International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *12 August 2023* ***Revised:*** *29 September 2023* ***Accepted:*** *16 October 2023*

Trust Score based Optimized Cluster Routing (TSOCR) approach for Enhancing the Lifetime of Wireless Sensor Networks

Sri S. Suresh Babu[1], Dr. N.Geethanjali[2]
[1]Research Scholar, CS&T,
Sri Krishnadevaraya University,
Ananthapuramu, India,
laksur.suresh@gmail.com
[2]Professor, CS&T,
Sri Krishnadevaraya University,
Ananthapuramu, India

Abstract — Energy efficiency is the most significant obstacle that Wireless Sensor Networks (WSN) must overcome, and the desire for solutions that maximize energy efficiency will nevergo away. There are a variety of methods that can be utilized to improve energy efficiency, with data transmission as the primary driver of maximum energy consumption. The transmission of data from the source to destination nodes uses more energy. When the transmission of data is handled better, the energy efficiency is improved and the lifetime of the network is increased. The purpose of this research is to propose an Trust Score based Optimized Cluster Routing (TSOCR) scheme for WSNs, which is based on Whale Optimization Algorithm (WOA). A total trust score is derived by combining the results of computing three distinct trust scores, such as the direct, indirect, and the most recent trust score. The path that has the highest trust score is chosen as the route and employed for data transmission. The effectiveness of the work is evaluated by looking at factors such as the rate of packet delivery, the latency, the amount of energy consumed and the lifetime of the network.

.

Keywords - WSN, Optimization, trust computation, energy efficiency, network lifetime.

I. INTRODUCTION

Many real-time applications make extensive use of sensor nodes due to their simple deployment and precise sensing capabilities. As stated by Sun et al. [1] and Liu et al. [2], sensors are typically used for monitoring the physical or environmental environment, allowing for climatic condition monitoring, object tracking, and localization. The primary purpose of sensor nodes in a network is to transmit sensed data to the control station, so that effective decisions can be made regarding a particular problem. However, communication between sensor nodes consumes more energy, thereby reducing the network's lifespan.

Typically, sensor networks are deployed in hostile environments where battery recharging or replacement is impossible. Therefore, the energy consumption pattern of sensor nodes must be balanced, in order to achieve energy efficiency. As stated by Yin et al. [3] and Shende and Nikhil [4], an effective communication strategy is necessary for improving energy efficiency in WSN. The sensor nodes gather environmental data and transmit it either directly to the control station or via the sink node. There are numerous methods for achieving energy efficiency, with clustering being the most effective.

The clustering concept contributes to load balancing, enabling scalability and dependable data transmission. Data transmission from source to destination can occur directly, which is faster, only when the network size is reduced. According to Kumar et al. [23] and Al Farraj et al. [24], multi-hop based routing supports larger networks more effectively. The clustering techniques can be either dynamic or static, with dynamic clustering techniques altering the network operation procedure at predetermined intervals and static clustering techniques adhering to the same node membership policy, though the Cluster Head (CH) can be altered at any time.

The CH swap is intended to conserve energy and balance the workload. The most difficult aspect of multi-hop routing is that the node closest to the Base Station (BS) uses more energy to transmit data. This may accelerate the failure or demise of nodes. This work acknowledges the significance of network lifetime and seeks to increase it by presenting an efficient route selection policy.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 12 August 2023 **Revised:** 29 September 2023 **Accepted:** 16 October 2023*

This work is based on clustering, trust theory and optimization concepts. The work objective is divided into three phases, including clustering, trust score computation and routing. The clustering phase combines nodes based on several potent metrics and computes the level of trust. Multiple routes are identified and the optimal route for data transmission is selected, which make up the main contribution of the work. The clustering process begins with the application of the Whale Optimization Algorithm (WOA). The direct and indirect trustworthiness of the nodes is computed and maintained, in order to generate more efficient routes. The optimal route from source to destination is determined by evaluating the degree of trust of each available node. The highlights of this endeavor are provided in the following section.

- The notion of clustering conserves energy and the optimization algorithm selects the best possible node as CH.
- The trust metric computation aids in determining the nature of a node, and this metric is used for route selection.
- The trustworthy route selection aids in achieving hassle-free, dependable datatransmission.

The remaining sections of this article are formatted as shown below. The second section examines and discusses existing related works on the routing process in WSN. Section 3 explains the proposed optimized routing policy, while section 4 evaluates the efficiency of the proposed work. The conclusion section of the paper is Section 5.

II. REVIEW OF LITERATURE

This section studies the trust and clustering based routing protocols of WSN in the existing literature.

Basha et al. [5] propose a secure routing protocol for WSN "Realisable Secure Aware Routing" (RSAR) that prioritizes energy efficiency via data aggregation. This work calculates the trustworthiness of all sensor nodes. The conditional tug of war optimization algorithm and optimal trust inference model are then employed. The data flow is minimized and superfluous data is eliminated. The collected data is then transmitted to the receiving side.

Yang et al. [6] present a behavior monitoring trust analysis scheme based on game theory and clustering. Evidence collection scheme is used to compute the node's trustworthiness, and clustering is also incorporated. Khalid et al. [7] propose a trust-based adaptive routing protocol for WSN. This study examines three distinct trust values, including direct, indirect, and witness trust. These calculated trust factors are contrasted pair-by-pair.

Hasan et al. [8] analyze routing policies in green Internet of Things (IoT) based on WSN using a cross-layer design. A mathematical model for computing Quality of Service (QoS) attributes to facilitate data transmission in IoT applications is presented. For analyzing the effects of multi-hop communication, a discrete-time Markov M/M/1 queuing model is employed. Analytical model and critical path-loss model are used to calculate the level of trust for the nodes that are utilized most frequently. The transmission of data relative to hop-by-hop and end-to-end nodes is analyzed.

Lyu et al. [9] present a Denial of Service (DoS)-resistant geographic routing protocol for IoT based on selective authentication. The wireless links are analyzed using statistical state information, and the trust model is constructed based on this data. A selective authentication algorithm based on entropy is used to ensure data integrity and reduce computational cost. This work eliminates duplicate data transmission and redundant signature verification. Haseeb et al. [10] present a trusted strategy for mobile wireless networks based on the Internet of Things. This endeavor is concerned with routing, data integrity, and privacy. For robust data routing, the optimal network parameters and wireless channel measurement are selected. Periodically, the location of the nodes is determined by the distance vector. This work is secured through the use of public-private key cryptography.

Sun and Li [11] present a trust-aware routing protocol with multiple attributes that consider data transmission, data, power, and suggestion. This work utilizes a sliding time window to identify anomalous user behavior. Sharma et al. [12] present a secure routing algorithm for WSN that relies on whale optimization clustering. This work determines the most reliable node to serve as the cluster's leader by weighing energy, cluster distance, latency, transmission rate, and cluster density.

Ling et al. [13] present a trust model-based routing scheme that is based on Reinforcement Learning (RL) and performs improved cluster size management. The RL monitors the activities of the users, and the security of the system is enhanced by dynamically adjusting the cluster size. Pasupuleti and Balasamy [14] present an optimized routing for WSN based on compressive sensing. Kronecker representation is utilized for data transmission, while Fractional Earthworm Optimization (FEWO) is utilized for CH selection. The CH forms multiple trajectories based on energy, trust, delay and distance.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *12 August 2023* ***Revised:*** *29 September 2023* ***Accepted:*** *16 October 2023*

Han et al. [15] present a self-healing secure key distribution scheme for IoT. A two- layer self-healing key distribution scheme for IoT objects is presented with self-healing. The first layer is responsible for providing security and access control based on polynomial-based approaches. The second layer consists of self-healing key distribution and SVD-based authentication. Kulkarni and Jesudason [16] present a multipath data transmission scheme based on Exponential Cat Swarm Optimization (ECSO) and fuzzy optimization. The Penguin Fuzzy based Ant Colony Optimization (PFuzzyACO) selects the cluster leader node, while ECSO handles routing. The optimal route is determined by weighing factors such as reliability, energy, distance, traffic and delay, among others.

Wang et al. [17] present an opportunistic routing scheme based on trust for social IoT. This work selects nodes for data forwarding based on the optimal halting concept and employs network coding for data transmission. Utilizing game theory, the trusted channel is assigned.

Hammi et al. [18] present a secure multi-path reactive protocol for the Internet of Things (IoT). This paper presents a trust-based multipath routing method. A probabilistic model takes the mobility and behavior of nodes into account. The authors of Al-kahtani et al. [19] claim that, their density cluster-based routing protocol is appropriate for emergency sensor applications. Saidi and Benahmed [20] propose a secure CH selection technique for WSN that measures the level of node trustworthiness. Multiple trust types are factored into the computation of sensor node behavior. The dubious CHs are identified and taken out of service. Djedjig et al. [21] present a trust-aware cooperative routing scheme for the security of the Internet of Things. Considering energy consumption, throughput, packet delivery rate, and so on, a trust-based routing topology construction is presented.

Motivated by these prior works, this article proposes a clustered routing scheme for WSN based on a trust metric. The primary objective of this endeavor is to ensure data transmission reliability, energy efficiency, and thus longer network lifetime.

III. PROPOSED TRUST SCORE BASED OPTIMIZED CLUSTER ROUTING (TSOCR) SCHEME FOR WSN

This section presents an overview of the proposed approach and all the involved phases are explained. Conventionally, a WSN consists of a large number of wireless sensors with limited processing capabilities. As WSNs are typically deployed for monitoring and surveillance applications, sensors are deployed in hostile environments, where node maintenance is unfeasible. Consequently, network lifetime is the primary concern that must be addressed, and it is best attained through an efficient routing policy. In addition, the WSN faces numerous security challenges, such as sybil, selective forwarding,black hole, and wormhole attacks, among others. All of these attacks compromise transmitted data through forgery or tampering.

Due to the nature of WSN, however, these security attacks cannot be managed by conventional cryptographic algorithms. Therefore, any routing algorithm must assure security, energy efficiency and dependability. The proposed work increases the network's lifetime by conserving energy using concepts such as optimized clustering and trust concepts. This proposed TSOCR algorithm optimizes the entire clustering process and the trust-based computation is performed. The routes are then formed and selected based on the trust score.

A. Optimized Clustering Phase

This phase is based on Whale Optimization Algorithm which is bio-inspired and is designed to imitate the behavior of whales. In most cases, whales attack a pool of fishes by blowing out bubbles that encircles the pool. The whales take two different approaches to catch the fish, which are called exploitation and exploration. The fish is surrounded by the exploitation step, while the exploration step searches for the fish in a more haphazard manner. The following illustration depicts the behaviors of whales in their environment.

$$P = \left|\overrightarrow{C_1}.\vec{X}^*(i) - \vec{X}(i)\right| \quad (1)$$

$$\vec{X}\,(i+1) = \vec{X}^*\,(i) - \overrightarrow{C_2} * P \quad (2)$$

In the above equations, i indicates the current iteration, $\vec{X}^*$ is the achieved optimal result and $\vec{X}$ denotes the position vector. The coefficient vectors are denoted by $\overrightarrow{C_1}$ and $\overrightarrow{C_2}$, which are calculated by the following equations.

$$\overrightarrow{C_2} = 2\,\overrightarrow{C_2} * \overrightarrow{rd} - \overrightarrow{C_2} \quad (3)$$

$$\overrightarrow{C_1} = 2 * \overrightarrow{rd} \quad (4)$$

In equations (3 and 4), the $\overrightarrow{C_2}$ decreases with increasing iterations and $\overrightarrow{rd}$ is the random vector, which lies in between 0 and 1. The whales tend to relocate themselves with respect to the location of the food availability on the basis of eqn.(3) and the location is taken care of by $\overrightarrow{C_1}$ and $\overrightarrow{C_2}$. As stated earlier,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *12 August 2023* ***Revised:*** *29 September 2023* ***Accepted:*** *16 October 2023*

the food stuffs of whale is encircled by reducing the $\overrightarrow{C_2}$, as shown in eqn.(5).

$$\overrightarrow{C_2} = \frac{2-2i}{Grt_i} \quad (5)$$

In the above equation, i represents the total number of iterations and Grt_i is the greatest number of iterations. The location of the neighbouring whale is calculated by considering the distance between the whales a and b, as given in the following equation.

$$\vec{X}(i+1) = P' \cdot d^{csrv} \cdot \cos(2\pi rv) + \vec{X}^*(i) \quad (6)$$

In eqn.(6), $P' = |\vec{X}^*(i) - \vec{X}(t)|$ indicates the distance between the n^{th} whale and the found optimal food source, cs is the constant that represents the curve and rv is the random number lies in the range from -1 to 1. The food source location and the path formation are carried out by means of a probability (prb) of 0.5, as represented in the following equation.

$$\vec{X}(i+1) = \begin{cases} \text{Encircling food source eqn. (2) when prb} < 0.5 \\ \text{path formation eqn. (6)} \quad \text{when prb} \geq 0.5 \end{cases} \quad (7)$$

In equation (7), prb is a random value lies in between 0 and 1. In the exploration step, the whales are selected randomly to search for the food source. The vector $\overrightarrow{C_1}$ with random numbers explores the best possible neighbouring whale as denoted by the following equations.

$$\vec{P} = \left|\overrightarrow{C_1} . \overrightarrow{X_{rd}} - \vec{X}\right| \quad (8)$$

$$\vec{X}(i+1) = \overrightarrow{X_{rd}} - \overrightarrow{C_2} . \vec{P} \quad (9)$$

$\overrightarrow{X_{rd}}$ is the whale selected randomly.

Hence, the functionality of WOA algorithm is explained and the CH is selected with the help of this algorithm, which is as follows.

B. CH Node Selection

The functioning of CH nodes is the foundation of the clustering paradigm. Several of the published works concentrate on energy and packet delivery rate as the primary criteria for choosing the CH node. The WOA algorithm is utilized in this study for the purpose of selecting the CH node. The fitness value of the method is determined with the assistance of the trust mechanism. The trust metrics of energy, packet transmission, distance, delay, and node density are all taken into consideration in this work. The following equation can be used to determine the fitness function that will be used for the selection of CH.

$$\text{Fit}_{\text{fn}}(\text{CH}) = \frac{\text{SN}_\text{e} \times \text{SN}_\text{pt}}{\text{SN}_\text{d} \times \text{SN}_\text{dn} \times \text{SN}_\text{cdis}} \quad (10)$$

Here, SN_e and SN_{pt} stand for remaining energy of the node after the completion of data transmission. SN_d denotes the delay being experienced during data transmission and SN_{dn} represents the density of nodes, which is the total count of member nodes in a cluster. SN_{cdis} is the cluster distance of a node from other nodes in the cluster and this is computed as follows.

$$\text{SN}_\text{cdis} = \frac{\sum_{\text{i=1}}^{\text{TN}-1}(\text{Dis}(\text{CL}_\text{a}, \text{CL}_\text{i}))}{\text{TN}} \quad (11)$$

In the above equation, TN is the total count of nodes in a cluster $CL.(CL_a, CL_i)$ denotes the distance between a specific node a with the remaining nodes of the cluster. All the nodes are processed and the node with greatest $Fit_{fn}(CH)$values are recommended to play the role of CH. The algorithm of cluster node selection is presented as follows.

CH Selection Algorithm

Input : Sensor nodes
Output : Node cluster Begin
Deploy sensor nodes;
Apply TSOCR to choose CH by $Fit_{fn}(CH)$*;*
Forward $List_{CH}$ *to all nodes;*
Compute distance from node to the CH;
Join the cluster with minimal distance;
CH builds TDMA for data forward to member nodes;Forward data during allotted slot;
End;

As soon as the fitness is calculated, the list of CH nodes ($List_{CH}$), is forwarded to every node of the network. After computing the distance between itself and the other nodes in $List_{CH}$, each node then joins the cluster that includes the minimum amount of distance between the nodes. After all of the nodes have joined a cluster, the CH generates a Time Division Multiple Access (TDMA) slot and then distributes it to the nodes that are part of the cluster. The pressure on the CH is lessened, since the member nodes can only send data to the CH within the time slot that has been allocated to them. This study makes use of 500 nodes spread across 1000×1000 m^2 and results in the formation of ten clusters. The following equation can be used to calculate the amount of

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *12 August 2023* ***Revised:*** *29 September 2023* ***Accepted:*** *16 October 2023*

energy needed for data transmission and reception, taking into account distance (dis) and data (r).

$$Tns_{Erg} = (EC_{Erg} \times r) + TA_{Erg} \times r \times dis^2 \quad (12)$$

$$Rcp_{Erg} = EC_{Erg} \times r \quad (13)$$

The values for Tns_{Erg} and Rcp_{Erg} represent the amount of energy used for transmitting and receiving data, respectively. The energy consumption of an electronic circuit is denoted by the EC_{Erg} variable, while the energy consumption of a transmitter amplifier is denoted by the TA_{Erg} variable. As a result, the process of clustering is carried out with the assistance of the clustering algorithm in conjunction with the trust-based idea. This procedure is carried out once every 180 seconds, after which the node with the best characteristics is chosen to be the CH. The procedure for data transfer is broken down into the following sections.

C. Data Transmission

As stated previously, data can only be transmitted to the CH during the allotted time window. This concept reduces unwelcome communication perplexity, as the CH may become inundated with messages. The CH node accumulates all data from member nodes according to a predetermined timetable. In order to keep account of energy consumption, the total amount of energy spent on data transmission is computed. This work returns multiple routes from source to destination, from which the most reliable route is selected. The trust metric is used to determine the optimal course of action. The transmission of data algorithm is demonstrated below.

Data Transmission Algorithm

Input : *Nodes with data transfer request*
Output : *Data transmission*
Begin
//CH
CH computes $Trst_{scr}$ of all nodes;Save $Trst_{scr}$;
Receive data transmission request;
Form multiple routes from source and destination;Choose the route with greatest $Trst_{scr}$;
Transmit data;
End;

The trust score is calculated by the neighboring nodes and is periodically updated. This work considers direct, indirect, and most recent sensor node trust scores when determining the optimal path. When multiple routes are identified, the route with the highest trust score is selected as the final route. This concept enhances the work's dependability while enhancing routing performance with minimal delay and overhead. On the other hand, the energy consumption is reduced to increase the network's lifespan. In addition, the incorporation of the trust concept ensures the implicit security of the routing algorithm. All nodes are continuously monitored to assure the computation of the trust score. The calculation of the trust score is explained in the following section.

C. Trust Score Computation for route selection

This work's trust score is based on three distinct types of trust : direct, indirect, and the most recent trust score. The trust-based concept is gaining popularity due to its dependability and superior performance. This work computes and adds together three distinct trust scores.

$$Trst_{scr} = Trst_1 + Trst_2 + Trst_3 \quad (14)$$

In equation (14), $Trst_1$, $Trst_2$, $Trst_3$ correspond to the most recent, direct and indirect trust scores respectively. The recent trust score is the sum of the node's direct and indirect trust scores and reflects its current behavior. The most recent trust of node y as computed by node x is as follows.

$$Trst1 = \alpha Trst2 + (1 - \alpha)\mathrm{T}rst3 \quad (15)$$

As node y contains the interaction count with node x, which emphasizes the trustworthiness of node y with respect to x, $Trst_2$ has a greater weight. α is the calculated weight value based on the total number of interactions and the average number of interactions between y and x nodes. The direct trust $Trst_2$ is computed based on the interaction behavior of node y with another node, as represented by

$$Trst_2 = \frac{1}{NHN} \sum_{\substack{x \in y}}^{NHN} x = y Com_{exp}(y, x) \quad (16)$$

The following equation determines the node's communication experience.

$$Com_{exp}(y, x) = \frac{\delta\,(y,x)}{TN} \quad (17)$$

In the above equation, $(y,\ x)$ denotes the successful interaction between the nodes y and x, TN is the total number of nodes. The indirect trust is calculated on the basis of the interaction experience of the neighbourhood nodes and is presented as follows.

$$Trst_3 = \frac{1}{NHN * NHN_1} \sum_{\substack{y \in x}}^{NHN} x = 1 \sum_{\substack{z \in y}}^{NHN_1} z = 1\ Com_{exp}\,(y, z) \quad (18)$$

NHN and NHN_1 represent the neighbouring nodes of the y and x nodes, respectively, in equation (18). Therefore, $Trst_{scr}$ selects the optimal path from all available paths between the source and destination. Once the available paths

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *12 August 2023* ***Revised:*** *29 September 2023* ***Accepted:*** *16 October 2023*

between the source and destination have been returned, the trust scores of the nodes along the path are computed and $Trst_{scr}$ is sorted in descending order. The path with the highest $Trst_{scr}$ score is selected as the final path. The effectiveness of the proposed task is evaluated in the section that follows.

IV. RESULTS AND DISCUSSION

NS3 is used to simulate the proposed Trust Score based Optimized Cluster Routing (TSOCR) scheme. The area under consideration is $1000 \times 1000\ m^2$ with 500 nodes. Certain abnormal nodes that lack an interest in data forwarding are arbitrarily distributed. The sensor nodes are mobile using a model of random mobility. Here, the sensor node begins at a particular location and travels to its destination. The BS does not move and remains immobile. Table 1 displays the simulation parameters used in this study.

Table. 1 Simulation parameters

Simulation Parameters	Values
Packet Length	4496 bits
Utilized energy for data transmission and reception	50 nJ/bit
Utilized energy for datacollection	5×10^{-9} J
Pause time interval	0.01 s

The performance of the proposed work is analyzed with respect to the performance measures such as packet delivery rate, average latency, energy consumption and network lifetime. The performance of the work is compared with the existing approaches such as trust based, multipath data and secure WSN, proposed by Khalid et al. [7], Kulkarni and Jesudason [16], Saidi and Benahmed [20] respectively.

The attained results are shown in the following figures from 1 to 4.

4.1 Packet Delivery Rate Analysis

This is the most crucial efficiency indicator for any routing algorithm. The primary objective of routing is to deliver messages from source to destination in a secure manner. In certain instances, the sensor node may not be interested in forwarding packets, which reduces the rate of packet delivery. When the rate of packet delivery is low, it makes sense for a node not to forward incoming packets. The results are depicted in figure 1 below.

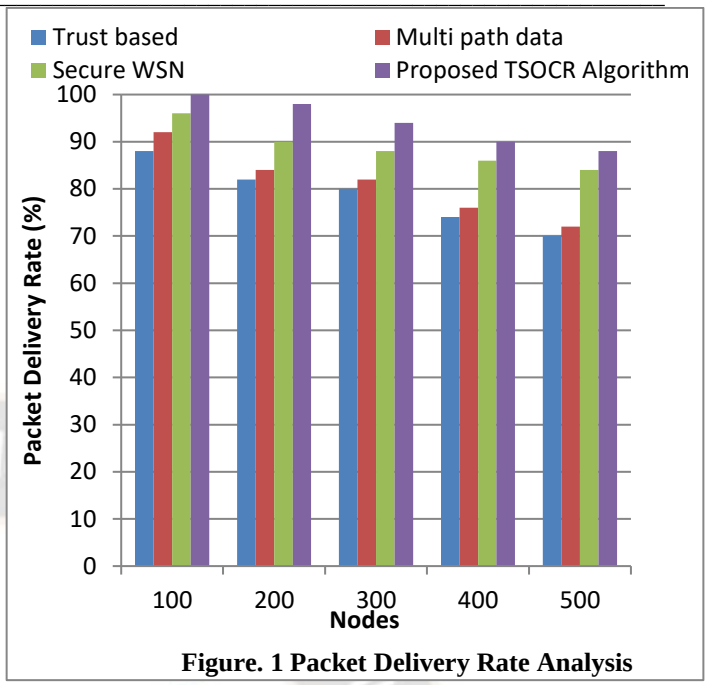

Figure. 1 Packet Delivery Rate Analysis

When carrying out this study, the number of nodes that are counted range from 100 to 500. According to the findings, it is clear that the planned work has an acceptable packet delivery rate, when measured against the existing works. It has been found that the delivery rate would slow down as the number of nodes increases; yet, this is acceptable. The following section illustrates an examination of the latency caused by the proposed work.

4.2 Average Latency Rate Analysis

This section provides an analysis of the latency rate of the proposed work. Latency refers to the amount of time it takes to send a packet to its intended destination. In order to improve routing performance, it is important that any routing algorithm experiences just a minimal amount of latency. The results of the latency test can be seen in figure 2.

The analysis of latency is carried out by shifting the number of nodes in the network from 100 to 500, with the latency being measured in seconds. The rate of latency grows proportionally with the number of sensor nodes in a network. However, the delay is somewhat manageable in contrast to other works. When there are 500 nodes, the network experiences a delay rate that is 18 seconds at its longest point. The analysis of the Energy Consumption Analysis is presented in the following section.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *12 August 2023* ***Revised:*** *29 September 2023* ***Accepted:*** *16 October 2023*

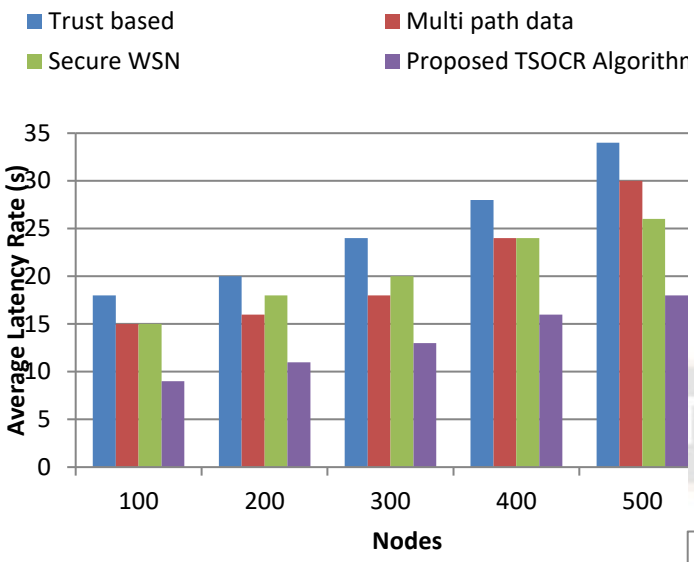

Figure. 2 Average Latency Rate Analysis

4.3 Energy consumption analysis

The amount of energy consumed by the proposed work is analyzed here. In order to lengthen the amount of time that a network is operational, the energy consumption of the routing algorithm must be kept to a minimum. At the beginning, all of the nodes are given the same amount of energy, and the rate at which their energy decreases is determined by the tasks that have been assigned to them. When calculating the amount of energy used, the number of seconds spent running the simulation is taken into account. Figure 3 presents the findings on the amount of energy that was consumed.

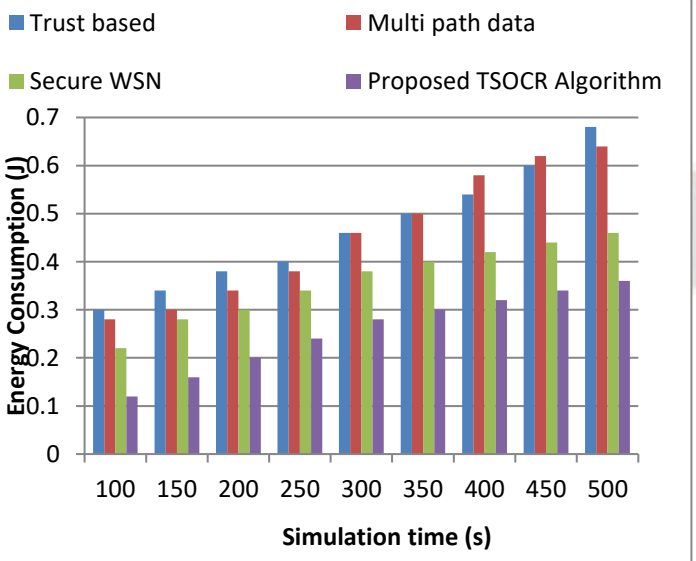

Figure. 3 Energy Consumption Analysis

The work that is being proposed has an energy consumption of 0.36 J at the 500th second, which is closely followed by the use of secure WSN. The longer the network can function with a lower overall energy consumption, the more reliable it will be. The discussion of the lifetime analysis continues in the next section.

4.4 Network lifetime analysis

In order to accomplish the intended goal, the lifetime of the network needs to be as long as it possibly can be. Utilizing a variety of different strategies, such as clustering, duty cycling, sleep cycle scheduling and so on, can be used to lengthen the lifespan of a network. The lifetime analysis of the network is analyzed, and the results are shown in figure 4

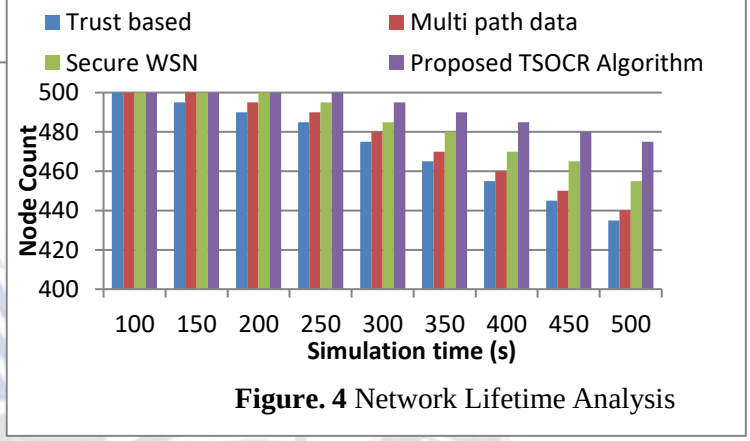

Figure. 4 Network Lifetime Analysis

Figure 4 provides an analysis of the network lifetime of the work that was proposed by calculating the total number of live nodes in relation to the amount of time spent simulating. When the simulation time is increased, the number of live nodes will decrease proportionately. In contrast to the methods that have been used previously, the proposed study results in a significantly lower rate of death among the network's nodes. The solution that has been suggested utilizes 475 nodes during the 500th second of simulation. As a result, the work that has been proposed guarantees reliable routing with improved network lifetime.

V. CONCLUSION

This article offers an improved and trustworthy routing strategy for WSN. The suggested routing strategy has a number of goals, the primary one of which is to assure energy efficiency and as a result, increase the network's lifetime. This effort is dependent on the successful completion of three significant steps, namely clustering, trust computation, and routing. During the clustering phase, the WOA optimization method is used to choose the CH. During the trust computation phase, direct, indirect, and most recent

trust are computed. The trust scores of all of the alternative paths are taken into consideration by the routing strategy, and the transmission of data is directed down the path with the highest trust score. In the future, this work could be improved by doing an analysis of its performance using several different metaheuristic methods.

REFERENCES

[1] Sun, B., Guo, Y., Li, N., Peng, L., & Fang, D. (2016). TDL: Two-dimensional localization for mobile targets using compressive sensing in wireless sensor networks. Computer Communications, 78, 45-55. https://doi.org/10.1016/j.comcom.2015.10.006

[2] Liu, X., Li, J., Dong, Z., & Xiong, F. (2017). Joint design of energy-efficient clustering and data recovery for wireless sensor networks. IEEE Access, 5, 3646-3656. Doi: 10.1109/ACCESS.2017.2660770.

[3] Yin, J., Yang, Y., Wang, L., & Yan, X. (2016). A reliable data transmission scheme based on compressed sensing and network coding for multi-hop-relay wireless sensor networks. Computers & Electrical Engineering, 56, 366-384. https://doi.org/10.1016/j.compeleceng.2015.12.025

[4] Shende, D. K., & Nikhil, S. (2018). IoT based geographic multicast routing protocol with DPA through WSN. Internat Journal Creative Research Thoughts, 6, 578-84.

[5] Basha, A. R. (2020). Energy efficient aggregation technique-based realisable secure aware routing protocol for wireless sensor network. IET Wireless Sensor Systems, 10:166-174. DoI: 10.1049/iet-wss.2019.0178

[6] Yang, L., Lu, Y., Liu, S., Guo, T., & Liang, Z. (2018). A dynamic behavior monitoring Game-Based trust evaluation scheme for clustering in wireless sensor networks. IEEE Access, 6, 71404-71412. DoI: 10.1109/ACCESS.2018.2879360

[7] Khalid, N. A., Bai, Q., & Al-Anbuky, A. (2019). Adaptive trust-based routing protocol for large scale WSNs. IEEE Access, 7, 143539-143549. DoI: 10.1109/ACCESS.2019.2944648

[8] Hasan, M. Z., Al-Turjman, F., & Al-Rizzo, H. (2018). Analysis of cross-layer design of quality-of-service forward geographic wireless sensor network routing strategies in green internet of things. IEEE Access, 6, 20371-20389. DoI: 10.1109/ACCESS.2018.2822551

[9] Lyu, C., Zhang, X., Liu, Z., & Chi, C. H. (2019). Selective authentication based geographic opportunistic routing in wireless sensor networks for Internet of Things against DoS attacks. IEEEAccess,7,31068-31082.DoI: 10.1109/ACCESS.2019.2902843

[10] Haseeb, K., Din, I. U., Almogren, A., Islam, N., & Altameem, A. (2020). RTS: A Robust and Trusted Scheme for IoT-based Mobile Wireless Mesh Networks. IEEE Access, 8, 68379-68390. DoI: 10.1109/ACCESS.2020.2985851

[11] Sun, B., & Li, D. (2017). A comprehensive trust-aware routing protocol with multi- attributes for WSNs. IEEE Access, 6, 4725-4741. DoI: 10.1109/ACCESS.2017.2786944

[12] Sharma, R., Vashisht, V., & Singh, U. (2020). WOATCA: A secure and energy aware scheme based on whale optimisation in clustered wireless sensor networks. IET Communications, 14(8), 1199-1208. DoI: 10.1049/iet-com.2019.0359

[13] Ling, M. H., Yau, K. L. A., Qadir, J., & Ni, Q. (2018). A reinforcement learning-based trust model for cluster size adjustment scheme in distributed cognitive radio networks. IEEE Transactions on Cognitive Communications and Networking, 5(1), 28-43. DoI: 10.1109/TCCN.2018.2881135

[14] Pasupuleti, V. R., & Balaswamy, C. (2020). Optimised routing and compressive sensing based data communication in wireless sensor network. IET Communications, 14(6), 982-993. DoI: 10.1049/iet-com.2019.0130

[15] Han, S., Gu, M., Yang, B., Lin, J., Hong, H., & Kong, M. (2019). A Secure Trust-Based Key Distribution With Self-Healing for Internet of Things. IEEE Access, 7, 114060-114076. DoI: 10.1109/ACCESS.2019.2935797

[16] Kulkarni, P. K. H., & Jesudason, P. M. (2019). Multipath data transmission in WSN using exponential cat swarm and fuzzy optimisation. IET Communications, 13(11), 1685-1695. DoI: 10.1049/iet-com.2018.5708

[17] Wang, X., Zhong, X., Li, L., Zhang, S., Lu, R., & Yang, T. (2020). TOT: Trust aware opportunistic transmission in cognitive radio Social Internet of Things. Computer Communications, 162, 1-11. DoI: https://doi.org/10.1016/j.comcom.2020.08.007

[18] Hammi, B., Zeadally, S., Labiod, H., Khatoun, R., Begriche, Y., & Khoukhi, L. (2020). A secure multipath reactive protocol for routing in IoT and HANETs. Ad Hoc Networks, 102118. DoI: https://doi.org/10.1016/j.adhoc.2020.102118

[19] Al-kahtani, M. S., Karim, L., & Khan, N. (2020). ODCR: Energy Efficient and Reliable Density Clustered-based routing protocol for emergency sensor applications. Applied Computing and Informatics. DOI: 10.1016/j.aci.2020.03.003

[20] Saidi, A., & Benahmed Pr, K. (2020). Secure cluster head election algorithm and misbehavior detection approach based on trust management technique for clustered wireless sensornetworks. AdHo Networks, 102215. DoI: https:// doi.org/ 10.1016/ j. adhoc. 2020.102215

[21] Djedjig, N., Tandjaoui, D., Medjek, F., & Romdhani, I. (2020). Trust-aware and cooperative routing protocol for IoT security. Journal of Information Security and Applications, 52, 102467. https://doi.org/10.1016/j.jisa.2020.102467

[22] Jahangiri, M., Hadianfard, M. A., Najafgholipour, M. A., Jahangiri, M., & Gerami, M. R. (2020). Interactive autodidactic school: A new metaheuristic optimization algorithm for solving mathematical and structural design optimization problems. Computers & Structures, 235, 106268. DoI: https://doi.org/10.1016/j.compstruc.2020.106268

[23] Kumar, M.H., Mohanraj, V., Suresh, Y. et al. (2020). Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in WSN. J Ambient Intell Human Comput.https://doi.org/10.1007/s12652-020-02007-w

[24] AlFarraj, O., AlZubi, A. & Tolba, (2018). A. Trust-based neighbor selection using activation function for secure routing in wireless sensor networks. J Ambient Intell Human Comput. DoI: https://doi.org/10.1007/s12652-018-0885-1