Research

Dragon fly algorithm based approach for escalating the security among the nodes in wireless sensor network based system

Shweta Sharma[1] · Amandeep Kaur[1] · Deepali Gupta[1] · Sapna Juneja[2] · Mukesh Kumar[3]

Received: 9 September 2023 / Accepted: 17 November 2023
Published online: 30 November 2023

Abstract

A new technology that is gaining popularity today is the Wireless Sensor Network. Smart sensors are being used in a variety of wireless network applications, including intruder detection, transportation, the Internet of Things, smart cities, the military, industrial, agricultural, and health monitoring, as a result of their rapid expansion. Sensor network technologies improve social advancement and life quality while having little to no negative impact on the environment or natural resources of the planet are examined in sensor networks for sustainable development. Real-world applications face challenges ensuring Quality of Service (QoS) due to dynamic network topology changes, resource constraints, and heterogeneous traffic flow. By enhancing its properties, such as maintainability, packet error ratio, reliability, scalability, availability, latency, jitter, throughput, priority, periodicity, deadline, security, and packet loss ratio, the optimized QoS may be attained. Real-world high performance is difficult to attain since sensors are spread out in a hostile environment. The performance parameters are divided into four categories: network-specific, deployment phase, layered WSN architecture, and measurability. Integrity, secrecy, safety, and security are among the privacy and security levels. This article leads emphasis on the trustworthiness of the routes as well as the nodes involved in those routes from where the data has to pass from source to destination. First of all, the nodes are deployed and cluster head selection is done by considering the total number of nodes and the distance from the base station. The proposed work uses AODV architecture for computing QoS parameters that are throughput, PDR and delay. K-means clustering algorithm is used to divide the aggregated data into three possible segments viz. good, moderate and bad as this process does not involve the labelling of aggregated data due to its supervised behavior. The proposed trust model works in two phases. In first phase, data is divided into 3 segments and labelling is done. In second phase, uses generated class objects are to be applied viz. the route records to publicize the rank of the routes followed by the rank of nodes. The proposed technique employed the statistical machine learning and swarm intelligence strategy with dragon fly algorithm in order to address the issues related effective rank generation of nodes and improving the network lifetime. Deep learning concepts can be combined with fuzzy logics approach for resolving issues like secure data transmission, trustworthiness of ranking nodes and efficient route discovery.

Article Highlights

- This paper implies certain techniques for the lifetime enhancement of WSN.
- A modified version of dragonfly algorithm is used for achieving the trustworthiness of nodes and routes in the network.
- Trustnet is compared with existing techniques and it showed improvement in the results thereby attaining the trustworthiness of the network.

✉ Mukesh Kumar, kumarmukesh.coe@asu.edu.et; Shweta Sharma, shweta.sharma7885@gmail.com; Amandeep Kaur, Amandeep.bhullar@chitkara.edu.in; Deepali Gupta, Deepali.gupta@chitkara.edu.in; Sapna Juneja, sapnajuneja1983@gmail.com | [1]Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India. [2]KIET Group of Institutions, Ghaziabad, India. [3]Assosa University, Assosa City, Ethiopia.

Keywords Trust · Dragonfly · K-means · Lifetime enhancement · Sustainability

1 Introduction

A WSN is a system of sensor nodes that transmits the information needed by the network. For the collecting of secure data, WSN is utilized in a variety of contexts, including weather forecasting, the military, underwater research, etc. [1–3]. Transceivers, external memory, microcontroller, power source, and one or more sensors are the components of a sensor node. The sensor node's battery cannot be replaced once it has been deployed. The node's functionality is impacted as the energy level decreases. The sensor node with the empty battery eventually dies and is unable to communicate with any other nodes in the network. Network lifetime is shortened as a result of increased energy usage [4, 5]. Usage of Energy increases and Lifetime of Network Decreases. Energy should be conserved to boost network efficiency and consequently lengthen the network's useful life. Now a days lifetime concern is one of the major aspects that must be taken into consideration in WSN. Several measures are taken in order to enhance the lifetime of batteries associated with sensor nodes so that networks can work under harsh environmental conditions. Lifetime is perhaps the most important problem in the design of sensor networks because the aim of most WSN applications is to deploy unattended nodes for months or years in the sensing sector. The lifetime of sensor network is the time from the start of the operation of the network until a fraction of the nodes drains from their power, resulting in a network routing hole or disconnected network, or a network with insufficient coverage. The life of a network of sensors is essentially hindered by the power consumption of nodes. In order to optimize proper usage of battery life, each node must control its own local power supply. It is not the typical node life that counts in many implementations but rather the minimum node life. Lifetime is a time period in which nodes in the network are functional and transfer the data. According to researchers, lifetime is

Lifetime = S (Total functional time of node) that is $\sum_{i=1}^{n} St$ where S is the Serving Time [24].

Energy and lifetime are the two major concerns which should be taken into consideration while working in Wireless Sensor Networks as both have a great impact on the working of the network. There is requirement of battery for power consumption while deploying any node in the network. The basic principle of any network is to transfer the data from source to destination. During data transfer, three things should be taken into consideration which are transferred packets (Tx), Received packets (Rx), and Data Aggregation (Ax). The power in watts associated with the nodes in the form of batteries is converted into energy in joules or millijoules that is consumed while the data is transferred from the input source to the receiver node. So, E is used for Energy Consumption as shown in equation

$$E = \int_{0}^{t} Power\ (time)$$

The energy associated with the node as per the attached battery is called the Residual Energy. One of the problems occurs in WSN during network deployment is that the battery cannot be changed during the simulation. In this situation, the nodes are required to continue operation with the available battery. Hence the node's energy consumption and lifetime are inversely proportional to each other as the more the energy consumed, the lesser the lifetime of that particular node [25].

Energy consumption ↑ life time ↓

When the node is functional in the network, then it is called the Alive node, and when the battery of the node gets finished, then it is called Dead node. WSN can be homogenous where similar nodes have equal attributes in terms of memory, residual energy, etc., and heterogeneous where different residual energies are associated with different nodes. If the nodes having smaller residual energy for data transfer in lieu of the nodes having larger residual energy, then the previous ones will be dead, thereby increasing the number of dead nodes in the network. This is also one of the major issues in WSN known as scalability. Nodes will participate at the given time according to their residual energy known as Active Nodes and which should be at the resting mode at the given time known as Normal nodes with the help of finding the Average Residual Energy of the nodes in the network. There are numerous methods for improving longevity and energy efficiency. The management of the trust is one strategy.

1.1 System of trust management

The first question is: What does the word "trust" mean? Trust can be defined as a conviction or assurance that something is true. Belief in the goodness, talent, or organization of something or someone. The possibility that nodes whose behaviours cannot be controlled may be behaving in a way that is in favours of the network is another definition of trust. One may say that the relationship between the node that one can trust and the other node that one can trust is positive [7, 8]. The concept of trust management contains two main entities: Trustor, the

one who trusts in something, and Trustee, the one who can be trusted on. Every node in the network needs to be examined to see whether it is reliable or not, and every node needs to be involved in this process. Differentiating between reliable and unreliable nodes in the network is the primary goal of a trust management system. The network only keeps the reliable nodes while eliminating the faulty nodes. This exclusion is justified by the possibility that unreliable nodes will increase network latency, energy use, throughput, and longevity. If network services are based on reliable data, they can be provided with no problem. As a result, before a data item is processed further and sent over the network, a system must assess whether it is reliable. Unreliable data is disregarded, and the source is given a lower reliability rating. It is vital to evaluate the veracity of data as soon as feasible to prevent mistrust information from being processed further, hence minimizing potential harm. Big networks may encounter poor performance and an excessive concentration of network traffic as a result of a dedicated node's centralized analysis. Each node in the network is expected to participate in the assessment of credibility and make judgments about trust [9, 10].

From the viewpoint of a WSN, trust is the action of accepting a message after determining if the data and its origin are trustworthy. A node in the network can operate as both a trustee and a trustor: for departing data, it assumes the role of a trustee, enabling other nodes to determine if it can be accepted; for arriving communication, it can act as a trustor, determining the sender's reliability in real-time. 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 basic assumption of the trust management model is that a kind of scale is used by all the nodes known as the "Trust Scale". A complete trust level node that is 100 percent reliable, the starting trust level, and the cut-off level are three typical values that can be taken into account concerning this scale [11]. The term "initial trust level" describes the amount of credit given to a node when it first joins the network and its trustors do not have any additional supporting information about its dependability. The "cut-off level" is the amount of confidence below which a node is deemed to be unreliable. Each node must participate in the trust management procedure, and current records of other nodes' reputations must be maintained. The Trust Table is created as a result of this data structure. Every entry in the trust database has a trust value assigned to it based on the trust scale. A dummy example of a Trust table based on the example network for node1 can be shown in Table 1.

Based on entries in the trust table, a node can approve any other node than itself. This process is referred to as recommendation [6]. Based on this, a model that contains details about each node in the network and generates the trust table can be created. Each node, message, a trust table item, and node's reputation are further contained in the following entities, which might act as a part of the trust table.

The model execution is done through cycles and each cycle has two phases namely the data phase and the recommendation phase.

The contributions of this paper can be summarized as follows:

According to the reviewed literature, there is plenty of room for the use of machine learning architecture and the use of SI algorithm architecture to develop and advance sensor node trust.

- The trust model that has been created against the sensor nodes is presented in this study together with its proposed work design and execution.
- The goal is to create a network with a high trust factor so that resources are not squandered, and the network can operate for an extended period.
- The proposed work is compared with a reward-based routing mechanism based on QoS parameters that are throughput, PDR, and delay.

The sensor nodes transfer data based on the requirement and to prevent the unwanted waste of resources within the network proper cluster arrangement of sensor nodes with higher trust level in the network is highly recommended. Various strategies have been used in order to provide solution but the problems still not encounter optimally. Hence in order to address the real time bottleneck issues related to network lifetime, we proposed an optimal solution which improves the ranking of the nodes with higher trust level. The proposed technique employed the statistical machine learning and swarm intelligence strategy with dragon fly algorithm in order to address the issues related effective rank generation of nodes and improving the network lifetime. The different QoS based parameters such as throughput, PDR and delay has been

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

ID of Node	Value of Trust
1	0.52
3	0.64
5	0.79
7	0.45

used in order to evaluate the efficacy of the proposed model.

Table 2 illustrates the notations used in the paper.

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 Materials and methods

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 lightweight, 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 of the growing effect of WSN in practical applications. The concept of trust management also played an important role over time.

The existing work illustrates the various trust management techniques and models being used in the field of WSN. A dynamic protocol was suggested in this article to accommodate the requirements of varied applications. This protocol focuses on real-time large-data transmission, making it more effective to employ in IoT-based applications. The proposed protocol consists of algorithms for data transmission, neighbor discovery, and routing table creation. Five algorithms were demonstrated in this article. A neighbor finder algorithm is one of them. Each node's cost to each of its neighbors as well as its cost to the BS are calculated. As a result, at the end of the procedure, each node can generate its own routing table. Pathfinder, the second approach, is suggested to discover the optimum

Table 2 Abbreviations

Abbreviations	Definitions
WSNs	Wireless sensor networks
IoT	Internet of things
DFA_U-Trust	Dragonfly Algorithm Updated-Trust
SI	Swarm Intelligence
PDR	Packet Delivery Ratio
ESRT	Energy-aware and secure routing with trust
R-AODV	Reliable AODV
TLB-AODV	Lightweight trust-based routing protocol
AF-TNS	Activation function based trusted neighbor selection
EATSRA	Energy aware trust based secure routing protocol
BTEM	Belief-based trust evaluation mechanism
ADT	Authentication-based data trust
HRFCHE	Hyper exponential reliability factor-based cluster head selection
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	The Bayesian network trust model for WSNs
RFSN	Reputation-based framework for sensor networks
TLEACH	Trust based leach
BRMSN	Behavior 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

path between sender and target (destination) nodes in the network. In contrast to many studies in the literature, this method operates more effectively because each node can modify its cost to target based on the information it acquired from nodes in its layer before broadcasting a packet to its neighbors. It effectively manages the CPU units and power. As a result, it behaves differently from greedy algorithms like Dijkstra and is more successful at locating optimized paths. Three additional data transmission techniques that can be used in a variety of situations and applications were also proposed. The three alternative mechanisms are suggested in order to demonstrate a dynamic routing system and broaden its usefulness. All of the proposed algorithms' performances were assessed both theoretically and experimentally [12].

An energy-saving dynamic clustering method for wireless sensor networks is proposed in this research. Our objective is to reduce the likelihood of missing the target and improve tracking accuracy. Cluster creation and cluster head selection make up the first phase. The following phase involves building a new cluster based on moving targets. Therefore, the cluster head determines the target's present location. Target tracking in the environment will be done in a later phase by routing the target across nodes. This situation results in network-wide energy savings. We used the ns-2 simulator to implement our tracking technique. Our algorithm's missing rate is 9% [13].

In order to identify the best paths, this article suggests two novel energy-efficient routing techniques based on the Incremental Grey Wolf Optimization (I-GWO) and Expanded Grey Wolf Optimization (Ex-GWO) algorithms. In addition, a general architecture has been suggested in this paper, allowing a variety of other metaheuristic algorithms to function adaptively alongside these algorithms. The new fitness function is defined in the proposed approaches to choose the next hop based on criteria including residual energy, traffic, distance, buffer size, and hop size. These measurements are crucial for making further node decisions. These techniques' primary goals are to reduce traffic, enhance associated systems' fault tolerance, and boost their dependability and lifetime. The ideal values for these parameters are determined using the two metaheuristic methods outlined above. The offered approaches determine the optimum path of any length between any source and destination node. The established network and system were used in this investigation, and a simulation environment was used instead of a ready dataset. The best path, as determined by the lowest cost of the best paths obtained using the suggested approaches, has thus been found. In distributed and decentralized peer-to-peer systems, these techniques can be highly helpful. Network lifetime, alive node ratio in the network, packet delivery ratio and lost data packets, routing overhead, throughput, and other metrics are used to evaluate and compare performance [14].

On the basis of energy conservation while facilitating communication between sensor nodes across the entire network, the Energy Effective-Accuracy Routing (EEAR) protocol is recommended for wireless sensor networks in this study. Through the use of the data center gradient diffusion routing protocol, EEAR can preserve energy while maintaining communication and pathways that go to the sink. By detecting and controlling radio frequency and other components of additional sensor nodes, this is realized. The Gradient-Based Routing (GBR) and Naps topology management protocols were combined to create EEAR, which maintains a nearly constant level of routing accuracy without the use of geographic position information. This protocol places additional nodes in a sleeping state after constructing communicative layers towards the sink while maintaining inter-layer connectivity. A node can actually enter a state of sleep in each layer by identifying some other nodes that can do its communication tasks in its place. EEAR produces significant results in continuous and event-driven models towards query-driven models despite conformance with all data delivery types. In this study, we applied EEAR and contrasted it with other approaches including GBR, Naps, and GAF. According to simulation studies, EEAR performs at least as well as location-based protocols in terms of topology control, routing, and energy conservation, as well as increasing packet delivery volume and lowering average packet delay [15].

The author discussed the trust models concept that is further categorized into three types namely "centralized" where the focus is on the head node of the network that undertakes the job of deciding the trustworthiness of the node based on the trust data collected on its own or by the data provided by all other nodes in the network, secondly, the "hierarchical" one in which network is divided into groups called clusters and it is the responsibility of cluster head to aggregate the data and calculating the trust and third one is "distributed" in which each node monitors its neighbour's behaviour and their trustworthiness is calculated. In nutshell, this paper discusses the nodes' capabilities, the network restrictions, and the risks involved in terms of the lifetime and bandwidth of the network to design and implement the trust model for enhanced security [16].

Besides the fruitfulness gained by WSN through the trust model, various attacks on these trusted models are discussed. These attacks reduce the efficiency of the trust model. Bad mouthing attack, On–Off attack, selective behaviour attack, Sybil attack, newcomer attack, etc. A set of best practices is discussed for designing the trust model for WSN. A set of best practices can be identified as considering trust and reputation, trust and the base

station, first-hand information gathering, second-hand information gathering, initial values, granularity, updating and aging, risk, and importance. Through the analysis of different techniques in trust management, it is concluded that the set of best practices should be taken into account to get a successful trust model for WSN [17].

The authors discussed the various trust models for ordinary WSNs and clustered WSNs.

For ordinary WSNs, two types of trust models are available i.e., Node trust models and Data trust models [7].

Authors proposed a new technique named ESRT, a new trust and energy-based routing protocol that gives efficient flexibility against the faulty nodes and their behaviours experienced while forwarding packets. This technique looks at the distributed trust. The simulation results in the performance improvement of ESRT against existing techniques like R-AODV and TLB-AODV when these are disclosed to various numbers of problematic nodes and fluctuating network demand [8]. The authors presented their work on the data trust model and used data correlation techniques to create defect detection and data restoration approaches. [18].

To improve network security for resource-constrained WSNs, this study suggests AF-TNS. To maintain the neighbours' level of trustworthiness, AF-TNS operates in two phases: trust evaluation with constrained energy and metric-based node evaluation. The AF's difficult decision-making process is made simpler by the random Tran sigmoid function's use of trustworthiness to maintain network performance and untrusted nodes. According to the results of the simulation, AF-TNS increases the likelihood that malicious activity will be detected and extends the lifetime of the network. According to the experimental findings, the AF-TNS approach ensures a minimum of 8.5 s of latency, 8.53 J of energy, 149 kbps of throughput, and 390 s of network lifetime when delivering network information. It also has a lower false detective rate of 1.5% [19].

To provide WSNs with optimum and safe routing, the new secure routing algorithm EATSRA is presented and implemented in this study. In this approach, the decision tree-based routing algorithm is utilized to choose the best and most secure path, and the trust scores are used to more effectively detect attackers in WSN. Additionally, spatial–temporal restrictions have been employed to make routing decisions. Through simulation-based testing, it has been found that the proposed EATSRA performs better by consuming less energy and improving security and packet delivery ratio [20].

In this paper, an efficient BTEM technique is proposed whose purpose is to defend the faulty nodes and internal attacks. For gathering the direct and indirect trust values of all the sensor nodes, Bayesian estimation is applied, and the correlation of data is done for a further selection of trustworthy nodes to forward the data packets. Simulation results state that not only it identifies and then isolate the faulty nodes but also the false positive detection rate is improved. As compared to other algorithms like AF-TNS [15] and Trust Doc [17], it has a better ability to defend against attacks [18].

The system is now safe and secure thanks to the integration of ADT. It is anticipated that integrating Equation for Scheduler-based Node Trust will enhance performance in terms of transmission overhead, a clustered method Using the scheduling technique, interdependence has been built between trusted nodes. The ability of trustworthy nodes to manage resources and memory has improved with the integration of task-scheduling mechanisms. Nodes may now manage memory and compute resources thanks to this technique. Communication is more reliable when data trust and cryptography techniques are combined. The proposed method used the intra-cluster (CM) and inter-cluster (CH) approaches to reduce the packed transmission overhead [21].

The HRFCHE through the Semi-Markov scheme is a prediction method that integrates energy and trust assessment to extend the lifetime of the network. The results of HRFCHE show that it performs better than competing cluster head election techniques because it increases the lifetime of the network and decreases energy usage by 28% and 34%, respectively [22].

A reliable method for choosing the right CH based on the use of an opportunistic parameter is the suggested MPOTFEM. The Markov chain and Preventive Maintenance (PM) idea are included in this proposed MPOTFEM scheme for determining how well the network is maintained. By reducing the frequency of CH elections, it is found that evil nodes do not become CHs. According to the simulation results, the suggested mechanism outperforms the existing ones in maintaining the average percentage of live and dead nodes in the network at 10.82% and 11.36%, respectively. The findings demonstrate that, in comparison to the widely used CH election processes, the suggested mechanism is capable of providing average improvements in PDR and Throughput of 9.14% and 10.56% [11].

This paper's contribution is the suggestion of LEACH-TM, an energy-efficient and trust management-based hierarchical routing system. The benefits of this technique include increasing the accessibility of the network, extending the network's life, and improving the network's capacity to fend off threats. The number of dynamic decision cluster head nodes, based on residual energy, and the density of neighbour nodes can all be used to better limit the cluster's size to improve energy efficiency and prevent excessive node energy consumption. The simulation findings show that the LEACH-TM outperforms LEACH-SWDN

and LEACH in terms of prolonging the life of the network and regulating energy usage. According to an investigation of the amount of transmitted data packets, the addition of trust value in the 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 [23].

In this study, the authors suggested a brand-new approach for assessing trust. This model combines behavioural information as well as historical information, in addition to being able to fully utilize sensor data. According to the data trust, it can determine a node's state. The approach has a greater anomalous detection rate compared to the assessment model (which simply considers behaviour trust). Additionally, a straightforward weighted average method is used to determine the trust value. Thus, it is lightweight enough to work effectively with WSNs without having a lot of overhead. A trust evaluation model can also dynamically build and update a trust list at the same time. 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 [26]. Authors anticipate that our methodology for evaluating trust will contribute to the accuracy of sensor data [24].

The authors proposed a new ribbon structure associated with C-MAC along with data aggregation and multihoping techniques. The energy is saved by reducing the time slots for data aggregation thereby increasing the saved energy. The proposed work can be applied to event detection also [41].

Based on reinforcement learning's Q learning model, the authors suggested an enhanced route discovery process. This is used to enhance the reward-based learning mechanism thereby improving the QoS parameters and decreasing the delay observed while overall communication is performed in WSN [42].

The concept of trust is discussed for providing security and privacy and reliable communication in the network whether a case of a distributed network is there, or a cloud is there [43].

An EEPC protocol has been proposed by engaging enhanced PSO and sensor data fusion techniques for enhancing the network lifetime and improvement in monitoring and tracking environment techniques [44]. A novel mechanism for the distribution of credits among nodes is proposed to eliminate the selfish behaviour prevailing in the network. An agent is allotted for the management of credits based on each node's trust value [45]. Memory and energy are two resources that are scarce in wireless sensor networks. Enhancing network longevity has drawn more and more attention in recent years. The longevity of a network is significantly influenced by node energy. However, there is growing worry over network longevity along with this astonishing growth in wireless sensor networks. This study's main goal is to better understand how various factors can affect the choice of a cluster head. A hybrid methodology that is normally based on the node's energy was used in this investigation. The energy of the node, the energy of the node's neighbors, the number of hops, and the number of links to neighbors have all been used by the authors to select the cluster head. Each of these factors influences how the cluster head is chosen. They precisely noted hop size, energy of each sensor node, average energy of sensor neighbors, linkages to sensor nodes (HEEL), and other parameters. ranking nodes Power-Efficient Gathering in Sensor Information System (PEGASIS), Energy-Aware Clustering Scheme with Transmission Power Control for Sensor Networks (EACLE), Low Energy Adaptive Clustering Hierarchy (Nr-LEACH), Modified Low Energy Adaptive Clustering Hierarchy (ModLEACH), Low Energy Adaptive Clustering Hierarchy-B (LEACH-B), Low Energy Adaptive Clustering Hierarchy (LEACH), and Hybrid Energy Efficient Distributed Cluster [46, 47]. In wireless sensor networks, effective resource use is a crucial problem. Energy is one of the most vital resources, and clustering structure has a significant impact on how effectively it is used. To fully utilize the advantages of these architectures, however, efficient and appropriate cluster head (CH) elements must be chosen. It is necessary to perform additional processing in order to solve the non-deterministic polynomial-time (NP-hard) problem of choosing the right CHs and determining the best coefficients for each parameter of a pertinent fitness function in CHs election. As a result, this paper's goal is to address the connected challenges while also suggesting effective ways to reach the main objective [51–54] (Table 3).

2.1 Existing trust management techniques

Some of the existing approaches are TBGRS, TCFL, STE, BNWSN, RFSN, TTSN and many others [27–40]. Some of the existing approaches in Trust Management are 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 [9].

Table 3 Existing Trust Management Techniques

Classification criteria	ATRM [27]	PLUS [28]	TRGR [29]	TLEACH [35]	BRMSN [36]	HTRM [38]	GTMS [39]	DTMS [40]
Year	2005	2006	2007	2008	2009	2010	2011	2016
Purpose	Faulty nodes detection	Faulty nodes detection	Trust based route	Trust based routing	Faulty nodes detection	Relationship establishment	Faulty nodes detection	Faulty data detection
Methodology	Trust computation through mobile agents	Recommendations	Neighbor, packet history	Beta distributed	Similarity matrix	Behavior based trust	Time based past interaction	Data correlation
Trust values	–	0–1	0–1	0–1	0–1	0–1	0–100	Range from -1 to +1
Architecture	Centralized	DISTRIBUTED	Distributed	Centralized	Distributed	Centralized and distributed	Clustered	–
Tool used for simulation	–	C++	NS2	OMNET++	MATLAB	JAVA	SENSE	Self-written

2.2 The problem statement

A network can be characterized as a collection of sensor nodes that are dispersed at random. While some sensors serve as intermediate nodes, others are designated as the transmission source. Via their participation in route setup activities, malicious sensors try to hinder network performance. It is anticipated that every sensor will take part in the routing procedure. Every sensor has a preventive record that contains misbehaviour nodes and a reliable list that stores the nodes' trustworthy values. The routing table of each node will increase the number of entries to contain the value of the reliability of other nodes. The following queries can help to summarize the issue:

- Which are the nodes in the deployed network that can be trusted?
- How an accurate trust threshold can be specified to differentiate between malicious nodes and trustworthy nodes?
- How the misbehaving nodes can be detected in the network?
- Which nodes should be considered as the next best hop in the route thereby resulting in minimizing the power consumption and maximizing the network lifetime?

As related to literature survey [12–20], certain key concepts are employed in the proposed technique such as distance of node from the base station, cluster creation and cluster head selection, route discovery, AODV concept, trustworthiness of route as well as node.

2.3 The proposed technique

To find out the solution for increasing the security and trust factor in the network and in return, enhancing the network lifetime, a model can be proposed.

The model in Fig. 1 states the relationship between the Service Consumer and the Service Provider. The service consumer requests the service provider by sending the Route Request for the suitable route through which the consumer can transfer the information to the destination in a reliable way. In place of this, the service provider acknowledges the service consumer by sending an acknowledgment if any reliable route is free to transfer the data at the given time. In the territory of service providers, many jobs are taking place. There is a Node List that contains N number of nodes that are bound together within a structure known as Service Layer Structure. It is so called because every exchange of information done is in the form of service that is Requests are there and they are being served to result in fruitful communication.

The offering Consumers submit requests for data access, and the architecture of the nodes that are linked to one another through service orientation comprises the provisioning blocks. The proposed technique deploys nodes in a heterogeneous environment where each sensor node has a variety of sensing and buffer capabilities. The nodes that have the data that the user has requested are known as the source nodes. Based on the evaluated QoS parameters, the node's trust is assessed. It is difficult to implement the trust value at the node level since each node has a zero initial trust value and participates in many route formations. Based on the reviewed algorithms from the SI list in the related work

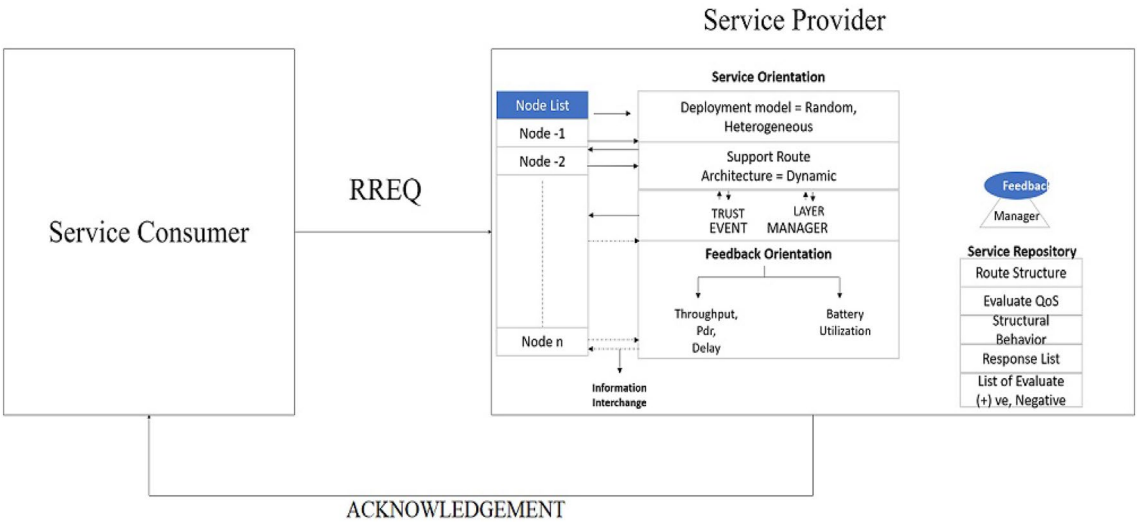


Fig. 1 Trustnet: System Model for Proposed Work

section [48–50], the swarm intelligence algorithm was used in the suggested study. Due to MATLAB's resources being readily available for wireless simulations, the entire project has been simulated on it.

The workflow of the entire procedure has been discussed in Fig. 2 followed by the Algorithm 1.

As stated in Algorithm 1, the network is deployed and cluster heads selection is done on the basis of LEACH algorithm. The source node and destination node are discovered in the network. CHs for source node and destination node are found out. Then AODV is initiated for broadcasting the RREQ and RREP is awaited from all the nearby CHs. Hence, Route Discovery is performed [51]. Once routes are discovered, QoS parameters are evaluated for all the routes thereby resulting in repository. K-means is applied for distinguishing the routes as Good, Bad and Moderate. Machine Learning helps in training and classifying the data, thereby resulting in the routes and nodes respectively, having higher ranks and lower ranks [52]. The lower ranks are avoided and higher ranks are considered in order to enhance the energy efficiency and lifetime of network. Figure 3 lights up the flow of the methodology being introduced in Trustnet. It is defined in detail in further section along with the figures.

The proposed work is comprised of heterogenous nodes that are deployed in the wireless field. To design the simulation environment, data acquisition toolbox

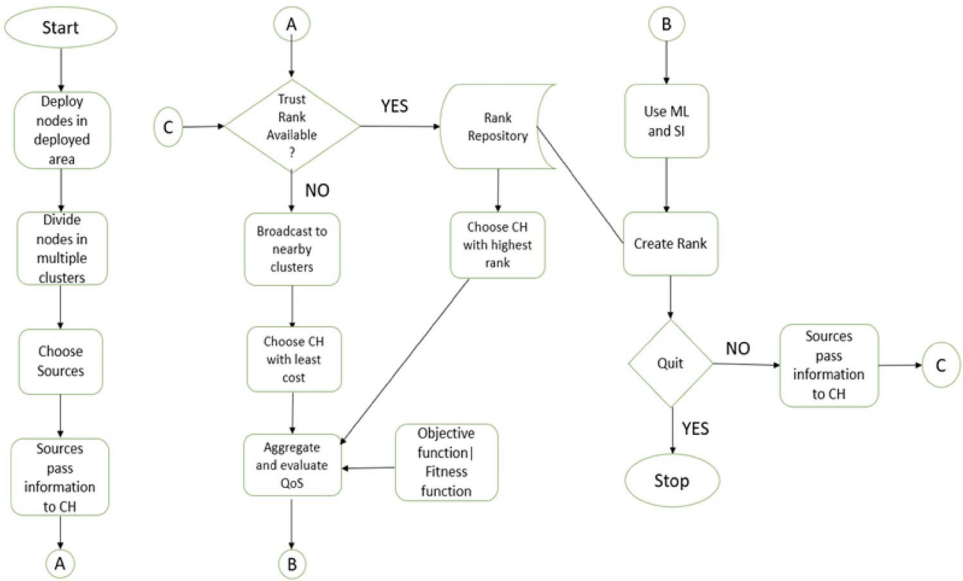


Fig. 2 Trustnet proposed workflow

Require: ns where ns is the node structure
1: Initiate network Net(ns,l,w) where l is the length of the Network and w is the width of the network.
2: Initiate CHs based on LEACH
3: sn=findNet.source;
4: dn=findNet.destination;
5: CHs=findNet.sn.CH (Find CH of Source Node)
6: CHd=findNet.dn.CH (Find CH of Destination node)
7: Initiate AODV
8: PerformDiscovery(CHs,CHd);
9: Evaluate QoS parameters Throughput, Delay, PC, PDR
10: [k-index,k-cent]=apply(k-mean,rankc) where rankc is total number of rank classes
11: Initiate Optimized Sampling
12: Initiate ML
13: Train and Classify using ML(k-index,k-cent)
14: Create Rank();
15: Assist AODV using Rank
16: Prefer High rank node, avoid Low rank node

Algorithm 1 Trustnet: Proposed Algorithm

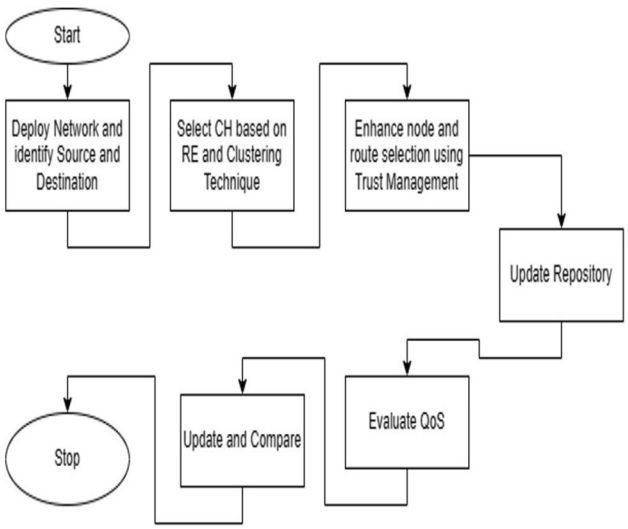


Fig. 3 Trustnet proposed methodology

has been utilized in MATLAB development environment (Fig. 4).

Initially the nodes were deployed using a network length and width of 1000/1000 m whereas the size of the network is increased to check the performance of the network and to check the possible elasticity in the designed network. In the first instance, the broadcasting node sends the data to its related CH for communication. To divide the data into multiple groups based on the locations. The CH is initially selected with the maximum battery in stock. The CH gets a rotational shift when it comes to selecting the CH viz. for a certain interval of time, a node can remain CH. Once a node becomes CH, all the nodes of the specific region will be sending data via. Its cluster head only. This concept has been borrowed from Least Energy Adaptive Routing Hierarchy (LEACH). The CH broadcasts the route requirements that includes the destination information and the direction of the destination. Now the seeker CH gets reply as Route Reply(R-REP) against the request made viz. Route Request(R-REQ).

The algorithm architecture to perform each single step that has been described here is popularly known as on demand distance vector routing protocol (ODV) [53] and if it is applied to mobile network, it would be termed as Ad-hoc-ODV(AODV) [54]. The proposed work uses the ODV architecture here and computes the following parameters in terms of QoS for the further computation (Table 4).

Considering the first route, there are a total number of 6 nodes in the list. As 42nd node is the source node that is associated with CH 2. The source node transfers the packets to the concerned CH and CH2 further broadcasts the requirement to other CHs. Based on the application of the algorithm illustrated earlier in this section, the proposed work chooses CH3 and CH4. CH4 further passes the data to 5 whose response time to acknowledge the data packet expires after a certain given threshold. In such a situation the respondent chooses CH9 which contains the destination node.

The proposed work aggregates the data for 10,000 simulations so that an analysis can be performed over the aggregated data. The proposed work reselects the data after the same threshold number of simulations. All the simulation architecture is done to attain maximum lifetime in the overall network. As it has been illustrated earlier also that lifetime refers to total amount of time that a node spends in the network. Here the lifetime of a sensor node is directly proportional to the power consumption as the total remaining power will evaluate the total time of survival of the sensor node.

The proposed work uses k-means clustering algorithm [55] to divide the data into 3 possible segments, namely good routes, moderate routes and bad routes. The purpose is to create a rank of the nodes based on the learning behavior of the node under given circumstances. As k-means is not able to label the divided groups due to its supervised behavior, the proposed work uses Fuzzy logic to label the divided segments [56]. The application of k-means algorithm has been done using statistical machine learning toolbox (SML)that is supplied in MATLAB for processing and communication of statistical data. As it has been illustrated earlier that k-means algorithm has been applied over the aggregated data to divide them into three categories namely good, moderate and bad, the deployment has been done using SML toolbox of MATLAB.

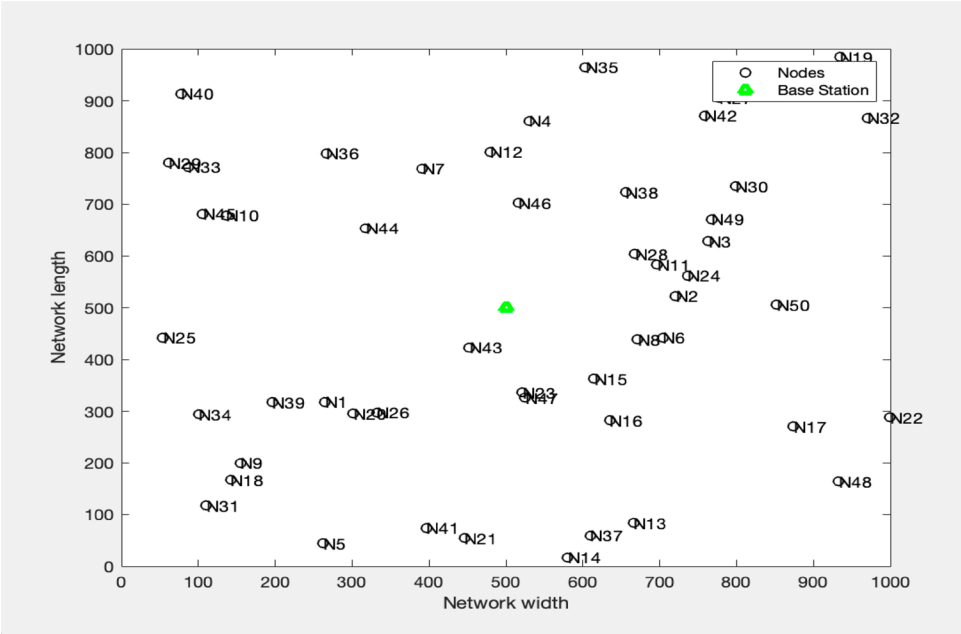


Fig. 4 Deployed network with 50 nodes and 1000/1000 area

Table 4 Discovered routes

Route	'Throughput'	'PDR'	'Power Consumption'
[2, 3, 3, 4, 4, 4, 5, 5, 9]	2440.3331	0.95545367	2.07457767
1 × 19 double	918.182245	0.91584899	4.23670207
1 × 26 double	643.437035	0.88402177	1.64416218
1 × 35 double	447.481595	0.84383968	3.85946479
1 × 40 double	340.068105	0.83198692	2.17562956
1 × 45 double	258.707342	0.8019026	1.62258756
1 × 50 double	203.461082	0.77954456	1.59450671
1 × 59 double	154.471017	0.73835408	4.50281664
1 × 64 double	123.641738	0.71779509	2.61584728
1 × 73 double	94.5198129	0.66945762	3.29621479

The data distribution, as in Fig. 5, has been done on the base of namely Throughput, PDR and Power Consumption. The fuzzy labelling has been done with the following pseudo code with Fuzzy inference engine. The proposed work has developed a Mamdani rule set. The inference engine has two sets of inputs and one set of output.

As shown in Fig. 6, the fuzzy engine is made up of two input parameters namely the R-MSE and SE. Each input set is bonded with Shweta Mamdani rule engine the produces the class as the output function.

As shown in Fig. 7, the surface viewer is the 3d mapping of the input and the output set. The input set that is MSE and SE are mapped via several membership function values that are associated as SE and MSE. The maximum and minimum range for both MSE and SE is between 0–1 whereas the output viz. the class lies in a membership value of 0.2 for minimum and 0.8 for maximum.

As has been discussed, the trust model generation involves two processes. The first part aggregates the data based on the collected routes, the proposed trust generation mechanism divides the data into three segments and labels them as "Good", "Moderate" and "Bad". The section aims to further use the generated class objects viz. the route records to publicize the rank of the routes followed by the rank of the nodes. The node ranking procedure will help in selecting the CH when the route discovery process will be made. The proposed work generates two step trust generation post the application of fuzzy logic. The first phase and the second phase are for the generation of trust value based on the entire route and based on the node. Phase 1 aims to rank down the routes of each category and the second phase ranks down the nodes as per their categorization in the GTs formed.

The trust is calculated only for the classified GT value from a trained architecture that is attained by Levenberg Feed Forward and Back Propagation mechanism. The proposed work has been implemented on MATLAB simulation tool that supports the propagation behaviour utilizing Neural Networks (NN) toolbox. The toolbox supports a range of training algorithms that are based on neural engines, but as Levenberg supports the forward movement and the backward movement and hence it has been considered as the algorithm to be a part of the proposed work.

As shown in Fig. 8, the training model is supplied with three input values viz. the throughput, PDR and delay. The delay is one of the major reasons in WSN for

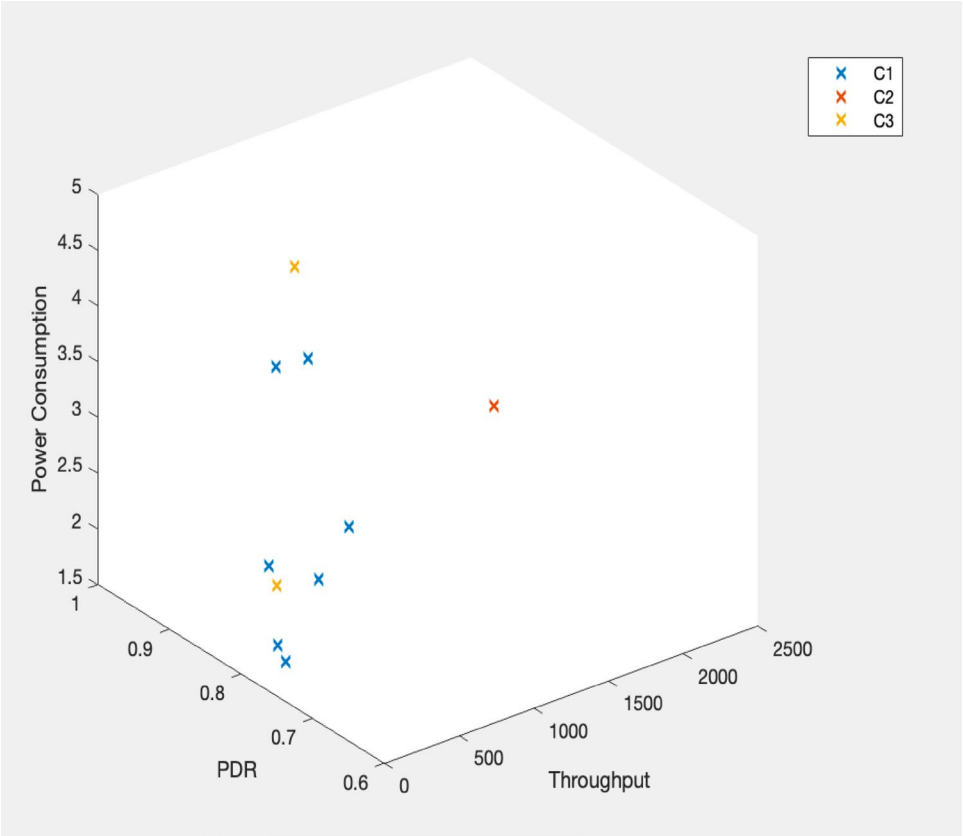


Fig. 5 Data distribution in three clusters based on three parameters

reduced lifetime. Lifetime refers to the total amount of time which a sensor node spends in a network to transfer, receive and aggregate the data packets from one end to another end. More delay will consume more power from the sensor nodes as the nodes will be consuming idle time energy. The trained Neural Network will be used to categories the node based on its classified rank. Once the network is trained, the classification score of the route will act as an activator of the dataset. The trust generation process is attained using the Dragon fly algorithm. The algorithm iteratively evaluates the fitness of different dragonflies based on their alignment and cohesion with other dragonflies in the same group, as well as their distance to a global food value. The algorithm also includes a random population generation and simulates Levy flights to explore the search space. The algorithm initializes several variables, including the number of dragonflies, a list of selected dragonflies, and a counter for the number of selected dragonflies. It then loops over each dragonfly in the dataset and performs the dragonfly optimization process. During each iteration, the current dragonfly is selected, and its group order and global food value are determined. The algorithm generates a random population of dragonflies and simulates Levy flights. The alignment and cohesion of each dragonfly in the population are calculated, and a fitness value is computed based on the dragonfly's alignment, cohesion, and distance to the global food value. The fitness values are used to determine which dragonflies are selected for the next iteration. If the average reward of the dragonflies in the current iteration is greater than 60, the current dragonfly is added to the list of selected dragonflies. The code also prints a message indicating whether the dragonfly was accepted or rejected. Overall, this code appears to be a working implementation of the dragonfly algorithm for optimization, although its effectiveness will depend on the specifics of the problem being solved and the parameter values used. The proposed SI algorithm helps to choose most appropriate CH based on the ranking of the node defined as per the cohesion and alignment of the dragonfly algorithm.

3 Results

In justify the research work, the section presents the evaluation of the proposed model and its performance analysis to claim its effectiveness. The simulation parameters used in the analysis are network throughput, packet delivery ratio and the observed network delay. The parameters used in the simulation analysis are listed in Table 5.

Fig. 6 Fuzzy rule engine

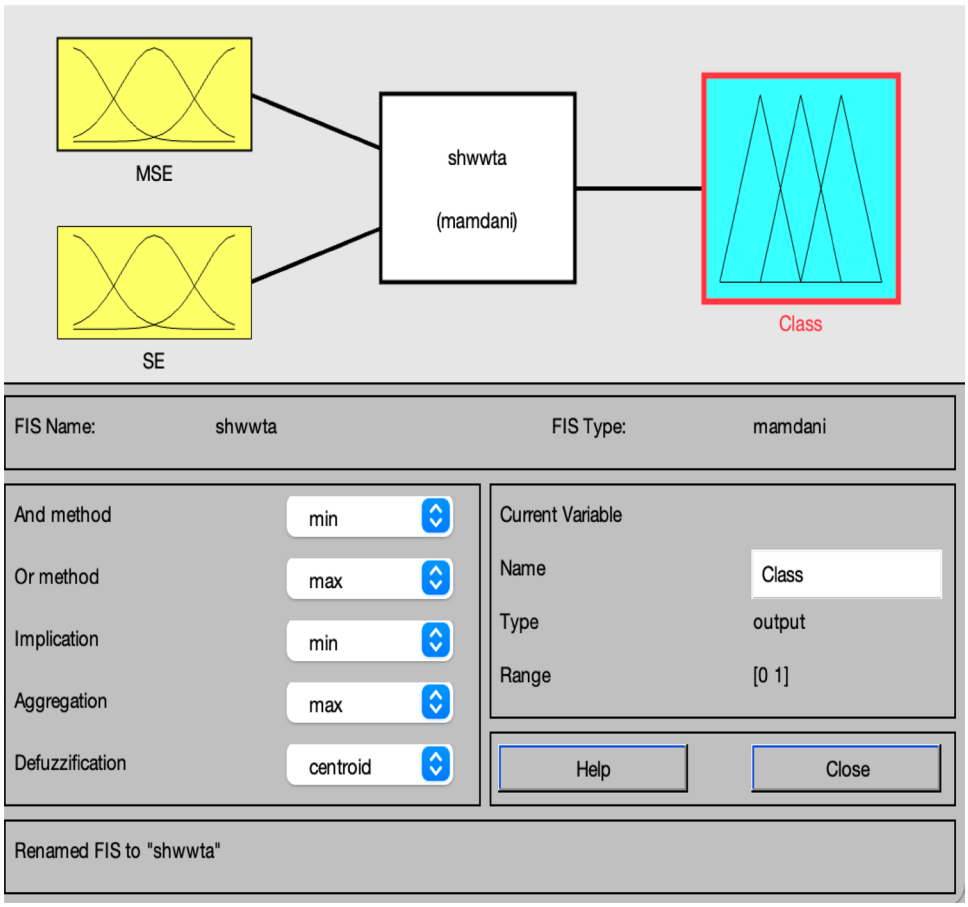
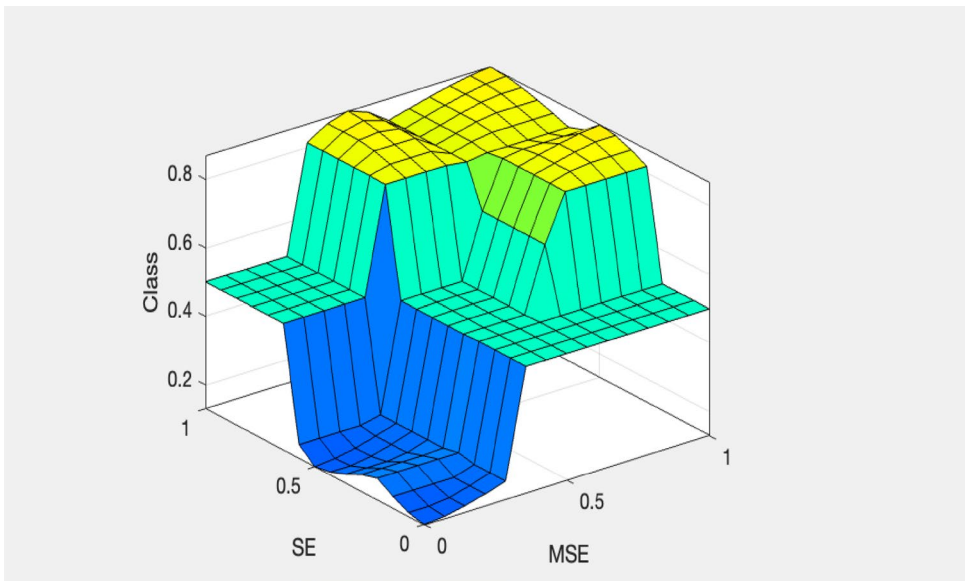


Fig. 7 Surface viewer



A comparative analysis-based evaluation is presented in the following section evaluating the proposed work for three performance measures namely, throughput, PDR and delay. To further, present a comparative analysis, the proposed "Trustnet" scenario compared with reference to variation in the simulation rounds ranging to 100 against four existing studies such as "Improved CH selection using Q-Learning"

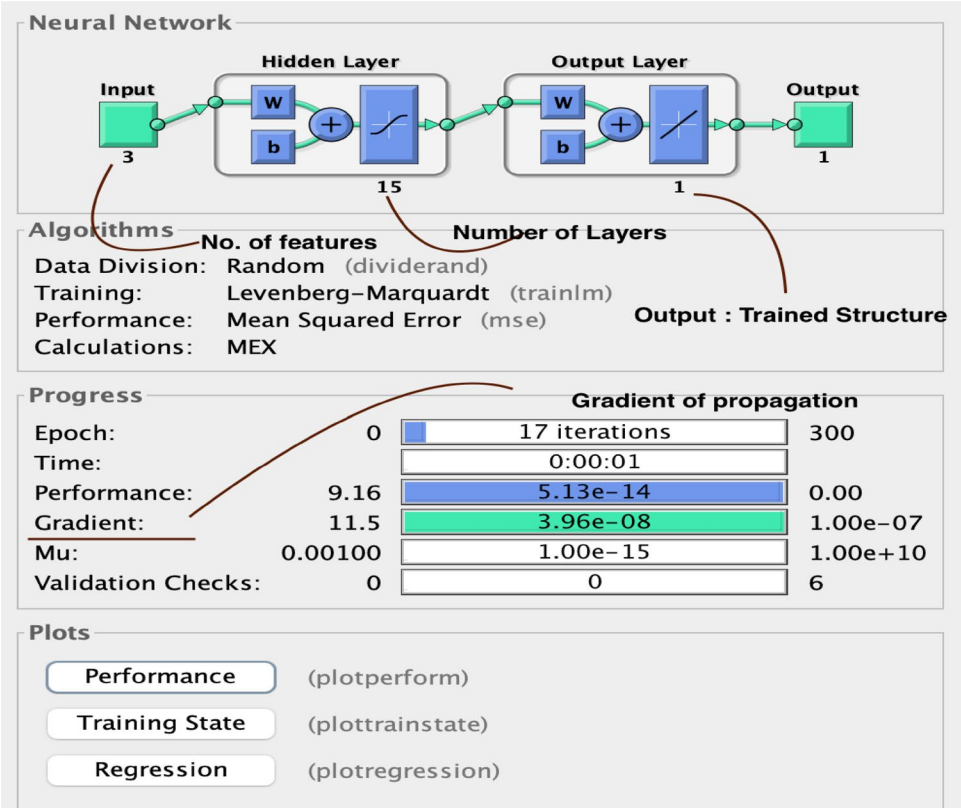


Fig. 8 The Levenberg training model

Table 5 Simulation Architecture

Parameters	Description
Network Size	1000 m by 1000 m
Number of nodes	150
Number of Simulation Rounds	1000
Improved trust model	Fuzzy logic and error metrics
Ranking Architecture	Artificial Neural Network
Evaluation Parameters	Throughput, PDR, Delay

based technique(RRM) proposed by Kaur et al. 2022, "Improved Bkd-Tree-Inspired Energy-Efficient Clustering-based Routing Protocol" (IBkd-Tree-IEFCRP) proposed by Janakiraman 2020, Fuzzy based "Ant colony optimization"(ACO) technique using hybrid protocol(FUCARH)" proposed by Arjunan and Sujatha 2018, "A multihop and data aggregation based modified media access control mechanism called co-operative MAC enhanced lifetime (C-MACEL)" proposed by Jothiprakasam and Muthial 2018 in order to obtain the significant outcomes in terms of performance parameters.

Throughput Analysis

In this analysis, the throughput has been computed for 150 nodes over different rounds of simulations such as 100. The proposed technique has been compared with other techniques such as RRM, IBkd-Tree-IEFCRP, FUCARH and C-MACEL, in order to find the optimal average throughput value.

It is observed from Table 6 that the average value of Throughput over 100 simulations for 150 nodes have been computed for techniques such as RRM, IBkd-Tree-IEFCRP, FUCARH, C-MACEL and Trustnet are 8451.6306 Mbps, 8250.0886 Mbps, 8213.467733 Mbps, 7991.8692 Mbps and 8564.634467 Mbps respectively. The obtained results showed that the proposed technique has the highest Throughput average value i.e., 8564.634467 Mbps over other techniques due to the integrated machine learning and SI strategy which enhance the performance of the QoS parameters.

In Fig. 9, the throughput improvement analysis is evaluated in order to find the best average value using 150 nodes against 100 rounds of simulations by comparing the proposed with other techniques.

Figure 9 represents the Throughput improvement analysis over 100 rounds of simulation. The proposed technique has shown a significant improvement in the throughput value as compared to other techniques such as RRM, IBkd-Tree-IEFCRP, FUCARH and C-MACEL. It is observed from the obtained results that the proposed technique has shown enhanced throughput with an increment in the simulation count. When 150 nodes are included for analysis, the proposed technique shown the average throughput improvement percentage value,

Table 6 Throughput analysis at 100 simulations

Number of Nodes	Trustnet	RRM	IBkd-Tree-IEFCRP	FUCARH	C-MACEL
10	8171.66	7996.28	7931.13	7839.39	7685.86
20	8211.07	8085.44	7958.01	7926.65	7691.86
30	8286.28	8132.57	7976.92	8005.56	7782.66
40	8340.35	8193.58	8052.63	8073.62	7867.53
50	8396.63	8259.64	8131.07	8148.74	7941.36
60	8481.22	8354.96	8206.82	8165.6	7970.43
70	8544.67	8405.57	8262.65	8217.86	7975.66
80	8575.66	8450.39	8286.14	8225.22	8033.24
90	8586.93	8542.35	8383.88	8226.77	8060.4
100	8664.56	8582.13	8394.61	8270.96	8078.21
110	8720.48	8585.45	8401.36	8330.64	8094.96
120	8781.85	8671.95	8405.32	8333.74	8132.7
130	8844.94	8757.14	8417.82	8431.12	8154.79
140	8896.19	8850.3	8443.62	8500.31	8188
150	8967.02	8906.72	8499.36	8505.84	8220.4

1.35% over RRM, 3.80% over IBkd-Tree-IEFCRP, 4.26% over FUCARH and 7.15% over C-MACEL. The obtained results showed that the proposed technique outperformed the other techniques due to the involvement of fuzzy logics which enhance the trust level of nodes.

PDR Analysis

In this analysis, the PDR has been computed for 150 nodes over different rounds of simulations such as 100. The proposed technique has been compared with other techniques in order to find the optimal average PDR value.

It is observed from Table 7 that the average value of PDR over 100 simulations for 150 nodes have been computed for techniques such as RRM, IBkd-Tree-IEFCRP, FUCARH, C-MACEL and Trustnet are 0.903066667, 0.874133333, 0.8366, 0.823866667 and 0.911 respectively. The obtained results showed that the proposed technique has the highest PDR average value i.e., 0.911 over other techniques due to the involvement of neural network with regression mechanism which improves the classification score of the routes.

In Fig. 10, the PDR improvement analysis is evaluated to find the best average value using 150 nodes against 100 rounds of simulations by comparing the proposed with other techniques.

Figure 10 represents the PDR improvement analysis of over 100 rounds of simulation. The proposed technique Trustnet has shown a significant improvement in the PDR value as compared to other techniques implemented RRM, IBkd-Tree-IEFCRP, FUCARH, C-MACEL. It is observed from the obtained results that the proposed technique has shown enhanced PDR with an increment in the simulation count. When 150 nodes are included for analysis, the proposed technique shown the average PDR improvement percentage value, 0.88% over RRM, 4.23% over IBkd-Tree-IEFCRP, 8.89% over FUCARH and 10.56% over C-MACEL. The obtained results showed that the proposed technique outperformed the other techniques due to the involvement of SI which improves the trust nodes during rank generation and increases the network lifetime.

Delay Analysis

In this analysis, the delay in seconds has been computed for 150 nodes over different rounds of simulations such as 100. The proposed technique has been compared with other techniques in order to find the minimum average delay value.

It is observed from Table 8 that the average value of delay over 100 simulations for 150 nodes have been computed for techniques implemented by Kaur et al. 2022, Janakiraman 2020, Arjunan and Sujatha 2018, Jothiprakasam and Muthial 2018 and proposed are 3.626933333 s, 3.725 s, 3.736533333 s, 3.8742 s and

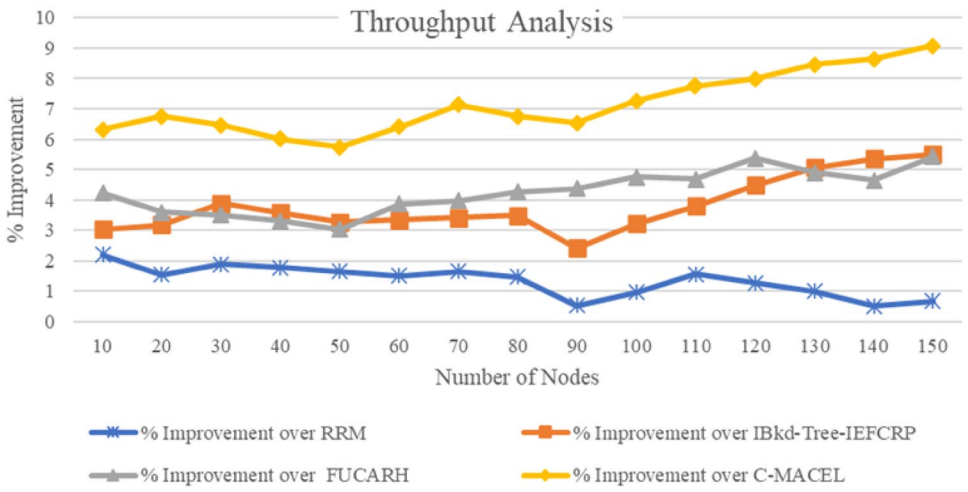


Fig. 9 Throughput improvement analysis at 100 simulations

Table 7 PDR analysis at 100 simulations

Number of Nodes	Trustnet	RRM	IBkd-Tree-IEFCRP	FUCARH	C-MACEL
10	0.859	0.831	0.805	0.791	0.859
20	0.868	0.836	0.806	0.801	0.868
30	0.873	0.839	0.81	0.811	0.873
40	0.877	0.849	0.813	0.813	0.877
50	0.883	0.852	0.818	0.815	0.883
60	0.889	0.862	0.827	0.817	0.889
70	0.899	0.867	0.83	0.821	0.899
80	0.906	0.877	0.833	0.824	0.906
90	0.913	0.887	0.839	0.829	0.913
100	0.919	0.889	0.846	0.831	0.919
110	0.926	0.892	0.854	0.835	0.926
120	0.928	0.894	0.862	0.839	0.928
130	0.93	0.905	0.866	0.841	0.93
140	0.935	0.912	0.869	0.843	0.935
150	0.941	0.92	0.871	0.847	0.941

3.238933333 s respectively. The obtained results showed that the proposed technique has the minimum delay average value i.e., 3.238933333 s over other techniques due to the involvement of fuzzy logics which enhance the trust level of nodes.

In Fig. 11, the delay improvement analysis is evaluated in order to find the least average value using 150 nodes against 100 rounds of simulations by comparing the proposed with other techniques.

Figure 11 represents the delay improvement analysis (in seconds) over 100 rounds of simulation. The proposed technique has shown a significant improvement in the delay value as compared to other techniques implemented by Kaur et al. 2022, Janakiraman 2020, Arjunan and Sujatha 2018, Jothiprakasam and Muthial 2018. When 150 nodes are included for analysis, the proposed technique shown the average delay improvement percentage value, 10.52% over Kaur et al. 2022, 12.56% over Janakiraman 2020, 12.69% over Arjunan and Sujatha 2018 and 15.96% over Jothiprakasam and Muthial 2018. The obtained results showed that the proposed technique outperformed the other techniques due to the involvement of ANN with fuzzy logics which enhanced the trust node ranking generation.

This section presented the results obtained while designing the efficient strategy for data delivery through optimal route. The proposed model employed machine learning and swarm intelligence-based neural network approach which has been evaluated and compared with other techniques as RRM, IBkd-Tree-IEFCRP, FUCARH, C-MACEL to find the higher level of trust node during the ranking generation process to increase the overall lifetime of the network. The results are obtained using the MATLAB simulation tool in terms of different QoS parameters such as Throughput, PDR, and Delay for different rounds of simulation (100).

4 Discussion and future scope

An enhanced version of the dragonfly optimization method can be applied in this study to achieve the best area coverage and energy consumption reduction. Throughput, PDR, and delay were the three measures this paper utilized to gauge its effectiveness. The outcomes of the proposed strategy were contrasted with those of some previously reported methods. Simulations demonstrated that, in terms of the given performance parameters, the suggested strategy outperformed the other evaluated methods. In this paper, SI can be implemented for finding reputation and trust management. The Levenberg Marquardt algorithm is used for training the network.

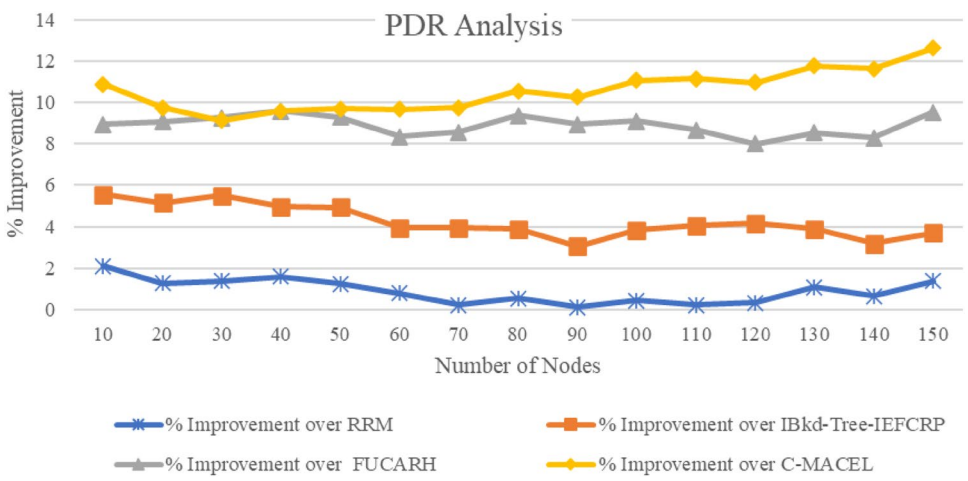


Fig. 10 PDR improvement analysis at 100 simulations

Table 8 Delay analysis at 100 simulations (in Seconds)

Number of Nodes	Trustnet	RRM	IBkd-Tree-IEFCRP	FUCARH	C-MACEL
10	2.542	2.636	2.738	2.764	2.858
20	2.673	2.778	2.803	2.78	2.963
30	2.686	2.986	2.988	2.891	3.044
40	2.702	3.218	3.148	3.134	3.11
50	2.818	3.403	3.344	3.25	3.325
60	2.881	3.488	3.351	3.31	3.596
70	3.061	3.497	3.388	3.578	3.63
80	3.262	3.526	3.537	3.594	3.836
90	3.269	3.608	3.823	3.733	4.154
100	3.473	3.806	4.045	4.006	4.205
110	3.64	3.886	4.176	4.159	4.358
120	3.709	4.21	4.446	4.449	4.586
130	3.764	4.396	4.498	4.647	4.719
140	4.002	4.399	4.621	4.842	4.828
150	4.102	4.567	4.969	4.911	4.901

The performance analysis of Trustnet shows number of future prospects to address the trust and security in data transmission in WSN. Some of the notable future expansion involves fusion of deep learning, animal-based meta-heuristics, and fuzzy logic heralds a promising in resolving complex network challenges. Novel algorithms with deep learning's prowess with meta-heuristics' efficiency will be tailored to specific networking contexts, optimizing network parameters while balancing exploration and exploitation. Real-time anomaly detection using deep learning models will support security by identifying threats within traffic patterns, complemented by fuzzy logic-driven adaptive security measures.

- An enhanced node evaluation via deep learning's historical data processing, paired with fuzzy logic trust assignments, promises more reliable node ranking.
- Optimized route discovery, aided by meta-heuristics, and congestion prediction through deep learning foster efficient networking. These hybrid methods also extend network lifespan by predicting energy usage patterns and preempting failures.
- With applications transcending networking, ethical considerations for increasingly autonomous algorithms will be addressed, ensuring responsible and privacy-centric operations in domains like IoT, smart cities, healthcare, and industrial automation.

5 Conclusion

The sensor nodes transfer data based on the requirement and to prevent the unwanted waste of resources within the network proper cluster arrangement of sensor nodes with higher trust level in the network is highly recommended. Various strategies have been used in order to provide solution but the problems still not encounter optimally. Hence in order to address the real time bottleneck issues related to network lifetime, we proposed an optimal solution which improves the ranking of the nodes with higher trust level. The Trustnet technique employed the statistical machine learning and swarm intelligence strategy with dragon fly algorithm in order to address the issues related effective rank generation of nodes and improving the network lifetime. The different QoS based parameters such as throughput, PDR and delay has been used in order to evaluate the efficacy of the proposed model. This presented the results obtained while designing the efficient strategy for data delivery through optimal route. The proposed model employed

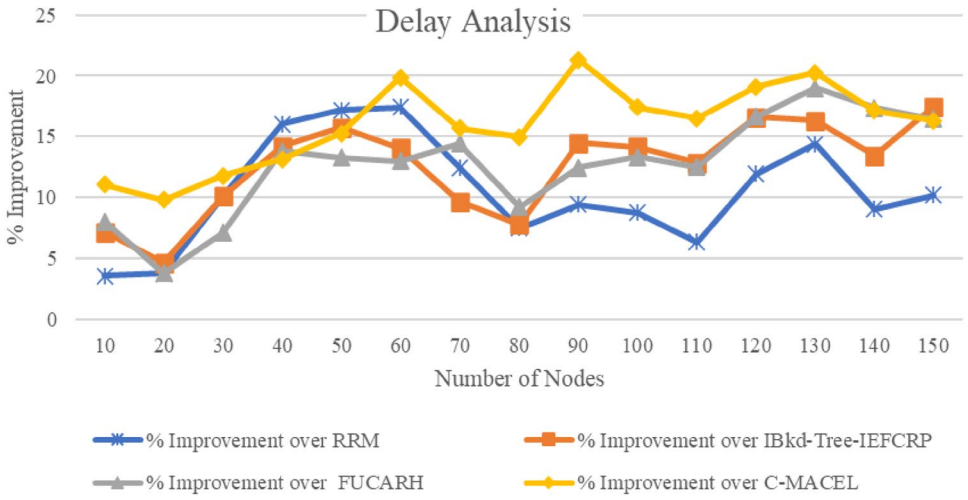


Fig. 11 Delay improvement analysis at 100 simulations

machine learning and swarm intelligence-based neural network approach which has been evaluated and compared with other techniques such as RRM, IBkd-Tree-IEFCRP, FUCARH, C-MACEL in order to find the higher level of trust node during the ranking generation process to increase the overall lifetime of the network. The results are obtained using the MATLAB simulation tool in terms of different QoS parameters such as Throughput, PDR, and Delay for different rounds of simulation (100, 200, 500 and 1000). (1) For 100 simulations, the average Throughput (Mbps) values for techniques such as RRM, IBkd-Tree-IEFCRP, FUCARH, C-MACEL and Trustnet are 8451.6306 Mbps, 8250.0886 Mbps, 8213.467733 Mbps, 7991.8692 Mbps and 8564.634467 Mbps respectively. (2) For 100 simulations, the average PDR values for techniques such as RRM, IBkd-Tree-IEFCRP, FUCARH, C-MACEL and Trustnet are 0.903066667, 0.874133333, 0.8366, 0.823866667 and 0.911 respectively. (3) For 100 simulations, the average Delay(sec) values for techniques such as RRM, IBkd-Tree-IEFCRP, FUCARH, C-MACEL and Trustnet are 3.626933333 s, 3.725 s, 3.736533333 s, 3.8742 s and 3.238933333 s respectively. With the involvement of deep learning and fuzzy logic techniques that enhances the security of complex networks from threats, along with the proposed technique can open new areas for research for exploring more in life time of network.

Author contributions SS and AK wrote the initial Draft, DG provided the software and resources, SJ wrote the final draft and performed the supervision, MK performed the supervision.

Funding The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Data availability The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

Declarations

Conflict of interest No, we declare that the authors have no competing interests as defined by Springer, or other interests that might be perceived to influence the results and/or discussion reported in this paper.

References

1. Ryu JH, Irfan M, Reyaz A (2015) A review on sensor network issues and robotics. J Sensors 6:1–14
2. Carlos LR, Manuel ZRV, del Rocio OLV, Gerardo ML (2018) Wireless sensor networks applications for monitoring environmental variables using evolutionary algorithms. In: Intelligent data sensing and processing for health and well-being applications. Academic Press, pp 257–281
3. Karl H, Willig A (2007) Protocols and architectures for wireless sensor networks. Wiley, Hoboken
4. Alkhatib AAA, Baicher GS (2012) Wireless sensor network architecture. In: 2012 International conference on computer networks and communication systems (CNCS 2012)
5. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E (2002) A survey on sensor networks. IEEE Commun Mag 40(8):102–114
6. Lopez J, Roman R, Agudo I, Fernandez-Gago C (2010) Trust management systems for wireless sensor networks: best practices. Comput Commun 33(9):1086–1093
7. Han G et al (2013) Management and applications of trust in wireless sensor networks: a survey. J Comput System Sci. https://doi.org/10.1016/j.jcss.2013.06.014
8. Ahmed A, Bakar KA, Channa MI, Khan AW, Haseeb K (2017) Energy-aware and secure routing with trust for disaster response wireless sensor network. Peer-to-Peer Netw Appl 10(1):216–237
9. Dhulipala VR, Karthik N (2017) Trust management technique in wireless sensor networks: challenges and issues for reliable communication: a review. CSI Trans ICT 5(3):281–294
10. Selvi M, Thangaramya K, Ganapathy S, Kulothungan K, Khannah Nehemiah H, Kannan A (2019) An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. Wirel Pers Commun 105(4):1475–1490
11. Khan T, Singh K (2019) Resource management based secure trust model for WSN. J Discrete Math Sci Cryptogr 22(8):1453–1462
12. Kiani F, Nematzadehmiandoab S, Seyyedabbasi A (2019) Designing a dynamic protocol for real-time Industrial Internet of Things-based applications by efficient management of system resources. Adv Mech Eng 11(10):1687814019866062
13. Kiyani F, Chalangari H, Yari S (2010) DCSE: a dynamic clustering for saving energy in wireless sensor network. In: 2010 Second international conference on communication software and networks. IEEE, pp 13–17
14. Seyyedabbasi A, Kiani F, Allahviranloo T, Fernandez-Gamiz U, Noeiaghdam S (2023) Optimal data transmission and path-finding for WSN and decentralized IoT systems using I-GWO and Ex-GWO algorithms. Alex Eng J 63:339–357
15. Kiani F, Rad A, Sis MK, Kut A, Alpkocak A (2013) EEAR: an energy effective-accuracy routing algorithm for wireless sensor networks. Life Sci J 10(2):39–45
16. Zahariadis T, Leligou HC, Trakadas P, Voliotis S (2010) Trust management in wireless sensor networks. Eur Trans Telecommun 21(4):386–395
17. Lopez J, Roman R, Agudo I, Fernandez-Gago C (2010) Trust Management Systems for Wireless Sensor Networks: Best practices. Comput Commun 33:0140–3664
18. Karthik N, Ananthanarayana VS (2017) Data trust model for event detection in wireless sensor networks using data correlation techniques. In: Fourth international conference on

signal processing, communication and networking (ICSCN), vol. 2017, pp. 1–5. IEEE
19. AlFarraj O, AlZubi A, Tolba A, Trust-based neighbor selection using activation function for secure routing in wireless sensor networks. J Ambient Intell Hum Comput 2018:1–11.
20. Selvi M, Thangaramya K, Ganapathy S, Kulothungan K, Khannah Nehemiah H, Kannan A (2019) An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. Wireless Pers Commun 105(4):1475–1490
21. Nie, S. A novel trust model of dynamic optimization based on entropy method in wireless sensor networks. Cluster Comput, 2017:1–10.
22. Anwar RW, Zainal A, Outay F et al (2019) BTEM: Belief based trust evaluation mechanism for wireless sensor networks. Futur Gener Comput Syst. https://doi.org/10.1016/j.future.2019.02.004
23. Amuthan A, Arulmurugan A (2021) Semi-Markov inspired hybrid trust prediction scheme for prolonging lifetime through reliable cluster head selection in WSNs. J King Saud Univ Comput Inf Sci 33(8):936–946
24. Janakiraman S, Priya MD, Devi SS, Sandhya G, Nivedhitha G, 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):e5–e5
25. Fang W, Zhang W, Yang W, Li Z, Gao W, Yang Y (2021) Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks. Digital Commun Netw 7(4):470–478
26. Chen Z, Tian L, Lin C (2017) Trust model of wireless sensor networks and its application in data fusion. Sensors 17(4):703
27. Boukerche A, Li X, El-Khatib K (2007) Trust-based security for wireless ad hoc and sensor networks. Comput Commun 30:2413–2427.
28. Yao Z, Kim D, Doh Y , 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), 2006, pp 437–446.
29. Liu K, Abu-Ghazaleh N, Kang K-D (2007) Location Verification and Trust Management for Resilient Geographic Routing. J Parallel Distrib Comput 67(2) pp:215–228.
30. Hung K-S, Lui K-S, Kwok Y-K, A trust-based geographical routing scheme in sensor networks. *Proceedings of WCNC* **, 2007**
31. Probst MJ, Kasera SK, Statistical trust establishment in wireless sensor networks. *International conference on parallel and distributed systems*, **2007**, vol 2.
32. Kim TK, Seo HS, A trust model using fuzzy logic in wireless sensor network. *World academy of science and engineering and Technology* ,**2008**, 42,pp:63–66
33. Momani M, Challa S, Alhmouz R , BNWSN: bayesian network trust model for wireless sensor networks. *Mosharaka international conference on communications, computers and applications (MIC-CCA '08), Amman, Jordan*, **2008**.
34. Ganeriwal S, Srivastava MB , Reputation-based framework for high integrity sensor networks. *Proceedings ACM workshop security of ad hoc and sensor networks (SASN'04)*, **2004**, pp 66–67.
35. Song F, Zhao B , Trust-based LEACH protocol for wireless sensor networks. *Second international conference on future generation communication and networking, FGCN '08.,* **2008.**
36. Zhou M-Z, Zhang Y, Wang J, Zhao S-Y, A reputation model based on behavior trust in wireless sensor networks. *Eighth IEEE international conference on scalable computing and communications*, **2009.**
37. Chen H (2009) Task-based trust management for wireless sensor networks. International Journal of Security and Its Applications 3(2):21–26
38. Gritzalis S, Aivaloglou E (2010) Hybrid trust and reputation management for sensor networks. Journal of Wireless Networks 16(5):1493–1510
39. Shaikh RA, Jameel H, d'Auriol BJ, Lee H, Lee S, Song Y-J, Group-based trust management scheme for clustered wireless sensor networks. *IEEE Trans Parallel Distrib Syst*., **2009**, 20(11) pp:1698–1712.
40. Karthik N, Ananthanarayana VS., Data trustworthiness in wireless sensor networks. *Trustcom/BigDataSE/ISPA*, **2016** IEEE.
41. Jothiprakasam, S., Muthial, C., 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/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. Enhanced Route Discovery Mechanism Using Improved CH Selection Using Q-Learning to Minimize Delay. *Scientific Programming*. **2022**.
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 AK, Goyal N, Sharma AK, Benslimane A, Singh A (2021) An enhanced energy proficient clustering (EEPC) algorithm for relay selection in heterogeneous WSNs. Ad Hoc Netw 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. J Supercomput 77(6):6036–6055
46. Meqdad, M.N.; Kadry, S.; Rauf, H.T. Improved Dragonfly Optimization Algorithm for Detecting IoT Outlier Sensors. *Future Internet* **2022**, 14, 297. https:// doi.org/https://doi.org/10.3390/fi14100297
47. Arjunan S, Sujatha P (2018) Lifetime maximization of wireless sensor network using fuzzy based unequal clustering and ACO based routing hybrid protocol. Appl Intell 48:2229–2246
48. Rathore PS, Chatterjee JM, Kumar A, Sujatha R (2021) Energy-efficient cluster head selection through relay approach for WSN. J Supercomput 77:7649–7675
49. Verma, K., Bhardwaj, S., Arya, R., Islam, U. L., Bhushan, M., Kumar, A., & Samant, P. Latest tools for data mining and machine learning, **2019**.
50. Rani, S., Koundal, D., Kavita, F., Ijaz, M. F., Elhoseny, M., & Alghamdi, M. I. An optimized framework for WSN routing in the context of industry 4.0. *Sensors*, **2021**, 21(19), 6474.
51. Seyyedabbasi A, Dogan G, Kiani F (2020) HEEL: A new clustering method to improve wireless sensor network lifetime. IET wireless sensor systems 10(3):130–136
52. Kiani F, Seyyedabbasi A, Nematzadeh S (2021) Improving the performance of hierarchical wireless sensor networks using the metaheuristic algorithms: efficient cluster head selection. Sens Rev 41(4):368–381
53. Juneja A, Juneja S, Bali V, Mahajan S (2021) Multi-criterion decision making for wireless communication technologies adoption in IoT. International Journal of System Dynamics Applications (IJSDA) 10(1):1–15
54. Monga, Chetna, et al. "Sustainable network by enhancing attribute-based selection mechanism using Lagrange in-terpolation." *Sustainability*, **2022**, 14.10: 6082.

55. J. H. Anajemba, T. Yue, C. Iwendi, P. Chatterjee, D. Ngabo and W. S. Alnumay, "A Secure Multiuser Privacy Technique for Wireless IoT Networks Using Stochastic Privacy Optimization," in IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2566–2577, 15 Feb.15, 2022, doi: https://doi.org/10.1109/JIOT.2021.3050755.

56. Roy AK, Nath K, Srivastava G, Gadekallu TR, Lin JCW (2022) Privacy preserving multi-party key exchange protocol for wireless mesh networks. Sensors 22(5):1958