IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 30, 2021, accepted October 10, 2021, date of publication October 18, 2021, date of current version November 1, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3121033

An Energy-Aware, Highly Available, and Fault-Tolerant Method for Reliable IoT Systems

MUHAMMAD BUKHSH[1], SAIMA ABDULLAH[1], ABDUL RAHMAN[2,3], MAMOONA NAVEED ASGHAR[4], HUMAIRA ARSHAD[1], AND ABDULATIF ALABDULATIF[5]

[1]Department of Computer Science, Faculty of Computing, The Islamia University of Bahawalpur, Punjab 63100, Pakistan
[2]Department of Computer Science, Superior University Lahore, Punjab 54600, Pakistan
[3]School of Computer Science and Technology, University of Science and Technology of China, Hefei, Anhui 230026, China
[4]Department of Computer and Software Engineering, Faculty of Engineering and Informatics, Technological University of the Shannon: Midlands Midwest, Athlone Campus, County Westmeath, N37 HD68 Ireland
[5]Department of Computer Science, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia

Corresponding author: Saima Abdullah (saima.abdullah@iub.edu.pk)

ABSTRACT The Internet of Things (IoT) is one of the highly influencing and promising technologies of today's world, consisting of sensor devices. The internet smoothly changes from an internet of people towards an Internet of Things (IoT), which allows different things and objects to connect wirelessly. Things and objects are grouped into IoT subgroups in the IoT system, which are called clusters, and each cluster is controlled by a central authority and checked by the broker's help. A concept of keeping backup data is used to increase the lifespan of IoT subgroups by avoiding re-clustering overhead for smooth transmission of packets and increasing availability concerns. A novel approach is used for the selection of cluster head/broker and backup nodes simultaneously. Cluster head and Backup Storage Point node (BSP) remain the same unless and until the residual power of the broker/cluster head is greater than the threshold energy. A novel Energy Efficient Message scheduling algorithm EAAFTMS (An Energy-Aware Available and Fault-Tolerant System with Message Scheduling in IoT) is incorporated at broker node for smooth transmission of messages. This proposed approach is not only solving availability issues over the wireless network but also proved to be energy efficient by prolonging the battery-powered network lifetime. Simulation results prove EAAFTMS, many folds better than benchmark protocols. This system ensures fault-tolerant and available schemes for IoT systems while stabilizing the energy of the overall system. The results shown prove the effectiveness and efficiency of the proposed system.

INDEX TERMS Energy efficiency, fault tolerance, availability, IoT systems, wireless sensor networks.

I. INTRODUCTION

In this era of Internet of Things (IoT) systems, millions of multiple wireless devices are connected for distant communication without any human interference. The IoT system is serving humanity to have a better and secure living style. An estimation by statistics website Statista, the number of IoT-connected devices all over the world will intensely rise from 23.14 billion in 2018 to 75.44 billion in 2025. According to Statista [1], the estimated rise in install-based IoT devices is more than 31 billion up to 2020 and more than one billion US dollars are being spent annually on Internet of Things projects. According to International Data Corporation (IDC) [2], IoT spending will increase from $698.6 billion to $1.3 trillion from 2015 to 2019, thus estimating a 17% compound annual growth rate (CAGR). Application domains of IoT systems exist in almost every field of life. Wireless sensor networks are being used for traffic flow on roads, military purposes, medical field, agricultural sector, personal assistance, commercial use of IoT systems in the industrial sector, prevent intrusion in any building, infrastructure, securing countries' borders, securing children inside and outside of the home, remotely controlling various household devices and cars on road. So, one cannot deny the importance of IoT systems in this era but the issue lies in its security and privacy of the communication. Reliability is the most wanted factor whether it is personal communication or sensitive military/accounts information being transmitted over the IoT network. In an IoT system, each device uses radio frequency identification for data transmission. The word ''Internet of Things'' was first used by Kevin Ashton, a British technologist in 1999. Recently, in an article of IEEE spectrum for the month of April 2018, China has made efficient use of more than 100,000 wireless sensor networks

The associate editor coordinating the review of this manuscript and approving it for publication was Amjad Mehmood.

to monitor its 1400 km canal to protect it from any unwanted human interference and saving human beings from drowning as well [3]. So, the fruits of IoT systems are becoming countless. Besides the countless benefits of secure fault-tolerant IoT systems, these are pruning healthy elements from the atmosphere by emitting CO2, enhancing global warming. A typical wireless sensor network consists of sensor nodes, a broker and a base station (usually termed as sink nodes). All types of nodes have varying resource capabilities. Sensor nodes come with limited range, storage, processing and energy capabilities. Base stations receive all the messages sent by the broker and due to this, the base station comes with more storage, processing power and consumes more energy than other sensor nodes. Hence, exhibiting more alarming heat waves. [4] In a recent study, there are more than four billion base stations, each base station consumes approximately 25MWh/year which is 80% of the overall wireless network energy consumption. To overcome this alarming situation the world is stepping forward towards green IoT systems.

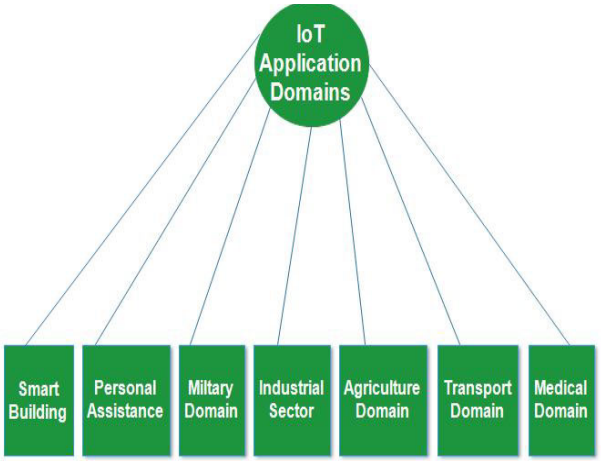

FIGURE 1. Different application domains of IoT system.

A typical wireless sensor network works in the following manner; first, clusters are formed by having a specific number of sensor nodes in distributed mode and they are responsible to sense a message and transmit that message to their broker node. Each cluster has one broker node which is responsible to collect, aggregate and transmit that message towards the sink node. After then, the sink node sends the message to the client/server. As these systems are battery-powered and have high exposure for intruders, there could be chances of fault occurrence. For graceful degradation of such an IoT system, we create backups for the broker node. For this purpose, we have an array of backup nodes with two parameters; i.e., backup node id and location. It creates a periodic backup for the broker node and copies all the data in a backup node so that whenever the broker node becomes faulty, the backup node takes place in the charge of the broker node. Keeping a backup storage point does not cost a lot. If the base station sends a request to the broker to resend the last aggregated data collected from all sensor nodes, then the broker will simply get that data from the backup node and send it again to the base station. Now the question arises as to why the base station doesn't receive data sent by the broker. Although, IoT made human life easier and smarter as one can control, track and analyze personal, social and professional activities. These systems are placed in an open environment so easily prone to attacks. An intruder can make intrusions in several ways; i.e., hacking the data, injecting false data, collecting sensitive information by placing a fake base station node, capturing sensor node and many others and to solve this need for retransmission of data due to any of the above-described reasons, a backup node is used.

Backup node increases network's reliability and fault tolerance even when the network has following threats due to its aired communication channel [5], [6].

- Privacy threats and encounters may include transmitted data privacy, device privacy and user privacy.
- Authentication may suffer from device authentication, user authentication, node capturing attacks and data authenticity.
- Confidentiality challenges are to cope with confidentiality of data, device, data ownership, eavesdropping attacks and network traffic analysis attacks.
- Accessibility challenges require to cope with access control, denial of service attacks and replay attacks.
- Integrity means data and devices both are reliable. It requires device-to-device data security over the network. Device mitigation and data modification are also integrity challenges in IoT systems.
- Strategy Implementation challenges may suffer from strategy standards and service level agreements.
- The heterogeneous nature of devices is also a major challenge in IoT systems. There is a need to have such an IoT system that can cope with a variety of heterogeneous devices by making them compatible with each other.

A wireless network that is more fault-tolerant and energy efficient is highly demanded. Therefore, this research proposes a simple, robust approach EAAFTMS (An Energy-Aware Available and Fault-Tolerant System with Message Scheduling in IoT) used to make wireless sensor networks more fault-tolerant with backup storage point and energy efficient by using M/M/1Q Architecture. Moreover, the results of this research prove it more energy-efficient and fault-tolerant as compared to previously used LEACH and CL-LEACH algorithms. The focus of this research is to reduce overall cost and maximize the energy throughput of the network.

Our key contributions are:

We have developed algorithm EAAFTMS for cluster head selection and fault tolerance with message scheduling to enhance the IoT network life. The EAAFTMS algorithm should create a periodic backup for the broker node to check the residual energy for broker selection. The EAAFTMS algorithm should create copy all the data in the backup storage point from broker so that whenever the broker node becomes faulty, the backup storage point node will take

the charge of the broker node. A well-organized broker backup storage point system is proposed for IoT network to enhance the IoT system availability. The message stability improvement in term of response time resulting in energy efficiency and increased lifetime of the system can be shown in the results evaluation of the implemented system. The simulation and results of the EAAFTMS algorithm should show the efficiency of the proposed framework. Results should confirm that there is minimal cost and maximum energy throughput of the network is ensured.

The rest of this paper is organized as follows; Section II reviews earlier research about fault tolerance and energy problems in wireless sensor networks. Section III discusses the architecture of the proposed framework in detail. Experimental results and simulations are provided in section IV, comparing our proposed framework with the previous ones. Section V contain discussion and section VI comprises concluding remarks and future work.

II. RELATED WORK

WSN is used for a variety of applications to help a human being to monitor surroundings, chase a target, track health records and assist in many other monitoring and prevention measures [7]–[10]. A framework for WSN is presented which integrates two routing protocol algorithms. These two algorithms are using the Energy Balanced Clustering algorithm to maximize fault tolerance of WSN. It is using the mechanism of automatically selecting base station and cluster head, based on power and energy load balancing, with the help of an organizer node. Furthermore, in case of any fault in the cluster head, the organizer is selecting a new one. In this manner, this framework is maximizing the lifetime and energy handling of WSN. This approach is termed as Energy Balanced with Fault Tolerance Capability (EEBFTC) protocol [11]. It proposes an energy-efficient approach for WSN which is based on centroids of nodes, called Energy Efficient Centroid based Routing Protocol (EECRP). It considers three parts for EECRP: a novel approach for distributed cluster creation, other approaches for cluster familiarization and then spinning the cluster head based on centroids for equal energy workload dispersal and to minimize the energy usage. In EECRP, the lingering energy of nodes is used to determine centroid position [12].

Virtualization in WSN also needs to optimize fault tolerance capability and in various other networks IoT applications designed to provide services. To maximize fault tolerance and to minimize communication time, the author is using a non-dominated sorting-based genetic algorithm [13]. The research was done to adopt a suitable framework to maximize fault tolerance. Fault can be in nodes or data transmission between them, the framework is used to detect fault and method to recover fault in nodes and communication between nodes. The framework is used to maximize fault tolerance and network lifetime. When network lifetime increases, it means network communication increases which also increases the energy consumption of the network [14].

[15] Presented the detailed fault-tolerant scheme for wireless sensor networks. As sensor nodes are usually placed in open access environments, malicious activities are invited from outside and inside the network. In a cluster of sensor nodes, there is one node with more storage, processing and power elected as cluster head. There are also some backup nodes which are called spare cluster heads. It presented the strategy for the election of a spare cluster head to take charge of the cluster head, in case the cluster head dies. The spare cluster head which is placed at a minimal distance from the cluster head will immediately become a cluster head if all the messages sent by sensor nodes are not received by the sink node. The message is divided into three parts: the first part is heartbeat (HB) sent by the sender node to cluster head and the second part consists of a summary which contains the heartbeat of all nearby nodes to make sure that they are alive and not in a dead state. The third part contains the actual data sent by the sensor node. It presented efficient reliable working of the wireless sensor network. Another limitation in this proposed fault tolerance scheme is the presented algorithm may exhaust high energy due to extensive message packets and time.

[16] Presented an algorithm for fluent message transmission between the sensor node and broker node by using the shortest processing time first algorithm in a wireless sensor network to avoid collision and minimize waiting time. Wireless sensor networks consist of N number of sensor nodes that sense the message from their surroundings and send those messages to the broker. The broker node is responsible for aggregation and transmits the received messages to the sink node. The paper presented the fault-tolerant scheme for efficient message transmission considering node failure in the Internet of Things systems. It deals with a fault in the sensor node only and uses the backup scheme. Whenever sensor node failure occurs, the node itself recovers the fault and if self-recovery doesn't happen then that sensor node is replaced with the backup sensor node considering the minimal distance for replacement. The proposed approach is energy efficient but deals only with the fault in the sensor node and with no consideration for fault in the broker node or sink node. [17] Routing protocols for efficient data transmission and communication within wireless sensor networks and also the fault tolerance issues faced in routing protocols. It provides a detailed analysis of different routing protocols. According to [18] wireless sensor networks are facing limitations in storage, resources, power and range. Different routing protocols face different fault tolerance challenges as described in [19]. Although, it provided a detailed comparison of different routing protocols and possible faults and their possible countermeasure.

Wireless sensor networks are being used to capture and send real-time information like monitoring of the surrounding environment and many factors can affect the fault tolerance capability of wireless sensor networks like temperature, wind, etc. [20]. LEACH protocol is the hierarchical routing protocol that is used to ensure the fault tolerance capability

PARAMETER ANALYSIS OF EXISTING METHODS FOR FAULT TOLERANCE

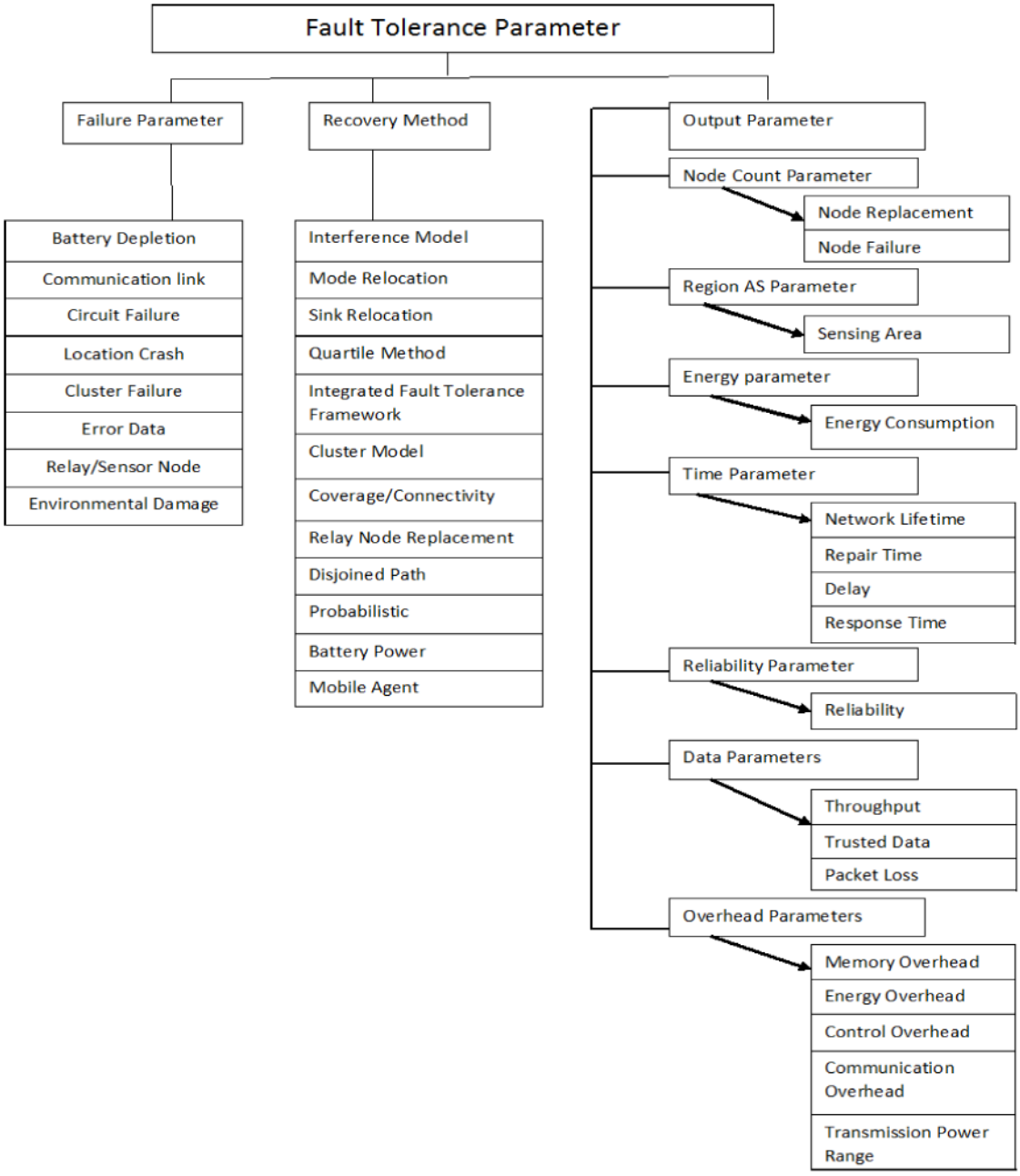

FIGURE 2. Fault tolerance parameter analysis.

of the wireless sensor network. It selects cluster heads on a random basis every time. Another protocol named LEACH-TLCH also uses the same cluster selection method as LEACH, but it is an extended version of LEACH to improve the energy consumption of the network [21]. There are many issues and weaknesses in the LEACH protocol as described in [22]. It presents a comprehensive report on weaknesses of the LEACH protocol considering various factors like data collection, flexibility and energy consumption. [2]. Discusses various successors of LEACH protocol and their analysis using parameters such as energy efficiency, overhead, reliability, density and scalability.

CL-LEACH is the extended version of LEACH. It is a cross-layered architecture that is used to increase the battery lifetime. It uses variant methodology by removing inter-section dependency in a network. It selects the cluster head of the wireless sensor network with the residual remaining energy of the node to use this remaining energy. It results in better energy consumption and fault tolerance capability as compared to the LEACH protocol [23].

Table 1 [29] presents the detailed analysis of fault tolerance techniques used by various authors. It discusses the faults that occur due to location crashes, cluster head failure and sensor node failure. Recovery methods used by various

TABLE 1. Parameter analysis for fault tolerance.

Parameter / Paper Reference Number		[2]	[5]	[11]	[17]	[18]	[20]	[24]	[25]	[26]	[28]	[31]	[33]	STT
Failure Parameters	Battery exhaustion		+	+		+	+	+		+	+			7
	Communication link		+	+	+	+	+	+	+	+	+	+	+	11
	Path		+	+	+	+					+		+	6
	Position clattering	+		+			+	+			+	+		6
	Clock Implication										+	+		2
	Group of nodes	+	+	+	+	+	+	+			+			8
	Faulty records		+		+	+	+				+	+	+	7
	Dispatched/Sensor Node	+		+	+	+	+	+		+				7
	Ecological Mutilation		+		+	+	+	+	+	+				7
Sub Total		3	6	6	6	7	7	6	2	4	7	4	3	61/61
Recovery Method	Intrusion exemplary	+	+				+	+						4
	Node Repositioning										+			1
	Sink Repositioning	+				+								2
	Quartile _method												+	1
	Integrated Fault Tolerance Framework		+											1
	Group model	+						+			+			3
	Exposure/connectivity	+	+		+	+	+	+			+			7
	Relay Node location/ node exchange					+		+			+			3
	Disjoined route				+	+								2
	Probabilistic	+			+		+						+	4
	Cordless power		+	+	+	+	+	+	+	+	+		+	10
	Portable Mediator					+	+			+	+	+		5
SUB TOTAL		5	4	1	4	6	5	5	1	2	6	1	3	43/42

authors to cope with location crashes, cluster head and sensor node failures are interference model, sink relocation, cluster model, connectivity model and probabilistic model. Different novel approaches have been discussed with parameters such

TABLE 1. *(Continued.)* **Parameter analysis for fault tolerance.**

Node Count Parameter	Sensor Node replacement		+		+			+			+			4
	sensor Node catastrophe	+	+	+	+	+	+	+		+	+	+		10
Region as parameter	Identifying Zone	+	+		+	+	+	+	+		+			8
Energy Parameter	Energy Usage	+	+	+	+	+	+	+	+		+	+	+	11
Time Parameter	Network Period		+	+	+	+	+	+			+			7
	Mending time											+		1
	Suspension time		+	+	+	+	+	+		+	+			8
	Reply Time		+								+			2
Reliability Parameter	Consistency	+	+		+	+	+	+	+		+	+	+	10
Data Parameter	Output		+	+	+	+								4
	Reliable Data			+										1
	Packet Damage	+	+	+	+	+	+	+		+	+		+	10
Overhead Parameter	Memory Overhead						+	+						2
	Energy Overhead			+		+								2
	Mechanism Overhead		+		+		+	+		+	+	+		7
	Message Overhead		+	+	+	+	+				+	+		7
	Broadcast Overhead					+		+						2
SUB TOTAL		5	12	9	11	11	10	11	3	4	11	6	3	96/96

as sensing area, node failure can be found with node count parameters and minimizing energy consumption. It didn't consider network lifetime enhancement and other time parameters such as repair time, delay time and response time.

A well-managed solution is described in this paper to decrease the issues of tasks failure, data management and healthcare IoT nodes in fog computing with a novel scheme with tasks level, and nodes level fault tolerance. The results show that the proposed system is better as compared to other system used for fog computing in health care environment [30]. In this paper, various existing green energy approaches in mobile crowdsensing discussed based on blockchain technology. Mobile crowdsensing included all computational characteristics connected with smart farming, smart industry, smart medical system, smart transportations, smart grid, smart home-care and smart city in Internet of Things (IoT) environments [31].

In this studied, a new energy-aware marine predators' algorithm (MPA) is developed based on metaheuristic algorithm for managing the TSFC issue in IoT system. In this studied, two types of MPA have been introduced for handling the TSFC. The first type is modification marine predators' algorithm (MMPA), this version improves the model one by using the historical updated positions and the other type of MPA has better-quality using a ranking strategy with reinitialization randomly [32]. This paper considered the energy management methods in IoT based on SLR approach. Showing 2151 papers, and 30 research studies were carried out in domain of 2013 and 2019 were selected as main domain of methodological analysis. For categorising prevailing topics on the energy solutions in IoT, an energy management classification was provided to determine technical features of each category [33].

In this paper, an energy-aware metaheuristic algorithm is proposed based on Harris Hawks optimization algorithm on a local search strategy (HHOLS) to improve the quality of services for task scheduling in IIoT environment. For the improvement of performance, HHOLS is connected with swap mutation operation and local search. To manage task scheduling discreate problem, the HHO Algorithm is used to manage endures problem [34]. In this article RPL-based method is introduced to diminish IoT device energy usage. The proposed technique considered the quality of service of IoT system, where time division multiple access slot is used among sender and receiver to synchronize and decrease energy consumption. Furthermore, the trickle timer controlled the DODAG routing topology [35].

Alazab *et al.* presented an enhanced rider optimization algorithm to find the optimal head nodes in IoT clusters which prolong the network lifetime [36]. Behera *et al.* has used a new election technique that suggests the Cluster Head (CH) based on the energy level between nodes. This technique closely decreases the responsibility in the topology by decreasing energy exhaustion [37]. Attempts have been discussed to develop a clustering scheme with ideal cluster head selection based on four main parameters such as delay, distance, security and energy. In addition, for selecting the optimal CHs, presented a new hybrid algorithm [38].

The huge number of nodes, low accessible data rates, and different resource limitations have restricted the serviceability of common ad-hoc routing protocols in WSN. To enhance the network life and overcome limited battery capacity, WSN routing protocols support resource-awareness and adaptivity [39]. The Multi-MBCA trace the node neighbours based on the communication range and makes a matrix of these nodes. The node life is assessed based on the percentage of node drain rate and remaining energy [40]. The intelligent optimization method of process control parameters represented by the genetic algorithm [41] has been fruitfully functional to industrial production industries such as mechanical processing and mineral processing. The above comparison [23] discoursed with a maximum of six failure causes. [24] Discussed the recovery method just for battery usage. [18] Discussed six methods for fault recovery. Better comparison scenario by using 11 parameters after implementation of the algorithm is given in [23], [18], [26] and [17].

III. PROPOSED EAAFTMS MANAGEMENT FRAMEWORK

EAAFTMS (An Energy-Aware Available and Fault-Tolerant System with Message Scheduling in IoT) is the proposed management framework, explained in this segment. The suggested framework is the improved variant of LEACH which has proven to work better than LEACH as well as CL-LEACH by eliminating the core issues associated with LEACH algorithm. In the EAAFTMS algorithm, not only the cluster head, termed as ''broker'' node is being elected from the specific IoT subgroup but also an extra node which is known as BSP (Backup Storage Point) is being elected from the same IoT subgroup. The elected BSP node will be used solely for data backup and will not sense data as other non-broker nodes do. The broker node is responsible for receiving data from non-broker nodes which lies in its own IoT subgroup, after then the broker node aggregates the received data and places a copy of this aggregated data on BSP for backup. Furthermore, the aggregated data is sent to the base station. As the proposed framework is the variant of LEACH which works in two phases; i.e., in the first phase, all the roles of nodes that specific IoT subgroup are defined by adding one extra role of BSP, and in the second phase all nodes start. Operating the assigned functions and this phase is known as the ''operational phase.''

In EAAFTMS, there are eight distinct modes of operation assigned to the broker node, which further can be categorized into the previously defined two phases. The first three modes of operation belong to the first phase, which is the IoT subgroup formation phase. The remaining five modes of operation are associated with the operational phase. Figure 3 shows these eight modes of operation.

At first, brokers are being selected randomly, so these can be any of the nodes in that specific IoT group assuming equal initial residual energy of all nodes. The selected broker nodes send joint signals to all non-broker nodes to let them know that I am the IoT subgroup head and I am responsible for receiving and collecting your sensed data. After the advertisement, all the available non-broker nodes that have

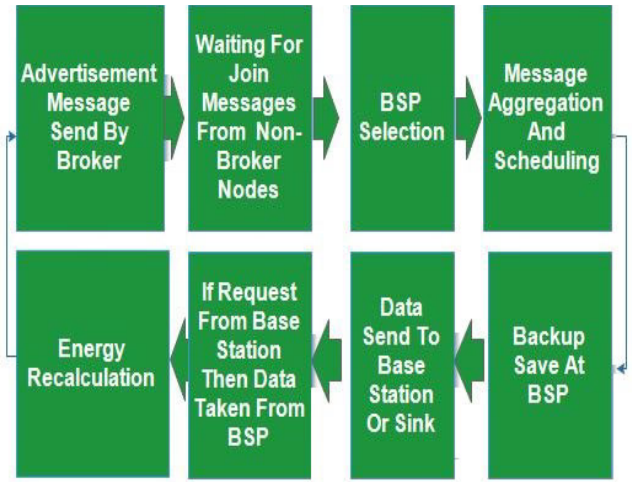

FIGURE 3. Modes of operation for broker node in the proposed management framework EAAFTMS.

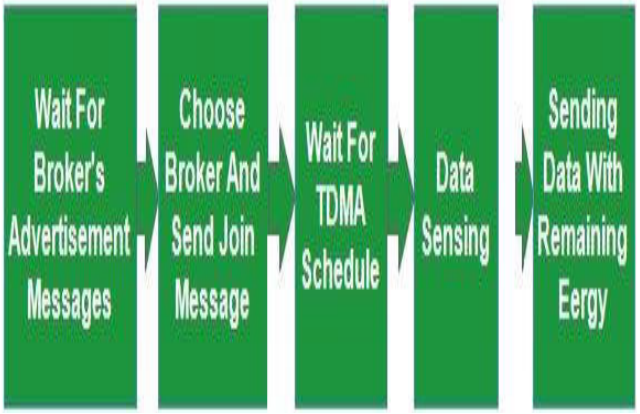

FIGURE 4. Different modes of normal nodes in EAAFTMS.

the least distance from their concerning broker node will join that broker node to form the IoT subgroup. In this way, all non-broker nodes acknowledge their presence and join the respective IoT subgroup for the further communication process.

The third and last step of the IoT subgroup formation phase is the selection of BSP nodes from the same IoT subgroup. After this, the fourth mode starts which is the first step of the operational phase. This mode is associated with sending the sensed data from non-broker nodes to broker nodes by allocation of time frames to each non-broker node. Broker node upholds all messages received from non-broker nodes into a queue and that queue is sorted as a product of the proposed energy-efficient message scheduler. These scheduled messages are then sent to the base station for further process. The proposed framework assures the uninterrupted and energy-efficient performance of the IoT subgroup. The proposed EAAFTMS framework works in two ways. Firstly, a new IoT subgroup is created so all eight modes of operation will be performed. Secondly, if the residual energy of the broker node is higher than threshold energy then there is no need to recreate a new IoT subgroup for the upcoming data transmission rounds as broker and BSP will remain the same. So, four to eight modes of operation will be needed to perform avoiding the first three modes. Therefore, reducing network overhead when compared to LEACH protocol where a new IoT subgroup needs to be created for every new round by selecting a broker node as well.

Figure 4 demonstrates different operational modes of non-broker nodes. To create IoT subgroup non-broker nodes, wait for the broker's advertisement message. Then, non-broker nodes will join the broker that has the least distance from them. On completing IoT subgroup formation, non-broker nodes start sensing their surrounding data and wait for the TDMA (Time Division Multiple Access) schedule to sense and send data towards the broker node. As wireless networks are more prone to attacks so the risk of data loss can never be ignored and to cope with this issue and to ensure the availability of data, the broker places a copy of assembled and sorted data in BSP. Furthermore, data is sent to the base station. Considering the risk of data loss during transmission from the broker to the base station, data might not successfully reach the base station. In such a case, the base station requests the broker node to resend data, and the broker will simply get it from BSP and resend it to the base station. BSP node is not an overhead for the network as it preserves residual energy of all non-broker nodes as well as broker node because it contains aggregated and sorted data and broker will need not to recollect data from each non-broker node, maintain messages queue and sort all messages in the queue and then resend it to the base station and non-broker nodes will also need not to sense surrounding data again. Thus, the proposed approach is a promising one to endure fault and preserve the energy of nodes. After completing one round of data transmission, energy checking is done as the last operation mode of the functional phase. This last step is done to decide whether the current broker will continue to work as a broker or it needs to be replaced with any node having higher residual energy as compared to the current broker node. For this purpose, energy checking is done for each non-broker node and broker node of the IoT subgroup.

If the residual energy of the broker node is less than the threshold energy that was calculated in the initial round, then the broker needs to be replaced with BSP and definitely, a new BSP will also be selected. Figure 6 demonstrates the functioning modes of the BSP node used in the proposed EAAFTMS protocol. It starts with the creation of the IoT subgroup.

Then, one node is selected as BSP. When the network is established and the broker starts receiving messages from the non-broker node, the BSP node remains in a wait state. When the broker completes the task of data aggregation and message scheduling is done by using M/M/1 Q architecture, the broker sends a copy of sorted data towards BSP. BSP nodes receive that data and save it for future use. The next mode is BSP waiting for the data request. This mode will

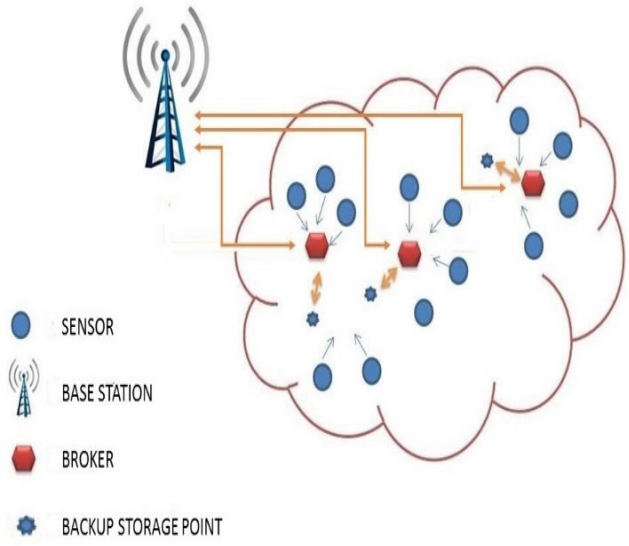

FIGURE 5. Proposed Wireless Sensor Network with Backup Storage Point.

FIGURE 6. Modes of Operation for BSP's (Backup Storage Point) in EAAFTMS.

be active in case data sent by the broker is not successfully received by the base station and the base station requests the broker to resend the last aggregated data. Then, the broker will simply request BSP for the copy of the last aggregated data. BSP will send the last aggregated data to the broker and the broker will resend it to the base station.

A. THE ENERGY CONSUMPTION MODEL

The energy consumption model defines factors used in simulation to measure the energy consumption of nodes. The fundamental network consists of N number of nodes arbitrarily placed which are then classified as IoT subgroups. Each IoT subgroup has one head node known as a broker. This broker node is responsible for receiving sensed data from non-broker nodes and then sending this towards the base station after placing a copy of this in the BSP (Backup Storage Point) node of the respective IoT subgroup.

Assuming all nodes in the IoT subgroup have the same capacity in terms of sensing, processing power and data transmission. The base station is located at a far-flung place from sensor nodes and it is immovable. Collection and incorporation of data are supplementary to the transmission protocol to lessen energy consumption in the incorporation of data transferred to the base station. Thus, data sent is measurable assuring wireless network dynamic and manageable. The broker receives data from non-broker nodes and before sending this data to the base station, data is compressed and transmission signals are amplified to assure data transmission between broker and base station. The values of E_{opr} and E_{str} are constant throughout the experiment.

E_{opr}: It is vital energy for the operation transmitter/receiver.
E_{str}: It is essential energy used to fortify transmission signals to assure data delivery at the base station.
Consequently, energy consumption of IoT subgroup can be determined by:
For transmission of a message m

$$\mathbf{ETm = Eopr + bpm + Estr + bpm + l2} \quad (1)$$

To receive a message m at receiver side

$$\mathbf{ERm = Eopr + bpm} \quad (2)$$

where bpm=no of data bits per message.
l= distance between terminals in eq (1) and eq (2).
These two terminals can be non-broker nodes, broker and base station.

B. IN PROPOSED SYSTEM USE OF M/M/1 QUEUING THEORY MODEL

In the proposed framework, the M/M/1 Queuing model is being used to handle the flow of messages and their processing time. As in the proposed system, each IoT subgroup has one head node called ''broker'' and one node is designated as ''BSP'' for backup storage and rest of the nodes are non-broker nodes and they are solely responsible for sensing data from surroundings. These non-broker nodes send sensed data towards the broker using TDMA (Time Division Multiple Access). Further, the brook of messages received by non-broker nodes is sorted and organized in a specific order to have smooth communication over the wireless network.

Here, ''n'' refers to the no. of messages received at broker nodes such that n = {1, 2, 3 ...r}. The arrival rate of nth messages is denoted by μn and the service rate of nth messages is represented by λn.

$$\boldsymbol{\rho n} = \frac{\text{Ttransmissionn}}{\text{TRequestn}}, \quad \text{for } n = \{1, 2, 3, , , , , , \}$$

$$\boldsymbol{\rho n} = \sum_{n=1}^{n} \frac{\text{Ttransmissionn}}{\text{TRequestn}} < 1$$

Here, r denotes the size of messages collected at the broker node. Whereas Ttransmission_n is the victorious broadcasting

time of the message and $TRequest_n$ is the message request time of service at the broker. Hence, ρn represents the message circulation strength at the broker. In suggesting the IoT subgroup, every message sent has service request time and successful transmission time. The rate at which messages are collected in the broker messages queue is represented by service request time.

In the proposed system the required traffic intensity is less than one to keep the stability in the responses of the message. Proposed work evaluates of message traffic intensity if the final value of $\rho n > 1$, then the period of the message is required to be rescheduled to have the ideal traffic intensity of message, which is less than 1.

C. PROPOSED EAAFTMS (AN ENERGY-AWARE AVAILABLE AND FAULT-TOLERANT SYSTEM WITH MESSAGE SCHEDULING IN IoT) ALGORITHM

EAAFTMS (An Energy-Aware Available and Fault-Tolerant System with Message Scheduling in IoT) is the proposed algorithm. It tries to remove the deficiency of the key system like LEACH. In EAAFTMS established the network of multiple sensor nodes. Non-broker nodes are responsible to sense data from surroundings and transmit this data towards the broker where the broker node is solely responsible to forward this data towards the base station. Sensor nodes are usually placed far away from the base station. At the time of IoT subgroup formation, broker nodes are selected randomly from that pool of sensor nodes as all sensor nodes have equal initial residual energy. After this, non-broker sensor nodes are classified and grouped to form an IoT subgroup by joining the nearest broker node. IoT subgroup formation is done on the successful joining of all non-broker sensor nodes with their nearest designated broker node. Subsequently, one node from each IoT subgroup is randomly selected as a BSP (Backup Storage Point) node for recording the brook of sensed data.

The IoT subgroup works in such a manner that the broker assembles data received by all non-broker sensor nodes and subsequently organizes it by using M/M/1 Queue model. After scheduling the data, the broker node sends a copy of this scheduled to be placed at the BSP node and then transmits it towards the base station. Here, the risk of intrusion can never be ignored, and the base station might not have received that data. The base station will request the broker to resend the last aggregated data. To handle this situation, the broker node will simply get a copy of the last aggregated data and will immediately send it to the base station. Before the next round of data transmission starts, the residual energy of the broker is compared with the threshold energy.

Threshold energy is calculated by:

$$\mathbf{EThresholdBROKER = ENBN + EBSP + EBS}$$

If the current residual energy of the broker node is greater than the threshold energy, then no change will be made in the broker and BSP.

The same broker and BSP will continue to work as they are designated. The same broker will be used for the next round of data transmission by aggregating data from non-broker

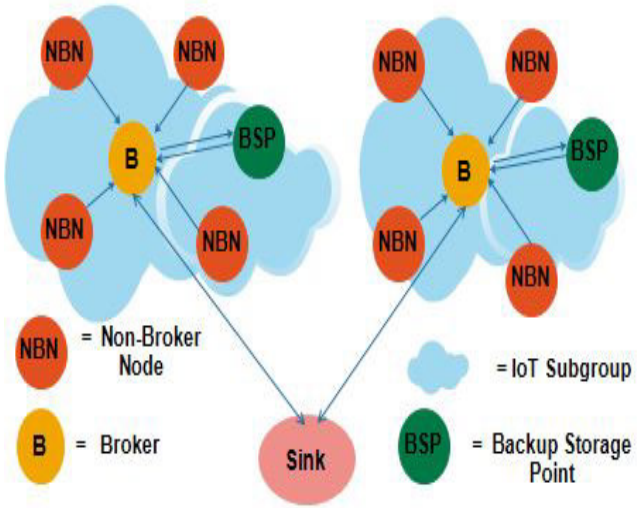

FIGURE 7. IoT Subgroups with Backup Storage Points.

sensor nodes, scheduling data, placing a copy of data on BSP and then transmitting it to the base station. The same process will continue unless and until the residual energy of the broker node becomes less than the threshold energy. At the stage, where residual energy becomes less than threshold energy, the broker and BSP exchange their positions. As BSP didn't perform any sensing, its residual energy was not much lower and it easily took charge of the broker and started functioning. Also, the broker node became BSP to keep records of data. Subsequently, when the residual energy of the swapped broker also becomes less than the threshold energy, two non-broker nodes are elected as broker and BSP, and these eligibility criteria are based on the maximum energy level.

The non-broker node with the highest residual energy becomes broker and the non-broker node with the second-highest residual energy becomes BSP and the process continues likewise. Now, assuming this IoT subgroup without BSP will answer the question of why the overhead of BSP is used in this proposed framework. It can be well explained in case data sent by the broker doesn't reach its destination (base station) due to any intrusion and the base station requests the broker to resend the data. Here, without BSP, the broker node will again collect data from non-broker nodes, schedule collected data and be able to resend the data to the base station, resulting in a time-consuming process and delayed information. Also, the energy usage of non-broker nodes (to re-sense surrounding data) and broker nodes (to recollect and re-schedule data) becomes double, which leads to shortened network lifetime. For instance, non-broker nodes sensed information of earthquake data, and the broker sends this information to the base station. Probability of information lost due to any fault and error and base station might not receive it. In this circumstance, when the base station requests the broker to resend the last collected information and the broker begins collecting the past information from all the non-broker nodes. At this point the earthquake gets normal and

the data identified with the earthquake could be lost because generally ask.

To adapt to the above-expressed circumstances and many others like that, the thought is to keep collected information being spared as a reinforcement in BSP utilizing the proposed EAAFTMS model. Hence, if there should be an occurrence of any failure in the broker node helpful data won't be lost. The EAAFTMS algorithm gives the adaptation to non-critical failure and provides fault recovery along with energy-efficient message scheduling. Because of any failure in information transmission from the broker to the base station, a duplicate of transmitted information will dependably be accessible in the BSP node and the broker will essentially recover lost information from BSP and resend it to the base station. Thusly accessibility which is the most imperative factor of any framework is being guaranteed in the proposed EAAFTMS algorithm. In the event, if broker crash because of any failure or error, at that point BSP happens to the broker and begins accepting a message from non-broker nodes inside its particular IoT subgroup. Along these lines adaptation to non-critical failure is installed in EAAFTMS demonstrate as well. Along with all benefits, some disadvantages / overheads of the proposed system are i.e., backup storage point implementation cost, high bandwidth, security and privacy. There is always trade-off between efficiency and overhead.

D. EAAFTMS ALGORITHM

Algorithm 1 Proposed EAAFTMS (ENERGY AWARE AVAILABLE AND FAULT TOLERANT SYSTEM WITH MESSAGE SCHEDULING) ALGORITHM)

The fundamental request time point $= f_{R_n}$;
$E_{Broker_{DB}} = 0$, $E_{thr} = 0$; // Initialize threshold and DB with zero
T_{Set} ($TDMA_{Broker}$);
E_{Broker} = rand (All Nodes, 1); // random selection of Broker
E_B = rand (Subgroup of Broker, 1); // rand choice of Backup Node
for $\mathbf{r}_{th}$ cyclic messages: $Mess_{\mathbf{r}}$ ($Time_{Req_{\mathbf{r}}}$, $Time_{trans_{\mathbf{r}}}$) **do**
  if ($\mathbf{E_{Broker}} < \mathbf{E_{thr}}$) then
    if ($\mathbf{E_B} > \mathbf{E_{thr}}$)
      Swap (E_{Broker}, E_B);
    Swap ($E_{Broker_{DB}}$, $E_{B_{DB}}$); // replacement the backup of broker (DB) to Backup Node (DB)
  else
    Novel SelectionofBrokerNodeWithBackupNode (); // depends on max residual energy node
  Collect_Data ();
  for rth movement intensity q_n **do**
  for all $Time_{Req_r} = f_{R_n}$;
  $q_r = \frac{Time_{trans_r}}{Time_{Req_r}}$, for r= {1,2,3,,,,,,}
  while q > 1 **do**
  Arrange $Message_r$ in a $Time_{Req_r}$ descendent order. For all r= {1,2,3,,,,,,}
    $Time_{Req_r} = Time_{Req_r} + \frac{Time_{Req_r}}{2^r}$;
    $q = \sum_{r=1}^{r} \frac{Time_{trans_r}}{Time_{Req_r}}$
  end while
  Req $Message_r$ in a descendant $\mu_r = \frac{1}{Time_{trans_r}}$ Order.
end for
Send ($E_{DataBase}$, E_{Backup}); //Broker send Database Data to Backup Node
Send ($E_{DataBase}$, SINK); // Broker send Database Backup to Sink
WaitForReceiving (message, node);
Case (message, type)
  IfSinkAgainRequestforData: **Send** (E_{Backup}, Database_Request);
    Wait_Request (EDatabase);
    Send (EDatabase, Sink)
end for
NovelSelectionofBrokerNodeWithBackupNode () **Start**
set (Subgroup), set (E_{NN}); //set energy of Subgroup and energy of Normal Node
$E_{Broker} = E_{MAX}$ (E_{NN});
$E_{Backup} = E_{MAX}$ ($E_{NN} - E_{Broker}$);
Swap ($E_{Backup_{Database}}$, $E_{Pre\_Backup_{DataBase}}$); **End** //exchange backup from previous Backup Node to new Backup Node

E. DESCRIPTION OF EAAFTMS ALGORITHM

EAAFTMS protocol selects broker nodes randomly for the first time to create a wireless network consisting of arbitrary sensor nodes having equal residual energy. BSP (Backup Storage Point) node is arbitrarily selected by the broker for keeping backup of data collected from sensor nodes of the same IoT subgroup. The broker will start collecting data from sensor nodes by allocating time segments to each non-broker node with the help of the TDMA (Time Division Multiple Access) technique.

Non-broker nodes start sensing from their surroundings and sending it to the broker turn by turn in their allocated time. The brook of sensed data collected by the broker is further processed by running M/M/1 Q message scheduling algorithm based on the shortest job first. A copy of this processed data is sent to BSP for backup to ensure fault tolerance in the proposed framework. In case the data sent by the broker isn't received by the base station due to any malicious activity and the base station requests broker to resend the last aggregated data then the broker will not need to recollect data and repeat the whole process consuming more energy of non-broker nodes as well as its own. The broker will request BSP for the last aggregated data and resend it to the base station. Therefore, the BSP node is not only tolerating the fault of the wireless sensor network but also preserving residual energies of nodes which prolongs network lifetime.

After initial variable declarations, setup and TDMA schedule for broker the energy of the broker is compared with the threshold energy. In the first round, it is obvious that the residual energy of the broker is higher than the threshold energy. On completion of the first round of data transmission unlike LEACH protocol, EAAFTMS protocol doesn't select a new broker node; instead, it calculates the remaining energy of the broker and compares it with threshold energy. If the residual energy of the broker is greater than the calculated threshold energy, then there will be no change in the broker node and it will get ready for the second round. Threshold energy is being calculated by estimating the least required energy vital for data transmission from sensor nodes to the base station. Unlike LEACH protocol, broker nodes will be assumed to be discharged only in case if residual energy of the broker becomes less than threshold energy.

Therefore, a comparison of residual energy of broker and calculated threshold energy is being done after completion of each round of data transmission. If threshold energy is calculated using EAAFTMS protocol, it becomes greater than residual energy of broker then broker needs to be swapped with BSP along with their database. When the residual energy of the current broker (previously worked as BSP) also becomes less than threshold energy, now it cannot be swapped with the BSP node as the current designated BSP already has residual energy lesser than threshold energy. Here, a method is called by EAAFTMS protocol, which is the NewSelectionOfBrokerAndBSP routine.

Two nodes having the highest residual energy are selected to act as the broker and BSP. Between these two nodes, the node having the highest residual energy is designated as a broker. The second one becomes BSP and immediately swaps the database with the previous BSP. Here, the newly designated broker and BSP start performing their duties to ensure successful data transmission from non-broker nodes to the base station. The whole described procedure is repeated unless and until that IoT subgroup left with no sensor node having residual energy greater than threshold energy.

F. FLOW DIAGRAM OF THE PROPOSED SOLUTION

The flow diagram of the proposed solution starts with the establishment, division and formation of IoT subgroups consisting of a specific number of sensor nodes. Initially, the broker and BSP are randomly selected after the EAAFTMS (An Energy-Aware Available and Fault-Tolerant System with Message Scheduling in IoT) algorithm is applied on each broker as shown in the flowchart (Figure No. 8).

For the first time, Broker and BSP are randomly selected. When non-broker nodes sense surrounding data and send that data to the broker node, all the messages received at the broker node are scheduled using M/M/1Q architecture. After message scheduling, the broker place one copy of scheduled messages at BSP for backup. After placing data at BSP, the broker sends that scheduled data towards the base station.

The energy of broker and BSP is compared with threshold energy, if the energy of broker and BSP is greater than threshold energy the broker and BSP will remain the same; otherwise, another comparison is made between BSP and threshold. If the energy of BSP is greater than threshold energy, then BSP and broker will swap, the broker acts as BSP and BSP takes the charge of the broker node. Otherwise, a new broker and BSP are selected from that particular IoT subgroup on the basis of maximum energy. The nodes that have the highest energy will be selected as the broker and the node with second highest energy will act as BSP. Hence, the process continues ensuring fault tolerance along with an efficient message scheduling algorithm for better transmission of data by reducing wait time.

The proposed algorithm has following 5 major processing in order to the time complexity of each operation mention in subsequent section.

In First operation depends on distance of two factors first factor is the number of non-broker nodes and second factor is number of broker nodes.

Cost: Number of non-broker nodes $*$ broker nodes

Mathematical Bound

brokerNodes $=$ BN, nonBrokerNodes $=$ NBN

$$T(n) := O(BN \times NBN)$$

In 2nd operation check the cost of the messages forwarding from non-broker nodes to broker nodes.

Cost: Number of non-broker nodes

$$T(n) := O(BN)$$

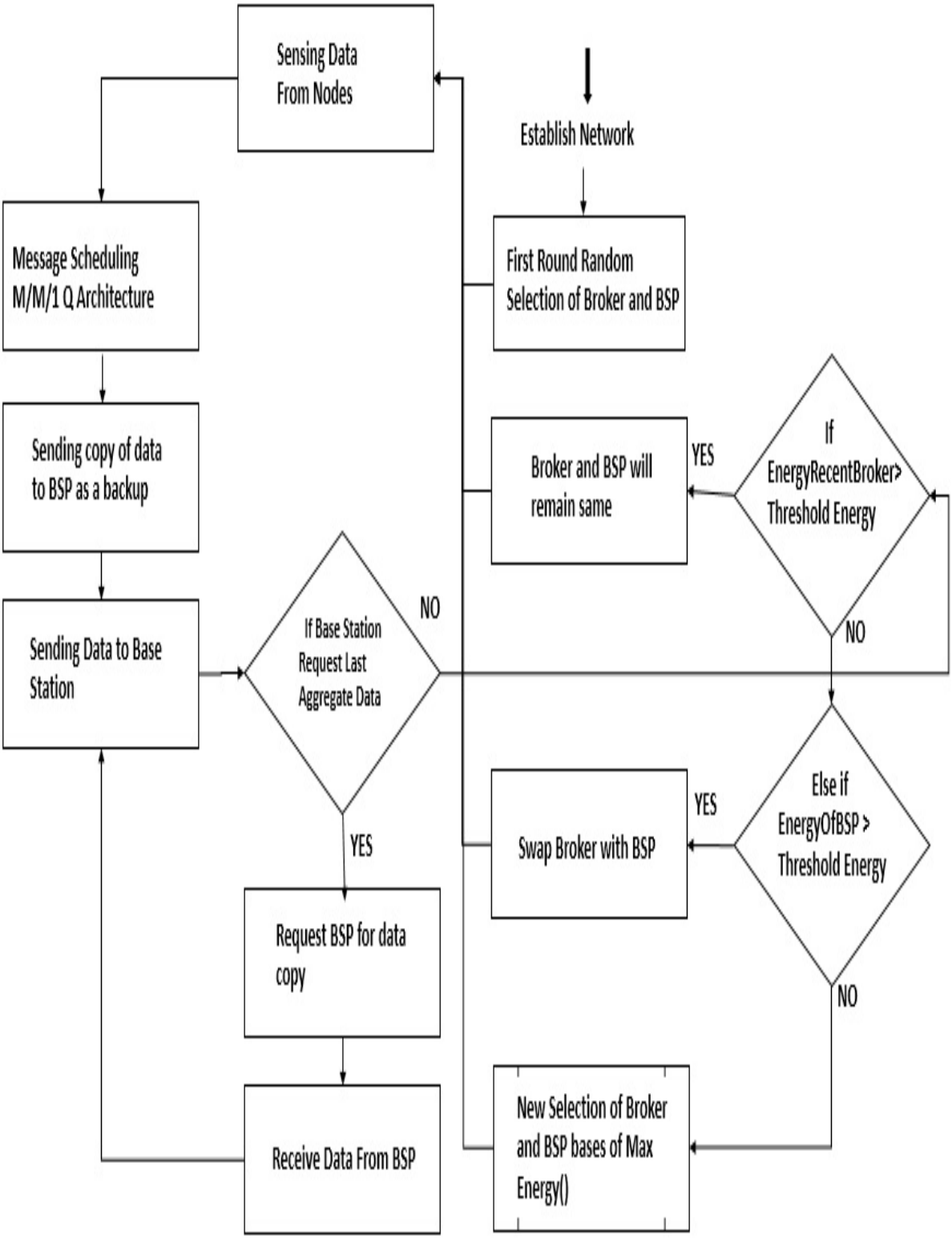

FIGURE 8. Flow diagram of the proposed solution.

In operation 3, schedule the messages using M/M/1 queue architecture.

Cost: The average time spent waiting is:

$$1/(\mu - \lambda) - 1/\mu = \rho/(\mu - \lambda)$$

In 4th operation messages transmitting from broker node to backup storage point.

Cost: Number of non-broker nodes:

$$T(n) := O(BN)$$

In operation 5 the cost depends on number of messages sending from broker to sink, which proportionally to the number of non-broker nodes.

Cost: Number of non-broker nodes:

$$T(n) := O(BN)$$

The maximum cost of proposed algorithm:

$$T(n) := O(BN \times NBN)$$

LEACH algorithm in operation 1 calculating the distance of nodes from the broker is:

Cost: for each cycle:

numberOfCycle: = NC

brokerNodes: = BN

nonBrokerNodes: =NBN

$$\mathrm{T(n)} := \mathrm{O(NC(BN \times NBN))}$$

In operation 2 check the cost of messages forwarding from non-broker nodes to broker nodes in the system.

Cost: Number of non-broker nodes.

Operation 3 cost depends on number of messages sending from broker to sink, which proportionally to the number of non-broker nodes

Cost: Number of non-broker nodes.

The maximum cost of LEACH algorithm is:

$$T(n) := O(NC(BN \times NBN))$$

CL-LEACH algorithm has extra cost depending on two factors residual energy and minimum distance of the node from the base station for cluster head selection is considered. The time complexity of EAAFTMS is improving against LEACH based on rounds, while establishing network, EAATMS establish its network just in one round but LEACH use variable rounds for establishing network. LEACH cost is coming in multiple and its impact will give very worst time complexity after some rounds. CL-LEACH have extra cost while calculating minimum distance and residual energy of each non-broker node for selecting broker in each round.

IV. RESULTS AND SIMULATIONS

A. AVERAGE NUMBER OF DEAD NODES IN DIFFERENT ROUNDS

Using MATLAB tool for simulation, broker node is being elected from the specific IoT subgroup but also an extra node which is known as BSP (Backup Storage Point) is being elected from the same IoT subgroup. In this scenario, there are 100 sensor nodes with 5 broker nodes and 5 BSP are deployed in the 5 IoT subgroups with same energy within IoT network. The various constraints which used in simulation are discussed in the Table 2.

Figure 9 shows an average number of dead nodes in different rounds of simulations when three different protocols or systems are applied separately in a simulation environment. The graph shows a clear discrepancy among LEACH, CL-LEACH and EAAFTMS LEACH protocols. In LEACH protocol, the average number of dead nodes dramatically increases as the number of rounds increases, after 1150 rounds the average number of dead nodes is 35 while the situation is slightly better in the case of CL-LEACH protocol. In CL-LEACH protocol, the average number of dead nodes after 1150 rounds are approximately 24. While the proposed EAAFTMS LEACH protocol is applied on a network the result is enormously better than LEACH and CL-LEACH protocols. As in EAAFTMS LEACH, the average number of dead nodes after 1150 rounds is only 10. Therefore, EAAFTMS LEACH protocol increases performance, fault tolerance capability and lifetime of a network more than three times when compared to LEACH protocol and more than two times when compared to CL-LEACH protocol.

TABLE 2. Different constraints for simulation setup.

Sink Node	1
Broker Nodes	5
Backup Storage Point (BSP)	5
IoT Subgroups	5
Each IoT Subgroup Sensor Nodes	20
Sensor Nodes	100

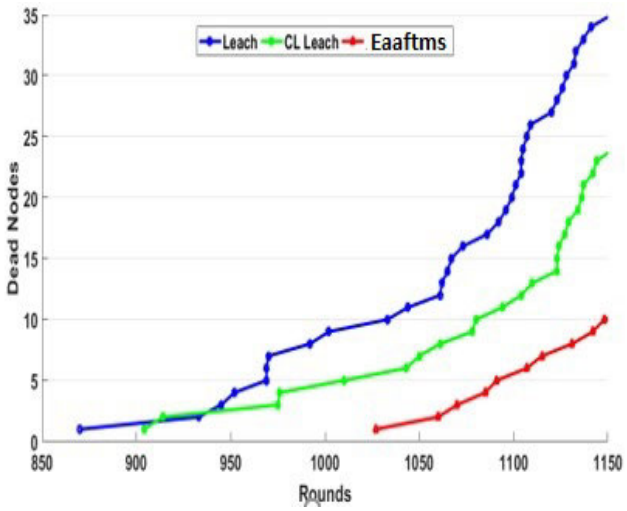

FIGURE 9. Average number of dead nodes in different rounds.

B. AVERAGE DISSIPATED ENERGY OF NON-BROKER NODES PER ROUND

Figure 10 shows a comparison of the average dissipated energy of non-broker nodes in each round of simulation with LEACH, CL CLEACH, and EAAFTMS LEACH protocol separately. In LEACH protocol comparing the average dissipated energy of non-broker nodes in 1 to 800 rounds varies from 0.0122J to 0.015J so a total of 0.0028J average energy dissipated in 800 rounds of operation. Using CL LEACH protocol, the dissipated energy of non-broker nodes from round 1 to 800 varies from 0.012J to 0.018J resulting

in 0.006J dissipated energy of non-broker nodes. When the proposed EAAFTMS LEACH protocol is applied on a network, dissipated energy of non-broker nodes observed from round 1 to 800 is approximately 0.013J to 0.012J which shows only 0.001J energy of non-broker nodes dissipated in 800 rounds of operation. Therefore, the EAAFTMS LEACH protocol has three times less dissipated energy of non-broker nodes as compared to the other two protocols.

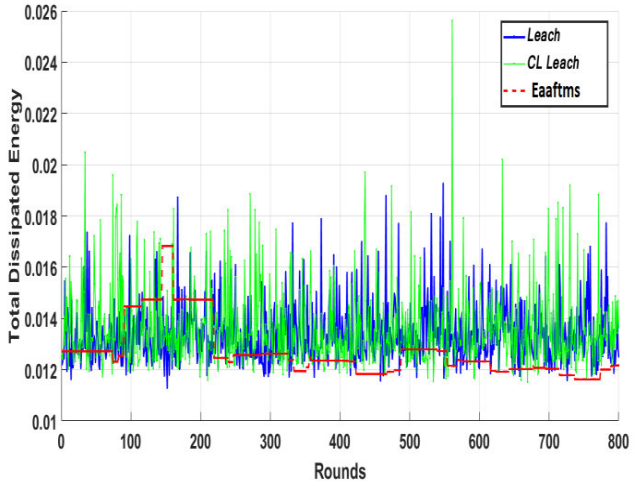

FIGURE 10. Average dissipated energy of non-broker nodes per round.

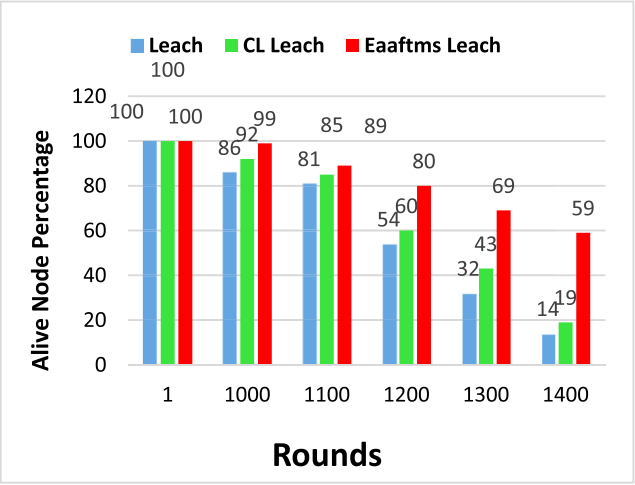

FIGURE 11. Average number of alive nodes in different round.

C. AVERAGE NUMBER OF ALIVE NODES IN DIFFERENT ROUNDS

Figure 11 showing the comparison of average alive nodes in different rounds of simulation among the three considered. After the first round of the simulation, all three systems provide 100% alive nodes. However, comparing the performance of these three protocols after 1000 rounds, LEACH provides 86% alive nodes. EAAFTMS LEACH provides 99% alive nodes, which is 13% higher than LEACH and 6% higher than CL LEACH. After 1100 rounds of operation, the network using LEACH protocol has 81% alive nodes and the other network that is using CL LEACH has 85% alive nodes. When the proposed EAAFTMS LEACH system was considered, it left with 89% alive nodes, However, after 1100 rounds performance of the EAAFTMS LEACH protocol increases with an increasing number of rounds of operation. After 1400 rounds, LEACH protocol provides only 14% alive nodes whereas CL LEACH protocol provides 19% alive nodes but EAAFTMS remarkably shows a clear difference, which is 59% average alive nodes. Therefore, EAAFTMS LEACH performed 45% better than LEACH and 40% better than CL LEACH protocol.

Hence, it is observable that EAAFTMS LEACH can increase the life of the IoT system. The network lifetime is approximately three times higher than the lifetime of the network-enabled by LEACH and CL-LEACH. Therefore, the EAAFTMS LEACH architecture is more energy-efficient and provides a better lifetime of the network, which ultimately makes it cost-efficient as well.

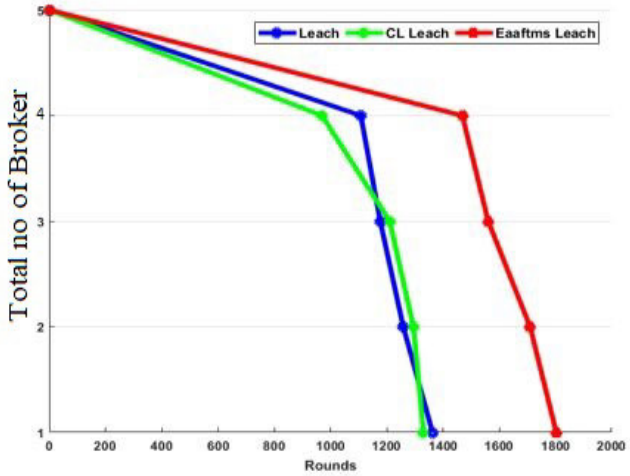

FIGURE 12. Average number of remaining brokers in different rounds.

D. THE AVERAGE NUMBER OF REMAINING BROKERS IN DIFFERENT ROUND

In Figure 12 the average number of remaining brokers are analyzed in various rounds of simulations. Among 100 nodes in the network, an average of five alive nodes are selected as brokers. A comparison is made among LEACH, CL Leach and EAAFTMS by applying these protocols on the network with the same specification and number of nodes. In LEACH protocol, after almost 1130 rounds, the number of remaining broker nodes is four, while CL Leach protocol has four remaining broker nodes after 950 rounds. When applying the proposed EAAFTMS protocol, the results are radically better than LEACH and CL LEACH protocols. EAAFTMS protocol has four remaining broker nodes after 1500 rounds. It proves that EAAFTMS fault-tolerant protocol is keeping a greater number of live brokers working as compared to LEACH and CL LEACH protocols. In the case of LEACH protocol, the network has one remaining broker after approximately

1370 rounds whereas CL Leach protocol is left with one broker after 1330 rounds, while EAAFTMS protocol has one remaining broker after 1800 rounds. Hence fault tolerance capability of the EAAFTMS protocol increases the network's lifetime more than LEACH and CL Leach protocol.

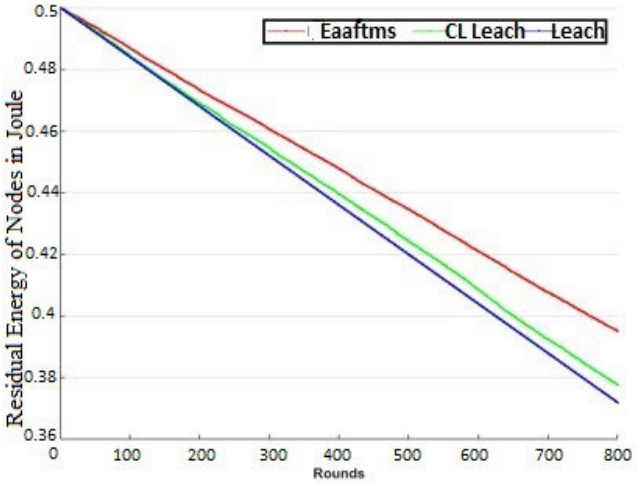

FIGURE 13. Average residual energy of one node in different rounds.

E. RESIDUAL ENERGY OF NODES

In this figure 13 average residual energy of one node in different rounds is shown. Consider starting energy of each node in LEACH, CL LEACH protocol and proposed protocol EAAFTMS is set to 0.5 joules. Comparison is made between these three protocols to check the average remaining energy of each node in different rounds. In LEACH protocol each node that started with the residual energy of 0.5 joules has dissipated 0.13-joule energy after 800 rounds. In CL LEACH protocol each node decreases its energy up to 0.12 joule after 800 rounds. In the proposed EAAFTMS protocol, the decrease in energy of each node after 800 rounds is comparatively lower than the other two protocols. When using the EAAFTMS protocol, each node has dissipated energy of only 0.1 joules after 800 rounds of operation which distinguishes its performance from the other two protocols discussed here. In the same way, after 1600 rounds each node has 0.26 joule dissipated energy using LEACH protocol, and dissipated energy in CL LEACH is 0.24 joule. Using the proposed EAAFTMS protocol, each node has dissipated energy of only two joules after 1600 rounds of operation, which proves the EAAFTMS protocol more energy efficient as compared to LEACH and CL-Leach.

V. DISCUSSIONS

The Internet of Things is facilitating people in almost every aspect of life whether it is education, health sector, electronic media, or industrial sector. The proposed idea is a promising one to enhance the trust and reliability of wireless sensor networks. In this research, a novel approach is used, which is a variant of LEACH protocol with enhanced capability of fault tolerance, fault recovery, and energy-efficient message scheduling for smooth communication between nodes. Head node; i.e., the broker is the one with the highest residual energy and a backup node; i.e., BSP (Backup Storage Point) is the one with second-highest residual energy. The broker collects data from non-broker nodes using TDMA (Time Division Multiple Access) and after aggregating data, messages are being scheduled at the broker node. The broker places a copy of scheduled messages on BSP and then sends scheduled aggregated data towards the base station. Every time, the residual energy of the broker is being compared with threshold energy to validate its capability to continue working as a broker. The same broker node acts as a broker unless and until its residual energy becomes less than threshold energy and when it reaches its limit then the broker node is placed with BSP which had been working just for backup purpose and didn't perform any sensing. The broker is swapped with BSP along with their databases. In case the base station didn't receive data sent by the broker due to any interruption and the base station requests the broker to resend. Assuming that the lost data was any real-time data sensed by non-broker nodes and this fault is being tolerated and recovered with the help of BSP, the broker node will simply request BSP for the last aggregated data and will resend it to the base station.

Now current work about our work is being discussed in this paragraph. Xiong *et al.* introduced a privacy and availability data clustering (PADC) scheme based on a k-means algorithm and privacy issues, which dealt with the selection of the initial center points and distance calculation method from normal node to center point. However, PADC reduced the detecting issues during the clustering process. Security analysis shows that the proposed scheme accomplishes the privacy issues. Moreover, performance evaluation shows that the proposed structure improves the availability of clustering results compared to the existing privacy k-means algorithms [42]. In this paper, Zhao *et al.* introduced a combined cognitive radio (CR) with a biological methodology called reaction-diffusion to support efficient spectrum allocation for CIoT. In the proposed method, calculate the best values of the algorithm's parameters (e.g., contention window) to maximize the network's adapting scenarios (e.g., spectrum homogeneity and heterogeneity), minimized convergence time, communication overhead, and calculation density [43]. Wireless sensor networks (WSN) are used to observe environmental circumstances, such as temperature, sound, pressure, disaster, earthquake, etc. WSN devices use high energy and power during the monitoring process. However, the main disadvantage is energy consumption and it is not easy to manage the energy level of each sensor node in the network. A new algorithm smart sensor network using the clustering approach is proposed to handle these issues. This approach replaces the dead cluster head with a normal cluster node to avoid energy consumption.

According to simulation results, the proposed clustering approach enhanced the packet delivery ratio by 80% and decreased the routing overhead, control overhead and

delay [44]. The agent can successfully copy a bad radio channel between the IoT devices and the relay. Such an approach maximizes the working load on the IoT devices and will drain their batteries at a high rate. To identify this issue, proposed hybrid intrusion detection systems that depend on the monitoring of uplink and downlink packets communicated between IoT devices and relay [45]. Sikeridis *et al.* proposed a strong learning procedure for empowering every IoT node to choose a sensing process mode according to the IoT infrastructure's provider. Also, a combined manufacturing mechanism of the IoT devices is relying on socio-physical associations between devices, titled spatial distance, energy availability, and detecting mode relationships [46]. In this article, Ansere *et al.* introduced an energy-efficient optimal transmit power allocation method to increase the dynamic spectrum sensing and data throughput. The simulation outputs authenticate that the described dynamic spectrum sensing technique can significantly decrease the energy consumption in CR-IoT networks [47].

Two algorithms Grey Wolf Optimizer (GWO) and Whale Optimization Algorithm (WOA), combined with the Imperialist Competitive Algorithm (ICA) proposed for based Cluster Head (CH) selection with a novel approach for heterogeneous networks. These algorithms can support data communication over a diverse Wireless Sensor Network (WSN) infrastructure to control the buffer overflow issue [48]. Wu *et al.* focused on the IoT's massive access and proposed a cluster-based reusable preamble allocation to improve random access algorithms for the NB-IoT environment. The simulation results show that the algorithm performs well and has a low probability of preamble collision by distributing the stations into clusters and allotting appropriate preamble sets [49]. In classical clustering LEACH algorithm, cluster heads are selected randomly to balance the energy usage of wireless sensor network nodes. Different parameters like residual energy, node position and node density of the nodes are not included. This issue is resolved by the exploration of LEACH protocol, the cluster head selection, communication methodology between cluster head and base station. The simulation results show that cluster head node energy consumption, network connectivity and availability are better [50]. Rahman *et al.* divide clustering methods into different categories depending on the Cluster Head (CH) selection criteria, which provides detail of clustering algorithms that vary from each other. Based on findings, proposed solutions, improve the performance of clustering methods [51].

VI. CONCLUSION AND FUTURE WORK

The Internet of Things is facilitating people in almost every aspect of life, whether it is education, health sector, electronic media or the industrial sector. The proposed approach has demonstrated a potentially promising way to enhance the trust and reliability of wireless sensor networks. This research has proposed a novel approach that variants the LEACH protocol with enhanced network availability, fault tolerance and energy-efficient message scheduling for smooth communication between nodes.

Availability is the key driver of IoT systems, so this approach is managing the fault and increasing availability but also energy consumption of non-broker as well as broker nodes is minimized by avoiding repeated sensing, aggregation and message scheduling process. Here IoT subgroup persists for a long time resulting in increasing network lifetime three to five times more than the existing protocols being used. Future research will be done to minimize data security threats by encrypting data being transferred over the network using a lightweight encryption algorithm. More security concerns will be considered in the existing systems which were not highlighted in the current scenario.

REFERENCES

[1] (2017). *IoT: Number of Connected Devices Worldwide 2012–2025 | Statista*. Accessed: Mar. 2, 2021. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[2] V. V. Shakhov, A. N. Yurgenson, and O. D. Sokolova, "Analysis of fault tolerance of wireless sensor networks," in *Proc. 13th Int. Sci.-Tech. Conf. Actual Problems Electron. Instrum. Eng. (APEIE)*, vol. 2, 2016, pp. 390–393.

[3] H. Mohapatra and A. K. Rath, "Survey on fault tolerance-based clustering evolution in WSN," *IET Netw.*, vol. 9, no. 4, pp. 145–155, Jul. 2020.

[4] T. N. Gia, A.-M. Rahmani, T. Westerlund, P. Liljeberg, and H. Tenhunen, "Fault tolerant and scalable IoT-based architecture for health monitoring," in *Proc. IEEE Sensors Appl. Symp. (SAS)*, Apr. 2015, pp. 1–6.

[5] M. Salayma, A. Al-Dubai, I. Romdhani, and Y. Nasser, "Wireless body area network (WBAN): A survey on reliability, fault tolerance, and technologies coexistence," *ACM Comput. Surv.*, vol. 50, no. 1, pp. 1–38, Apr. 2017.

[6] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci.*, 2000, p. 10.

[7] P. U. Maheswari and P. G. Kumar, "Dynamic detection and prevention of clone attack in wireless sensor networks," *Wireless Pers. Commun.*, vol. 94, no. 4, pp. 2043–2054, Jun. 2017.

[8] J. Patil and M. Sharma, "Survey of prevention techniques for denial service attacks (DoS) in wireless sensor network," *Int. J. Sci. Res.*, vol. 5, no. 3, pp. 1065–1069, 2016.

[9] M. Pawar and J. Agarwal, "A literature survey on security issues of WSN and different types of attacks in network," *Indian J. Comput. Sci. Eng*, vol. 8, no. 2, pp. 80–83, 2017.

[10] P. Hejazi and G. Ferrari, "Energy and memory efficient data loss prevention in wireless sensor networks," *Sensors*, pp. 1–18, 2018.

[11] M. M. Jamjoom, "EEBFTC: Extended energy balanced with fault tolerance capability protocol for WSN," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 1, pp. 253–258, 2017.

[12] J. Shen, A. Wang, C. Wang, P. C. Hung, and C. F. Lai, "An efficient centroid-based routing protocol for energy management in WSN-assisted IoT," *IEEE Access*, vol. 5, pp. 1847–18469, 2017.

[13] O. Kaiwartya, A. H. Abdullah, Y. Cao, J. Lloret, S. Kumar, R. R. Shah, M. Prasad, and S. Prakash, "Virtualization in wireless sensor networks: Fault tolerant embedding for Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 571–580, Apr. 2018.

[14] M. N. Cheraghlou, A. Khadem-Zadeh, and M. Haghparast, "Increasing lifetime and fault tolerance capability in wireless sensor networks by providing a novel management framework," *Wireless Pers. Commun.*, vol. 92, no. 2, pp. 603–622, Jan. 2017.

[15] E. Moridi, M. Haghparast, M. Hosseinzadeh, and S. J. Jassbi, "Fault management frameworks in wireless sensor networks: A survey," *Comput. Commun.*, vol. 155, pp. 205–226, Apr. 2020.

[16] S. Abdullah and K. Yang, "An energy efficient message scheduling algorithm considering node failure in IoT environment," *Wireless Pers. Commun.*, vol. 79, no. 3, pp. 1815–1835, Dec. 2014.

[17] M. Z. Hasan and F. Al-Turjman, "Optimizing multipath routing with guaranteed fault tolerance in Internet of Things," *IEEE Sensors J.*, vol. 17, no. 19, pp. 6463–6473, Oct. 2017.
[18] H. Yetgin, K. T. K. Cheung, M. El-Hajjar, and L. H. Hanzo, "A survey of network lifetime maximization techniques in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 828–854, 2nd Quart., 2017.
[19] B. Bhushan and G. Sahoo, "Requirements, protocols and security challenges in wireless sensor networks: An industrial perspective," in *Handbook of Computer Networks and Cyber Security*. Cham, Switzerland: Springer, 2020, pp. 683–713.
[20] F. T. Giuntini, D. M. Beder, and J. Ueyama, "Exploiting self-organization and fault tolerance in wireless sensor networks: A case study on wildfire detection application," *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 4, pp. 1–16, Apr. 2017.
[21] C. Fu, Z. Jiang, W. E. I. Wei, and A. Wei, "An energy balanced algorithm of LEACH protocol in WSN," *Int. J. Comput. Sci. Issues*, vol. 10, no. 1, p. 354, 2013.
[22] S. Varshney and R. Kuma, "Variants of LEACH routing protocol in WSN: A comparative analysis," in *Proc. 8th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence)*, Jan. 2018, pp. 199–204.
[23] S. De, L. M. Sá, H. Vogt, and M. Beigl, "A survey on fault tolerance in wireless sensor networks," Interner Bericht. Dept. Informatik, Univ. Karlsruhe, Karlsruhe, Germany, 2007.
[24] T. N. Gia, A.-M. Rahmani, T. Westerlund, P. Liljeberg, and H. Tenhunen, "Fault tolerant and scalable IoT-based architecture for health monitoring," in *Proc. IEEE Sensors Appl. Symp. (SAS)*, Apr. 2015, pp. 1–6.
[25] T. Yuan and S. Zhang, "Secure fault tolerance in wireless sensor networks," in *Proc. IEEE 8th Int. Conf. Comput. Inf. Technol. Workshops*, Jul. 2008, pp. 477–482.
[26] W. M. Elsayed, S. F. Sabbeh, and A. M. Riad, "A distributed fault tolerance mechanism for self-maintenance of clusters in wireless sensor networks," *Arabian J. Sci. Eng.*, vol. 43, no. 12, pp. 6891–6907, Dec. 2018.
[27] D. Scazzoli, A. Kumar, N. Sharma, M. Magarini, and G. Verticale, "Fault recovery in time-synchronized mission critical ZigBee-based wireless sensor networks," *Int. J. Wireless Inf. Netw.*, vol. 24, no. 3, pp. 268–277, Sep. 2017.
[28] Y.-M. Sun, X.-J. Liu, X.-G. Chen, Q.-Y. Sun, and J. Zhao, "Research and application of a fault self-diagnosis method for roots flowmeter based on WSN node," *Wireless Pers. Commun.*, vol. 95, no. 3, pp. 2315–2330, Apr. 2017.
[29] P. Marappan and P. Rodrigues, "An energy efficient routing protocol for correlated data using CL-LEACH in WSN," *Wireless Netw.*, vol. 22, no. 4, pp. 1415–1423, May 2016.
[30] W. Saeed, Z. Ahmad, A. I. Jehangiri, N. Mohamed, and A. I. Umar, "A fault tolerant data management scheme for healthcare Internet of Things in fog computing," *KSII Trans. Internet Inf. Syst.*, vol. 15, no. 1, pp. 35–57, 2021.
[31] Z. Sisi and A. Souri, "Blockchain technology for energy-aware mobile crowd sensing approaches in Internet of Things," *Trans. Emerg. Telecommun. Technol.*, p. e4217, Jan. 2021.
[32] M. Abdel-Basset, R. Mohamed, M. Elhoseny, A. K. Bashir, A. Jolfaei, and N. Kumar, "Energy-aware marine predators algorithm for task scheduling in IoT-based fog computing applications," *IEEE Trans. Ind. Informat.*, vol. 17, no. 7, pp. 5068–5076, Jul. 2021.
[33] D. Wang, D. Zhong, and A. Souri, "Energy management solutions in the Internet of Things applications: Technical analysis and new research directions," *Cognit. Syst. Res.*, vol. 67, pp. 33–49, Jun. 2021.
[34] M. Abdel-Basset, D. El-Shahat, M. Elhoseny, and H. Song, "Energy-aware metaheuristic algorithm for industrial-Internet-of-Things task scheduling problems in fog computing applications," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12638–12649, Aug. 2021.
[35] F. Safara, A. Souri, T. Baker, I. A. Ridhawi, and M. Aloqaily, "PriNergy: A priority-based energy-efficient routing method for IoT systems," *J. Supercomput.*, vol. 76, pp. 1–18, Jan. 2020.
[36] M. Alazab, K. Lakshmanna, T. Reddy, Q.-V. Pham, and P. K. R. Maddikunta, "Multi-objective cluster head selection using fitness averaged rider optimization algorithm for IoT networks in smart cities," *Sustain. Energy Technol. Assessments*, vol. 43, Feb. 2021, Art. no. 100973.
[37] T. M. Behera, S. K. Mohapatra, U. C. Samal, M. S. Khan, M. Daneshmand, and A. H. Gandomi, "Residual energy-based cluster-head selection in WSNs for IoT application," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5132–5139, Jun. 2019.
[38] T. A. Alghamdi, "Energy efficient protocol in wireless sensor network: Optimized cluster head selection model," *Telecommun. Syst.*, vol. 74, no. 3, pp. 331–345, Jul. 2020.
[39] A. Al-Baz and A. El-Sayed, "A new algorithm for cluster head selection in LEACH protocol for wireless sensor networks," *Int. J. Commun. Syst.*, vol. 31, no. 1, p. e3407, Jan. 2018.
[40] Q. Ren and G. Yao, "An energy-efficient cluster head selection scheme for energy-harvesting wireless sensor networks," *Sensors*, vol. 20, no. 1, p. 187, Dec. 2019.
[41] A. S. Nandan, S. Singh, and L. K. Awasthi, "An efficient cluster head election based on optimized genetic algorithm for movable sinks in IoT enabled HWSNs," *Appl. Soft Comput.*, vol. 107, Aug. 2021, Art. no. 107318.
[42] J. Xiong, J. Ren, L. Chen, Z. Yao, M. Lin, D. Wu, and B. Niu, "Enhancing privacy and availability for data clustering in intelligent electrical service of IoT," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1530–1540, Apr. 2019.
[43] J. Li, H. Zhao, A. S. Hafid, J. Wei, H. Yin, and B. Ren, "A bio-inspired solution to cluster-based distributed spectrum allocation in high-density cognitive Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9294–9307, Dec. 2019.
[44] J. V. Ananthi, V. Chinnalagi, R. Murugeshwari, T. Priyadharshni, and K. Rajalakshmi, "An effective performance of smart sensor network using IoT," *Int. J. Advance Res., Ideas Innov. Technol.*, vol. 3, no. 2, pp. 638–646, Apr. 2017.
[45] N. V. Abhishek, A. Tandon, T. J. Lim, and B. Sikdar, "A GLRT-based mechanism for detecting relay misbehavior in clustered IoT networks," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 435–446, 2020.
[46] D. Sikeridis, E. E. Tsiropoulou, M. Devetsikiotis, and S. Papavassiliou, "Energy-efficient orchestration in wireless powered Internet of Things infrastructures," *IEEE Trans. Green Commun. Netw.*, vol. 3, no. 2, pp. 317–328, Jun. 2019.
[47] J. A. Ansere, G. Han, H. Wang, C. Choi, and C. Wu, "A reliable energy efficient dynamic spectrum sensing for cognitive radio IoT networks," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6748–6759, Aug. 2019.
[48] R. Hamidouche, Z. Aliouat, A. A. A. Ari, and M. Gueroui, "An efficient clustering strategy avoiding buffer overflow in IoT sensors: A bio-inspired based approach," *IEEE Access*, vol. 7, pp. 156733–156751, 2019.
[49] F. Wu, B. Zhang, W. Fan, X. Tian, S. Huang, C. Yu, and Y. Liu, "An enhanced random access algorithm based on the clustering-reuse preamble allocation in NB-IoT system," *IEEE Access*, vol. 7, pp. 183847–183859, 2019.
[50] Y. Xu, Z. Yue, and L. Lv, "Clustering routing algorithm and simulation of Internet of Things perception layer based on energy balance," *IEEE Access*, vol. 7, pp. 145667–145676, 2019.
[51] T. Rahman, I. Ullah, A. Rehman, and R. A. Naqvi, "Clustering schemes in mantes: Performance evaluation, open challenges, and proposed solutions," *IEEE Access*, vol. 8, pp. 25135–25158, 2020.

MUHAMMAD BUKHSH received the master's degree in information technology from the University of Education, Lahore, Pakistan, and the M.S. degree in computer sciences from The Islamia University of Bahawalpur, where he is currently pursuing the Ph.D. degree. His main research interests include ad-hoc networks, the IoT systems, energy efficiency, edge commuting, high availability, and fault tolerance.

SAIMA ABDULLAH received the Ph.D. degree from the Department of Computer Science and Electronic Engineering, University of Essex, U.K. She is currently an Assistant Professor with the Department of Computer Science and Information Technology, The Islamia University of Bahawalpur, Pakistan. She is a member of the Multimedia Research Group, DCS, where she has been involved in efficient and secure communication of multimedia data over future generation network technologies. Her main research interests include wireless networks and communications, future internet technology, and network performance analysis. She has authored around ten articles in the above research areas. She serves as a reviewer for international journals.

ABDUL RAHMAN received the M.S. degree in computer sciences from The Islamia University of Bahawalpur, Punjab, Pakistan. He is currently pursuing the Ph.D. degree with Chinese university. He is working as a Lecturer in computer science at a leading university in Lahore. His main research interests include the IoT and blockchain technology.

MAMOONA NAVEED ASGHAR received the Ph.D. degree from the School of Computer Science and Electronic Engineering, University of Essex, Colchester, U.K., in 2013. Since June 2018, she has been working as a Marie Sklodowska-Curie (MSC) Career-Fit Research Fellow with the Software Research Institute, Athlone Institute of Technology (AIT), Ireland. She is currently a Regular Faculty Member with the Department of Computer Science and Information Technology (DCS & IT), The Islamia University of Bahawalpur, Punjab, Pakistan, and currently on postdoctoral leave. She has more than 14 years of teaching and research and development experience. She has published several ISI indexed journal articles along with numerous international conference papers. She is also actively involved in reviewing for renowned journals and conferences. Her research interests include security aspects of multimedia (image, audio and video), compression, visual privacy, encryption, steganography, secure transmission in future networks, the Internet of Multimedia Things, video quality metrics, and key management schemes.

HUMAIRA ARSHAD received the master's degree in information technology from the National University of Science and Technology (NUST), Pakistan, and the Ph.D. degree from the School of Computer Science, University Sains Malaysia. She joined the Faculty of Computer Sciences & IT, in 2004. She is currently an Assistant Professor with the Department of Computer Sciences & IT, The Islamia University of Bahawalpur, Pakistan. Her research interests include digital and social media forensics, information security, online social networks, cybersecurity, intrusion detection, reverse engineering, and semantic web.

ABDULATIF ALABDULATIF received the B.Sc. degree in computer science from Qassim University, Saudi Arabia, in 2008, and the M.Sc. and Ph.D. degrees in computer science from RMIT University, Australia, in 2013 and 2018, respectively. He is currently an Assistant Professor with the School of Computer Science and IT, Qassim University. His research interests include applied cryptography, cloud computing, data mining, and remote healthcare.