Journal of Autonomous Intelligence (2024) Volume 7 Issue 4
doi: 10.32629/jai.v7i4.1380

ORIGINAL RESEARCH ARTICLE

An optimized deep learning-based fault-tolerant mechanism for energy efficient data transmission in IoT

Siddharth Kumar[1,*], Mahadev[1], Reema Goyal[2], Preet Kamal[1], Alankrita Aggarwal[1]

[1] *Department of Computer Science and Engineering, Apex Institute of Technology, Chandigarh University, Mohali 140413, India*

[2] *Computer Science and Engineering Department, Chandigarh University, Mohali 140413, India*

*** Corresponding author:** Siddharth Kumar, siddharth.e12853@cumail.in

ABSTRACT

Artificial Intelligence (AI) based framework for the Internet of Things (IoTs) have gained worldwide attention in recent years, mainly with the explosion of Micro-Electro-Mechanical Systems (MEMS) technology. Basically, MEMS has facilitated the development of tiny and smart sensors for the IoT-based framework. An AI-based IoT model is an emerging technology that helps in both fault-tolerant as well as energy-efficient data transmission purposes. For efficient data transmission in an IoT-based model, the concept of Wireless Sensor Network (WSN) plays a vital role that comprises various sensor nodes that communicate together to monitor and gather information from the various Region of Interest (RoI). Generally, sensor nodes are tiny in size and having a small battery life, limited sensing, processing, and communication capabilities. So, the fault-tolerant mechanism for energy efficient data transmission in IoT is a good initiative with the combination of Deep Learning as an AI approach. In this research article, the concept of deep learning-based fault-tolerant mechanism in IoT frameworks for energy efficient data transmission is proposed in an optimized manner. Here, the concept of the Grouped-Bee Colony (GBC) algorithm is designed for the fault detection mechanism as an optimization approach along with the Deep Learning as an AI.

Keywords: internet; Internet of Things; fault analysis; WSN; Artificial Intelligence; GBC; deep learning

ARTICLE INFO

Received: 20 October 2023
Accepted: 1 December 2023
Available online: 2 February 2024

1. Introduction

Nowadays, due popularity of the internet as well as the things related to internets, Internet of Things (IoT) achieved major focus of researchers and industrial people[1]. IoT is a network of inter-connected devices, physical components, digital equipment's, people, and living creatures that permits the exchange of information without the necessity of human interaction. Humans with embedded monitoring devices, farm animals with biosensor transceivers as well as other devices that are allotted an IP address and transmit datagrams over a network are examples of things[2]. Businesses from a variety of industries are using IoT more frequently to run more efficiently, help us understand their consumers to offer superior service, response and increase company's worth. The IoT environment is made up of internet-connected devices that gather and transmit information from surroundings using embedded systems like processing elements, detectors, and telecommunications equipment. IoT systems share sensor information by linking to an IoT gateway, which either explores data locally or transmits

it to cloud for examination[3]. These devices connect with other devices and take actions based on shared data among them. Though consumers can connect with devices to start them up, give instructions, or access information, gadgets do maximum work without additional support. These systems have a massive effect on network protocols that these web-enabled devices use. IoT could use ML and Al to make data gathering simpler and more flexible. When something is connected to internet, it either sends or receives data. The ability to transmit and receive data makes things smart. A thing is not required to have a high storage or super-computer within it to be intelligent. Everything is linked to a super storage or a super computer. So, IoT is implemented on things to make them smart. Being connected is good. The IoT is connection of one billion interrelated devices that can detect, collect, and transfer data between itself without human intervention[4]. IoT-enabled services that improve people's lives include health care tracking, building automation, logistics, linked cars, smart agricultural, and other IoT-enabled services. According to this scenario, networked smart products will replace the Internet as a new paradigm. IoT has the potential to change the Internet in a way that makes machine-to-machine (M-2-M learning a reality. The IoT will develop as a result of the reconfiguration taking place by making physical objects "smart," enabling them to do tasks on their own. IoT promises to increase the accessibility of modern gadgets by allowing connections to be made at any time and in any place. **Figure 1**. displays IoT block diagram which is used in common environment.

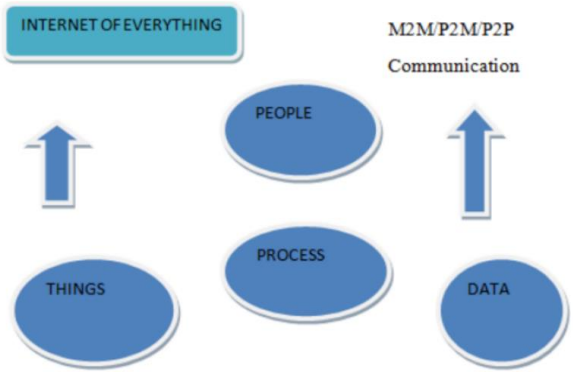

Figure 1. IoT block diagram.

IoT is made up of people, things, processes, and data and encompasses commercial and industrial operations that support people's daily lives. IoT essentially enables the independent, secure communication of physical items[5]. The IoT eliminates physical labour by automating routine tasks. The number of things with Internet access is always growing. Numerous sensors found in smart phones may gather information, process it, and forward it over the Internet. Numerous applications can be created using that system and various sensor-equipped devices, each of which will offer compelling advantages.

- It can aid in the more sophisticated mobile device management of cities and houses. It enhances safety for people.
- Time spent is reduced by automating chores.
- Despite the distance between us and our exact position, data is still easily accessible and updated frequently.
- Electric devices are usually linked to and connect with controller computer, like cell phone to utilize electricity more effectively. Consequently, there won't be unnecessary consumption of electrical gadget.
- IoT apps give assistance by maintaining daily schedule.
- It is useful for safety since it recognizes any possible threat and warns users.
- IoT devices interact with each another, carry out many tasks without human intervention, and reduce amount of labour that needs to be done by human.

There are four basic elements of IoT systems that are Sensor/devices, Gateways, Data Processing (Cloud and Analytics), and User Interface[6].

a) Sensor or devices: A sensor is a piece of hardware that collects data from its surroundings and gives to the system by transforming it and actuator transforms electric signals into physical trials.

b) Smart sensors: These are the component of device connectivity layer. It collects data from environment and forwards to gateway. Modern sensors are linked to low power networks like Wi-Fi etc.

c) Gateway: It can be arranged to pre-process the recorded information from thousands of sensors before forwarding it to cloud. It serves as an intermediate among devices and cloud, protecting network from attacks.

d) Cloud and analytics: IoT cloud provides tools for data collection, processing, and management and store big data generated by gadgets, applications and users. Analytics converts analogy data from sensors into useful information which is used for detailed analysis[4].

e) User interface: It should be well designed, so that users can perform minimum efforts to operate the IoT devices through it. Multicolour touch panels, for example, have overtaken hard switches in home appliances.

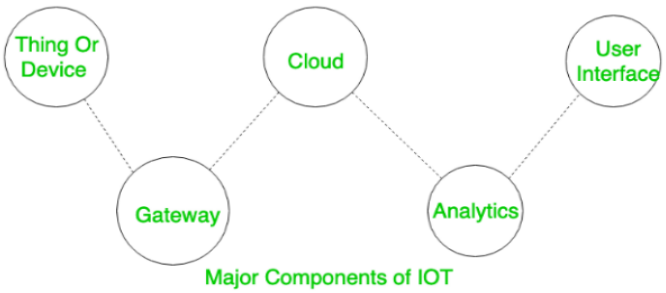

Figure 2. Major components of IoT networks.

After analysing the structure of IoT enabled networks based on **Figure 2**, we have concluded some drawbacks that are listed here[7]:

- As there are more connected devices and data is transferred more broadly among devices, there is greater chance that hackers may be able to access confidential details.
- It could be necessary for businesses to deal with billions or even enormous numbers of IoT gadgets in future, and managing and gathering data from all those gadgets will be challenging.
- If there is problem with system, every connected device would most likely get damaged.
- Since there isn't universal IoT interoperability benchmark, connecting gadgets from different manufacturers can be difficult.

To deal with such drawbacks, the concept of Wireless Sensor Network (WSN) plays a vital role. WSNs are systems of sensor devices that receive as well as process information to a base station. Sensor nodes are made up of signalling, storage, integration, behaving, as well as energy components[8]. It gathers data from each device as well as sends it to the Base Station either instantly through other nodes for more processing. SNs are either manually or instantaneously distributed. WSNs help society by incorporating sensor nodes into a variety of environments. The base station serves as the main hub for all nodes which can be stationary or mobile in order to gather data from SNs and perform complicated data processing. Base stations typically have greater capacities than sensor nodes as they have more processing power, memory, and effort. The base stations could even detect the sensor network to the current transmission line, i.e., the internet, where the information generated by connected node could be accessed by a remote device. WSNs could be utilised in multiple devices for monitoring pollution levels, natural disasters,

tsunamis, battlefields, as well as floods, and enemy intrusion detection, targeting, forest fire detection, industry tracking, evaluation apparatus, agriculture etc. Wireless Sensor Network's main limitations are energy, a limited battery, communication, computation, and memory. The adaptability of Wireless Sensor Networks in providing a low-cost as well as feasible method to the distant place has caught the interest of research teams. WSN's power saving scenarios for maximizing network lifespan are very necessary. In these days, WSN-based IoT has become a significant technology in today's interconnected society, with the potential to alter multiple industries such as healthcare and agriculture. The utilization of WSNs is of great significance in the context of IoT applications, as they play a crucial role in the collection and transmission of vital data from the physical environment to decision-making systems. Nevertheless, as the scale and diversity IoT installations increase, a significant problem arises, namely the need to guarantee dependable and energy-efficient transmission of data in contexts with limited resources. The importance of ensuring the dependability of data transmission in the IoT cannot be overstated, as it has a direct influence on various applications such as remote monitoring, predictive maintenance, and real-time decision-making. Failures or disruptions in data transmission can have significant ramifications in many situations. These repercussions range from affecting patient care in healthcare settings to diminishing the efficiency of industrial processes. Moreover, the rapid expansion of IoT devices has brought about a significant increase in energy consumption. This has emerged as a critical issue due to the adverse environmental implications associated with excessive energy usage, as well as the detrimental impact it has on the operational longevity of battery-powered IoT sensors[9]. Conventional fault-tolerant techniques and energy-efficient protocols frequently prove insufficient in effectively resolving these two concurrent concerns. In order to address this disparity, our research aims to leverage the capabilities of deep learning methodologies. Deep learning has demonstrated significant potential in diverse fields, ranging from the identification of visual patterns to the analysis of human language. Our objective is to improve the transmission of IoT data by adapting and optimizing deep learning techniques for fault detection and tolerance within WSNs. The motivation behind this study is complex and encompasses various factors. First and foremost, the objective is to improve the dependability of IoT systems by actively detecting and addressing errors in real-time. This aims to guarantee the uninterrupted transmission of crucial data to its intended recipient. Additionally, our research endeavours to enhance the longevity of IoT devices by maximizing energy-efficient data transfer, hence mitigating maintenance expenses and minimizing environmental repercussions. This study makes a valuable contribution to the wider domain of the IoT, enhancing its fundamental principles and promoting the development of innovative applications with potential positive effects on society, industry, and the environment[10]. The underlying motivation for our research lies in the conviction that the development of an enhanced deep learning-driven fault-tolerant mechanism for energy-efficient data transmission in IoT through WSNs holds the promise of expanding the horizons of IoT applications. This advancement has the potential to enhance their dependability, sustainability, and overall significance to a greater extent than previously achievable. The major contribution of this article is given as:

- This text aims to provide a concise overview of the current research on fault-tolerant mechanisms for energy-efficient data transmission in a WSN-based IoT paradigm.
- Utilize the concept of Grouped-Bee Colony (GBC) algorithm along with the Deep Learning for efficient data transmission with fault tolerant mechanism.
- To validate the efficiency of the proposed mechanism, we evaluate the Quality of service (QoS) parameters and compare with the existing work.

The remainder of this research article is organized as follows: In Section 2, we present an overview of related studies that focus on the current state of fault tolerance with energy efficient manner using deep learning. Section 3 investigates regarding the method and materials with methodology of the developed model, and experimental

findings of our proposed model is discussed in the Section 4. In Section 5, we conclude our system's analysis and discuss associated challenges and potential future outcomes.

2. Literature survey

In this segment of article, lots of existing work are analysed to find out the issues related to the fault tolerance as well as efficient data transmission based on the concept of WSN-based IoT model using the different techniques or algorithms. Towards this step, in 2021, Maheshwari et al.[11] used Butterfly Optimization in this study to select CH among various nodes and reduce overall energy usage while enhancing network lifetime. Residual energy of nodes, distance to BS and node degree are used to optimize CH selection. ACO finds best route among CH and BS based on node centrality. Proposed methodology is examined with metrics like alive and dead nodes, energy usage, and datagrams obtained at BS. The outcomes of suggested technique are contrasted to LEACH, DEEC, FUCHAR, CRHS, BERA, CPSO, ALOC, and FLION. Proposed methodology has 200 alive nodes after 1500 iterations i.e., greater than CRHS and BERA. In 2020, El Khediri et al.[12] had suggested K-means clustering technique for WSNs. Given the limited amount of space available, this method manages node energy usage and improve WSN running time. Since there are many nodes and radio channel are not stable, the development of clusters is organized as a k-means sample space partitioning. After measuring total energy usage, best CHs are determined based on network size. For objective function, distance between CH and node is measured, and membership weight are considered. We propose Optimal K-means, a method for forming multiple node clusters that use an improved K-means clustering (OK-means). Authors propose K-means clustering for intra-cluster interaction, whereas inter-cluster interaction uses a multi-hop interaction. Performance is evaluated in Ns-2 simulator. According to the simulation results, suggested technique obtains even distribution in the spatial domain of CH. As a result, energy consumption is properly balanced. Furthermore, extensive simulations with varying node densities have been run to demonstrate OK-means' full potential. In 2019, Daneshvar et al.[13] presented a latest clustering technique that takes the grey wolf optimizer (GWO) to select Cluster Heads (CHs). GWO is a latest multi-agent approach based on grey wolf behaviours that has remarkable attributes as well as competitor outcomes. The alternatives are valued focused on the predicted energy usage as well as current remaining energy of every node in important to target CHs. The suggested technique employs the same clustering in numerous consecutive matches to enhance energy efficiency. This enables the procedure to save the energy needed to transform the clustering Researchers also introduce a latest dual-hop routing protocol for CHs located far from the BS as well as demonstrate that the proposed method guarantees the least & most balanced power consumption while the remaining nodes communicate using single-hop interaction. The system is assessed in a range of circumstances, and it is demonstrated that the routing framework enhances life of the system when compared to a series of recent similar algorithms. In 2019, Zhao et al.[14] suggest the optimal CH feature to pick the CH of every cluster in every loop, as well as the optimal CH feature is built using the RE & node roles. Eventually, a few variables of the optimal CH feature are decided based on the system framework to maximize the CH economic plan. The simulation outcomes demonstrate that proposed routing approach is high reliable than 4 other procedures, which is important for the app.in 3D environment monitoring. In same year, Altakhayneh et al.[15] presented a Genetic LEACH algorithm which is tested for 100 nodes in aspects of alive nodes, energy usage, cluster head count, and packet delivery to CHs. CH is chosen by using a genetic algorithm that can identify the most efficient CHs. Stability zone of G-LEACH is 358 rounds larger than LEACH because first node in G-LEACH dies after 1544 rounds. That means that using G-LEACH extends network's lifetime by 61.7% and increase CHs efficiency by 10%. In 2019, Bongale et al.[16] describes a CH selection approach for WSNs relying on FA and Harmony Search Algorithm in this paper. Suggested hybrid protocol makes following contributions to avoid problems caused by early convergence in nature-inspired optimization techniques. HSA in first stage finds CHs that are isolated from one another by some distance. Sharma and Kulkarni[17] in 2018 had

suggested novel routing protocol in this paper which primarily depends on Improved Energy Efficient Chain Based Routing. It employs the HBO for optimal node selection operation. To improve Honey Bee Optimization-based IECBR. they enhanced HBO based on autonomous localization, which confirms that nodes aren't depleted of energy beyond their threshold, as load is distributed among nodes, and strength of node in minimum route has attained threshold. Modified H-IECBR is the name given to this new routing protocol (MH-IECBR). MH-IECBR outperforms other methods as per network lifetime. In 2018, Arjunan and Sujatha[18] had introduced Fuzzy logic-based Unequal clustering algorithm and ACO based Routing in this paper to remove hot spots and enhance network lifespan. Cluster formation and inter-cluster routing are part of this protocol. FL efficiently chooses CHs and segments network into unequal clusters as per remaining energy, distance to BS and neighbouring nodes. It employs ACO for inter-cluster routing between CHs and BS. Furthermore, it transfers data in hybrid mode, that is, both proactive and reactive. In addition to periodic data transfer, a threshold value is used to inform about instant needs in network. A new routing approach is also used for proper load balancing, in which threshold-based data transfer occur in smallest route and periodic data transfer occurs in unused routes. For uniform load distribution, the cross-layer cluster formation is also used. The proposed method has been extensively tested and contrasted to LEACH, TEEN, DEEC, and EAUCF. It achieves better lifetime, removes hot spots, and efficiently balances energy usage across all nodes. In 2017, Chen et al.[19] had proposed ant colony path optimization-based clustering for the energy-efficient transmission protocol (CEETP-ACPO) for WSN. Distributed cluster computing selects CHs based on node's energy. Secondly, optimal route is chosen by using improved ACO. Next-hop range of nodes is controlled by ring-angle search model and transition probability is assessed by pheromone and proximity of node. Outcomes reveal that proposed protocol work better than others.

Based on the study made in the above section of article, the study is divided into two segments namely fault identification or classification and fault tolerance scheme. Most of the article cited in section, aims to either increase the classification accuracy of the system or to enhance the tolerant behaviour of the network. The identified gaps are as follows:

- Most of researchers had employed machine learning for fault detection in a sensor network. The work exhibited high fault detection and prevents the reoccurrence of fault. However, the upcoming faults were not quantified or predicted using the SVM classifier.
- Some researchers had represented a comparative analysis of six different machine learning classifiers but does not discuss the analysis of scalability in the comparison. The analysis lacks on the explanation on the behavior of the classification algorithms when the network load is increased in the system.
- One researcher had focused on link failure only considered network level faults. Inter and intra cluster faults were also not discussed. In addition to that integration of machine learning is also found to be missing which could have increased the true alarm detection rate.
- Few of them had integrated fuzzy logic with deep neural networks to diagnose faults. Deep neural network requires bulk volume of data whereas the chances to have increased ruleset with bulk volume of data is high which would further increase the computation complexity.
- Few had integrated machine learning based Swarm Intelligence oriented PSO for the enhancement of fault tolerance and also incorporated inter and intra clustering concept but, misses out on the trial of other Swarm Intelligence algorithm like Grasshopper, Firefly, Artificial Bee Colony (ABC), etc.
- Some researchers had proposed clustering and routing mechanism based on cost function that was in turn dependent on the energy consumption. However, researchers did not focused failures that are caused due to individual sensor node failure that interrupted the network performance.

- A distributed fault prediction model was proposed by El Khediri et al.[12] 2018 for wireless sensor networks. But this model was more suitable for meteorological sensor networks, capable of predicting when the node density is low.

Based on the above-mentioned gaps, we decided to proposed a model named as an optimized deep learning-based fault-tolerant mechanism for energy efficient data transmission in WSN-based IoT model.

3. Method and material

In this segment, we explain the working mechanism of the proposed an optimized deep learning-based fault-tolerant mechanism for energy efficient data transmission in WSN-based IoT model. Based on the study made in the literature and by considering the gaps, the proposed methodology is divided into two sub-sequent sections. Section A integrates the architecture of machine learning for the selection of the Cluster Heads (CHs). Section B illustrates the working behaviour and architecture of the fault identification or classification. To extend the fault tolerance capacity of the network, section A is quite helpful and is explained as follows.

The CH selection policy in WSN-based IoT Model: The cluster heads in WSN are created to reduce the overhead of the nodes and to reduce the computation complexity of searching the nodes by applying broadcast mechanism. Under the broadcast mechanism, the seeking node sends hello packets to the nearby nodes and waits for the response message from other nodes. In case of clusters, this work is performed by cluster heads itself. The proposed work aims to integrate machine learning based advancement in the cluster mechanism to enhance the efficiency of the network. The selection of the cluster head will be preliminary done by utilizing two factors.

M1. Distance to base-station

M2. Residual energy of the nodes

In the cited CH selection policies, every node contains a probability of being the CH which is calculated as follows[13,15,20–22].

$$Threshold_{selection}(Ts) = \frac{Desired_{percentage}(Dp)}{1 - D_p(Sim_{itr} \times \left|\frac{1}{Dp}\right|)} \quad (1)$$

where Dp is the desired percentage of the node to be CH in the network. Sim_{itr} is the simulation iteration or current simulation round. The high precision threshold containing nodes are selected as the CH and the nodes must have moderate values for distance to base station and residual energy.

The threshold for the selection of the distance to base station and residual energy both can be calculated by computing average value of each value in the list. The policy keeps on updating the remaining residual energy data and a check point will be established where the information collection process will be applied. The application of machine learning architecture will further segregate the collected data into ground truth values which will be represented by a set of labels as {'Not-faulty', 'Moderate-faulty', 'Faulty'}. The extracted ground truth values will be used in the training process of fault identification and classification. The process of the application of machine learning can be explained through the following flow diagram.

$$Energy_{consumption} = Tx + Rx + Ax \quad (2)$$

where, Tx is the transmitter energy, Rx receiver energy and Ax is aggregation energy.

The Fault identification mechanism: The fault detection mechanism utilizes the ground truth generated in Section A. The fault identification mechanism will consist of two sub-sequent processes namely training and classification. The training process will use the repository shown in **Figure 3** as evaluation properties. The training

process will be done by utilizing propagation-based learning mechanisms as SVM, Neural Networks or Deep Neural Network. Based on the complexity of the data, the selection of the classification algorithm will be done. The proposed work aims to utilize semi-supervised learning approach. The semi-supervised learning approach divides the data into two portions, one for training and another for classification. The distribution % could be 70% for training and the rest 30% for the classification. Semi-supervised learning approach is used to testify the rigidness of the classification algorithm. The classification process uses the trained structure and finds out best suitable matching ground truth value as a result. The overall process can be represented by a work flow diagram as shown in **Figure 4**.

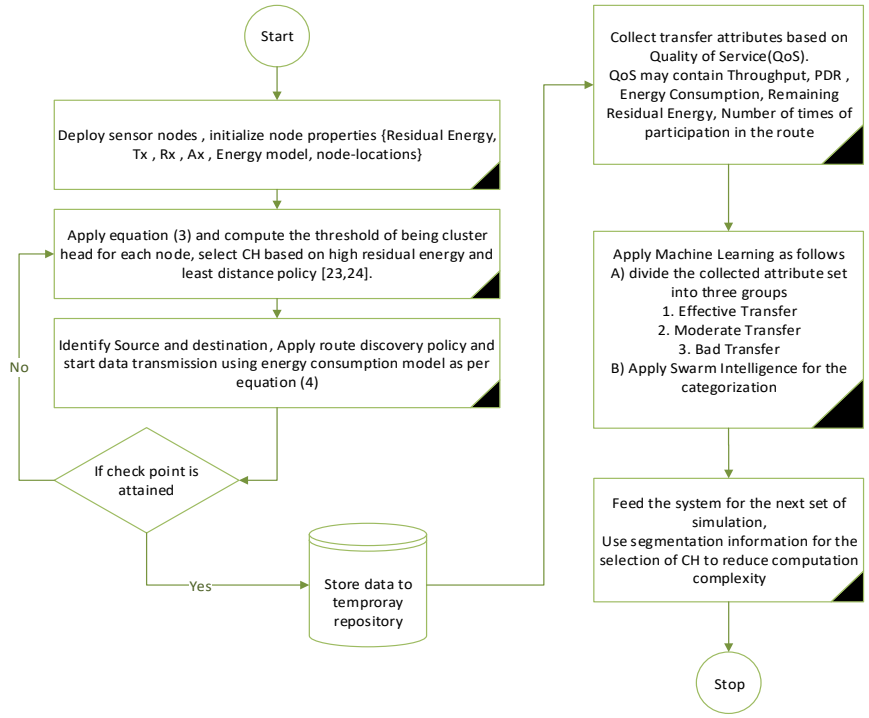

Figure 3. Proposed work flow policy for CH selection.

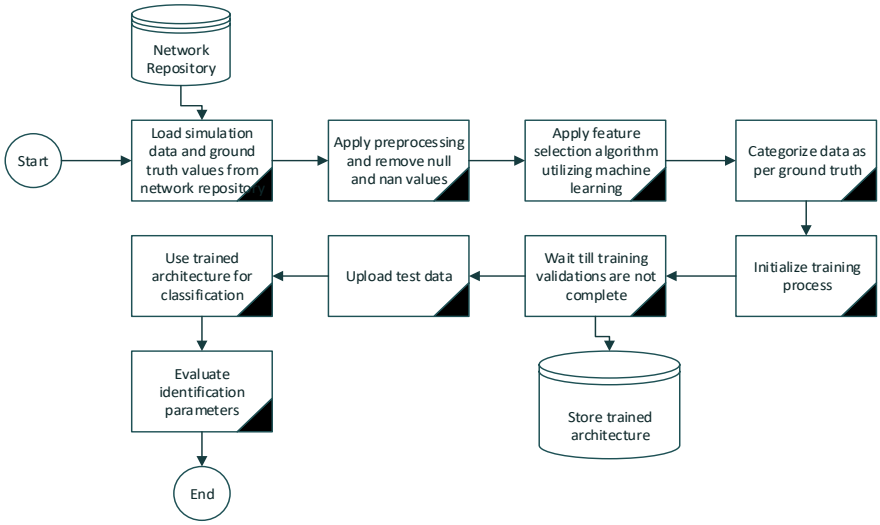

Figure 4. Fault identification.

Here, we introduced the concept of GBC algorithm along with the deep learning mechanism and the flow of GBC algorithm is shown in the **Figure 5**.

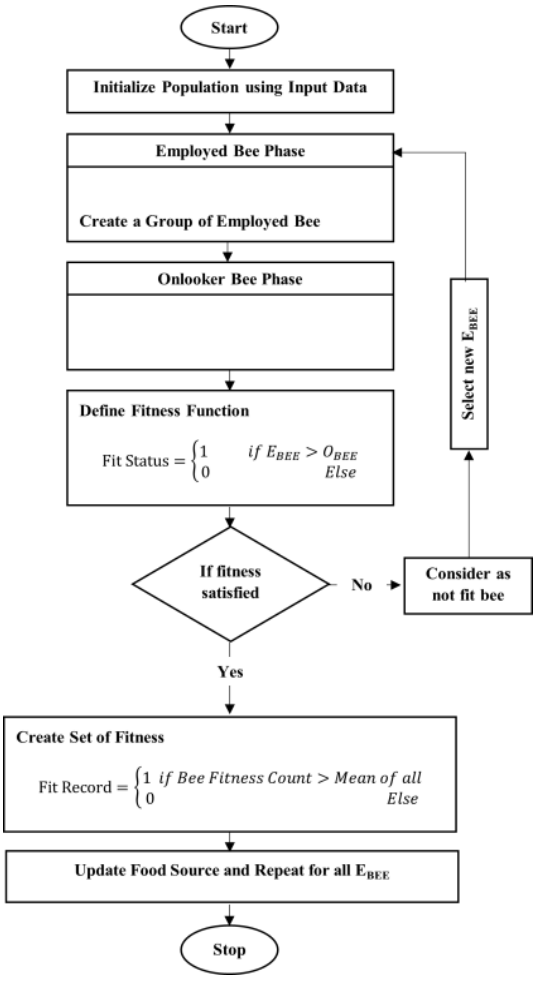

Figure 5. Flow of GBC Algorithm.

Algorithm 1 G-ABC

Input: N_{DATA} ← Normalized data after pre-processing
Output: S_{DATA} ← Selected data from normalized data based on their fitness
Calculate Size, [Row, Col] = Size (N_{DATA})
Final Record = []
Count = 1
For I in range (N_{DATA}, Col)
    Current Feature Col = N_{DATA} (All Row, I)
    All Grouped Bee Record = []
    For J in range (5)
        Ebee = [Current Feature Col (1), Other five Current Feature Col (Randomly)]
        $Obee = \frac{\sum_1^J Ebee(J)}{Number\ of\ Ebee}$
        Define fitness function of G-ABC
            All Fit Record = []
            Fit Status = 0
            For K in range (Ebee)
                If Ebee (K) > Obee
                    Fit Status = 1

Algorithm 1 (*Continued*)

```
                Else
                    Fit Status = 0
                End – If
            All Fit Record (K) = Fit Status
            End – For
        End – For
        All Fit = fitness function(Ebee, Obee)
        If count of non-zeros in All Fit > 1
            Bee Status = 1
        Else
            Bee Status = 0
        End – If
        All Bee Record (J) = Bee Status
        End – For
        If count of non-zeros in All Bee Record > Average (All Bee Record)
            Final Record (count) = I
            Count = Count + 1
        End – If
End – For
Select data from normalized data according to selected index by G-ABC
S_DATA = N_DATA (All Row, Final Record)
Return: SDATA as a selected data
End – Algorithm
```

The algorithm of proposed model with GBC is written above (Algorithm 1) and based on this mechanism we evaluated the performance of the model in terms of QoS parameters. The simulation results of proposed WSN-based IoT model using deep learning algorithm are described in the below section of paper.

4. Results and analysis

This work utilises a swarm-based technique to optimise the performance of deep learning as a classifier for the goal of categorising nodes as either malevolent or failing. The classification is based on the experiment conducted, without the usage of a pre-existing dataset. The classification is determined by the most advantageous attributes of wireless sensor nodes within an IoT network. This section showcases the simulation outcomes of a proposed Internet of Things (IoT) network designed for machine-to-machine (M-2-M) communication. The network employs an energy-efficient routing protocol and an optimised deep learning algorithm for an energy-aware, fault-tolerant routing protocol. The efficiency of the proposed Internet of Things (IoT) network is subsequently evaluated by comparing it to existing research using measures such as energy consumption, loss rate, and end-to-end delay. The authors propose an Internet of Things (IoT) paradigm that integrates a very effective routing mechanism for emergency response in their paper. The IoT network's performance is improved by utilising an emergency-based routing mechanism. The current study employs a simulation environment, which is described in the table. The results of the simulations are explained in the next section. The simulation results of the suggested study are shown in comparison to the current work[11], as noted earlier. This section presents the simulation results of a proposed optimised deep learning-based fault-tolerant mechanism for energy-efficient data transmission in IoT. The efficiency of the suggested work is compared with existing work[11]. **Table 1** displays the simulation environment used in the proposed study, while the next part offers a description of the simulation results.

Table 1. Proposed network setup & requirements.

Parameters	Values/Description
Number of sensor nodes	50–1000
Area of WSN-Based IoT network	1000 × 1000 m^2
Simulation tool	Data Acquisition, Machine Learning, Communication and Optimization Toolbox
Routing protocol	Cluster-based Fault-Tolerant Mechanism for Energy Efficient Data Transmission
Swarm-based optimizer	Grouped-Artificial Bee Colony (GBC) according to Algorithm
Classifier	Deep Neural Network (DNN) as Deep Learning
Simulation parameter	Faulty and Non-faulty, Delay of transmission and Energy Consumption
Evaluation parameter	Throughput, Loss Rate, Energy Consumption Rate, Number of Alive Nodes, End to End Delay and Detection Rate

In this research, GBC-based optimization algorithm with DNN is used as classifier to classify the faulty or fails nodes based on the optimized properties of communicating wireless sensor nodes in IoT network. The table illustrates the simulation environment of the proposed study, while the subsequent section provides a description of the simulation results. Based on the aforementioned scenario, the simulation outcomes of the proposed study in comparison to the current work[11] are shown as follows:

From the standpoint of optimised WSN-based IoT networks, throughput refers to the intricate evaluation of the highest quantity of data packets that can be transmitted between a transmitting (Tx) sensor node and a receiving (Rx) sensor node via a safe or trustworthy pathway.

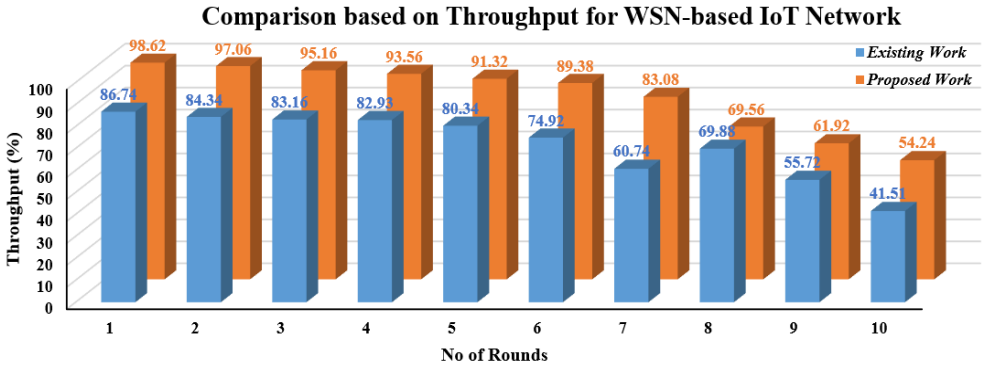

Figure 6. Comparison of throughput for WSN-based IoT network.

The throughput value for the planned IoT network utilising a cluster-based fault-tolerant mechanism for an energy-efficient data transmission routing protocol based on the optimised DNN may be calculated using Equation (3).

$$Throughput = \frac{\sum_{i=1}^{IOT\ Node}\left(P_{Successful\ delivered}\right) \times \left(P_{AverageSize}\right)}{P_{SentTime}} \quad (3)$$

where, $P_{\text{Successful delivered}}$ is the successful packet with respect to each communicating IoT nodes, $P_{\text{AverageSize}}$ is average packet size and P_{SentTime} is total time taken by nodes to send packets. The figure presented in **Figure 6** displays the achieved throughput of the developed WSN-based IoT network. It provides a comparison between the proposed work and existing research. The image illustrates the relationship between the number of simulation

rounds on the x-axis and the measured throughput values for the proposed WSN-based IoT network on the y-axis. The orange colour bar line is indicative of the measured throughput value derived from the planned WSN-based IoT network. Based on the comparative graph provided, it is evident that the throughput value observed for the WSN-based IoT network surpasses that of the current technique. This improvement is achieved by the integration of the GBC with the Deep Neural Network (DNN) as a classifier.

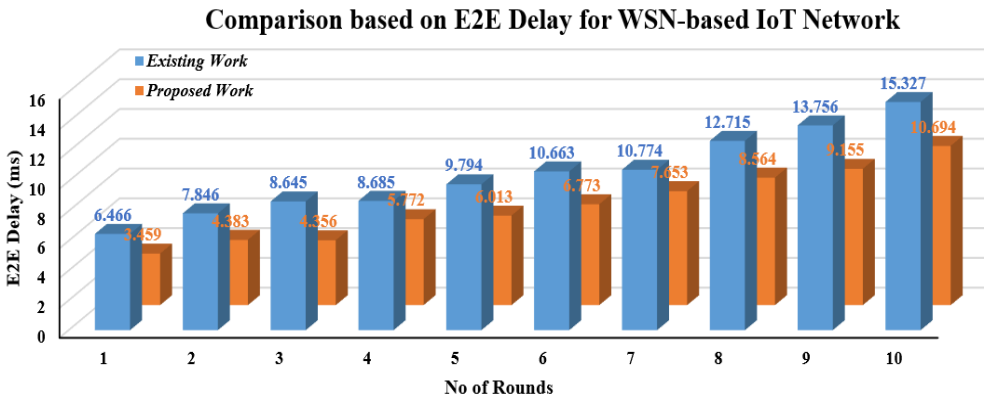

Figure 7. Comparison of E2E delay for WSN-based IoT network.

The total amount of time it takes to send a packet of data through the planned IoT network is measured in terms of its E2E (end-to-end delay) value. The planned work's total delay value can be calculated with the help of the provided equation.

$$E2E - Delay = \sum_{i=1}^{SIoT\ Node} T_t + R_t + W_t \tag{4}$$

Time spent transmitting packet data (Tt), time spent receiving packet data (Rt), and time spent waiting (Wt) are all considered. **Figure 7** compare the proposed WSN-based IoT network's end-to-end delay for packet data transfer to that of existing work. The graph shows the measured end-to-end delay for the proposed protocol in orange color and the existing in red color. With the hybridization of GBC and DNN, the new approach reduces latency compared to the state-of-the-art routing protocol.

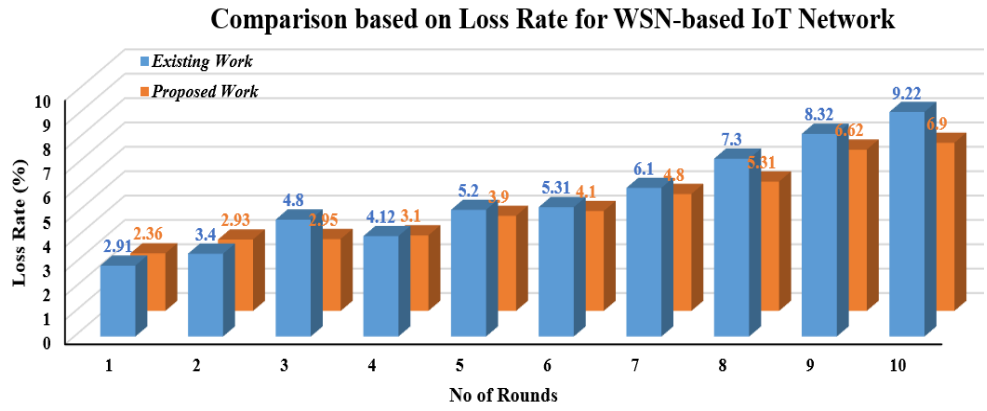

Figure 8. Comparison of loss rate for WSN-based IoT network.

When two sensor nodes in the same network try to send a data packet at nearly the same time, this causes a loss rate. When two data packets are sent at once, the Internet of Things network detects a "collision of sensor nodes"

and drops one or both of them. Loss is a common occurrence in WSN-based IoT networks. **Figure 8** presents the loss value of the proposed IoT network, which compares the proposed model to the current one. Existing work and an enhanced cluster-based routing protocol utilizing GBC and DNN are represented by blue and red bars, respectively, in the graph. Using the proposed technique significantly improves the IoT network's loss rate.

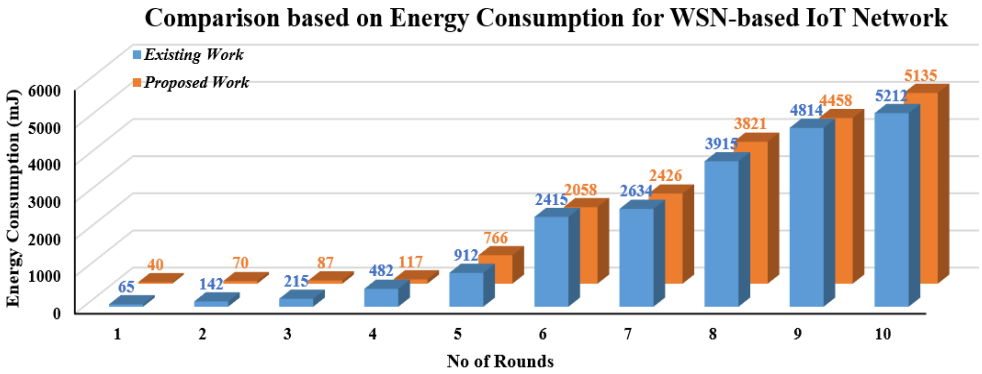

Figure 9. Comparison of energy consumption for WSN-based IoT Network.

Our suggested cluster-based routing protocol's effectiveness in conserving energy is measured by the aforementioned indicators for the WSN-based IoT network and **Figure 9** shows the obtained energy consumption. The formula for determining the total amount of energy used in a WSN-based IoT network every data packet successfully delivered to a target sensor node is as follows:

$$E_C = \sum_{i=1}^{IoT\ Node} T_E + R_E + W_E \tag{5}$$

where T_E is the total energy used by a sensor node during packet transmission in an IoT network, R_E is the total energy used by a receiver sensor node, and W_E is the rate at which energy is used by sensor nodes while they wait to receive a data packet. **Figure 9** compares the suggested approach with the state of the art regarding the amount of energy used by sensor nodes in an IoT network while sending packets of data from one node to another. The above graph shows that the cluster-based protocol, which combines GBC and DNN as a deep learning, reduces energy consumption by 8.72% when compared to the standard routing protocol. The fault classification performance comparison of proposed WSN-based IoT network for fault-tolerant mechanism for energy efficient data transmission as a routing mechanism based on the GBC and DNN as a classifier is described in below section with simulation results.

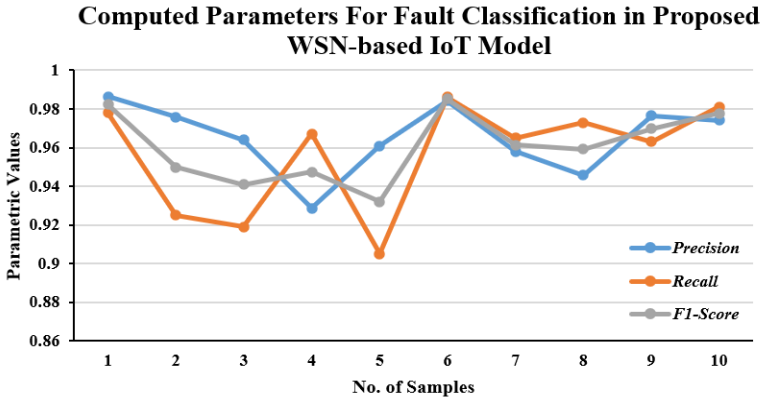

Figure 10. Precision of FND system.

Above **Figure 10** represents the calculated parameters of the WSN-based IoT network to classify the fault in terms of precision, recall and F1-score to verify the model effectiveness in terms of classification. Precision, recall, and f1-score are all significantly improved by utilizing the concept of GBC along with the DNN to identify the fault and tolerate their effects during the data transmission securely. The overall conclusion with future possibilities in the era of WSN-based IoT networks are discussed in the next section of article.

5. Conclusion and future work

In this research work, an optimized deep learning-based fault-tolerant mechanism for energy efficient data transmission in IoT is proposed for secure data transmission. This innovative approach addresses two critical challenges that have long impeded the widespread adoption of IoT technology: energy consumption and system reliability in terms of fault-tolerant mechanisms for secure data transmission. By optimizing energy consumption within the WSN, we can extend the operational lifespan of battery-powered sensors, making them more practical and sustainable for various applications. This enhanced energy efficiency not only reduces maintenance and operational costs but also minimizes the environmental impact associated with frequent battery replacements. Furthermore, the integration of fault tolerance mechanisms ensures that the IoT network remains robust and resilient even in the face of unexpected failures and disruptions. This is vital for applications where uninterrupted data flow and system reliability are paramount, such as in industrial automation, healthcare, and environmental monitoring. As the IoT landscape continues to expand and evolve, energy-efficient and fault-tolerant WSNs are becoming increasingly indispensable. The combined benefits of reduced energy consumption and enhanced reliability pave the way for new possibilities in a wide range of sectors, from smart cities and agriculture to healthcare and logistics. The value of Precision, Recall and F1-score of proposed WSN-based IoT network is 0.965, 0.9562 and 0.9605 that is very good for the prospective fault classification within the network.

In this context, further research and development are needed to refine existing techniques and develop new methodologies that can optimize energy efficiency and fault tolerance even further. These innovations will not only strengthen the foundation of IoT but also drive forward the realization of a more interconnected, intelligent, and sustainable world.

Author contributions

Conceptualization, SK; methodology, SK; software, M; validation, SK, M and AA; formal analysis, AA; investigation, SK; resources, SK; data curation, AA; writing—original draft preparation, SK; writing—review and editing, AA; visualization, RG; supervision, RG and PK; project administration, M; funding acquisition, AA. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. Panda M, Gouda BS, Panigrahi T. Distributed Online Fault Diagnosis in Wireless Sensor Networks. Design Frameworks for Wireless Networks. Published online August 11, 2019: 197-221. doi: 10.1007/978-981-13-9574-1_9
2. Shih HC, Ho JH, Liao BY, et al. Fault Node Recovery Algorithm for a Wireless Sensor Network. IEEE Sensors Journal. 2013, 13(7): 2683-2689. doi: 10.1109/jsen.2013.2255591
3. Vihman L, Kruusmaa M, Raik J. Overview of fault tolerant techniques in underwater sensor networks. arXiv. 2019, arXiv:1910.00889.
4. Liu M, Cao J, Chen G, et al. An Energy-Aware Routing Protocol in Wireless Sensor Networks. Sensors. 2009, 9(1): 445-462. doi: 10.3390/s90100445

5. Ram Prabha V, Latha P. Enhanced multi-attribute trust protocol for malicious node detection in wireless sensor networks. Sādhanā. 2017, 42(2): 143-151. doi: 10.1007/s12046-016-0588-2
6. Fu C, Jiang Z, Wei WEI, Wei A. An energy balanced algorithm of LEACH protocol in WSN. International Journal of Computer Science Issues (IJCSI). 2013, 10(1): 354.
7. Singh R, Singh J, Singh R. Fuzzy Based Advanced Hybrid Intrusion Detection System to Detect Malicious Nodes in Wireless Sensor Networks. Wireless Communications and Mobile Computing. 2017, 2017: 1-14. doi: 10.1155/2017/3548607
8. Azharuddin M, Kuila P, Jana PK. Energy efficient fault tolerant clustering and routing algorithms for wireless sensor networks. Computers & Electrical Engineering. 2015, 41: 177-190. doi: 10.1016/j.compeleceng.2014.07.019
9. Aishwarya C, Padmakumari P, Umamakeswari A. Energy Aware Fault Tolerant Clustering and Routing Mechanism for Wireless Sensor Networks. Indian Journal of Science and Technology. 2016, 9(48). doi: 10.17485/ijst/2016/v9i48/108000
10. Boddu N, Vatambeti R, Bobba V. Achieving Energy Efficiency and Increasing the Network Life Time in MANET through Fault Tolerant Multi-Path Routing. International Journal of Intelligent Engineering and Systems. 2017, 10(3): 166-172. doi: 10.22266/ijies2017.0630.18
11. Maheshwari P, Sharma AK, Verma K. Energy efficient cluster based routing protocol for WSN using butterfly optimization algorithm and ant colony optimization. Ad Hoc Networks. 2021, 110: 102317. doi: 10.1016/j.adhoc.2020.102317
12. El Khediri S, Fakhet W, Moulahi T, et al. Improved node localization using K-means clustering for Wireless Sensor Networks. Computer Science Review. 2020, 37: 100284. doi: 10.1016/j.cosrev.2020.100284
13. Daneshvar SMMH, Alikhah Ahari Mohajer P, Mazinani SM. Energy-Efficient Routing in WSN: A Centralized Cluster-Based Approach via Grey Wolf Optimizer. IEEE Access. 2019, 7: 170019-170031. doi: 10.1109/access.2019.2955993
14. Zhao Z, Shi D, Hui G, et al. An Energy-Optimization Clustering Routing Protocol Based on Dynamic Hierarchical Clustering in 3D WSNs. IEEE Access. 2019, 7: 80159-80173. doi: 10.1109/access.2019.2923882
15. Altakhayneh WA, Ismail M, Altahrawi MA, et al. Cluster Head Selection Using Genetic Algorithm in Wireless Network. 2019 IEEE 14th Malaysia International Conference on Communication (MICC). Published online December 2019. doi: 10.1109/micc48337.2019.9037609
16. Bongale AM, Nirmala CR, Bongale AM. Hybrid Cluster Head Election for WSN Based on Firefly and Harmony Search Algorithms. Wireless Personal Communications. 2019, 106(2): 275-306. doi: 10.1007/s11277-018-5780-8
17. Sharma D, Kulkarni S. Network Lifetime Enhancement Using Improved Honey Bee Optimization Based Routing Protocol for WSN. 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT). Published online April 2018. doi: 10.1109/icicct.2018.8473267
18. Arjunan S, Sujatha P. Lifetime maximization of wireless sensor network using fuzzy based unequal clustering and ACO based routing hybrid protocol. Applied Intelligence. 2017, 48(8): 2229-2246. doi: 10.1007/s10489-017-1077-y
19. Chen H, Lv Z, Tang R, et al. Clustering energy-efficient transmission protocol for Wireless Sensor Networks based on ant colony path optimization. 2017 International Conference on Computer, Information and Telecommunication Systems (CITS). Published online July 2017. doi: 10.1109/cits.2017.8035280
20. Mazumdar N, Om H. DUCR: Distributed unequal cluster‐based routing algorithm for heterogeneous wireless sensor networks. International Journal of Communication Systems. 2017, 30(18). doi: 10.1002/dac.3374
21. Rajeswari K, Neduncheliyan S. Genetic algorithm-based fault tolerant clustering in wireless sensor network. IET Communications. 2017, 11(12): 1927-1932. doi: 10.1049/iet-com.2016.1074
22. Sharma KP, Sharma TP. rDFD: reactive distributed fault detection in wireless sensor networks. Wireless Networks. 2016, 23(4): 1145-1160. doi: 10.1007/s11276-016-1207-1