devices rapid advancement, several data and network risks arise, limiting their development.



**FIGURE 1. IoT BASED WSN ARCHITECTURE**

Figure 1 shows the IoT-WSN, detecting the data, the SN transmits it to the sink or BS. After that, the user receives the data via the Internet to complete any additional tasks that are required. Because of their small size, all of the SN in a WSN has limited resources. An Analog-to-Digital Conversion (ADC) unit, a sense unit with a sensor, a processor unit for various computations, and a transceiver for DT, and Data receiving are all included, and a power unit for the SN's power supply are the essential parts of any SN [6].

Data Aggregation (DA) and DT algorithms can be broadly classified into two classes. Firstly, there is a framework technique that uses partial data for DA and collects sensor information without requiring a fixed framework. Then, from many clusters, the network field is divided using a framework method. Within each area, there is a single local DA node that performs aggregation operations and collects information from all of its linked members. Then, through an established network, the DA is transmitted to the sink node [7].In the majority of WSN systems, SN function independently and are open to several security threats. During clustering, a single CH and a few typical CM nodes are present in every cluster. Because there is a significant disparity in the level of EC among CHs and other nodes, clustering can lessen total EC and balance node workload. In order to lengthen NL and boost EE, clustering is an EE approach. Additionally, in order to prevent SNs from dying too soon and to further increase the network's lifespan, the majority of clustering protocols use optimal CHS [8].

The most effective method for CHS is Swarm Intelligence (SI). The research of the collective behaviors of systems composed of numerous components that cooperate through self-organization and decentralized controls is addressed. In order to create efficient algorithms for distributed optimization, a significant portion of SI research has concentrated on reverse engineering and adapting collective behaviors seen in natural systems [9]. Many new SI optimization algorithms have been suggested recently by researchers. These algorithms have high experimental findings as well as substantial application in addressing issues of CHS. Alternatively, as the count of relevant sensor information rises, the network can become vulnerable to different types of cyber attacks from malicious nodes. Mission-critical data loss or drop page poses a serious threat to mission operations because it makes it more difficult to provide sensor data to the gateway [10].

Research that take into account Quality of Service (QoS) metrics and trust assessment are needed to address these issues. The effectiveness of this strategy in energy balancing has been demonstrated, and as a result, the NL in the WSN model is significantly increased [11]. The three primary categories into which the Machine Learning (ML) techniques can be classified: Reinforcement Learning (RL), Supervised Learning (SL0), Non-supervised Learning. In difficult situations, adaptive trust can be attained by the application of RL. In order to identify malicious nodes, Q-learning is used to determine each SN trust score [12]. Clustering Trust Energy Efficient Routing Protocol (CTEERP) approach is introduced which improves connections and extends the lifespan of networks in IoT enabled smart agriculture. A novel method for choosing an effective set of CH and a route to the target is presented the CMPOA. It also reduces EC and helps to reduce the number of sleepy SN. The Deep Q Network (DQN) is developed with energy, QoS, and trust in consideration for IoT enabled smart agriculture. It associates the action value functions with the visual input sequence. In terms of important performance measures, experimental simulations show that the suggested model executes better than a number of widely recognized methods.

1. **LITERATURE REVIEW**

In order to detect different types of attacks and ensure network performance,[13] created a Trust-based Intelligent Routing Protocol (TIRP) that uses Q-learning to learn the trust factors. The suggested method assures reliable transmission of mission-critical sensor data and timely identification of potential cyber threats in a mission-critical WSN. The introduction of distributed transmission technology gives priority to mission-critical data trustworthiness by using Q-learning outcomes that take EC, QoS, and trustworthiness into account. This technique can consistently run procedures with limited resources and is appropriate for use in mission-critical WSN operational settings. Utilizing the Optimized Network Engineering Tool (OPNET) simulator to implement the system and carry out a thorough evaluation.For WSN-assisted IoT systems, the adaptive fuzzy rule based Energy Efficient and Immune-Inspired Routing (FEEC-IIR) protocol was proposed in [14].The method called as Adaptive Fuzzy Multi-Criteria Decision Making (AF-MCDM) is used to choose the best CH. The EE clustering algorithm known as Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) is used in conjunction with the Fuzzy Analytic Hierarchy Process (FAHP). Energy status, QoS impact, and node placement are the three main factors that can affect CHS; each of these factors includes a variety of enabling criteria. A TIRP technique is used in routing to improve the reliability of DT.

For WSN-based IoT applications that face bias in networks with large traffic loads, in [15] developed the Energy-Efficient Optimal Multi-path Routing Protocol (EOMR). The suggested approach considers three factors: traffic intensity, longevity, and reliability at the next-hop node, to determine the optimal routing. To enhance the durability of WSN-based IoT, in [16] suggested the Improved Energy-Efficient Clustering Protocol (IEECP). There are 3 successive components to the suggested method. The optimum amount of clusters needs to be determined before creating the overlapping balanced clusters. Next, a novel version of the Fuzzy C-means (FCM) approach is combined with an approach to reduce and balance the EC of the SN to construct balanced-static clusters. Finally, with rotation of the CH function across CM, CHs are picked in the majority of ideal positions using a novel CHS-rotation technique that blends a back-off timed mechanism to rotate CHS with a rotation mechanism for CH rotation. IEECP is suitable for networks that require a long lifespan since it especially enhances the clustering structure to reduce and optimize the energy consumption of nodes. The assessment's outcomes demonstrate that the IEECP outperforms standard approaches.

In order to reduce packet loss, and packet latency, increase throughput, extend the lifetime of the network, and further adapt while facing malicious nodes, in [17] set out to achieve these goals. The Trust based energy-efficient routing protocol (TBEERP) mechanism is a three-tier clustering that incorporates an integrated security mechanism for detecting the suspicious activities on SN and exclude them from participation. The sink node chooses the grid head in this center-based clustering protocol depends on the value of its cost function. Additionally, in order ensure the efficiency of links and increase routing efficiency, hardware-based link quality estimators are employed. To verify the efficiency of the suggested approach, a wide research was performed. Using the node' resource and trust factors as provided in [18], the Crow Whale optimization algorithm for energy and trust aware multicast routing (CrowWhale-ETR) and Whale Optimization Algorithm (WOA) based on the Objective Function (OF). In order to identify the best pathways, CWOA is first used to evaluate the nodes' trust and energy. In order to identify secure nodes and enhance secure communication inside the network, this ideally determined path is employed for DT. Every transmission concludes with an update of every node's energy and trusts.

A Deep Reinforcement Learning (DRL) based intelligent routing system that greatly reduces latency and lengthens network lifetime was suggested in [19] for IoT-enabled WSN. Based on the present data load in the SN, the suggested technique splits the entire network into several uneven clusters, so avoiding the network's premature death. NS3 is used in a comprehensive experiment on the suggested algorithm. Then in terms of active nodes, packet delivery, communication delay, and EE in the network, the efficiency of the suggested technique is demonstrated, and the experimental outcomes are compared with the most recent techniques.The Secure Trust-Based Routing (STBR) process was introduced in [20] in order to establish QoS settings for the Internet of Things network. Changes in rates of delays, EC, power input, PDR, and jitter were investigated in three different situations including a secure network, sidechains (SC), and the use of SC and TBR. The efficacy of several network settings has been evaluated to ascertain the network's ability to withstand different kinds of attacks while maintaining QoS standards.

A dynamic cluster head-based energy-efficient routing system was introduced in [21]. Setup, transmission, and measurement are the 3 stages of the Improved Coyote Optimization Algorithm (ICOA). The path among the BS and the CH is then determined, by the Improved Jaya Jaya Optimization Algorithm with Levy Flight (IJO-LF). It selects the optimal course depends on the distance, node degree, and RE. In [22] proposed an improved Orphan-Low Energy Adaptive Clustering Hierarchy (O-LEACH) process to facilitate the creation of a novel clustering strategy that may result in decreased EC and greater network lifetime. The orphan node will try to expand the network as a whole because of its abundance of energy. The O-LEACH protocol has the lowest number of orphaned nodes over the whole network and very high connectivity rates. Simulated Annealing with Lightning Search Algorithm (SA-LSA) and Particle Swarm Optimization with LSA (PSO-LSA) are used in this hybrid optimization.The longevity of the WSN is increased by these suggested methods for managing the CH election in an efficient manner, which leads to optimal path routing and EC minimization.

Enhanced Smart-Energy-Efficient Routing Protocol (ESEERP) technique that strengthens and prolongs the network's lifetime was presented in [23]. Using an effective optimization technique derived from several objectives, it selects the CH. It helps lower EC and the number of sleepy SN. To find the optimal path for DT to the sink node, a Sail Fish Optimizer (SFO) is applied after CHS. The suggested methodology is statistically examined with respect to EC, BandWidth(BW), PDR, and network longevity. The results are compared with similar conventional techniques like Ant Lion Optimization (ALO), Particle Swarm Optimization (PSO), and Genetic Algorithm (GA). A novel technique named Chaotic Bumble Bees Mating Optimization (CBBMO) is employed for secure DT with Trust Sensing Model (TSM), as it has been suggested in [24]. The bumble bee swarm's mating behavior stimulates BBMO. The framework of the CBBMO is described by integrating the chaotic theory into the traditional BBMO technique for enhancing its rate of convergence. The suggested approach uses the CBMO algorithm to implement secure routing and build a TSM. To detect the Malicious Node (MN), the suggested approach first builds a TSM by combining direct and indirect trusts. This allows for the determination of the Trust Value (TV) of the IoT nodes. Additionally, the TSM is used to identify the most efficient and secure method for DT, which enables the secure RP with the CMBO procedure. A series of experiments are examined in terms of several metrics to assess the superior efficiency of the technique that is being provided.

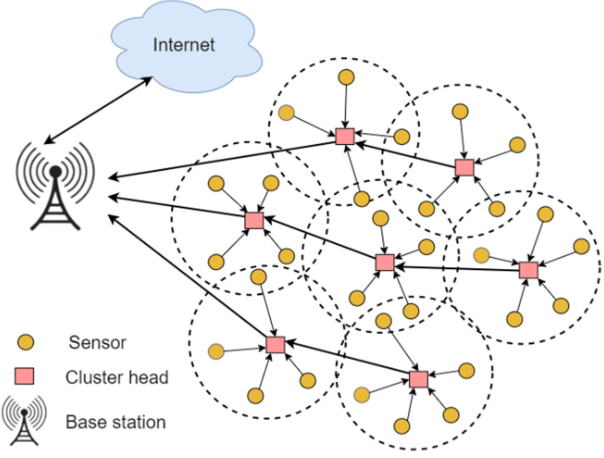
An IoT hybrid optimization algorithm-based QoS aware energy Efficient Multipath Routing (QEMR) approach is proposed in [25]. In the beginning, a Modified Teaching Learning based Optimization (MTLO) was used to achieve optimal clustering. The Nonlinear Regression-based Pigeon Optimization (NR-PO) technique is used to estimate the CH. Deep Kronecker Neural Network (DKNN) is introduced for routing and path optimization. The QEMR scheme is assessed for efficacy using the Network Simulator (NS3) simulation tool. Simulation outcomes are compared with current techniques regarding the factors like node density, node speed, and network traffic. In the cluster to select optimal CH, in WSN-IoT an innovative optimization technique based on Energy-Efficient CHS (SWARAM) was presented in [26]. Cluster formation and CH selection are the 2 stages of the suggested swarm technique. The Osprey Optimization Algorithm (OOA) is used to choose CH in order to maximize network throughput and longevity. Prior to the CH node being chosen by the SWARAM approach, using Euclidean Distance (ED) the nodes are clustered. To achieve EE CH selection, with distance and Residual Energy (RE) parameters, the Fitness Function (FF) is created. When the CH rotates, the OOA convergence time is rapid.

1. **PROPOSED METHODOLOGY**

This study presents the CTEERP technology, which enhances network connectivity and prolongs network lifetime. Chaotic Map Pufferfish Optimization Algorithm (CMPOA) is introduced to select an efficient set of CH and route to destination. In order to attain network longevity and energy efficiency, CMPOA is selected for each round. Considering energy, QoS, and trust, the Deep Q Network (DQN) is developed. Lastly, data processing and route management are handled by the trust route maintenance and update phase. This stage maintains the multipath computed trust value while periodically managing and ensuring distributed DT. Metrics are used to evaluate the performance of routing methods.

* 1. **CLUSTERING MODEL**

When it comes to maintaining the nodes' energy, clustering shows potential. As seen in Figure 2, it is described as the clustering of SN to form a cluster. Depending on the routing topology being used, each cluster has a single CH that gathers, aggregates, and sends data from the cluster to either the BS or the next CH. When implementing clustering topology, choosing the CH is the primary consideration. The distance of the node from sink and RE may have an impact. Still, choosing the best CH is a challenge [27].

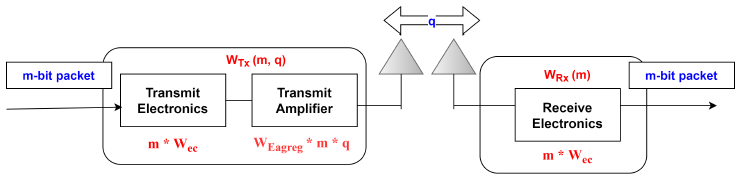


**FIGURE 2. CLUSTERING BASED WSN MODEL**

Smart energy routing algorithms mainly employ DA, multi-objective-based CH selection, trust evaluation, and path selection for DT. Its primary focus is the problem of traffic congestion around the sink. The steps in this method are configuration, energy modeling, node aggregation, and path selection. The configuration step includes an explanation of the creation and setup of the sensor network. Energy modeling includes data transfer via the nodes as well as an estimate of EC. The methods for categorizing network nodes and forming clusters are described by the node aggregation and CHS. During the path selection stage, the optimal path for DT will be recognized via the CMPOA method. Graph G = V, E represents a network, here V is the BS, often known as the sink node, and the link needed for DT between SN is E. Construct a number of network-related assumptions. A (2-D) two-dimensional Euclidean method for randomized sensor placement. Every SN comes with a non-rechargeable power supply; once placed, SN cannot be relocated. The radio receiver utilizes energy while it is also being amplified and transmitted by the transmitter, it causes radio energy to be dissipated. The multiple paths framework is used when a distance D, the distance square for the radio energy loss in the (MP) multipath method, between the transmitter and the receiver is more than the threshold value. Equation (1) demonstrates the m-bit transmission of packets for the consumption of energy .

|  |  |
| --- | --- |
|  | (1) |

To determine the energy amplification in either (FS) free space or the MP approach among the receiver and transmitter, the SN's electrical circuit requires energy , as shown in Figure 3.

****

**FIGURE 3. FRAMEWORK FOR ENERGY DISSIPATION**

The model is represented as and , and it is bit-rate tolerant. is the distance determined by applying the threshold in equation (2). The energy needed to transmit a bit into the FS via the MP channel at a distance of g between the transmitter and receiver is then represented by and .

|  |  |
| --- | --- |
|  | (2) |

Equation (3) indicates the way energy is utilized for packets of m bits that are received.

|  |  |
| --- | --- |
|  | (3) |

Equation (4) represents the energy used for the DA.

|  |  |
| --- | --- |
|  | (4) |

Here, "" represents the amount of bits collected in a packet, "" denotes the number of messages, and "" denotes the energy used for one-bit aggregation.

* 1. **CLUSTER HEAD SELECTION**

A Cluster formation is a CH that has several nodes that can function as nodes. Utilizing a hybrid Medium Access Control (MAC) protocol, these are capable of gathering and analyzing information from CM before transmitting it to the CH. The Carrier-Sense Multiple Access using Collision Avoidance (CSMA/CA) method is used by cluster node members to acquire the channel in order to transmit sensed information to its cluster congregation (low-level MAC). All cluster congregations transmit the collected data to their CH via assigned Time Division Multiple Access (TDMA) session (high-level MAC). To transmit the sensed data to the relevant cluster congregation, each cluster member activates its radio communication module during the steady state phase. The cluster congregation compiles, compresses, and transmits the data to the CH. Consequently, multi-hopping is the intra-cluster communication technique [28]. To the BS, each CH also transmits the data it receives. After the BS receives all of the data, the CH notify the participants of the END round. The total EC by the CH for every round is presented in Equation 5. Here, the total EC by a CH in each round is denoted by . The energy used throughout the CHS process is represented as . The energy used to transmit the CH advertisement is also denoted as . is the EC for obtaining the connection demand from non-CH node.The energy used to obtain the sensed information from cluster members (CM) is . The energy used to transmit the combined data from the CH to the BS is denoted as .

|  |  |
| --- | --- |
|  | (5) |

In represents,

|  |  |
| --- | --- |
|  | (6) |

Here, the control packet size is represented by .

|  |  |
| --- | --- |
|  | (7) |
|  | (8) |
|  | (9) |
|  | (10) |

Then, the total energy used in each round () by the cluster members and each cluster node congregations. Equation (11) describes the way is computed. Then, represents the overall EC by a CM in every round. It takes of energy to send sensed data from a CM to the CH, as it symbolizes the energy required in sending a coordinated signal to the CH.

|  |  |
| --- | --- |
|  | (11) |
|  | (12) |

indicates the energy used by the cluster congregation. the energy used to send the cluster congregation advertisement is identified as , the energy used by the DA process can be denoted as .The suggested protocol, which implies that node should assume one of three roles for each round: CH, cluster member, or gathering of clusters depicts the behavior of the node based on its EC. As a result, the role across each round is used to evaluate the amount of energy W is used for node . The OF describes the FF for each cluster for each round of the CMPOA.

|  |  |
| --- | --- |
|  | (13) |

Evaluating the CH with BW, which includes high data count that can be sent from the CH to the BS, represents a target in keeping the sink node from failing. Several metrics are needed to calculate the NL and smart EE, depending on various features.

**Network Coverage:** The coverage rate of the initial node deployments and whether or not these nodes are able to fully and correctly acquire signals are the main components of the coverage metric, which measures the quality of WSN services.

**Network Connectivity**: Connection guarantees that information acquired by sensors that can be transmit to sink nodes, as sensor networks are usually large in scale.

**Network Longevity:** The NL is defined as the period of time from its creation until the point at which the proportion of dead nodes reaches a predetermined level.

* 1. **CHAOTIC MAP PUFFERFISH OPTIMIZATION ALGORITHM (CMPOA) BASED CHS**

Using its population search in an iterative way, the CMPOA approach is a population-based technique for CHS. Based on its node position in the Search Space (SS), every member of the CMPOA chooses the choices for the CH election's parameters. As a result, every member of CMPOA is a potential solution to the CHS, and each member of this vector may be mathematically described using a Fitness Value (FV) for each of its elements. Equation (14) can be utilized to model the collection of these vectors using a matrix. At the beginning of the procedure, each CMPOA member's main position is initialized using equation (15) [29],

|  |  |
| --- | --- |
|  | (14) |
|  | (15) |

In this case, N is the number of population members, similar to the amount of CM and CH in the IoT-WSN model. The number of parameters for CHS is denoted as . random number, . The lower bound of the dth parameter is represented as and the upper bounds of the dth parameter is denoted as and the CMPOA population matrix can be denoted as X. The ith CMPOA member (selected CH for path selection and routing) is represented as ; The dth dimension in the CH with SS is denoted as . The OF of the CH election and optimal path can be assessed with each CMPOA member serving as a potential candidate solution (CS). Equation (16) [29] allows for the vector representation of the collection of assessed values for the OF of the path selection and CHS.

|  |  |
| --- | --- |
|  | (16) |

In this case, the evaluated OF based on the ith CMPOA member is denoted by , while F is the evaluated OF vector. Every CMPOA member uses the assessed FV for the OF for assessing the quality of potential CH solutions. The optimal CS, or the best member, is represented by the best evaluated value for the FF, and the worst CS, or the worst CH and route from source to destination, is represented via the worst evaluated value for the OF. The CS should be changed in each iteration depends on the comparison of newly assessed values for the OF, since the position of CMPOA members in the CH SS and path selection are modified in every iteration [29].Based on a simulation of natural interactions among pufferfish and their predators, the suggested CMPOA technique updates the location of population members in the CH selection space in its design. The pufferfish is attacked first by the predator in this natural process. In order to defend against the predator and attempt for escape, the defense mechanism was employed by the pufferfish to transform into a ball of pointed spines. Exploration and Exploitation are the 2 phases in CMPOA. In this case, the simulation of a predator attacking a pufferfish serves as the basis for exploration, the basis of exploitation is the simulations of the predator escaping from a spiny pufferfish and these two steps comprise the updating of CMPOA population position members [29].

**Phase 1: (Exploration Phase) Predator Attack towards Pufferfish**

Predator attack strategy against pufferfish was simulated the node positions of the population members are modified during the first phase of CMPOA. The predator’s node location change during the pufferfish attack is simulated for updating the CH location of the CMPOA members in the CHS space. In the CMPOA design, every member of the population acting as a predator takes into account the node position of other members of the population that have a higher value for the OF when determining the candidate pufferfish for attack. Equation (17) is used to determine each population member's set of pufferfish.

|  |  |
| --- | --- |
|  | (17) |

In this case, the population member with an OF value is higher than that of the ith predator is represented as , is its OF value, and the collection of prospective pufferfish node positions for the ith predator is denoted as . The selected pufferfish (SP) in the CMPOA design is thought to be the one that the predator chooses from the candidate pufferfish identified in the CP set. Equation (18) is used for each CMPOA member to determine a novel node position in the CH space depends on the modelling of the pufferfish approach by the predator. Then, in accordance with Equation (19), if the new position OF is increased, that new position takes the place of the corresponding member's prior node position.

|  |  |
| --- | --- |
|  | (18) |
|  | (19) |

In this case, The jth dimension is denoted as . The new position for the ith predator based on initial stage of the suggested CMPOA method is denoted as , That is its jth dimension, . It’s OF value is and the numbers that are arbitrarily chosen as 1 or 2 is denoted as . are random numbers from the interval [0, 1].The randomly chosen pufferfish for the ith predator chosen from the set is denoted as ; that is, is a member of the set.

**Phase 2: DM of Pufferfish against Predators (Exploitation Phase)**

By protecting against predator attacks with a DM simulation of a pufferfish, the CH location of population members is updated throughout the second phase of CMPOA. The exploitation potential of the (LS) Local Search method is increased by simulating the predictor’s escape from the pufferfish, which causes little variations in the positions of the CMPOA members. Equation (20) is used to determine a new node position for each member of the CMPOA according to the simulation of the way the predator's position varies when it moves away from it. Then, in accordance with Equation (21), If the value of the OF increases its associated member is replaced by this new CH position. Equation (21) is included because efforts have been made to enhance the algorithm in the CMPOA design. Actually, when a new CH location is computed for a CMPOA member, whether or not this novel node location for the associated member results in a better solution to the problem is determined by comparing the values of the OF. Equation (21) demonstrates that increasing the OF value is a need for each CMPOA member's update procedure.

|  |  |
| --- | --- |
|  | (20) |
|  | (21) |

Based on the 2nd stage of the established POA, the new CH position for the ith predator is . Its jth dimension is denoted as Its iteration counter is t, its OF value is , and random values from the interval [0, 1] are . The iterative chaotic map equation is used to create the random numbers that are given in the POA. It has the following definition:

|  |  |
| --- | --- |
|  | (22) |

The control parameter is denoted as .

|  |
| --- |
| **Algorithm 1. Pseudocode of CMPOA** |
| **Start CMPOA** |
| 1. Input problem information: variables, OF, and constraints |
| 1. Set CMPOA population size (N) and iterations (T) |
| 1. Create the initial population matrix as node matrix at arbitrary with Equation (18) |
| 1. Calculate the OF |
| 1. For t = 1 to T |
| 1. For i = 1 to N |
| **Phase 1: Exploration phase** |
| 1. Calculate the candidate pufferfish set for the ith CMPOA member with Equation (17) |
| 1. Choose the target pufferfish for the ith CMPOA member at arbitrary |
| 1. Compute novel location of ith CMPOA member with Equation (18) |
| 1. Update ith CMPOA member with Equation (19) |
| **Phase 2: Exploitation phase** |
| 1. Compute new location of ith CMPOA member by Equation (20) |
| 1. Update ith CMPOA member by Equation (21) |
| 1. End |
| 1. Save the best CS so far |
| 1. End |
| 1. Output the best quasi-optimal solution obtained using the CMPOA |
| **End CMPOA** |

* 1. **DEEP Q NETWORK (DQN) BASED TRUST MODEL**

Trusted route discovery, Trust Evaluation (TE), and trust upgrading and maintenance are the steps included in the suggested method. The foundation for identifying and maintaining a dependable and trustworthy path using DQN is TV, which are found in WSN. Based on the TE score, the suggested approach first finds multiple pathways and filters out malicious nodes. In order to transfer data in a dispersed manner, DQN considers energy, QoS, and trust aspects after identifying a trust-based multi-path. Additionally, it is capable of efficiently preventing malevolent nodes that carry out on-off attacks (OOA), as learning results also take previous performance take into account. Under the Precedence Based Assured Service (PBAS) principle, the distributed transmission mechanism used by the algorithm sacrifices data that is relatively irrelevant in order to ensure the dependability of DT that is crucial to the objective. Multiple routes and data processing are handled by the trust Route Maintenance (RM) and update phase, which comes to an end. This stage maintains the multipath computed trust value while periodically managing and ensuring distributed DT.

**Trusted Route Discovery:** For the purpose of sharing the essential trust and learning values, TE and trust discovery collaborate closely. To find a trusted route to the Gateway Node (GN), the source node sends the RREQ (Route REQuest). Intermediate node reply to the source node with trusted data after receiving the request message. Nodes that check the blacklist is not a MN. The intermediate node deliberates the TV and performs multiple loop-free RD methods before broadcasting the RREQ. The RREP (Route REPly) and R sent by the destination in response to the RREQ message. More routes might be available in a wireless environment depending on the circumstances, and the operator can decide which ones to use [13].

**Trust Evaluation:** Local trust evaluations and global trust evaluations are the two categories under which trust evaluations fall. Initially, each node evaluates its energy value, trustworthiness, and QoS to determine local trust (LT), which is then learned by rewarding it. The reward is obtained by deriving a (GT) global trust for the whole route. The GT evaluation is dependent on the LT node value within the MP. This enables the transfer of critical data to a secure path, leading to the discovery of the optimal route [13].

**Local Trust Evaluation:** Learning from the outcomes of the discovery component serves as the basis for trust evaluation. The energy, Packet Forwarding Ratio (PFR), and Expected Transmission Time (ETT) was computed and the SN observes the way its neighbors behave [13].

|  |  |
| --- | --- |
|  | (23) |

Equation (23) demonstrates the way PFR is calculated, is obtained by monitoring the manner in which nearby nodes use the promiscuous mode to forward packets. is the number of packets that node i sent to node j while node j forwards packets to node i. On the other hand, sophisticated attacks like on-off that are executed in accordance with a set time are hard to identify using a basic approach to PFR calculation [13]. To address these problems, the IoT-WSN architecture introduces DQN and a flexible blacklist threshold. Malicious nodes (0 ≤ ≤ 0.75) are identified using a blacklist threshold value (γ). Equation (24) illustrates the measurement of the blacklist threshold, which takes into account the tactical network of nodes that is mission-critical [13].

|  |  |
| --- | --- |
|  | (24) |

The fastest possible DT level across a specific link is known as Link BW (LBW). In bits per second (bps), the current BW represents an approximation of the network interface's current BW. It is challenging to identify if a bottleneck or a malicious node attack is responsible for the decline in network performance when there is a high current BW demand. In order to facilitate the hidden resolution of malicious node exclusions, the blacklist threshold has been lowered [30].

Witness trust, Indirect Trust (IDT), and Direct Trust (DT) are the three categories into which trust evaluation is divided [31]. By examining the actions of their direct neighbor nodes, assessors can determine DT. The evaluator’s ID node serves as a base for the IDT and it is the recommended value for the Target Node (TN). While it is challenging to assess trust accurately based just on DT, computations depends on references from ID nodes can be used to assess trust more accurately. The (DN) direct node forwards the IDT value to the source node that can be employed for evaluating the total trust value. When a verified DN assesses an ID node and suggests a value to the source node, that evaluation is known as a witness trust. Indirect trusts are different from witness trusts in that certified direct nodes perform the witness trust evaluation and recommendation, whereas indirect nodes generate the indirect trust. For a more precise and useful assessment of trust, take into account both direct and indirect witness trust. Equation (25) illustrates the way ETT is used to measure the QoS factor of links.

|  |  |
| --- | --- |
|  | (25) |

Because ETT accounts for variations in link transmission rates, Expected Transmission Count (ETX) is improved. B represents the LBW, or raw data rate, and X stands for the packet's size [32]. An energy discharge that prevents the devices from functioning in an IoT-WSN can have an enormous impact on operations. Equation (26), in which is the ith node RE and the initial energy of node I can be denoted as , demonstrates the way the recommended method calculates the energy required for a device with limited resources [13].

|  |  |
| --- | --- |
|  | (26) |

Equation (27) demonstrates that these obtained parameters are used by the node with limited RE for calculating Energy-based QoS and Trust Value (EQTV). By weighing the metrics according to the node's energy condition, the EQTV equation determines which metrics should be prioritized: energy, QoS, and trust [13].

|  |  |
| --- | --- |
|  | (27) |
|  | (28) |

In order to distribute weights adaptively based on a device's status, a flexible weight module is presented in this work. Equation (28) is used to calculate based on , while is determined based on RE. When a node has enough energy, it gives dependability and QoS more weight; when it doesn't have enough energy, it gives energy a greater importance. Therefore, an energy-based flexible weighting approach can be used to improve survivability. The Local trust level is the trust value that is obtained by applying the following formula. Equation (29), which lists the techniques to compute the TV of k neighbor nodes of node j, and LT, can be implemented. As a result of averaging the TV assessed by n nodes, the total amount of k neighbor nodes in the local trust represented as n [13],

|  |  |
| --- | --- |
|  | (29) |

***Global Trust Evaluation:*** When the conditions for mission-critical data are met, a destination node can reward it using a process called Global Trust (GT) evaluation [30]. Consequently, a reward mechanism becomes active when all conditions along the entire path are met, even though evaluating LT among nodes is crucial. Equation (30) [13] illustrates the manner in which the TV of the complete path can be determined by averaging the LT values of all the nodes in each path, which is the calculation of GT.

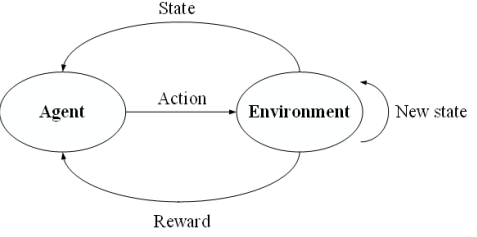
|  |  |
| --- | --- |
|  | (30) |

When IoT applications have communication requirements of < 100 ms and the PTV (Path TV) is >0.65 , GT is compensated in the case of E2E delay. As indicated by Formula (31) For each node in the trusted route, assign the PTV with the lowest PFR.PTV values can verify that mission-critical data Trust are met by the measured path TL.

|  |  |
| --- | --- |
|  | (31) |

The reward in this GT evaluation is determined by whether the packet transferred from the SN to the destination complies with the standards for IoT data. In order to meet the needs of IoT applications, this guarantees the accuracy of the data.

**Deep Q Network (DQN) based trust evaluation:** A Markov decision process (MDP) is analogous to the Q-Learning (QL) process. The next state, immediate reward, and a fixed state transition probability distribution are determined by the agent's selected action and current state. The Q-learning basic framework is depicted in Figure 4. The agent chooses an action in QL based on current state of the environment. The environment sends a (R) reward signal back to the agent and updates the current state to the new state after accepting the action (A).The agent subsequently chooses and performs the subsequent A in accordance with the R. Since the environment is typically random, the next (S) state is also random. Consequently, a MDP is made up of the collection of S and A as well as the procedures for switching among S [33].

****

**FIGURE 4. BASIC STRUCTURE OF QL**

The periodic sequence of states (S), Actions (A), Rewards (R) was created in this procedure.

|  |  |
| --- | --- |
|  | (32) |

Here, the action can be denoted as , and after completing the , the reward earned is denoted as . Additionally, every node’s trust status and updates it with R based on the estimated LT and GT values are denoted as . The last state moving to marks the end of the episode. The foundation of an MDP is the Markov assumption, which states that rather of relying on the prior state and action, the chance of the next state, , depends on the present state, , and . The agent's learning objective is to maximize the future rewards' cumulative value. The following equation (33) [33] can be used to get the total R for sequence for a certain execution of the MDP, taking into account both immediate and future rewards.

|  |  |
| --- | --- |
|  | (33) |

Still, the reward will vary following the next same action due to the randomness of the environments. Over time, the error grows larger. Future rewards are therefore discounted using a factor , thath indicates the degree to which time impacts R. The following is one way to express the entire reward [33],

|  |  |
| --- | --- |
|  | (34) |

According to a certain policy π, a Q-value in QL represents the TV of an in a state . The Q-value can be obtained as follows [33], per equation (34).

|  |  |
| --- | --- |
|  | (35) |

Here, the possibility of substituting to following in is represented as , and the R of in state can be represented as [33],

|  |  |
| --- | --- |
|  | (36) |

represents the ideal Q-value of in the .Next, use equation (37) to update the Q-value [33].

|  |  |
| --- | --- |
|  | (37) |

Here, the learning rate is expressed as α (0, 1]. The alpha ratio α and decay factor are adjusted to 0.5 and 0.9 to depict the trust state of nodes and networks.Either the maximum Q value or the epsilon value may be used to randomly select the action a. The action result determines the reward to be given, and the QL process updates a new Q value. The suggested method uses trust information that is periodically received from nearby nodes to evaluate LT. GT is applied as a reward when the Data Packet (DP) reaches the gateway [33].The optimal can be found using Equation (38),

|  |  |
| --- | --- |
|  | (38) |

As a result, the optimal action can be used to determine the optimal policy. Basically, DQN is a Neural Network (NN) where the Q-network can output a vector of action Q-values for any given state. Training the NN is the key to the DQN. Create a loss function first. Get the following loss function by defining the target function with the Mean Square Deviation (MSD).

|  |  |
| --- | --- |
|  | (39) |

where

|  |  |
| --- | --- |
|  | (40) |

The Q-value that needs to be updated from QL is called and is the network parameter. A predicted Q-value is . Network training involves updating w until the loss function converges. Assume P() = 1 for simplicity.Nevertheless, the process becomes unstable since the DQN substitutes a DNN for the task of calculating Q-values in QL. Mainly because minor adjustments to a signal action Q-value will affect all A in the network and their Q-values in other S, which will change the manner in which the sample data is distributed [33]. This is due to the strong connection that occurs among continuous S and A inputs.

**Trust Route Update and Maintenance Component:** The procedure of determining methods to Path update or RM in the case of a change in network condition, such as data usage, link status, or link disconnection, is known as route update and RM. At predetermined periods, the trusted path is validated by the RM procedure. A new trust route retrieval procedure is initiated when the validity period of a trust route cache entry is exceeded. Every SN uses adjustable weights to determine EQTV. The nodes and paths TL are routinely simplified via an EQTV hello message in order to determine a reliable route. Next, determine the significance of the mission data if the Epsilon value is higher than a predetermined threshold. Since selecting arbitrary actions too frequently can deteriorate efficiency of the network, the Epsilon criteria was chosen. A random path is chosen if the data to be communicated does not have much significance; otherwise, the max-Q value path is chosen. At last, as a reward for their efforts, SN learns and updates the routing table's LT value. When the mission-critical conditions are met, the GN updates the E2E delay and PTV of the pathways and is rewarded globally. At last, as a reward, the GN learns and updates the routing table's GT value. Therefore, learning the Q factor of the route that satisfies the demands is essential for effective path management.

* 1. **TRANSMITTING DATA TO THE BS**

There is a single point of contact for all data sent from CH to BS [34]. The optimal route for DT across the network is found using the CMPOA. The SFO-based routing approach has 3 primary stages: DT, modifying the route, and initializing the route selection mechanism [35]. As a population-based metaheuristic procedure, CMPOA is recognized. Depending on its Fitness Value (FV), the optimal nearby CH is identified, and the route is selected. Subsequently, a new CH that recognizes the optimal path takes position of the previously identified best adjacent CH [36]. Once the optimal path has been identified from every possible route, the DT process will begin. The CH could die or have its energy use minimized as a result of the packets EC during DT to the BS [37].

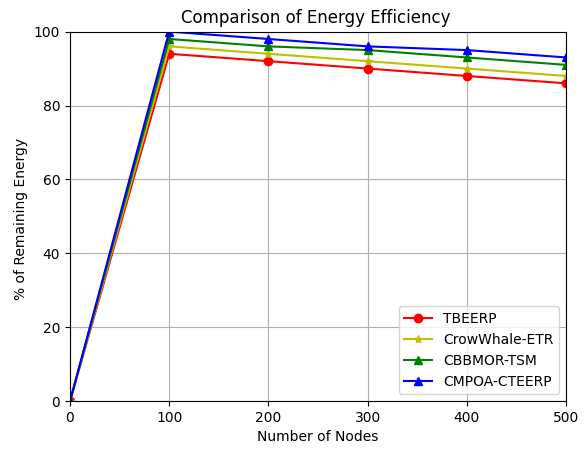
1. **PERFORMANCE ANALYSIS AND EVALUATION**

TBEERP [17], CrowWhale-ETR [18], and CBBMOR-TSM [24] are a few examples of existing algorithms that are compared with OPNET 18.0 implementation of performances evaluation. PDR, throughput, E2E delay, EE, and Network Lifetime (NL) are the metrics used to quantify the performance of these algorithms. Table 1 describes the settings of the simulation environment. The simulation was set up with 500 nodes, covering an area of 1000 m × 1000 m. An attacker has the ability to continually launch all behaviors, 40% of which are bad and 60% of which are beneficial. Grey hole attack malicious nodes lose packets at a forty percent rate. A malicious node could attack the target node with a lot of packets during a DoS attack. Different kinds of traffic are produced by DoS attacks, and the state of the network is always changing. In order to simulate, 99 SN and a fixed gateway node were used. Attacks (such as denial-of-service and Gray Hole Attacks (GHA)) were conducted with the fraction of malicious nodes set between 0 and 40%. The Constant Bit Rate (CBR) data flow framework considers type, size, and sensor DT. To simulate the IoT-WSN condition, more data than the LBW capability was transmitted in the experimental setting. The PHY was fixed to 2 Mbps in order to mimic the tactical network's limited by resources communication [38].

**TABLE 1. SIMULATION ENVIRONMENT SETTINGS**

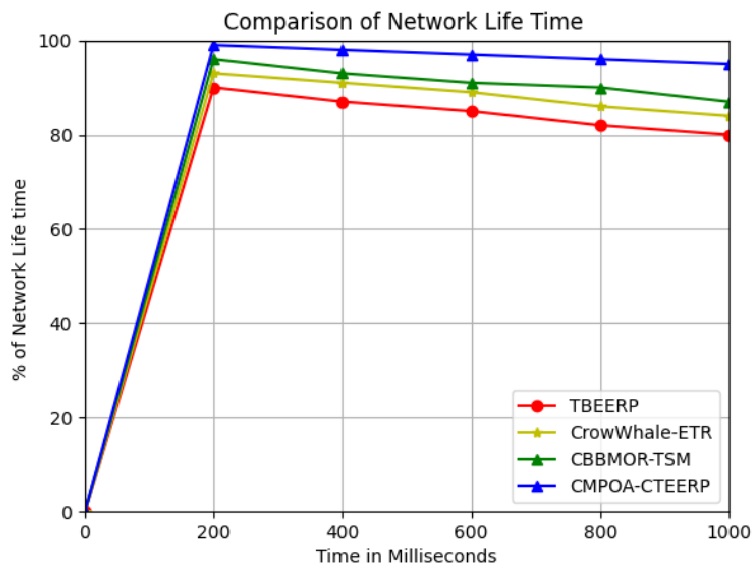
|  |  |
| --- | --- |
| **Parameters** | **Values** |
| Simulator | OPNET 18.0 |
| Simulation time(s) | 1000 |
| Routing | TBEERP, CrowWhale-ETR, CBBMOR-TSM and CMPOA- CTEERP |
| Amount of nodes | 500 |
| % of MN | 0-40% |
| Attack model | GHA, OOA, and DoS attack |
| Traffic kind (Avg. Packet Dimension) | VoIP G.723.1 (24 bytes) |
| Fire Alarm, Chat(100 bytes) |
| Humidity Sensors, Health, Temperature (120 bytes) |
| Security, Smart Meter(200 bytes) |
| Bulk Information, CCTV camera(2000 bytes) |
| MAC | CSMA/CA |
| PHY | 802.11b |
| α | 0.5 |
|  | 0.9 |

The energy was computed by taking the original energy and dividing it by the PDR. The quantity of energy that the network's SN use is measured by their EE. The rounds or duration of the operation of the network is indicated by its NL. It describes the amount of rounds the nodes in the field will run out of time to finish their tasks. From the moment the packet was delivered by the sending node to the moment it was obtained by the destination node, is known as the E2E delay. Throughput was evaluated via counting the amount of packets sent in a predetermined amount of time. The quantity of packets that were transmitted and received was taken into consideration when measuring PDR. Metrics such as EE, NL, E2E Delay, throughput, and PDR are used to evaluate the efficiency of the network.

****

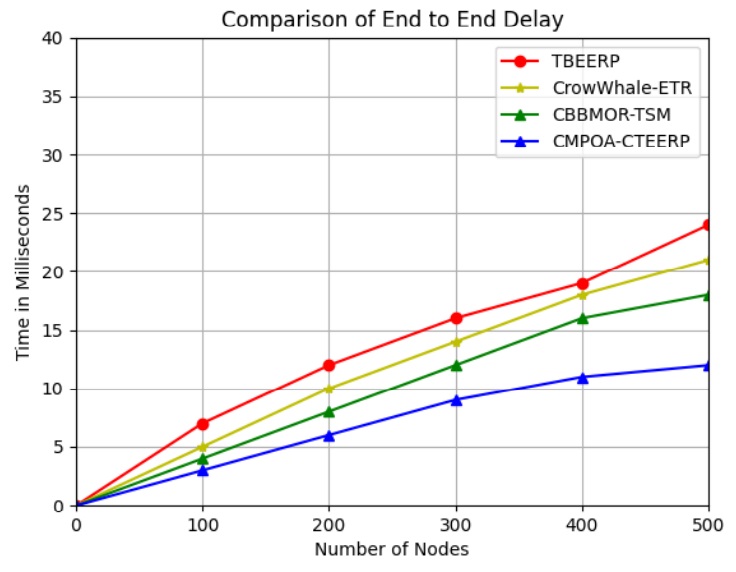
**FIGURE 5. ENERGY EFFICIENCY WITH RESPECT TO NUMBER OF NODES**

The existing method TBEERP uses 6% energy for 100 nodes, while Crow Whale-ETR uses 96%, CBBMOR-TSM uses 98%, and CMPOA-CTEERP uses 0%. In the same case, the existing method TBEERP uses 14% energy for 500 nodes, while Crow Whale-ETR uses 12%, CBBMOR-TSM uses 9%, and CMPOA-CTEERP uses 7%. The other existing methods consume more energy than the suggested strategy. The suggested system has the lowest energy consumption compared to other methods. The suggested system has 93% of remaining energy when compared to other methods such as TBEERP, CrowWhale-ETR, and CBBMOR-TSM shown in Figure 5.



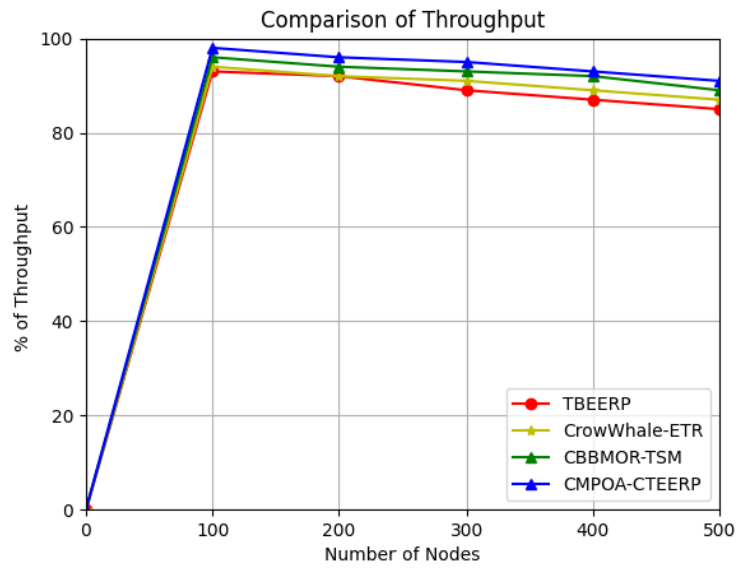
**FIGURE 6. NETWORK LIFETIME WITH RESPECT TO SIMULATION TIME**

In Figure 6, the simulation time ranges from 200 to 1000 seconds. When compared to other current methods, the suggested framework demonstrates that it achieves a longer NL. Depending on the number of rounds, the suggested framework effectively delivered the packets for a simulation time of 1000 seconds; the NL rises with each round. The suggested system has an increased NL of 99% in round 1, 98% in round 2, 97% in round 3, 96% in round 4, and 95% in round 5. The other approaches, such as TBEERP, CrowWhale-ETR, and CBBMOR-TSM, have the lowest NL compared with the proposed method.



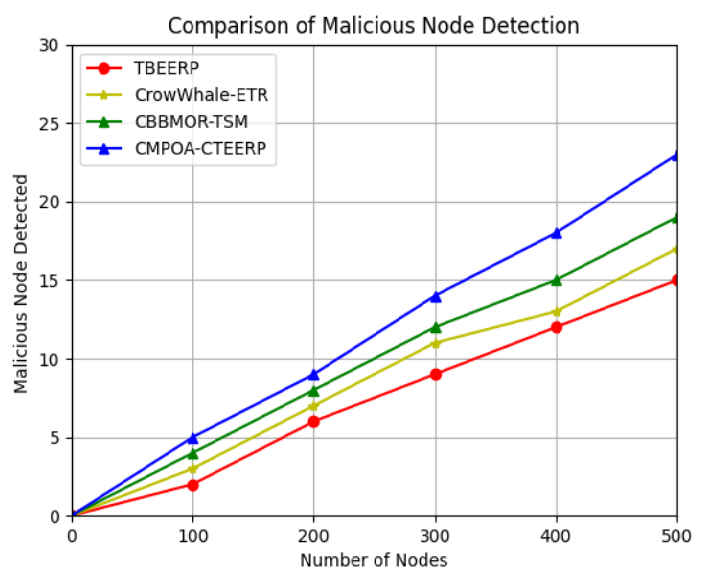
**FIGURE 7. E2E DELAY WITH RESPECT TO NUMBER OF NODES**

Figure 7 shows the E2E delay as a function of the number of nodes in the routing protocols. Current techniques such as TBEERP, CrowWhale-ETR, and CBBMOR-TSM exhibit high E2E latency. When transferring data, TBEERP employs only dependability measurements and ignores QoS considerations, resulting in the longest E2E time when compared to other techniques. Since the suggested approach was trained with consistency and QoS elements in mind, and dispersed transmission based on the importance of IoT applications, it demonstrated the minimal E2E delay compared to other methods. Figure 8: Out of 100 nodes, the proposed system has decreased E2E delay by 3%; other methods, such as TBEERP, CrowWhale-ETR, and CBBMOR-TSM, have increased E2E delay by 4%, 5%, and 7%. The proposed system has 12% delay out of 500 nodes, whereas the existing methods are 18%, 21%, and 24%. Compared to other methods such as TBEERP, CrowWhale-ETR, and CBBMOR-TSM, the proposed system exhibits a delay of 12% out of 500 nodes.



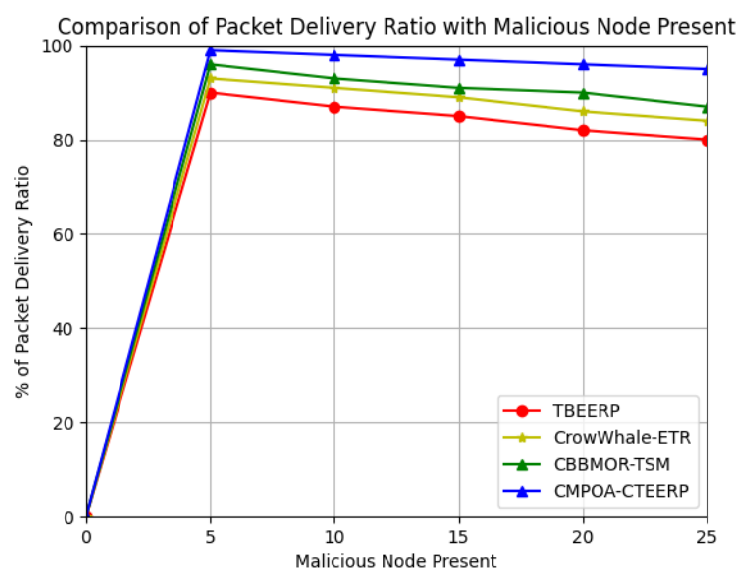
**FIGURE 8. THROUGHPUT WITH RESPECT TO NUMBER OF NODES**

Figure 8 presents the throughput performance. For 100 nodes, the throughput  was 98%, whereas the existing methods such as TBEERP, CrowWhale-ETR, and CBBMOR-TSM exhibit low throughput. In a similar scenario involving 500 nodes, the throughput reached 91%, while previous methods like TBEERP, CrowWhale-ETR, and CBBMOR-TSM achieved 85%, 87%, and 89%. It shows the efficiency of the proposed method.

****

**FIGURE 9. MALICIOUS NODE DETECTION WITH PROPOSED MEHTOD**

The above figure 9 illustrates the performance of MN. Considering 5 malicious nodes out of 100, the proposed method efficiently detects all of them, while other methods like TBEERP, CrowWhale-ETR, and CBBMOR-TSM only detect 2, 3, and 4 nodes. In the same scenario, we are considering 25 nodes out of a total of 500. Out of these, the proposed method will detect 23 nodes  other methods such as TBEERP, CrowWhale-ETR, and CBBMOR-TSM will detect 15, 17, and 19 nodes only.



**FIGURE10. PACKET DELIVERY RATIO WITH MALICIOUS NODE PRESENT**

The above Figure 10 shows the PDR with the actual malicious node. When there are five malicious nodes, the proposed method effectively identifies all of them, resulting in a PDR of 99%. However, other methods such as TBEERP, CrowWhale-ETR, and CBBMOR-TSM lower the PDR by 96%, 93%, and 90% because they can't find the malicious nodes, which slows down packet delivery. In the same situation, if there are 25 malicious nodes, the proposed method finds them 95% of the time, while TBEERP, CrowWhale-ETR, and CBBMOR-TSM all miss them 87%, 84%, and 80% of the time, respectively. You can use the percentage of MN to gauge a system's response rate to an attack.

1. **CONCLUSION AND FUTURE WORK**

In this paper, CTEERP is presented to boost the lifetime and trust of IoT-enabled smart agriculture in WSN systems. CTEERP, CMPOA is used to determine which CH is best for cluster formation. Using CH selection, CMPOA is employed to determine the best path to the sink node for DT. In order to attain NL and EE, a different CHS mechanism is selected for each round. The main procedures in the CTEERP are DA, multi-objective-based CH selection, trust assessment, and path selection for DT. The CMPOA compiles the data, assesses the trust, compresses it, and sends it to the CH. Based on its FV, the optimal nearby CH is identified, and the route is selected. The CMPOA member uses its node location in the SS to determine the values for the CH election's parameters. By simulating the natural behaviors of pufferfish and their predators, the CMPOA technique updates the location of population members in the CHS space. A trusting scheme comprises several components for trusted route discovery, trust evaluation, and trust update and maintenance. Based on the trust evaluation score, the suggested approach first finds multiple pathways and filters out malicious nodes. For DT in a dispersed manner, DQN takes into account energy, QoS, and trust aspects after identifying a trust-based multi-path. At last, data processing and route maintenance are handled by the trust route maintenance and update phase. In order to meet the needs of IoT applications, this guarantees the accuracy of the data. Future research will look on cluster optimization to enhance efficiency and attain balanced EC.

**REFERENCES**

1. Joao Luis Sobrinho, Correctness of routing vector protocols as a property of network cycles. IEEE Transactions on Networking, 2017,Vol. 25(1), pp. 150–163.
2. Mouapi, A. and Hakem, N., 2018. A new approach to design autonomous wireless sensor node based on RF energy harvesting system. Sensors, 18(1), pp.1-24.
3. Zhang, Y., Liu, M. and Liu, Q., 2018. An energy-balanced clustering protocol based on an improved CFSFDP algorithm for wireless sensor networks. Sensors, 18(3), pp.1-18.
4. Bahbahani, M.S.; Alsusa, E. A cooperative clustering protocol with duty cycling for energy harvesting enabled wireless sensor networks. IEEE Trans. Wirel. Commun. 2018, 17, 101–111.
5. Padmanaban, Y. and Muthukumarasamy, M., 2018. Energy‐efficient clustering algorithm for structured wireless sensor networks. IET Networks, 7(4), pp.265-272.
6. Sharma, D.; Bhondekar, A.P. Traffic and energy aware routing for heterogeneous wireless sensor networks. IEEE Communication Letters, 2018, 22, 1608–1611.
7. Kaur, T.; Kumar, D. Particle swarm optimization-based unequal and fault tolerant clustering protocol for wireless sensor networks. IEEE Sens. J. 2018, 18, 4614–4622.
8. Trupti Mayee Behera, Umesh Chandra Samal and Sushanta Kumar Mohapatra. Energy-efficient modified LEACH protocol forIoT application. IET Wireless Sensor System , 2018, 8, 223–228.
9. Cao, L., Cai, Y. and Yue, Y., 2019. Swarm intelligence-based performance optimization for mobile wireless sensor networks: survey, challenges, and future directions. IEEE Access, 7, pp.161524-161553.
10. Devika, G., Ramesh, D. and Karegowda, A.G., 2020. Swarm intelligence–based energy efficient clustering algorithms for WSN: overview of algorithms, analysis, and applications. Swarm intelligence optimization: algorithms and applications, pp.207-261.
11. Quan Tang and Fang Nie, 2023. Clustering routing algorithm of wireless sensor network based on swarm intelligence. Wireless Networks, pp.1-12.
12. Padmalaya Nayak, Kavitha, K. and Nausheed Khan 2019, Cluster head selection in wireless sensor network using bio-inspired algorithm. IEEE Region 10 Conference (TENCON), pp. 1690-1696.
13. Keum, D. and Ko, Y.B., 2022. Trust-based intelligent routing protocol with Q-learning for mission-critical wireless sensor networks. Sensors, 22(11), pp.1-17.
14. Preeth, S.S.L., Dhanalakshmi, R., Kumar, R. and Shakeel, P.M., 2018. An adaptive fuzzy rule based energy efficient clustering and immune-inspired routing protocol for WSN-assisted IoT system. Journal of Ambient Intelligence and Humanized Computing, pp.1-13.
15. Jaiswal, K. and Anand, V., 2020. EOMR: An energy-efficient optimal multi-path routing protocol to improve QoS in wireless sensor network for IoT applications. Wireless Personal Communications, 111(4), pp.2493-2515.
16. Hassan, A.A.H., Shah, W.M., Habeb, A.H.H., Othman, M.F.I. and Al-Mhiqani, M.N., 2020. An improved energy-efficient clustering protocol to prolong the lifetime of the WSN-based IoT. IEEE Access, 8, pp.200500-200517.
17. Ilyas, M., Ullah, Z., Khan, F.A., Chaudary, M.H., Malik, M.S.A., Zaheer, Z. and Durrani, H.U.R., 2020. Trust-based energy-efficient routing protocol for Internet of things–based sensor networks. International Journal of Distributed Sensor Networks, 16(10), p.1550147720964358.
18. Shende, D.K. and Sonavane, S.S., 2020. CrowWhale-ETR: CrowWhale optimization algorithm for energy and trust aware multicast routing in WSN for IoT applications. Wireless Networks, 26, pp.4011-4029.
19. Kaur, G., Chanak, P. and Bhattacharya, M., 2021. Energy-efficient intelligent routing scheme for IoT-enabled WSNs. IEEE Internet of Things Journal, 8(14), pp.11440-11449.
20. Sheikh, A., Kumar, S. and Ambhaikar, A., 2021. A Secure Trust-Based Routing Framework for Improving the QoS of Internet of Things Based Networks. International Conference on Computing and Communications Technologies (ICCCT), pp. 149-154.
21. Adumbabu, I. and Selvakumar, K., 2022. Energy efficient routing and dynamic cluster head selection using enhanced optimization algorithms for wireless sensor networks. Energies, 15(21), pp.1-18.
22. Senthil, G.A, Arun Raaza and N. Kumar, 2022. Internet of things energy efficient cluster-based routing using hybrid particle swarm optimization for wireless sensor network. Wireless Personal Communications, 122(3), pp.2603-2619.
23. Roopali Dogra, Shali Rani, Kavita, Jane Shafi, Seongki Kim, and Muhammad Fazal Ijaz, 2022. ESEERP: Enhanced smart energy efficient routing protocol for internet of things in wireless sensor nodes. Sensors, 22(16), pp.1-15.
24. Gali, S. and Nidumolu, V., 2022. An intelligent trust sensing scheme with metaheuristic based secure routing protocol for Internet of Things. Cluster Computing, 25(3), pp.1779-1789.
25. Srinivasulu, M., Shivamurthy, G. and Venkataramana, B., 2023. Quality of service aware energy efficient multipath routing protocol for internet of things using hybrid optimization algorithm. Multimedia Tools and Applications, 82(17), pp.26829-26858.
26. Somula, R., Cho, Y. and Mohanta, B.K., 2024. SWARAM: osprey optimization algorithm-based energy-efficient cluster head selection for wireless sensor network-based internet of things. Sensors, 24(2),pp.1-19.
27. Smys, S.; Bashar, A.; Haoxiang,W. Taxonomy classification and comparison of routing protocol based on energy efficient rate. J. ISMAC 2021, 3, 96–110.
28. Rahiminasab, A., Tirandazi, P., Ebadi, M.J., Ahmadian, A. and Salimi, M., 2020. An energy-aware method for selecting cluster heads in wireless sensor networks. Applied Sciences, 10(21), pp.1-19.
29. Al-Baik, O., Alomari, S., Alssayed, O., Gochhait, S., Leonova, I., Dutta, U., Malik, O.P., Montazeri, Z. and Dehghani, M., 2024. Pufferfish Optimization Algorithm: A New Bio-Inspired Metaheuristic Algorithm for Solving Optimization Problems. Biomimetics, 9(2), pp.1-54.
30. Keum, D., Lim, J. and Ko, Y.B., 2020. Trust based multipath QoS routing protocol for mission-critical data transmission in tactical ad-hoc networks. Sensors, 20(11), pp.1-15.
31. Nor Azimah Khalid, Quan Bai, Adnan Al-Anbuky,” Adaptive trust-based routing protocol for large scale WSNS. IEEE Access 2019, 7, PP. 143539–143549.
32. Mario Pons, Estuardo Valenzuela, Brandon Rodriguez, Juan Arturo Nolazco Flores and Carolina Del Valle Soto,” Utilization of 5G Technologies in IoT Applications : Current Limitations by Inference and Network Optimization Difficulties - A Review,” Sensors, Vol. 23, 2023, PP. 1-41.
33. Su, Y., Fan, R., Fu, X. and Jin, Z., 2019. DQELR: An adaptive deep Q-network-based energy-and latency-aware routing protocol design for underwater acoustic sensor networks. IEEE Access, 7, pp.9091-9104.
34. Saba, T.; Haseeb, K.; Shah, A.A.; Rehman, A.; Tariq, U.; Mehmood, Z. A Machine-Learning-Based Approach for Autonomous IoT Security. IT Prof. 2021, 23, 69–75.
35. Haseeb, K.; Islam, N.; Almogren, A.; Din, I.U.; Almajed, H.N.; Guizani, N. Secret sharing-based energy-aware and multi- hop routing protocol for IoT based WSNs. IEEE Access 2019, 7, 79980–79988.
36. Haseeb, K.; Jan, Z.; Alzahrani, F.A.; Jeon, G. A Secure Mobile Wireless Sensor Networks based Protocol for Smart Data Gathering with Cloud. Comput. Electr. Eng. 2021, 97, 107584.
37. Rehman, A., Saba, T., Haseeb, K., Larabi Marie-Sainte, S. and Lloret, J., 2021. Energy-efficient IoT e-health using artificial intelligence model with homomorphic secret sharing. Energies, 14(19), pp.1-15.
38. DooHo Keum, Jihun Lim, and Young-Bae Ko,” A trusted low-latency multipath routing for mission-critical tactical data transfer. The Journal of . Korean Institute of Communication and Information Sciences, 2020, 45, 391–399.