Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777605

# LIFETIME ENHANCEMENT OF EFFICIENT ENERGY FOR RELIABLE WIRELESS SENSOR NETWORK USING SWARM INTELLIGENCE OPTIMIZATION

**Shweta Sharma[1] Amandeep Kaur[2]**
[1]Goswami Ganesh Dutta Sanatan Dharma College, Chandigarh
[1,2]Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab, 140401, India
Mail.ID: shweta.sharma@ggdsd.ac.in

**Abstract**
Current technological and manufacturing advancements have made it possible to create compact, powerful, energy-efficient, cost-effective sensor nodes that are "smart" enough to be capable of adaptability, self-awareness, and self-organization. These nodes are intended for generalised telecommunication applications. In sensor networks for sustainable development, it is looked at how sensor network technologies increase social development and living quality while having little to no detrimental effects on the environment or the planet's natural resources. In a wide range of applications, such as the military, healthcare, traffic monitoring, and remote image sensing, wireless sensor networks (WSNs) are unquestionably advantageous. Due to the limits of sensor networks, different levels of security are required for these crucial applications, making it challenging to employ traditional algorithms. Security has arisen as one of the main problems with IoT and smart city applications, and sensor networks are also considered of as the cornerstone of IoTs and smart cities. A routing algorithm, network strength, packet loss, energy loss, and other complicated concerns are covered by the WSN. Other complex issues covered by the WSN include energy consumption, an efficient method for selecting cluster heads, and other issues. Because of the unique characteristics and constraints of nodes, it is now more challenging to provide trustworthy and reliable data since the recent development of WSNs. The integrity of the network can be readily compromised by hostile nodes through the insertion of false and malicious data as well as the initiation of internal assaults. To identify rogue nodes, trust-based security is used, which offers a powerful and mobile defence. Trust evaluation models are an essential security-enhancement technique for boosting sensor node dependability (cooperation) in wireless sensor networks. The unique trust approach DFA U-Trust is recommended by this study to address the security requirements of WSNs.
Keywords: Trust, Dragonfly, K-means, Lifetime enhancement, Sustainability

## 1. INTRODUCTION

A system of sensor nodes known as a wireless sensor network sends the data required by the network. WSN is used in many applications, such as weather forecasting, the military, underwater research, etc., for the accumulation of secure data. [1][2][3]. A sensor node is made up of a transceiver, external memory, microcontroller, power source, and one or more sensors. Once deployed, the sensor node's battery cannot be changed. As the energy level drops, so does the node's performance. Eventually, the sensor node with the empty battery expires, cutting off all communication with other nodes in the network. A summary of network lifetime due to higher energy use [4][5].

Usage of Energy ⬆ Lifetime of Network ⬇

Energy should be conserved in order to boost network efficiency and consequently lengthen the network's useful life. There are numerous methods for improving longevity and energy efficiency. The management of trust is one strategy.

**1.1 System of Trust Management**

What is the definition of the word "trust"? is the main query. A conviction or certainty that something is true can be used to define trust. believe in something or someone's goodness, talent, or organisation. Another definition of trust is the prospect that nodes whose behaviour cannot be controlled may behave in a way that is advantageous to the network. One could claim that there is a good link between the two nodes that one can trust [7][8]. The two essential components of trust management are Trust or, the person in whom something is trusted, and Trustee, the person in whom one can have confidence. To determine if a node is reliable or not, each node in the network must be inspected, and each node must participate in this process. The main objective of a trust management system is to distinguish between trustworthy and trustworthy nodes in the network. The faulty nodes are removed from the network, leaving only the trustworthy nodes. The possibility that faulty nodes will increase network latency, energy consumption, throughput, and longevity justify this exclusion.

Network services can be delivered without issue if they are based on trustworthy data. As a result, a system must determine the reliability of a data item before further processing and sending it across the network. Unreliable information is ignored, and the source is rated as less reliable. In order to minimise potential harm, it is essential to assess the reliability of data as soon as is practical. This will prevent doubtful information from being processed further. The centralised analysis performed by a dedicated node may cause poor performance and an excessive concentration of network traffic in large networks. Being that each node in the network is required to take part in the evaluation of trustworthiness and make credibility-related decisions. [9][10]. From the perspective of a WSN, trust is the decision to accept a message after confirming the validity of the data and the message's source.

In the network, a node can act as both a trustee and a trustor: for departing data, it adopts the trustee position, allowing other nodes to decide if it can be accepted; for entering communication, it can act as a trustor, determining the sender's dependability in real-time. The relationship between the trustee and the trustor is shown in figure 1.

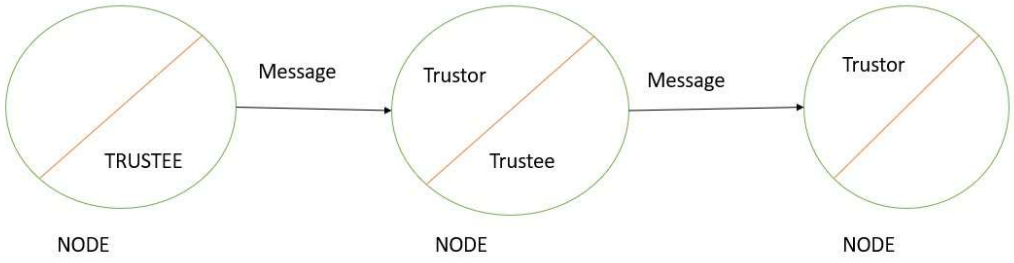


**Figure 1**: Idea of Trustor and Trustee role

Since the receiving node (the trustor) determines if the message is trustworthy and authentic at the time of delivery, a trustee is always a notification sent by one node to another.

### 1.2 Trust Management Model Working

The fundamental tenet of the trust management paradigm is that every node uses a scale known as the "Trust Scale" in some way. Three typical values that can be considered in relation to this scale are a complete trust level node that is 100% dependable, the initial trust level, and the cut-off level [11]. The phrase "initial trust level" refers to the degree of trust placed in a node when it first enters the network and its trustors have no other supporting data about its dependability. The level of confidence below which a node is regarded as unreliable is known as the "cut-off level".

Figure: 2 states about the status of nodes at different trust levels.

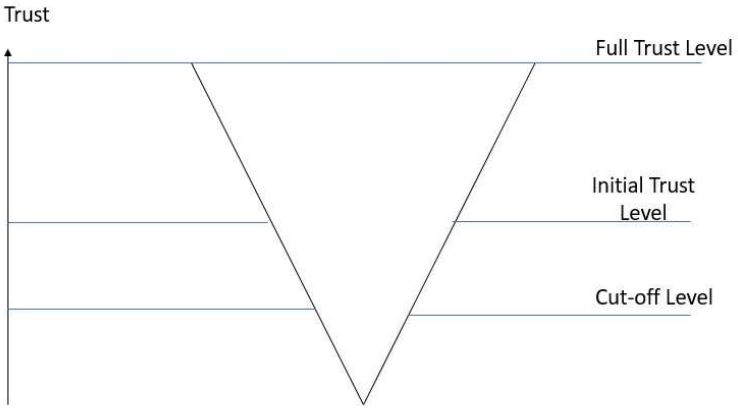


**Figure 2**: The Trust Scale

Each node is required to take part in the trust management process and maintain up-to-date records of other nodes' reputations. This data structure leads to the creation of the Trust Table. Based on the trust scale, a trust value is assigned to each record in the trust database. Table1 can be used to display a fake example of a trust table based on the example network for node1.

| ID of Node | Value of Trust |
|---|---|
| 9 | 0.51 |
| 11 | 0.66 |
| 13 | 0.74 |
| 17 | 0.48 |

**Table 1**: Dummy example of Trust values of different nodes in the network

A node can approve any other node than itself based on entries in the trust table. Recommendation is the name of this procedure [6]. On the basis of this, a model that generates the trust table and contains information about each node in the network can be built. The following entities, which could function as components of the trust table, additionally contain each node, message, trust table item, and node's reputation. Cycles are used to execute the model, and each cycle consists of two phases: the data phase and the recommendation phase.

The following is a summary of the contributions made by this paper:

i. The examined literature indicates that there is room for both the usage of SI algorithm architecture and machine learning architecture to advance sensor node trust.

ii. The study's recommended work design and execution, as well as the trust model that has been developed against the sensor nodes, are provided.

iii. The intention is to build a network with a high trust factor so that resources won't be wasted and the network can function for a long time.
iv. The proposed approach is evaluated against reward-based routing methods using the QoS metrics of throughput, PDR, and latency.

Table 2 illustrates the notations used in the paper.

| ABBREVIATIONS | DEFINITION |
|---|---|
| **WSNS** | Wireless Sensor Networks |
| **IOT** | Internet of Things |
| **DFA_U-TRUST** | Dragonfly Algorithm Updated-Trust |
| **SI** | Swarm Intelligence |
| **QOS** | Quality of Service |
| **PDR** | Packet Delivery Ratio |
| **ESRT** | Energy aware and secure routing with trust |
| **R-AODV** | Reliable AODV |
| **TLB-AODV** | Light weight trust-based routing protocol |
| **AF-TNS** | Activation function based trusted neighbour selection |
| **EATSRA** | Energy aware trust based secure routing algorithm |
| **BTEM** | Belief based trust evaluation mechanism |
| **ADT** | Authentication based data trust |
| **HRFCHE** | Hyper exponential reliability factor-based cluster head election |
| **MPOTFEM** | Markov Process-based opportunistic trust factor estimation mechanism |
| **ATRM** | Agent based trust and reputation management scheme |
| **PLUS** | Parameterized and localized trust management scheme for sensor network security |
| **TRGR** | Trust management scheme for resilient geographic routing |
| **TBGRS** | Trust based geographical routing scheme |
| **STE** | Statistical trust establishment in WSNs |
| **TCFL** | Trust model using fuzzy logic |
| **BNWSN** | Bayesian network trust model for WSNs |
| **RFSN** | Reputation based framework for sensor networks |
| **TLEACH** | Trust based leach |
| **BRMSN** | Behaviour reputation method for sensor networks |
| **TTSN** | Task based trust management for WSN |
| **HTRM** | Hybrid trust and reputation management |
| **GTMS** | Group based trust management scheme |
| **DTMS** | Data trust management scheme |
| **LSTM** | Long short-term memory |

**Table 2**: Abbreviations

The rest of the article is written in the following way. Section 2 illustrates the related work. Section 3 states the problem statement. Section 4 presents the detailed work architecture of the

proposed algorithm. Section 5 contains the result and analysis. Section 6 gives the conclusion and future scope.

## 2. RELATED WORK

Over time, there has been a revolution in the way that WSN sensors are designed. The development of sensors is taken into account, including their light weight, small size, and low power consumption. Battery depletion, which causes a delay in sensing and transmitting data, however, continues to be a major problem. The research into various ways to assure network stability and reduce consumption of energy and end-to-end delay throughout data transfer has accelerated because to the growing effect of WSN in practical applications. Concept of trust management also played an important role over the time.

The existing work illustrates the various trust management techniques and models being used in the field of WSN.

The author discussed the concept of trust models, which are further divided into three types: "centralised," where the focus is on the head node of the network, which undertakes the job of determining the trustworthiness of node based on the trust data it has gathered on its own or by data provided by all other nodes in the network; secondly, "hierarchical," where the network is divided into groups called clusters, and it is the responsibility of cluster head to determine whether a node is trustworthy; and In a nutshell, this study outlines the lifespan risks, network limits, and nodes' capabilities, the network restrictions and the risks involved in terms of lifetime and bandwidth of network in order to design and implement the trust model for enhanced security [12].

Along with the success that WSN has achieved through its trust model, numerous attacks on these trusted models are also covered. The effectiveness of the trust paradigm is decreased by these attacks. Attacks such as "bad mouthing," "On-Off," "selective behaviour," "Sybil," and "newcomer," among others. The development of the trust model for WSN is explained along with a set of best practises. Best practises include taking into account trust and reputation, trust and the base station, first-hand and second-hand information collection, initial values, granularity, updating and ageing, risk and importance, as well as trust and reputation. It has been determined via the examination of various trust management strategies that a set of best practises should be taken into consideration in order to create a successful trust model for WSN [13].

The various trust models for conventional WSNs and clustered WSNs were examined by the authors. Two types of trust models, namely Node trust models and Data trust models, are accessible for common WSNs [14].

The new technique, dubbed ESRT, was put out by the authors. It is a novel trust- and energy-based routing protocol that provides effective flexibility against the malfunctioning nodes and their behaviours encountered while forwarding packets.

This method considers dispersed trust. When they are shown to varying numbers of problematic nodes and shifting network demand, the simulation shows that ESRT performs better than existing solutions like R-AODV and TLB-AODV [15].

The authors discussed their work on the data trust model and how they developed methodologies for defect identification and data restoration using data correlation techniques. [16]. This study proposes AF-TNS to enhance network security for resource-constrained

WSNs. The AF-TNS functions in two phases: trust evaluation with a restricted energy and metric-based node evaluation. This ensures that the neighbours' degree of trustworthiness is maintained. The random Tran sigmoid function uses trustworthy node to ensure network performance and untrusted node to simplify the challenging decision-making process in the AF. The simulation's findings indicate that AF-TNS both lengthens the lifespan of networks and increases the possibility that harmful behaviour would be discovered. The experimental results show that the AF-TNS technique guarantees a minimum of 8.5 seconds of latency, 8.53 J of energy, 149 kbps of throughput, and 390 seconds of network lifetime when delivering network information. It also has a lower false detective rate of 1.5% [17].

The new secure routing algorithm EATSRA is introduced and used in this work to give WSNs the best and safest routing possible. In this method, the trust ratings are utilised to more accurately identify attackers in WSN while the decision tree-based routing algorithm is used to select the best and most secure path. Furthermore, spatial-temporal constraints have been used to improve routing decisions. The suggested EATSRA has been shown to operate better through simulation-based testing by using less energy and enhancing security and packet delivery ratio [18].

In this research [20], an effective BTEM approach is put forth to protect against internal attacks and weak nodes. Bayesian estimation is used to collect the direct and indirect trust ratings of each sensor node, and data correlation is done to further narrow down the pool of reliable nodes from which to transfer data packets. According to simulation data, the rate of false positive detection is increased in addition to the identification and subsequent isolation of problematic nodes. It is more capable of fending off attacks than other algorithms like AF-TNS [17] and Trust Doc [19].

Thanks to the ADT's integration, the system is now safe and secure. Equation for Scheduler-based Node Trust integration is projected to improve performance in terms of transmission overhead; a clustered approach Interdependence between trusted nodes has been created using the scheduling technique. The incorporation of job scheduling techniques has improved the capacity of trustworthy nodes to manage resources and memory. This approach allows nodes to manage memory and computation resources. When data trust and cryptographic approaches are coupled, communication is more dependable. To reduce the packed transmission overhead, the suggested solution used the intra-cluster (CM) and inter-cluster (CH) approaches [21].

A prediction approach that incorporates energy and trust assessment to increase network lifetime is the HRFCHE via Semi-Markov scheme. Because HRFCHE extends network longevity and reduces energy consumption by 28% and 34%, respectively, it outperforms rival cluster head election procedures [22].

The proposed MPOTFEM is a robust approach for selecting the appropriate CH based on the use of an opportunistic parameter. This suggested MPOTFEM scheme includes the Markov chain and the Preventive Maintenance (PM) concept to assess the network maintenance quality. We find that wicked nodes do not become CHs by limiting the number of CH elections. The simulation results show that the recommended technique performs better than the current ones in keeping the network's average live and dead node percentages at 10.82% and 11.36%, respectively. The results show that the recommended method can provide average improvements in PDR and Throughput of 9.14% and 10.56% compared to the commonly utilised CH election processes [23].

LEACH-TM, a hierarchical routing system that is energy-efficient and based on trust management, is suggested in this work as a contribution. This method has the advantages of boosting network accessibility, extending network lifespan, and enhancing network threat resistance. In order to increase energy efficiency and prevent excessive node energy consumption, it is possible to better limit the cluster's size by taking into account the number of dynamic decision cluster head nodes and the density of nearby nodes. The results of the simulation demonstrate that the LEACH-TM beats LEACH-SWDN and LEACH in terms of extending network life and controlling energy consumption. According to an investigation of the amount of transmitted data packets, the addition of trust value in Beta-based trust control framework can effectively minimize the impact of compromised nodes on the choice of cluster heads and retain security third-party routing nodes, which can significantly improve network security [24].

The authors of this study proposed a novel methodology for measuring trust. In addition to being able to fully employ sensor data, this model blends behavioural data with historical data. It is able to ascertain a node's state in accordance with the data trust. The approach has a higher rate of anomalous identification than the assessment model (which only takes behaviour trust into account). In addition, the trust value is calculated using a simple weighted average method. As a result, it is minimally invasive enough to operate with WSNs effectively. A trust list can also be dynamically created and updated at the same time by a trust evaluation mechanism. The data fusion only takes into account the data from a trusted node when using the trust list, which saves on communication costs and lowers energy usage. OMNET++ simulation results demonstrate that the trust model can increase node survival time and provide a more accurate picture of their state. Furthermore, compared to the LDTS model, the trust model has a higher rate of anomaly detection. Authors anticipate that our methodology for evaluating trust will contribute to the accuracy of sensor data [25].

The authors also suggested data aggregation and a multi-hoping technique, along with a novel ribbon structure connected to C-MAC. The amount of energy conserved is increased by shortening the time windows for data aggregation. The proposed work can also be used to detect events [41].

The authors proposed an improved route discovery technique based on the Q learning model of reinforcement learning. This is used to improve the reward-based learning mechanism, which enhances the QoS parameters and reduces the observed delay during general WSN connection [42].

Whether a dispersed network or cloud is present, the concept of trust is emphasised for ensuring security, privacy, and reliable communication in the network [43].

For improving the network lifetime and environment tracking and monitoring technique, an EEPC protocol has been presented [44].

It uses enhanced PSO and sensor data fusion. To stop the dominant selfish behaviour in the network, a novel technique for credit distribution across nodes is proposed. Based on the trust value of each node, an agent is assigned for the management of credits [45].

### 2.1 Existing Trust Management Techniques [26-39]

| Classification Criteria | ATRM | PLUS | TRGR | TBGRS | STE | TCFL | BNWSN | RFSN | TLEACH | BRMSN | TTSN | HTRM | GTMS | DTMS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Year and Publisher | 2005 IEEE | 2006 IEEE | 2007 JPDC | 2007 IEEE | 2007 IEEE | 2008 World Academy | 2008 IEEE | 2008ACM | 2008IEEE | 2009 IEEE | 2009 IJSA | 2010 Springer | 2011 IEEE | 2016 IEEE |
| Purpose | Detect malicious faulty nodes | Detect malicious nodes | Trust based route selection | Trust based routing scheme | Find the type of behavior | path selection, safe communication | for detecting malicious nodes | detect malicious, selfish | Trust based secure routing | Detect malicious nodes | Detect malicious nodes | Establishing relationship between nodes | Malicious, selfish,faulty | Detecting faulty data |
| Methodology | Mobile agent performs trust computation | Recommendations and personal reference | RSS, TOA | Neighbor selection, packet history | Statistical Trust | fizzy logic | bayesian network | bayesian theory | Beta distribution | Similarity Matrix | Bayes theorem | Certificate and behaviour based trust | time based past interaction | Data correlation |
| Performance Matrics | NA | Number of nodes infected, Additional packets wasted | Delivery ratio, path stretch | lifetime, percentage of malicious node | System lifetime, node count, trust cache size | trust values of paths | total trust value | number of packets | Packet delivery ratio | Detection Probability | Lifetime, time to detect malicious behavior | Functional and referral trust metric | trust levels at node, cluster head, BS | time series analysis, energy depletion method |
| Trust Values | NA | 0-1 | 0-1 | 0-1 | Range from -1 to +1 | 0-1 | 0-1 | 0-1 | 0-1 | 0-1 | NA | 0-1 | 0-100 | Range from -1 to +1 |
| Architecture | Centralized | Distributed | Distributed | NA | Distributed | Centralized | NA | Distributed | Centralized | Distributed | Distributed | Centralized and distributed | Clustered | NA |
| Advantages | Reduces communication Cost | efficiently detecty malicious nodes | Location verification | Increase of Network Lifetime | trust confidence interval | fuzzy detection can quantize uncertain data | robust and generic | no single to failure in trust computation | Situational and decision trust | Reduce number of data exchange | depends on task | flexibility in trust establishment | light weight | efficiently detects untrustworthy data |
| Disadvantages | works with agent based platform | Trust convergence time is high | Security implications of routing | No Attacks | do not consider external attack | centralized scheme is not suitable for most wsn | usage of distributions | can not improve system robustness | maintaining a neighbour trust table | do not consider attacks | Task collection and requires more memory | depend on third party | do not consider attacks against trust model | interdependency between data and node is not considered |
| Simulation Tool | NA | C++ | NS2 | Self-Written | Trust sensim | NA | Self Written | NESLsim | ONMET++ | NS2, Matlab | Self written | JAVA | SENSE | self written |

**Table 3**: Existing Trust Management Techniques

The existing approaches in Trust Management are being discussed in the above table along with their methodology, performance metrics, advantages, disadvantages, simulation tools used, purpose and trust values as key indicators to choose the suitable model according to the need [40].

## 3. THE PROBLEM FORMULATION

A collection of randomly distributed sensor nodes is referred to as a network. Some sensors are classified as transmission sources, while others are used as intermediate nodes. Malicious sensors aim to impede network performance by taking part in route setup activities. Every sensor is expected to participate in the routing process. Every sensor has a preventive record with misbehaviour nodes and a reliable list with the nodes' reliable values stored in it. Each node's routing table will have more entries in order to account for the reliability of other nodes. The issues can be summed up by asking the questions below:

i. Which nodes in the deployed network may be trusted, according to question?

ii. How can a precise trust threshold be defined to distinguish between trustworthy and malicious nodes?
iii. How may misbehaving nodes in a network be identified?
iv. Which nodes should be taken into account as the next-best hop in the route to minimise power consumption and increase network lifetime?

## 4. THE PROPOSED WORK OF THE SYSTEM

A model can be suggested in order to determine the rationale for improving the network's lifetime by raising the security and trust factor. The relationship between the service consumer and service provider is described in the model. By making a path Request, the service user asks the service provider for the best path that would allow them to convey their information in a reliable manner to their intended destination. If any dependable route is open to transfer the data at the specified time, the service provider will acknowledge the service consumer by sending an acknowledgement in its place. There are many of jobs being performed in the service provider's area. The term "Service Layer Structure" refers to the binding of N number of nodes in a Node List into this structure. The reason it is so named is that every information exchange is done in the form of a service, fulfilling needs that result in successful communication. the donation The architecture of the nodes connected to one another by service orientation includes the provisioning blocks, and consumers submit requests for data access. Each sensor node in the proposed technique is equipped with a variety of sensing and buffer capabilities, and nodes are deployed in a heterogeneous environment. The source nodes are those that contain the data that the user has requested. The node's trustworthiness is evaluated using the evaluated QoS parameters. Since each node has a zero starting trust value and takes part in numerous route formations, implementing the trust value at the node level is challenging. The swarm intelligence algorithm was employed in the recommended study and was based on the reviewed algorithms from the SI list in the relevant work section. The entire project has been simulated on MATLAB because it contains resources that are easily accessible for wireless simulations.

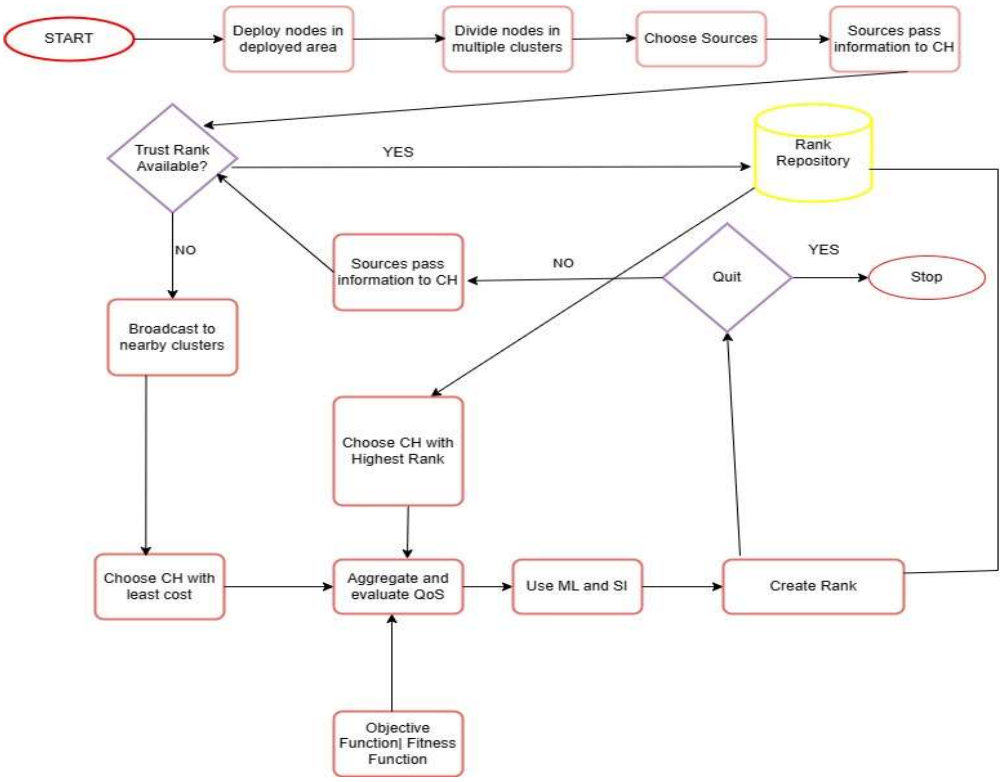


**Figure 3:** Proposed Work Flow of the System

The work flow of the entire procedure has been discussed in figure 3.

1. First of all, the network is initiated with 50 nodes and 1000/1000 area.

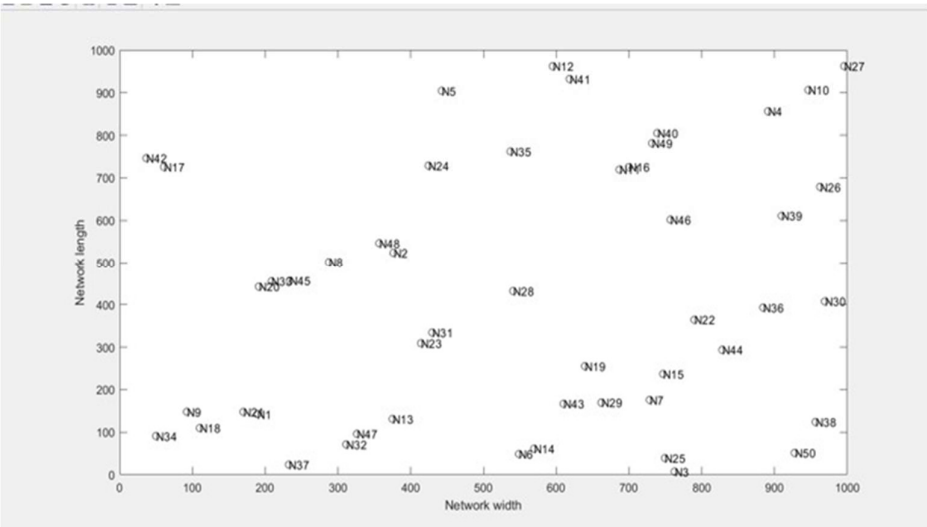


**Figure 4**: Deployment of network 1000*1000

2. Based on the LEACH protocol, in which sensors arrangement is in the form of clusters and one of the sensors acts as a cluster head (CH), Each node has a 1/P chance of ever again serving as the cluster head. Each node that is not a cluster head chooses the closest cluster head and joins that cluster at the conclusion of each round. The cluster head then develops a transmission schedule for each node in the cluster.

3. Source node and destination node has to be found out in the deployed network.

4. CHs of corresponding source node and destination node is taken in consideration.

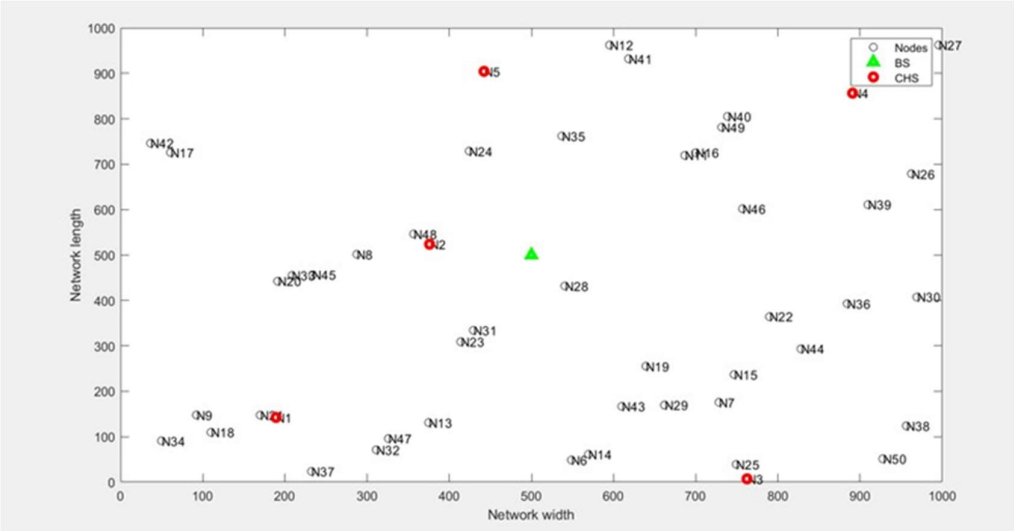


**Figure 5**: Deployment of 5 Cluster Heads and Base Station

5. Only when asked by source nodes does the AODV protocol create routes between nodes. As a result, AODV is regarded as an on-demand algorithm and does not add extra traffic to the networks for communication. As long as the sources require them, the routes are kept up. To connect the members of a multicast group, they also form trees. Sequence numbers are used by AODV to guarantee route freshness. They scale to multiple mobile nodes while also being self-starting and loop-free. Networks are silent in AODV until connections are made. A connection request is published by network nodes that require connections. The message is forwarded by the other AODV nodes, who also note the node that made the connection request. As a result, they build a number of transitory routes to the node making the request. Sending a backward message across temporary routes to the asking node is done by a node that receives such messages and holds a route to the desired node. The route with the fewest hops across other nodes is taken by the node that made the request. After some time, the entries that are not used in routing tables are recycled. The process is repeated if a link fails, and the routing error is sent back to the transmitting node.

6. Route Discovery is done between the source node and the destination node. The parameters are calculated for each route. These parameters are throughput, Packet delivery ratio (PDR), Power consumption (PC) and Delay.

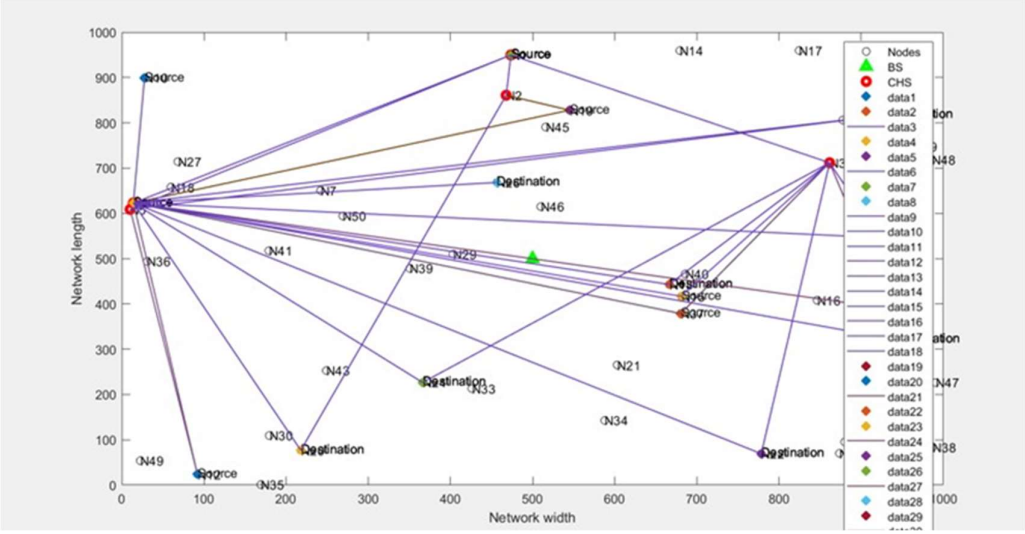


**Figure 6**: Route Discovery

7. As there are multiple routes and it may be possible for the single node to be present in multiple routes, so the decision of a reliable route or a reliable node can't be made. For this, all the four parameters are to be divided in three clusters respectively so that it can be differentiated which are the best ones and which are the worst ones.

8. This can be done through K-Means algorithm. K-Means clustering is an unsupervised learning algorithm in which the unlabelled dataset is divided into several clusters. In this case, K indicates the minimum number of predefined clusters that must be generated as part of the process, for instance, if K=2, means two clusters will be there, if K=3, means three clusters will be there and so on. The unlabelled dataset is divided into K different clusters using an iterative process. Each cluster comprises just one dataset and has a unique set of properties.

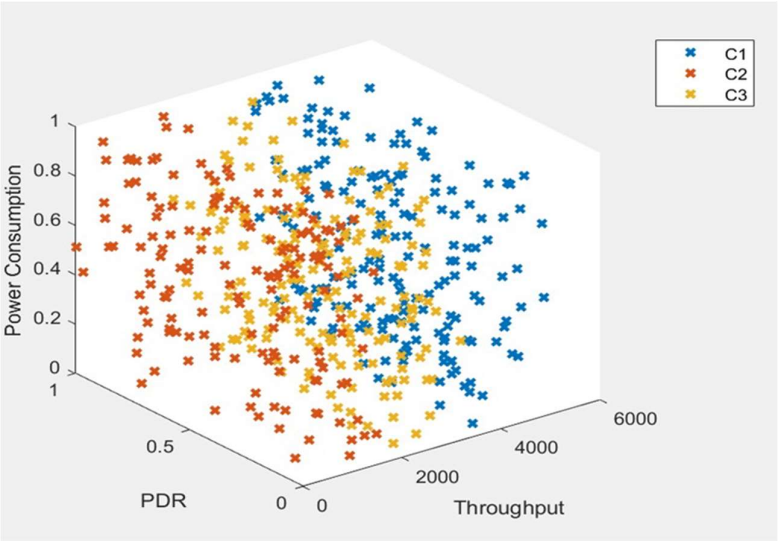


**Figure 7**: Formation of 3 centroids

9. Optimized Sampling is initiated on the basis of Mean Square Error and on this sampling, Swarm Intelligence technique is initiated.

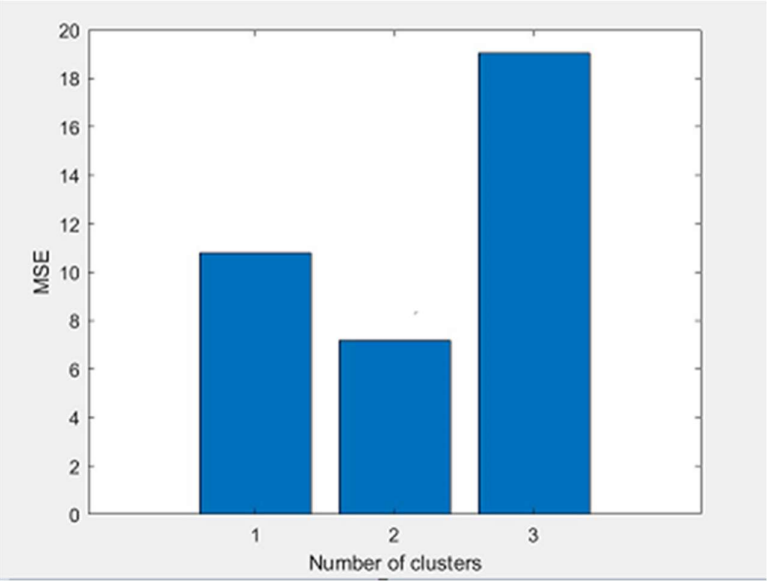


**Figure 8**: Calculation of Mean Square Error

10. Sample size selection is classified and then trained by neural network. For sample size selection, Dragon Fly algorithm (DA) is initiated along with its modified behaviour.

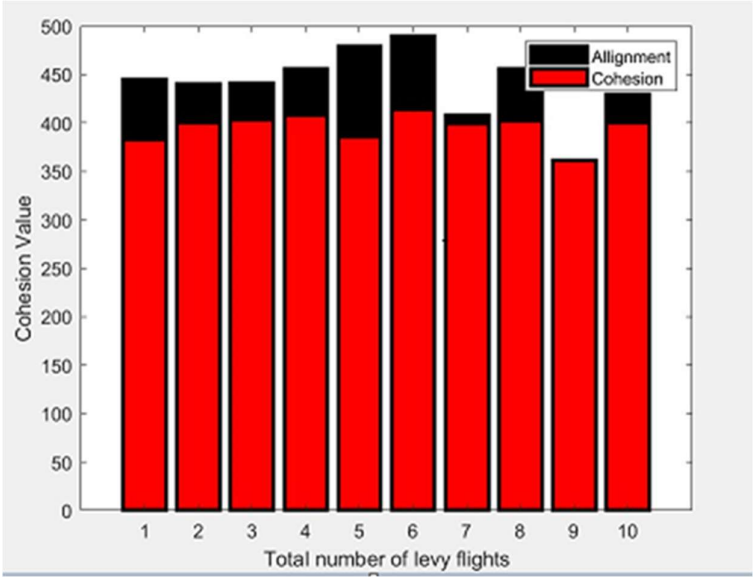


**Figure 9**: Dragon Fly algorithm initiation

11. The nodes with high ranks are to be taken into consideration and low ranked nodes are to be avoided.

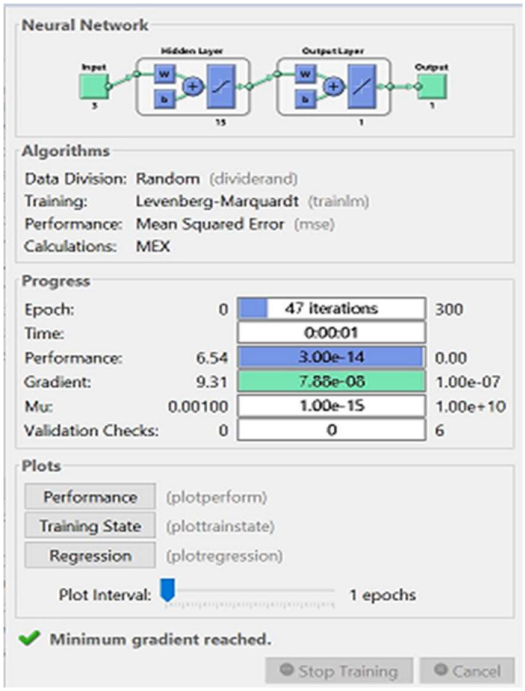


**Figure 10**: Neural Network

12. In this way, Trust management is done.

## 5. EXPERIMENTAL RESULTS AND ANALYSIS

When the proposed algorithm is compared with [41,42], an improvement is seen in terms of throughput, PDR and delay.

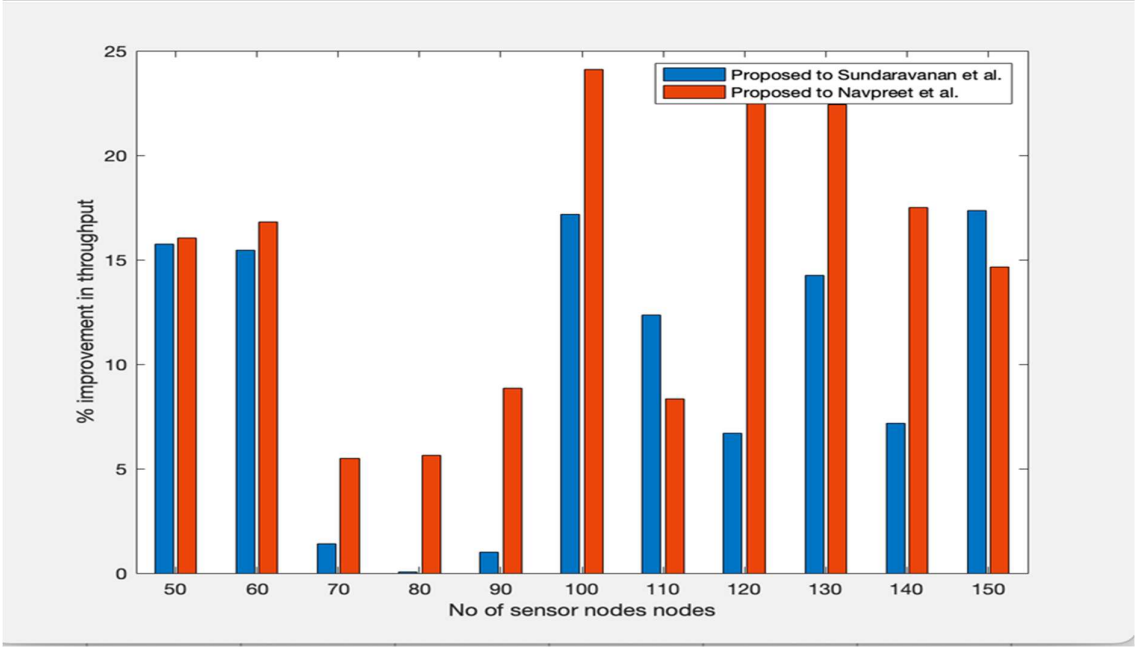


**Figure 13**: Improvement in Throughput when compared with [41,42]

Delay is the total time taken by the data packets to be delivered from source to destination.

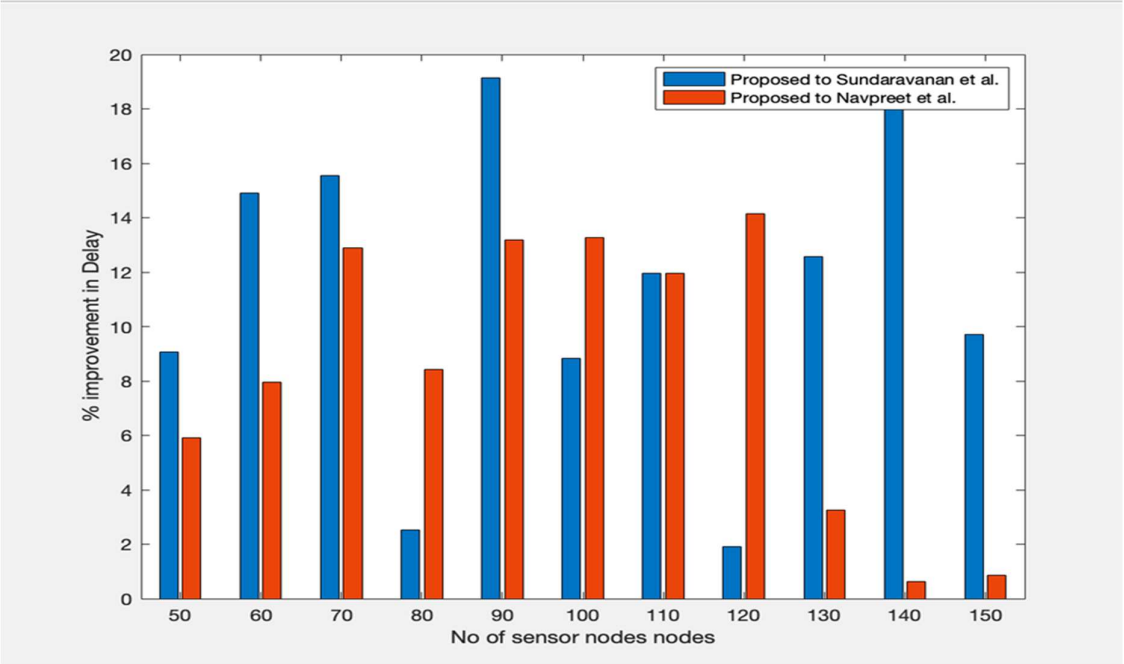


**Figure 14**: Improvement in Delay when compared with [41,42]

PDR is the packet delivery ratio. It means percentage of packets lost with respect to the number of packets sent.

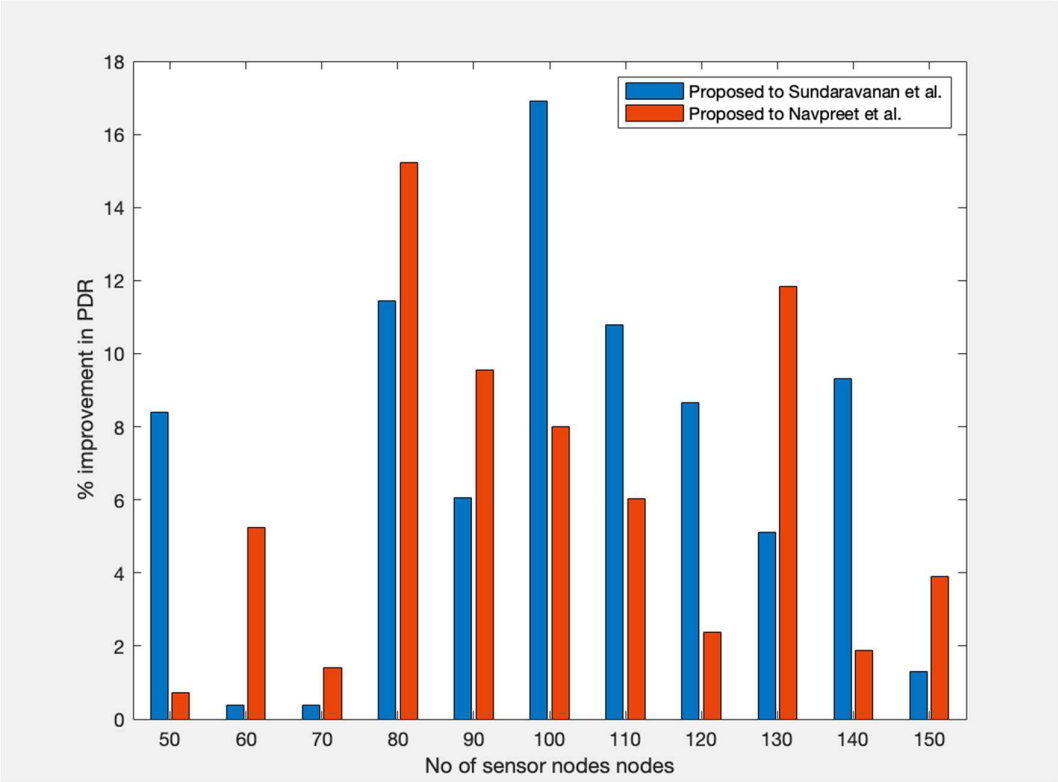


**Figure 15**: Improvement in PDR when compared with [41,42]

| no of sensor nodes' | 'Throughput proposed p/s' | 'PDR proposed' | 'Delay Proposed sec' | 'Throughput Sundaravanan et al. ' | 'PDR Sundaravanan et al. ' | 'Delay Sundaravanan et al. sec' | Throughput Navpreet et al p/s' | PDR Navpreet et al' | 'Delay Navpreet et al.' |
|---|---|---|---|---|---|---|---|---|---|
| 50 | 8844.544879 | 0.91205625 | 3.79881182 | 7641.903609 | 0.84151247 | 4.17735199 | 7620.77881 | 0.90552069 | 4.03809015 |
| 60 | 8574.534596 | 0.90191432 | 3.36181751 | 7425.582719 | 0.89853008 | 3.9506128 | 7339.97458 | 0.85699217 | 3.65205082 |
| 70 | 8796.24778 | 0.90780271 | 4.50327189 | 8674.522342 | 0.90439363 | 5.33236634 | 8339.52615 | 0.89520036 | 5.16913824 |
| 80 | 8579.786218 | 0.88092129 | 5.39486525 | 8575.569183 | 0.79040063 | 5.53429395 | 8120.91973 | 0.76448992 | 5.89177732 |
| 90 | 8646.26203 | 0.94153323 | 5.0187617 | 8558.940553 | 0.88773952 | 6.20639096 | 7942.32084 | 0.85953255 | 5.780502 |
| 100 | 8595.880611 | 0.92576351 | 5.81094482 | 7335.905099 | 0.79180179 | 6.37318216 | 6926.91579 | 0.85718281 | 6.69915441 |
| 110 | 8777.150043 | 0.97276425 | 5.52580552 | 7812.382346 | 0.87809838 | 6.27712107 | 8100.22212 | 0.91742549 | 6.27623824 |
| 120 | 9041.196238 | 0.98590326 | 6.43220233 | 8474.935701 | 0.90740542 | 6.55678867 | 7281.67792 | 0.96295194 | 7.49239436 |
| 130 | 8790.67638 | 0.97 | 7.91017091 | 7693.470177 | 0.92276872 | 9.04699541 | 7180.47175 | 0.86739212 | 8.17655908 |
| 140 | 9085.769704 | 0.91364862 | 8.41734818 | 8476.572381 | 0.83588307 | 10.4274356 | 7733.2252 | 0.89680793 | 8.46948661 |
| 150 | 8922.167248 | 0.90576428 | 8.29761353 | 7602.067847 | 0.89416858 | 9.19110494 | 7781.45555 | 0.87176029 | 8.36961493 |

**Figure 16**: Results after comparison of the proposed with [41,42]

## 6. CONCLUSION AND FUTURE SCOPE

An unmistakable, the trust table and the trust management system allow us to visualise the operation of each node. The unreliable nodes can be removed based on where they are in the network, which will ensure the network's smooth operation [6]. The correct operation of the nodes increases the longevity and energy efficiency of the network. Systems for managing convictions use a variety of algorithms. The specifications of the problem may affect the algorithm's choice. SI can be used to find reputation and trust management in this study article. In order to train the network, the Levenberg Marquardt algorithm is utilised. The following factors can be considered while determining the future scope:

i. Node-level load balancing is an option. Forecasting algorithms are taken into account for this.

ii. The Long Short-Term Memory (LSTM) technique can be used as the foundation for deep neural networks. It uses temporal forecasting as the basis for its prediction method.

## REFERENCES

[1] Ryu, J. H., Irfan, M., & Reyaz, A. (2015). A review on sensor network issues and robotics. *Journal of Sensors*, *2015*.

[2] Carlos, L. R., Manuel, Z. R. V., del Rocio, O. L. V., & Gerardo, M. L. (2018). Wireless sensor networks applications for monitoring environmental variables using evolutionary algorithms. In *Intelligent Data Sensing and Processing for Health and Well-Being Applications* (pp. 257-281). Academic Press.

[3] (Karl, H., & Willig, A. (2007). *Protocols and architectures for wireless sensor networks*. John Wiley & Sons.

[4] Alkhatib, A. A. A., & Baicher, G. S. (2012). Wireless sensor network architecture. In *2012 International Conference on Computer Networks and Communication Systems (CNCS 2012)*.

[5] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. *IEEE Communications magazine*, *40*(8), 102-114.

[6] Lopez, J., Roman, R., Agudo, I. and Fernandez-Gago, C., 2010. Trust management systems for wireless sensor networks: Best practices. *Computer Communications*, *33*(9), pp.1086-1093.

[7] G. Han et al., Management and applications of trust in Wireless Sensor Networks: A survey, J. Comput. System Sci. (2013), http://dx.doi.org/10.1016/j.jcss.2013.06.014

[8] Ahmed, A., Bakar, K.A., Channa, M.I., Khan, A.W. and Haseeb, K., 2017. Energy-aware and secure routing with trust for disaster response wireless sensor network. *Peer-to-Peer Networking and Applications*, *10*(1), pp.216-237.

[9] Dhulipala, V.R. and Karthik, N., 2017. Trust management technique in wireless sensor networks: challenges and issues for reliable communication: a review. *CSI Transactions on ICT*, *5*(3), pp.281-294.

[10] Selvi, M., Thangaramya, K., Ganapathy, S., Kulothungan, K., Khannah Nehemiah, H. and Kannan, A., 2019. An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. *Wireless Personal Communications*, *105*(4), pp.1475-1490.

[11] Khan, T. and Singh, K., 2019. Resource management based secure trust model for WSN. *Journal of Discrete Mathematical Sciences and Cryptography*, *22*(8), pp.1453-1462.

[12] T. Zahariadis, H. C. Leligou, P. Trakadas, and S. Voliotis, "Trust management in wireless sensor networks," European Transactions on Telecommunications, vol. 21, no. 4, pp. n/a– 395, 2010.

[13] J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago, "Trust Management Systems for Wireless Sensor Networks: Best practices", Computer Communications, vol. 33, pp. 0140- 3664, 2010.

[14] G. Han et al., Management and applications of trust in Wireless Sensor Networks: A survey, J. Comput. System Sci. (2013), http://dx.doi.org/10.1016/j.jcss.2013.06.014

[15] Ahmed, A., Bakar, K.A., Channa, M.I., Khan, A.W. and Haseeb, K., 2017. Energy-aware and secure routing with trust for disaster response wireless sensor network. *Peer-to-Peer Networking and Applications*, *10*(1), pp.216-237.

[16] Karthik, N. and Ananthanarayana, V.S., 2017, March. Data trust model for event detection in wireless sensor networks using data correlation techniques. In *2017 fourth international conference on signal processing, communication and networking (ICSCN)* (pp. 1-5). IEEE.

[17] AlFarraj, O., AlZubi, A. and Tolba, A., 2018. Trust-based neighbor selection using activation function for secure routing in wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing*, pp.1-11.

[18] Selvi, M., Thangaramya, K., Ganapathy, S., Kulothungan, K., Khannah Nehemiah, H. and Kannan, A., 2019. An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. *Wireless Personal Communications*, *105*(4), pp.1475-1490.

[19] Nie, S. (2017). A novel trust model of dynamic optimization based on entropy method in wireless sensor networks. Cluster Computing, 1-10.

[20] R.W. Anwar, A. Zainal, F. Outay et al., BTEM: Belief based trust evaluvation mechanism for wireless sensor networks, Future Generation Computer Systems (2019), https://doi.org/10.1016/j.future.2019.02.004

[21] Tayyab Khan & Karan Singh (2019) Resource management based secure trust model for WSN, Journal of Discrete Mathematical Sciences and Cryptography, 22:8, 1453-1462, DOI: 10.1080/09720529.2019.1695897

[22] Amuthan, A. and Arulmurugan, A., 2021. Semi-Markov inspired hybrid trust prediction scheme for prolonging lifetime through reliable cluster head selection in WSNs. *Journal of King Saud University-Computer and Information Sciences*, *33*(8), pp.936-946.

[23] Janakiraman, S., Priya, M.D., Devi, S.S., Sandhya, G., Nivedhitha, G. and Padmavathi, S., 2021. A Markov process-based opportunistic trust factor estimation mechanism for efficient cluster head selection and extending the lifetime of wireless sensor networks. *EAI Endorsed Transactions on Energy Web*, *8*(35), pp.e5-e5.

[24] Fang, W., Zhang, W., Yang, W., Li, Z., Gao, W. and Yang, Y., 2021. Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks. *Digital Communications and Networks*, *7*(4), pp.470-478.

[25] Chen, Z., Tian, L. and Lin, C., 2017. Trust model of wireless sensor networks and its application in data fusion. *Sensors*, *17*(4), p.703.

[26] Boukerche A, Li X, El-Khatib K (2007) Trust-based security for wireless ad hoc and sensor networks. Comput Commun 30:2413–2427.

[27] Yao Z, Kim D, Doh Y (2006) PLUS: parameterized and localized trust management scheme for sensor networks security. In: Proceedings of the third IEEE international conference on mobile adhoc and sensor systems (MASS'06), pp 437–446.

[28] Liu K, Abu-Ghazaleh N, Kang K-D (2007) Location Verification and Trust Management for Resilient Geographic Routing. J. Parallel and Distributed Computing 67(2):215–228.

[29] Hung K-S, Lui K-S, Kwok Y-K (2007) A trust-based geographical routing scheme in sensor networks. In: Proceedings of WCNC 2007

[30] Probst MJ, Kasera SK (2007) Statistical trust establishment in wireless sensor networks. In: International conference on parallel and distributed systems, vol 2

[31] Kim TK, Seo HS (2008) A trust model using fuzzy logic in wireless sensor network. World academy of science and engineering and Technology 42:63–66

[32] Momani M, Challa S, Alhmouz R (2008) BNWSN: bayesian network trust model for wireless sensor networks. In: Mosharaka international conference on communications, computers and applications (MIC-CCA '08), Amman, Jordan.

[33] Ganeriwal S, Srivastava MB (2004) Reputation-based framework for high integrity sensor networks. In: Proceedings ACM workshop security of ad hoc and sensor networks (SASN'04), pp 66–67.

[34] Song F, Zhao B (2008) Trust-based LEACH protocol for wireless sensor networks. In: Second international conference on future generation communication and networking, FGCN '08.

[35] Zhou M-Z, Zhang Y, Wang J, Zhao S-Y (2009) A reputation model based on behavior trust in wireless sensor networks. In: Eighth IEEE international conference on scalable computing and communications.

[36] Chen H (2009) Task-based trust management for wireless sensor networks. International Journal of Security and Its Applications 3(2):21–26.

[37] Gritzalis S, Aivaloglou E (2010) Hybrid trust and reputation management for sensor networks. Journal of Wireless Networks 16(5):1493–1510.

[38] Shaikh RA, Jameel H, d'Auriol BJ, Lee H, Lee S, Song Y-J (2009) Group-based trust management scheme for clustered wireless sensor networks. IEEE Trans Parallel Distrib Syst 20(11):1698–1712.

[39] Karthik N, Ananthanarayana VS (2016) Data trustworthiness in wireless sensor networks. Trustcom/BigDataSE/ISPA, 2016 IEEE. IEEE

[40] Dhulipala, V.R. and Karthik, N., 2017. Trust management technique in wireless sensor networks: challenges and issues for reliable communication: a review. *CSI Transactions on ICT*, *5*(3), pp.281-294.

[41] S. Jothiprakasam, C. Muthial, A Method to Enhance Lifetime in Data Aggregation for Multi-hop Wireless Sensor Networks, International Journal of Electronics and Communications (2018), doi: https:// doi.org/10.1016/j.aeue.2018.01.004.

[42] Kaur, N., Aulakh, I.K., Tharewal, S., Keshta, I., Rahmani, A.W. and Ta, T.D., 2022. Enhanced Route Discovery Mechanism Using Improved CH Selection Using Q-Learning to Minimize Delay. Scientific Programming.

[43] Rani, S., 2022, February. Mitigating Security Problems in Fog Computing System. In *Innovations in Bio-Inspired Computing and Applications: Proceedings of the 12th International Conference on Innovations in Bio-Inspired Computing and Applications (IBICA 2021) Held During December 16–18, 2021* (pp. 612-622). Cham: Springer International Publishing.

[44] Guleria, K., Verma, A. K., Goyal, N., Sharma, A. K., Benslimane, A., & Singh, A. (2021). An enhanced energy proficient clustering (EEPC) algorithm for relay selection in heterogeneous WSNs. Ad Hoc Networks, 116, 102473.

[45] Sharma, A., Goyal, N., & Guleria, K. (2021). Performance optimization in delay tolerant networks using backtracking algorithm for fully credits distribution to contrast selfish nodes. The Journal of Supercomputing, 77(6), 6036-6055.